Commission nationale de contrôle des interceptions de sécurité

20e rapport d'activité 2011-2012

Commission nationale de contrôle des interceptions de sécurité

35, rue Saint-Dominique
75007 Paris

Téléphone : 01 45 55 70 20
Courriel : secretariat.cncis@pm.gouv.fr

ISBN : 978-2-11-009085-0

Sommaire

Avant-propos

Ce rapport 2011-2012 correspond au 20e anniversaire de la CNCIS, créée par la loi du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques. Cette échéance est l'occasion non seulement de dresser un bilan, mais également de tracer des perspectives d'avenir.

Après plus de vingt ans d'exercice, la CNCIS a démontré qu'elle avait pleinement investi la mission de contrôle que lui a confiée le législateur en 1991. Les chiffres reproduits dans ce rapport révèlent, à l'évidence, l'efficacité des vérifications opérées et la constante vigilance dont la Commission a fait preuve quant au respect par les services de la loi et de sa jurisprudence durant ces deux décennies.

La CNCIS a su faire face, à travers l'évolution de ses avis et recommandations qui constituent sa jurisprudence, au défi de l'évolution permanente des technologies en matière de communications électroniques, pour garantir un contrôle de l'ensemble des mesures attentatoires aux libertés et protéger ainsi le secret des correspondances. La spécificité de son champ d'intervention, comme des modalités dont elle use pour effectuer ses contrôles, ont ainsi confirmé son rôle indispensable dans le paysage des autorités administratives indépendantes.

Si la jurisprudence de la Commission a su s'adapter depuis deux décennies aux changements majeurs ayant affecté le domaine des communications électroniques et constitue une source de production de droit, elle n'est pas la loi. Or, face à des menaces d'atteintes aux intérêts fondamentaux de la Nation de plus en plus transversales, au caractère que l'on peut qualifier de « multi-cartes » des personnes visées par ces mesures d'investigation, qui s'adonnent à des activités illicites mêlant souvent certains aspects de la criminalité organisée, des atteintes à la sécurité nationale et même parfois du terrorisme, au développement constant des technologies de communications et des utilisations frauduleuses toujours plus ingénieuses que tentent d'en faire les cybercriminels, le texte issu de la loi du 10 juillet 1991 rencontre certaines limites.

Au regard de ces éléments, mais aussi sous l'influence du droit européen, il m'apparaît incontournable que, dans un proche avenir, afin de donner aux enquêteurs les moyens de travailler efficacement tout en renforçant les garanties de la protection des libertés de nos concitoyens,

la législation en matière d'interceptions de sécurité et de recueil de données techniques de communications soit modernisée.

L'ordonnance du 12 mars 2012, relative à la partie législative du Code de la sécurité intérieure, a conduit à l'abrogation, depuis le 1er mai 2012, de la loi du 10 juillet 1991 et à l'intégration de ses dispositions administratives dans le nouveau Code de la sécurité intérieure. Cette codification, quasi-exclusivement à droit constant, ne répond pas aux attentes réformatrices que porte la CNCIS.

La disparition de la loi fondatrice du 10 juillet 1991, symbole de la protection du secret des correspondances, et qui a créé la Commission que je préside, ne fait que souligner l'urgence d'entamer une réflexion approfondie et interministérielle sur les nécessaires améliorations à apporter à la législation encadrant le domaine des communications électroniques, et en particulier les interceptions de sécurité et le recueil de données techniques. La CNCIS, qui dispose d'une réelle expertise, issue des contrôles effectués comme des avis rendus depuis plus de vingt ans, entend évidemment prendre toute sa part dans les travaux normatifs qui seront conduits.

Cette position désormais incontournable de la CNCIS a été acquise et maintenue notamment grâce à l'investissement sans faille, à mes côtés, des deux membres parlementaires. Alors que le mandat au sein de la Commission de M. Daniel Vaillant, député de Paris et ancien ministre de l'Intérieur, s'est achevé en juin 2012, avec la fin de la XIIIe législature, je tiens à lui rendre hommage pour le travail remarquable qu'il a accompli pendant cinq années. Il a pleinement mesuré l'importance des enjeux actuels comme des sujets d'avenir dans le domaine des interceptions de sécurité. Il a, en toutes circonstances, mis son envergure politique au service de la Commission. Je saisis l'occasion de ce rapport public pour lui rendre un hommage appuyé et le remercier pour son implication au sein de la CNCIS.

