Aux USA, en Allemagne, en France, quelle protection de la vie privée en matière d'interceptions de télécommunication ?

Claudine Guerrier
Enseignant-chercheur à Institut Telecom/TELECOM
§ Management SudParis (ex-INT)/DEFIS/Cemantic

E-mail : Claudine.Guerrier@it-sudparis.eu

Introduction

Les interceptions de télécommunication sont actuellement très nombreuses, notamment aux USA pour le continent américain et la *common law*, en Italie pour l'Europe et le droit romano-germanique. L'interception est définie comme « *le fait de s'emparer de* »[1]. Il y a captation, qui est généralement contraire au droit. Comme l'écoute, l'interception est intentionnelle, volontaire, lucide. Néanmoins, la marque de la volonté est plus forte dans l'interception que dans l'écoute. L'écoute peut s'interrompre à tout moment, avec la dilution de la volonté et de l'intention. La cessation de l'interception induit une réflexion, puisque la finalité en est que la captation disparaît avec elle. L'interception englobe l'écoute, mais l'écoute ne peut constituer le chapeau d'une interception. Voilà pourquoi l'écoute téléphonique est perçue par le droit comme une sous-catégorie des interceptions de télécommunications. Ces dernières concernent notamment la téléphonie et les méls : par le moyen des télécommunications ou des communications électroniques, la correspondance est un échange de paroles ou de signes.

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, audiovisuel. Les directives sont transposées en juillet 2003. Depuis la mi- 2003 au sein de l'Union européenne, et en France depuis 2004[2], on parle d'interceptions de communications électroniques. Dans les autres pays, on continue à évoquer les interceptions de télécommunications.

Ces interceptions constituent une dérogation à l'inviolabilité du secret de la correspondance, garanti, selon les Etats, par la Constitution et par la loi. La licéité de ces interceptions 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. Aux USA, en Allemagne, en France, ces interceptions sont soit judiciaires, soit de sécurité.

Dans la mesure où les Droits de l'homme sont en cause, des conventions internationales ont été élaborées et la hiérarchie des normes imposée. La Déclaration universelle des droits de l'homme de 1948[3] 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[4]. Le Pacte a été ratifié par l'Allemagne et par la France, mais non par les USA, qui considèrent qu'il existe une incompatibilité entre certains articles du Pacte et le premier amendement

[1] Petit Larousse, 2007.

[2] Loi 2004-669 du 9 juin 2004 sur le « paquet télécoms ».

[3] 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* ».

[4] 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 correspondances, 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*. »

de la Constitution américaine[5]. La Convention européenne de sauvegarde des droits de l'homme, à travers son article huit protège le secret de la correspondance et la vie privée.

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. Le droit pénal vise l'intimité de la vie privée, définie de façon restrictive par une partie de la doctrine[7] et de la jurisprudence[8]. 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[9], 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.

Aux USA, Etat fédéral, aucun texte ne consacre expressément le droit à la vie privée. La Cour suprême a néanmoins dégagé l'existence d'un tel droit des premier, troisième, quatrième, cinquième et quatorzième amendement. Le premier amendement protège la liberté d'expression et d'association. Le troisième amendement interdit aux militaires de se « dissimuler dans les maisons ». Le quatrième amendement protège les citoyens contre les enquêtes et les saisies arbitraires. Le cinquième amendement écarte les « témoignages contre soi-même ». Le quatorzième amendement garantit la liberté d'opinion en matière de mariage et d'éducation.

Dans certains Etats, le droit à la vie privée a été proclamé et a une valeur constitutionnelle. Ainsi, la Californie considère que le droit à la vie privée est un droit inaliénable[10].

En matière d'interceptions de télécommunications, des organismes ou des procédures de contrôle ont été instaurées, précisément pour protéger la vie privée des personnes physiques. En Europe, l'initiative revient au Conseil de l'Europe. Aux USA, c'est l'Etat fédéral qui s'est préoccupé du respect de la vie privée dans le cadre des interceptions de télécommunications. Dans la dernière décennie du vingtième siècle, ces organismes et ces procédures de contrôle ont été mis en place. Dans la première décennie du vingt-et-unième siècle, alors que les exigences sécuritaires semblent s'imposer à la société civile via les normes législatives, les organismes de contrôle jouent un rôle de plus en plus contrasté alors que les nouvelles technologies semblent être utilisées pour satisfaire les besoins des autorités publiques. Pourtant, les rouages et les procédures de ces organismes de contrôle continuent à fonctionner. Il est donc peu pertinent de vouloir occulter le fonctionnement et le rôle de ces entités. Le temps est donc venu de dresser un bilan, en se focalisant sur les USA, pour la *common law*, sur l'Allemagne et la France, pour le droit romano-germanique européen. Les interceptions de télécommunications, ou de communications électroniques[11] font partie des procédés technologiques, au même titre que la biométrie, la vidéosurveillance, l'Internet qui doivent parvenir à un équilibre entre souci de l'ordre public- objectif de sécurité et protection de la vie privée-objectif de préservation des libertés individuelles.

I. Les organismes de contrôle continuent à apporter des garanties dans le domaine des interceptions de communications électroniques et de télécommunications : ils permettent un recours indispensable et disposent dans certains cas de nouvelles prérogatives.

A. Ces organismes de contrôle constituent un recours nécessaire

1. Le recours paraissait nécessaire à l'origine

Le législateur qui s'est penché sur les interceptions de télécommunications considérait que l'organisme de contrôle était une garantie minimale dans la mesure où les interceptions sont une dérogation à l'interdiction de la violation des correspondances.

---

[5] Afférent à la liberté d'expression.

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

[7] Ecrits de MM.Levasseur, Lindon, Bécourt.

[8] Vie conjugale et sentimentale, en excluant parfois les aspects matériels de cette vie conjugale et sentimentale.

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

[10] Constitution de l'Etat de Californie, article un, Declaration of Rights section 1 : « All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing and protecting property, and pursuing and obtaining safety, happiness, and privacy ».

[11] Pour la France et l'Allemagne.

1.1. Le Conseil de l'Europe et la CEDH ont joué un rôle privilégié dans ce secteur en Europe

1.1.1. L'Allemagne

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[12] de la Convention sont assujettis à la jurisprudence de la CEDH et sont tenus de l'appliquer.

L'affaire Klass et autres[13] : 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 RFA. Ils arguent de ce que l'article 10, alinéa 2, de la Grundgesetz et la loi du 13 août 1968[14] 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. Ils avaient auparavant épuisé les voies de recours internes, ayant été déboutés par la Cour constitutionnelle fédérale. La loi du 13 août 1968 indique les motifs susceptibles de permettre les interceptions de télécommunications. 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 limitative de cet arrêt, ne voulant pas faire courir le moindre risque à la sécurité nationale. MM.Klass, 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 former un recours constitutionnel contre une loi, il faut alléguer que cette dernière, et non un acte d'exécution, viole un droit fondamental* ». M. Klass et autres saisissent alors la CEDH. Selon le gouvernement de la RFA, la commission et la CEDH sont incompétents. Leur rôle est de contrôler la bonne application de la Convention quand un requérant s'estime victime d'une violation de ses droits, non pas d'entrer dans des arguties juridiques. La commission estime que la Cour est compétente pour déterminer si les requérants peuvent se prétendre victimes. La question principale est la suivante : la CEDH doit-elle priver quelqu'un de la faculté d'introduire une requête parce que le caractère secret des mesures litigieuses l'empêche de signaler une mesure concrète qui le toucherait spécifiquement ? 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. 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 subi une violation des droits de l'homme. Cette jurisprudence est essentielle : elle donne une interprétation extensive du droit de requête individuelle, qui ne doit pas être oblitérée par des mesures internes[15].

MM. Klass et autres estiment qu'il a été porté atteinte à l'article huit de la Convention qui protège la sphère privée et la correspondance. La commission et la CEDH admettent toutes deux que les conversations par voie de télécommunications, même si elles ne sont pas explicitement citées au paragraphe un de l'article huit, sont comprises dans les notions de « vie privée » et de « correspondance ». La Cour examine la loi de 1968 pour déterminer si elle contient des garanties suffisantes contre des abus. La Cour ne reconnaît pas le danger de tels abus.

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 un organisme de contrôle.

---

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

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

[14] Gesetz zur Beschränkung des Briefs, Post und Fermelde Geheimisses.

[15] Les clauses procédurales.

1.1.2. La France : elle a ratifié la Convention européenne des droits de l'homme et notamment son article 25 en 1981[16]. Deux affaires, Kruslin[17] et époux Huvig[18] ont joué un rôle éminent dans la condamnation du système d'interceptions français. Nous analysons l'affaire Kruslin.

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 conversations. Jean Kruslin, hébergé alors par M. Terrieux, dont il utilise l'appareil téléphonique, a participé à plusieurs d'entre elles. Lors de ces entretiens, Jean Kruslin et son interlocuteur évoquent une 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[19].

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.