Je souhaite la bienvenue à M. Jean-Jacques Urvoas, député du Finistère et président de la Commission des lois, qui a été nommé membre de la CNCIS le 23 juillet 2012 par le président de l'Assemblée nationale. Je me réjouis de la nomination de M. Urvoas puisque, à l'instar de M. Jean-Jacques Hyest, sénateur de Seine-et-Marne et second membre parlementaire, il montre un profond intérêt pour les domaines de compétence de la Commission et une volonté de contribuer à la modernisation de la législation qui les encadre.

Au-delà de la modification de la composition de son assemblée plénière, la Commission a connu, au cours de la période 2011-2012, un renouvellement de ses agents. M. Rémi Récio, délégué général, a rejoint une nouvelle affectation dans l'administration préfectorale. Je le remercie très vivement et chaleureusement pour l'action qu'il a menée. Il a été remplacé par M. Olivier Guérin, qui occupait jusqu'alors le poste

de chargé de mission. Pour lui succéder dans cette dernière fonction, M. Loïc Abrial nous a rejoints.

Je tiens également, dans cet avant-propos, à saluer l'action du général de brigade aérienne Claude Baillet, qui vient de quitter son poste de directeur du Groupement interministériel de contrôle (GIC). Durant les années qu'il a passées à la tête du GIC, la coopération quotidienne avec la CNCIS, dans le respect des prérogatives de chacun, s'est déroulée dans une parfaite confiance et s'est avérée extrêmement fructueuse. Je souhaite la bienvenue au contre-amiral Bruno Durteste, qui lui a récemment succédé.

Enfin, j'adresse mes plus vifs remerciements à mon prédécesseur, M. Jean-Louis Dewost, à M^me^ Isabelle Harel-Dutirou, conseillère référendaire à la Cour de cassation et à M^me^ Virginie Peltier, maître de conférences à l'université Montesquieu à Bordeaux, pour leur riche contribution à ce 20^e^ rapport d'activité.

Hervé PELLETIER
Président de la Commission

Chapitre liminaire

Le 20e anniversaire de la Commission nationale de contrôle des interceptions de sécurité

Indépendance, confiance, et vigilance

Jean-Louis Dewost
Président de section honoraire au Conseil d'État
Ancien président de la CNCIS

Le président Pelletier a sollicité quelques réflexions de ma part à l'occasion des vingt ans de la loi de 1991 qui a institué la Commission nationale de contrôle des interceptions de sécurité.

Ma contribution sera brève, aussi peu technique que possible, et centrée sur ce qui me paraît être l'essentiel dans ce domaine sensible – et parfois « sulfureux »… – des écoutes administratives, à savoir *L'indépendance* de l'Autorité de contrôle que j'ai eu l'honneur de présider de 2003 à 2009.

Indépendance

Pour certains « beaux esprits », l'indépendance – comme la solitude pour Gilbert Bécaud – « ça n'existe pas ! »… Ils se réfèrent bien entendu

aux théories socio-psychologiques, selon lesquelles nous serions tous « conditionnés » par notre éducation, notre milieu social, etc.

Parlant d'une institution publique, ce n'est pas à cette indépendance-là à laquelle je me réfère, mais à celle qui doit présider à toute décision prise au nom de l'intérêt général, en particulier lorsqu'il s'agit de « faire la balance » entre la protection des droits individuels qui s'impose dans toute démocratie, et les nécessités tout aussi impérieuses de sauvegarde de la population et de l'État contre les menaces criminelles ou terroristes.

Il s'agira donc de protéger l'indépendance de l'institution et de ses membres, non seulement contre d'éventuelles pressions de l'exécutif, mais aussi contre les pressions médiatiques dont l'importance s'est accrue dans nos sociétés modernes.

Sur ces deux terrains, le législateur de 1991 comme celui de 2006, ont fait preuve d'une grande sagesse.

Une Commission restreinte (trois membres), un choix pour la désignation du président effectué parmi les deux cours suprêmes de l'ordre judiciaire et administratif, et enfin une nomination de celui-ci pour une durée suffisamment longue (six ans) nomination *non renouvelable*, ont été au cours des années un gage de succès.