Dans son rapport afférent à l'affaire Kruslin[20], 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 CEDH[21], 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, contrôle éventuel du juge d'instruction de la part de la Chambre d'accusation, des juridictions du fond, de la Cour de cassation, obligation de prendre en compte les droits de la défense, en particulier la confidentialité des relations entre l'avocat et le suspect. 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[22]. La procédure est insuffisamment protectrice : *« Le droit français, écrit ou non écrit, n'indique pas avec assez de clarté[23] 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* ». La France est condamnée ; elle doit verser des dommages-intérêts à M.Kruslin[24]. Surtout, elle doit revoir l'état de son droit en matière d'interceptions de télécommunications et suivre les recommandations de la CEDH. Elle doit notamment créer un organisme de contrôle des interceptions de sécurité. Le législateur français s'inspire surtout du rapport Schmelck. Peu après sa nomination en tant que premier ministre en 1981, Pierre Mauroy charge une commission d'étude placée sous la présidence

[16] Décret n° 81 917 du 9 octobre 1981.
[17] CEDH, Kruslin, 24 avril 1990, Dalloz, 1990, 353, Notes Pradel.
[18] CEDH, époux Huvig, 24 avril 1990.
[19] Cour de cassation, crim, 23 juillet 1985, Bull.crim, n° 275.
[20] Du 14 décembre 1988.
[21] CEDH, Kruslin c.France, 24 avril 1990.
[22] Crimes, délits, peines encourues.
[23] Critique de l'insécurité juridique.
[24] Elle devra aussi payer une amende aux époux Huvig.

du premier président de la Cour de cassation, Robert Schmelck, d'une mission d'investigation sur les interceptions de télécommunication. La commission comprend des parlementaires, des magistrats, des professeurs de droit, des hauts fonctionnaires. 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, Jacques Chirac, alors premier ministre s'engageait devant l'Assemblée nationale à limiter les interceptions de télécommunication 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 ministre de l'Intérieur, M. Pasqua avisaient la presse qu'un projet de loi, inspiré du rapport Schmelck, était préparé. Le projet 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[25] 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 interceptions téléphoniques, et certains ont collaboré au rapport Schmelck, qui n'avait pas encore été publié à l'époque[26]. 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 CEDH.

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 européens ont institué des organismes de contrôle.

1.2. Les USA se sont attachés aussi à la mise en place de procédures de contrôle en matière d'interceptions.

Citons l' « Omnibus Crime Control and Safe Streets Act » (Titre III), plus connu sous la dénomination « Title III », adopté en 1968, le Foreign Intelligence Surveillance Act[27] de 1978, la CALEA, de 1994.

1.2.1. Le « Title III » : pour les interceptions judiciaires

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 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[28] ou l'un de ses collaborateurs[29]. 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[30] ou le procureur du comté[31]. 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. Avant de donner son accord, le juge détermine 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 pourront être obtenues par une interception de télécommunications et que les autres procédures d'investigation ont échoué. En cas d'urgence, lorsque le danger est imminent, le Title 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

[25] Police.
[26] Il fut publié lors de la première parution du rapport d'activité de la CNCIS 1991-1992, La Documentation française, 1993.
[27] FISA Act.
[28] L'Attorney General.
[29] Deputy Attorney General, Associate Attorney General.
[30] District Attorney.
[31] County Prosecutor.

un représentant d'une administration locale, à réaliser une interception de télécommunications. Cette interception est régularisée dans les 48 heures pour ne pas être déclarée illégale.

Cependant, dans l'Etat de New York, même une situation d'urgence nécessite une décision du juge fédéral à 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.

1.2.2. La FISA, adoptée en 1978, afférente aux interceptions de sécurité

A cette époque, 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.

En matière pénale, les informations sont utilisables, après accord de l'Attorney General ; la personne concernée et son avocat sont informés. La personne mise en cause est en droit de saisir le tribunal fédéral de première instance[32] territorialement compétent et d'invoquer la non-recevabilité des preuves recueillies par ces moyens spécifiques. Elle tente 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 ne peut être réexaminée que par les Cours d'appel et la Cour suprême.

2. Le contrôle s'est imposé en Europe et aux USA

2.1. L'Allemagne : le contrôle est effectué par deux commissions, le PKG et la commission G10.

La commission 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 postériori 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, expire après l'élection d'une nouvelle chambre. La renouvelabilité est possible. Les membres de la commission peuvent être parlementaires mais ne peuvent exercer de fonctions gouvernementales. L'opposition est obligatoirement représentée. 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[33] 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, en cas d'extrême urgence, l'interception est exécutée avec le seul accord du ministre ; ce dernier régularise rapidement la situation auprès de la commission G10.

[32] District Court.

[33] Article premier, alinéa un 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. La commission 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.

Enfin, la Cour constitutionnelle allemande peut être saisie par tout citoyen estimant que ses droits fondamentaux ne sont pas respectés : cela englobe les interceptions de télécommunications.

2.2. La France : le contrôle concerne les interceptions de sécurité. Les interceptions judiciaires se font, dans la loi du 10 juillet 1991, sous la conduite du juge d'instruction.

Les interceptions de sécurité impliquent la conformité à des motifs qui sont contrôlés par la CNCIS[34].

Dans cette CNCIS, autorité administrative indépendante composée de trois membres, le président exerce un rôle prépondérant. Le président est une personnalité désignée, en raison de son autorité et de sa compétence, pour une durée de six ans, par le président de la République. La CNCIS comprend également un député et un sénateur désignés, qui par le président de l'Assemblée nationale, qui par le président du Sénat. Ces mandats sont irrévocables et non-renouvelables. Dans la pratique et conformément aux souhaits de la CEDH, l'un des deux membres représente l'opposition. La loi ne comprend aucun article afférent à cette obligation, qui peut être remise en cause.

Quant au contrôle, c'est un contrôle à priori, sauf en cas d'urgence absolue. La CNCIS émet un avis, qui est cependant généralement suivi par le premier ministre habilité à délivrer les autorisations en matière d'interceptions de sécurité.

B. Les organismes de contrôle disposent parfois de nouvelles prérogatives

1. Le contrôle de l'urgence absolue :

1.1. En Allemagne : la commission G10 régularise la situation à postériori, mais c'est le ministre qui arrête la décision.

1.2. En France : dans la loi du 10 juillet 1991, aucune mention n'était faite de l'urgence. Pourtant, les services des ministères concernés ont souvent l'impression, voire la certitude, d'être cernés par l'urgence. Dans la pratique, les demandes sont accompagnées, quand une diligence semble indispensable, d'une mention « en urgence » ou « en extrême urgence », en « urgence absolue ». Le traitement en urgence n'a jamais présenté de problèmes particuliers : les agents sont seulement invités à travailler avec rapidité. Le cas est différent en cas d'extrême urgence.

1.2.1. Jusqu'en 2003, l'examen de la justification des motifs n'est effectué en cas d'urgence par l'organisme de contrôle qu'a postériori. Cette mesure s'explique 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.

Dès 1994, la CNCIS a constaté que l'extrême-urgence était quelquefois invoquée sans justification suffisante ; la régularisation n'intervenait qu'après plusieurs jours.

Une recommandation de février 1995 a été suivie d'effets. Les mentions « extrême urgence » ont été utilisées avec davantage de précaution. A partir de 1996, les demandes en urgence absolue n'ont au contraire cessé de croître : + 10, 96% en 1997, 14, 59% en 1998. La CNCIS renouvelle son invite à utiliser exceptionnellement l'extrême urgence.

1.2.2. En avril 2003, le contrôle de l'extrême urgence se fait a priori. Sans modification de la loi de 1991, et en accord avec Jean-Pierre Raffarin[35], le régime d'avis préalable aux demandes d'interceptions a été étendu aux demandes en extrême-urgence. 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

[34] Commission nationale de contrôle des interceptions de sécurité.

[35] Alors premier ministre.

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. En matière d'urgence, le dispositif qui existe depuis 2003 semble fiable et réactif.

2. La nomination d'une personnalité qualifiée en France

2.1. La loi de lutte anti-terrorisme[36] : la loi de lutte anti-terrorisme est à l'origine de nouvelles dispositions concernant souvent les technologies de l'information : vidéosurveillance, notamment., et interceptions de communications électroniques

. Cette loi permet un relatif consensus de la classe politique, à l'exception des Verts et du PCF. Au nom de la sécurité et de la prévention du terrorisme, les politiques sont prêts à privilégier l'ordre public qui devient une priorité absolue

2.2. La personnalité qualifiée

Afin de prévenir les actes de terrorisme, les agents individuellement désignés et dûment habilités des services de police et de gendarmerie nationale 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 afférentes à la localisation des équipements terminaux utilisés ainsi qu'aux données techniques relatives aux communications d'un abonné portant sur la liste de numéros appelés et appelants, la durée et la date des communications. 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

Ce texte a fait précédemment l'objet d'un projet quelque peu différent. Initialement, la personnalité qualifiée était désignée par le ministre de l'intérieur. Les débats devant l'Assemblée nationale et le Sénat ont permis d'éclairer les différentes facettes afférentes à la personnalité qualifiée.

Devant l'Assemblée nationale, l'amendement 15 a pour objectif de faire nommer la personnalité chargée d'examiner les demandes des agents habilités par la CNCIS et non par le ministre de l'intérieur. C'est un gage d'impartialité et cela correspond à la première mouture du texte[37].

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, les discussions sont encore plus animées. Un amendement 40 est proposé par Mmes Boumediene-Thiery, Blandin et M.Desessard, inspiré par l'inquiétude qu'induit la procédure de

[36] Loi n° 2006-64 du 23 janvier 2006.

[37] « *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.

réquisition administrative, qui ne respecterait pas le principe de proportionnalité. Les auteurs de l'amendement 40 se félicitent de l'accroissement des compétences dévolues à la CNCIS, tout en déplorant que la CNCIS ne dispose pas de davantage de moyens financiers et souhaitent que cette autorité administrative indépendante gagne en autonomie. Ils regrettent que la CNIL n'exerce pas de contrôle.

Néanmoins, le gouvernement et les sénateurs sont d'accord pour que la CNCIS 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 rédigé :

« *Les demandes des agents sont motivées et soumises à la décision de la CNCIS. 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 CNCIS*… ».

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 CNCIS 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. *« 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[38]*.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 L 34-1-1 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 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.

[38] « *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.

Le rapporteur[39] 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[40]. 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 CNCIS 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[41]. 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[42]. 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 à priori.

Le rapporteur se prononce en faveur de l'amendement 54 rectifié ter ; la CNCIS pourra choisir entre trois noms présentés par le ministre de l'intérieur[43] ; 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[44]. Il demande donc le retrait de l'amendement 55 rectifié bis, ce qui est fait.

Le texte définitif du projet de loi a été adopté par le Parlement, l'Assemblée nationale et le Sénat ayant trouvé un accord sur le texte mis au point par la Commission mixte paritaire. La CNCIS se voit confier des tâches supplémentaires. Tout semble dépendre des relations instituées entre le ministre de l'Intérieur et la CNCIS. Jusqu'en 2006, l'interlocuteur privilégié, au sein de l'Exécutif de la CNCIS, était le premier ministre, chef de l'administration. La première personnalité qualifiée est François Jaspart, ancien responsable à la police judiciaire.

II. Les organismes de contrôle n'assurent plus de véritable protection de la vie privée

A. Les organismes de contrôle ne constituent plus un recours suffisant

1. Les recours sont limités, dans certains cas : c'est surtout le cas aux USA, avec le Patriot Act, pendant une durée limitée, le décret-loi de 2002, les lois de 2007 et 2008, et en Allemagne.

1.1. **Le Patriot Act** a été adopté le 26 octobre 2001, dans un contexte d'unanimisme. 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[45] aux termes de la FISA. 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

[39] Jean-Patrick Courtois.

[40] « *…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.

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

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

[43] « *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.

[44] « *Je crains qu'il n'engendre un enchevêtrement entre les missions de la CNCIS et celles de la CNIL* », Sénat, séance du 15 décembre 2005.

[45] Roving orders.

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[46] 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 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.

1.2. Le décret-loi de 2002

En certaines occurrences, il n'est plus nécessaire aux USA de demander et d'obtenir une autorisation judiciaire pour procéder à des interceptions. En 2002, le président Bush a signé un décret-loi secret autorisant la National Security Agency, 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[47]. Le président aurait le pouvoir requis pour prendre ce décret-loi en vertu de la compétence que lui confère l'article deux[48]de la Constitution américaine et conformément à une résolution mixte des deux chambres du Congrès, issue du Sénat[49], portant le titre *Authorization for Use of Military Force*[50]. 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. Des études ont été menées à ce sujet[51]. 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 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.[52] Sont possibles 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[53] et la surveillance électronique sans mandat pendant quinze jours suivant une

[46] 50 U.S.C. 1805 c(2)(D) et 1805(d).

[47] E.Lichtblau et J.Risen « *Bush Lets US Spy on Callers Without Courts* », The New York Times, 18 décembre 2005, p 1.

[48] Cet article spécifie quels sont les pouvoirs exécutifs du Président, y compris ses pouvoirs en tant que commandant en chef des forces armées américaines.

[49] SJ Res 23.

[50] AUMF, autorisation du recours à la force militaire, promulguée par le Président Bush le 18 septembre 2001

[51] 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.

[52] 50 U S C 1802.

[53] 50 USC 1805 (f).

déclaration de guerre par le Congrès[54]. 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[55] 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)[56]. Selon le groupement dirigé par l'ACLU, le programme de la NSA violerait le premier amendement 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[57]. 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[58].

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 ont été rendus publics, divers comités du Congrès se sont prononcé 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*[59], 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 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 à deux reprises. 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.

1.3. La réforme de la FISA

1.3.1. La loi du 5 août 2007

La loi promulguée le 5 Août 2007 réforme la FISA. 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. Certains opposants ont fait remarquer qu'il y avait danger de dérive, qu'il était désormais possible d'intercepter des Américains

[54] 50 USC 1811.

[55] Tribunal fédéral de district de Detroit.

[56] Tribunal fédéral de district de Manhattan.

[57] Voir ACLU : « *ACLU Sues to Stop Illegal Spying on Americans, Saying President Is Not Above the Law* » communiqué du 17 janvier 2006.

[58] Voir CCR : « CCR Files Suit over NSA Domestic Spying Program », communiqué du 17 janvier 2006.

[59] SCJ, comité sénatorial des affaires judiciaires.

communiquant avec des personnes à l'étranger, sans intention délictueuse ou criminelle. Une garantie existe cependant : si un Américain devient la cible principale des interceptions, un mandat devient obligatoire pour poursuivre la surveillance. La FISA Court, le tribunal de la FISA ne joue plus de rôle actuellement. Le contrôle par un organisme indépendant du gouvernement a vécu. Mais cette réforme n'est valable que pour six mois.

1.3.2. La loi de 2008

Compte-tenu des discussions qui étaient apparues avec le programme précédent permettant les interceptions sans mandat, une loi a été déposée et adoptée définitivement par la Chambre des Représentants et par le Sénat le 10 juillet 2008[60]. La loi autorise 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 72 heures pour obtenir un mandat. Elles doivent avoir 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. Ainsi la protection de la vie privée est-elle réduite, et, pour cette raison même, un organisme de contrôle est mis en place. « *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.

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'interceptions téléphoniques aux USA. Le projet initial ne mentionnait pas l'immunité juridique mais cette dernière semblait essentielle à l'Exécutif et aux compagnies de télécommunications. Le président Bush a fait savoir qu'il n'attendrait pas la fin des débats pour autoriser la surveillance des communications[61] des présumés terroristes. Pour justifier cette attitude, le président invoque d'éventuelles menaces contre la sécurité nationale. 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.

2. En Allemagne : le contrôle est limité

2.1. L'amendement de la loi G10 et la loi de 2004

2.1.1. L'amendement de la loi G10 :

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 ; le champ d'application de la G10 s'est considérablement élargi au détriment des garanties consenties en matière de droits fondamentaux. La nouvelle loi sur les télécommunications est adoptée fin 2001, et entre en vigueur en janvier 2002. L'ordonnance sur l'interception des télécommunications permet notamment 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.

2.1.2. La loi de mars 2004 sur les communications électroniques. L'initiateur du texte[62] avait fait savoir qu'il voulait contraindre les fournisseurs de service Internet à conserver les données du trafic

[60] Par 69 voix, dont celle de M. Obama, contre 28.

[61] Conversations téléphoniques et échanges de méls.

[62] Le ministre de l'intérieur de l'époque, Otto Schily.

Internet pendant un an. Il n'a pas été suivi sur ce point par les parlementaires et a du renoncer à ces dispositions. A l'initiative des Grünen et des sociaux-démocrates, le texte a été amendé dans un sens qui prend en compte la confidentialité des communications.

2.2. Un contrôle demeure, diligenté notamment par la cour constitutionnelle

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 du Land de Nordhein-Westphalen autorisait la police 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, mais seulement dans certains cas bien circonscrits. La police a le droit de surveiller à distance la navigation sur Internet des personnes soupçonnées de crimes, mais en suivant des procédures précises : premièrement, les perquisitions en ligne sont autorisées par un juge. Deuxièmement, ces perquisitions en ligne ne sont autorisées 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 peuvent 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. Selon l'éditorial du Hamburger Abendblatt[63] : « *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 menaçant notre existence* ». En bref, selon Gilles Guglielmi[64], 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[65], qui s'était heurté à la ministre de la Justice[66].

Ainsi, si le contrôle existe toujours en Allemagne dans le domaine des interceptions, il s'est considérablement réduit.

Le même constat peut être établi pour la quasi-totalité des pays occidentaux, qui se différencient par leur culture juridique et historique, mais ont la maîtrise des organismes de contrôle en matière d'interceptions de communications électroniques et de télécommunications.

B. Cette situation s'explique par les liens toujours plus étroits entre les Exécutifs et les organismes de contrôle

Les lois, votées par les Parlements, sont en général d'origine gouvernementale. C'est pourquoi, dans un contexte où le facteur sécurité est privilégié aux dépens de la protection de la vie privée les organismes de contrôle ont de plus en plus de difficultés à conserver leur indépendance et c'est pourquoi aussi le concept de personnalité « protégée » perd de son importance

1. Les organismes de contrôle sont de moins en moins indépendants vis-à-vis de l'Exécutif : l'exemple de la France

Avec la loi du 23 janvier 2006[67], sur la lutte anti-terrorisme, une personnalité « qualifiée », désignée par la CNCIS sur une liste de trois personnes établie par le ministre de l'intérieur autorise l'identification précise des téléphones fixe ou mobile, les adresses IP de ses moyens informatiques, la communication des abonnements liés aux numéros repérés et des documents d'inscription, relevé de toutes les connexions téléphoniques[68], destinataires ou émetteurs de SMS, dates et heures, géolocalisation des connexions par téléphone portable. Ces identifiants ne concernent pas le contenu des messages, mais ils sont utiles aux agents habilités pour demander que soient rassemblés des renseignements sur la cible. Les demandes des agents individuellement désignés et dûment habilités

[63] Maike Röttger, 28 février 2008, traduction de Francis Segond.
[64] Professeur de droit à l'Université Panthéon-Assas.
[65] Wolfgang Schäuble.
[66] Brigitte Zypries.
[67] Article six.
[68] Entrées et sorties.

des services de police et de gendarmerie nationale spécialement chargés des missions de surveillance sont motivées et soumises à la décision de la personnalité qualifiée. Le mandat est de trois ans renouvelable. Des adjoints suppléants sont désignés dans les mêmes conditions que la personnalité qualifiée. La CNCIS contrôle a posteriori les opérations et saisit le ministre de l'Intérieur d' « une recommandation » lorsqu'elle « constate un manquement aux règles…ou une atteinte aux droits et libertés.

1.1. Le dispositif normatif :

1.1.1. L'article 6 de la loi[69] du 21 juin 2004 pour la confiance dans l'économie numérique, modifié par la loi[70]du 23 janvier 2006 relative à la lutte contre le terrorisme et portant diverses dispositions afférentes à la sécurité et aux contrôles frontaliers.

1.1.2. L'article L 34-1-1 du Code des postes et des communications électroniques.

1.1.3. Le décret[71] du 22 décembre 2006 pris pour l'application du I de l'article 6 de la loi du 23 janvier 2006 : la première personnalité qualifiée est François Jaspart ; les six adjoints sont nommés dans les mêmes conditions par la CNCIS le 21 mars et le 28 septembre 2007

1.1.4. Arrêtés du 31 mars 2006 pris pour l'application de l'article 33 de la loi du 23 janvier 2006 et du 10 mai 2007 pris pour l'application de l'article R.10-20 du Code des postes et des communications électroniques

1.2. Entre garantie des libertés publiques et dépendance vis-à-vis de l'Exécutif :

1.2.1. Selon François Jaspart, le dispositif garantit les libertés publiques puisque toutes les demandes sont instruites et autorisées avant mise en œuvre. Un fonctionnaire habilité passe un message crypté à la plate-forme technique des données de connexion aux systèmes de communication, gérée par l'UCLAT[72]. La plate-forme est un simple relais technique. Il ne faut au système que quelques heures pour que la demande soit autorisée par la personnalité qualifiée. En fait, trois cas d'école sont possibles : la réponse est positive, la réponse est négative, ou bien la demande implique des éclaircissements complémentaires. Si la réponse est positive, l'UCLAT peut saisir tous les opérateurs téléphoniques ou informatiques qui sont tenus de communiquer les informations qu'ils possèdent. Selon la CNCIS[73], dans son approche du premier rapport rendu par la personnalité qualifiée, la personnalité qualifiée relève que sur huit mois d'activité en 2007, 27701 demandes ont été examinées, 25982 ont reçu une réponse positives, 243 ont donné lieu à une réponse négative, 1476 ont induit des demandes d'éclaircissements supplémentaires. Ces chiffres paraissent importants. En réalité, plusieurs dizaines de demandes concernent une seule « cible », c'est-à-dire une seule personne soupçonnée d'activités terroristes. Un dialogue a été élaboré entre les demandeurs et la personnalité qualifiée.

De son côté, la CNCIS a élaboré un système de contrôle gradué, considérant que la motivation des demandes devait être examinée en tenant compte du caractère plus ou moins intrusif de la prestation en matière de libertés individuelles. Elle a institué des réunions bimensuelles avec la personnalité qualifiée afin de parvenir à une harmonisation des critères d'appréciation afférents au motif « terrorisme », pour parvenir à une unité de jurisprudence entre la CNCIS et la personnalité qualifiée.

1.2.2. La prééminence de l'Exécutif :

- Au sein de la CNCIS : un ancien ministre de l'Intérieur a été désigné comme membre de la CNCIS désigné par le président de l'Assemblée nationale.

- La personnalité qualifiée désignée par la CNCIS a longtemps travaillé pour les services de police et est particulièrement sensible aux préoccupations du ministère de l'intérieur

- La CNCIS a émis une seule recommandation. Cela peut signifier et cela signifie sans doute que le dialogue entre la CNCIS et la personnalité qualifiée est constructif. Mais cela peut suggérer que l'autonomie de la personnalité qualifiée à l'égard de la CNCIS est significative. Est-ce positif ? Il est trop tôt pour se prononcer

[69] Loi 2004-575.
[70] 2006-64.
[71] 2006-1651.
[72] Unité de coordination de la lutte anti-terroriste.
[73] Rapport d'activité 2007, La documentation française, 2008, pp 29-32.

- Le rapport annuel de la personnalité qualifiée est adressé au ministre de l'Intérieur, autorité exécutive, et à la CNCIS, autorité administrative indépendante. Il n'est pas destiné au Parlement et à la société civile.

Ces indices concordants laissent penser que la personnalité qualifiée peut être tentée, dans certains cas, d'accepter l'influence exercée par le ministre de l'intérieur.

2. Les dispositifs récents pour les organismes de contrôle en matière d'interceptions de télécommunication sont marqués par le sceau de l'ambiguïté.

2.1. Aux USA, avec la loi de 2008, un tribunal spécial a été instauré pour permettre l'interception des conversations d'un Américain à l'étranger. On peut considérer, si l'on envisage cet aspect de la question que l'objectif de garantie dans le domaine des libertés individuelles n'est pas perdu de vue. Néanmoins, si l'on suit le fil conducteur initié par le *Patriot Act* en 2001, si l'on examine les autres aspects de la loi de 2008, et notamment le fait que les autorités disposent à présent d'une semaine, et non de 72 h afin d'obtenir un mandat, si on souligne qu'il est possible de pratiquer sans autorisation préalable des interceptions de télécommunications à l'étranger, dans les affaires d'espionnage ou de terrorisme, l'équilibre entre ordre public et protection de la vie privée penche clairement du côté de l'ordre public, même si les autorités américaines font remarquer que la sauvegarde des libertés individuelles reste une priorité.

2.2. En France, l'institution de la personnalité qualifiée est aussi une réforme à double facette :

La personnalité qualifiée autorise la conservation de données techniques. Cela peut être considéré comme une garantie dans le domaine des libertés individuelles. Par ailleurs, si l'on comptabilise[74] les dizaines de milliers d'interceptions techniques, même en sachant que plusieurs interceptions techniques concernent la même personne, une « cible » identique, si on s'interroge sur le statut de la personnalité qualifiée, choisie par la CNCIS, sur une liste de trois personnalités désignées par le ministre de l'intérieur, on est susceptible de se poser des questions sur la protection de la vie privée en France. De plus, les interceptions techniques justifient de nouvelles interceptions de sécurité, sur le motif « lutte contre le terrorisme ». L'équilibre entre l'ordre public et la garantie des libertés individuelles est incertain.

Conclusion

Cette ambiguïté prévaut dans tous les Etats occidentaux. Les mesures juridiques sécuritaires se multiplient. Cependant, la garantie par les organismes de contrôle dans le secteur des interceptions n'est pas remise en cause. Souvent, une mesure sécuritaire est adoptée et, dans le même temps, un organisme de contrôle est créé. L'organisme de contrôle est-il un alibi, destiné à occulter les dérives d'un système où les interceptions, techniques et « de contenu », sont de plus en plus fréquentes ? Il faut se garder de toute conclusion hasardeuse mais conserver cette hypothèse à l'esprit. L'exemple récent de la Suède va aussi dans ce sens. Le 18 juin 2008, le Parlement suédois a adopté à une courte majorité[75] 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 militaires 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. La justification juridique repose sur les mécanismes de contrôle, deux commissions qui sont chargées de procéder à la surveillance des interceptions. L'équilibre ordre public/protection de la vie privée dépend du fonctionnement de ces nouveaux organismes de contrôle.

On assiste donc à un essor des interceptions de communications électroniques et de télécommunications, concomitant à la création, presque systématique d'organismes de contrôle.

[74] Rapport d'activité de la CNCIS.

[75] 143 voix pour, 138 contre, une abstention.

Ces contrôles s'exercent le plus souvent dans des espaces mixtes[76], mais aussi dans des espaces judiciaires[77], dans des espaces de sécurité[78]. Les cultures sont bien différentes mais la marge de libertés individuelles dans le cadre sécuritaire général et dans le cadre des interceptions de télécommunications en particulier dépend du devenir des organismes de contrôle, notamment du degré d'indépendance auquel ils peuvent accéder.

C. G.

[76] Judiciaires et de sécurité.
[77] Ex : Suisse.
[78] Royaume-Uni.