Savoir qu'on peut prendre des décisions, parfois difficiles, sans être « démissionné », et symétriquement sans être soupçonné d'« espérer » quoi que ce soit pour l'avenir, surtout quand on a sa carrière derrière soi, conforte même ceux qui sont déjà naturellement indépendants d'esprit…

Les dispositions de la loi relative au *secret-défense* qui gouvernent les activités de la Commission sont, elles, tout à fait essentielles pour préserver celle-ci d'éventuelles pressions médiatiques. Je sais pertinemment que dans ce monde dominé par l'idéologie (trompeuse) de la transparence, le secret a mauvaise presse… Il n'empêche qu'en la matière il est indispensable, et n'empêche pas la Commission de « communiquer », ce qu'elle fait chaque année à travers son rapport public.

Confiance

L'indépendance de la Commission, affirmée par la loi, ne peut être effective dans les faits sans la confiance.

Celle-ci s'exprime dans quatre domaines :

Confiance entre les membres de la Commission

La sagesse du législateur a prévu que le président est assisté de deux parlementaires, un député et un sénateur, désignés par les

présidents respectifs des deux chambres : l'expérience politique des deux parlementaires vient ainsi conforter la vision plus juridique du président.

La sagesse des présidents successifs a fait en sorte que les deux parlementaires soient issus, l'un de la majorité, l'autre de l'opposition.

Même si, en théorie, les décisions peuvent se prendre à la majorité, je peux dire sans violer le secret, que, dans la pratique le consensus est recherché et obtenu. Ceci crée une atmosphère de confiance qui a permis de confier au président, par le règlement intérieur, la possibilité de régler les cas urgents ente deux réunions de la Commission, à condition d'appliquer la « jurisprudence » de la Commission.

Confiance entre la Commission et la « personnalité qualifiée » de la loi de 2006

La loi de 2006, relative à la lutte contre le terrorisme, a conféré à des agents dûment habilités des services de police et de gendarmerie la responsabilité de requérir certaines prestations des opérateurs téléphoniques : les demandes de ces agents sont soumises à l'approbation d'une « personnalité qualifiée » désignée par la CNCIS parmi les trois noms proposés par le ministre de l'Intérieur. Cette procédure, assez innovante, a été prise très au sérieux par la Commission qui a su créer, au fil des années, avec la « personnalité » qu'elle désigne, des relations de confiance qui prennent la forme de réunions régulières : celles-ci permettent d'harmoniser la « jurisprudence » de la personnalité qualifiée avec celle de la Commission.

Confiance entre la Commission et le Groupement interministériel de contrôle (GIC)

Les opérations matérielles d'interception des communications autorisées par le Premier ministre après avis de la Commission, sont ordonnées par le GIC (décret en Conseil d'État du 12 avril 2002), placé traditionnellement sous l'autorité d'un officier général nommé par le Premier ministre.

Le GIC, qui, avec ses ingénieurs et ses agents civils et militaires, est en mesure de dialoguer d'égal à égal avec les opérateurs comme avec les services de renseignement, est en contact quotidien avec la Commission. Il l'assiste sur le plan technique, et constitue en quelque sorte son « bras armé ». J'ai toujours entretenu, tout au long de mon mandat, des relations – indispensables – de confiance totale avec les trois officiers généraux que j'ai connus comme directeurs du GIC, ainsi qu'avec leur adjoint. La pratique consistant à recueillir officieusement l'avis du président de la Commission avant de nommer le directeur du GIC s'inscrit dans ce contexte.

Confiance entre la Commission et le cabinet du Premier ministre

Formellement, la Commission est investie d'un pouvoir de *recommandation a posteriori* d'interruption d'écoutes déjà autorisées par le Premier ministre.

Dès les premières années, ce pouvoir a été exercé *a priori,* avec le plein accord du Premier ministre, ce qui a transformé *de facto*, le pouvoir de recommandation en un quasi pouvoir de décision. Ceci suppose, ici aussi, une grande confiance entre la Commission et le cabinet de Matignon.

La franchise est de règle, et, s'il y a désaccord, il est « assumé » de part et d'autre. La statistique prouve s'il en était besoin que ces divergences d'appréciation sont extrêmement rares, pour ne pas dire inexistantes.

Vigilance

Indépendance et confiance n'excluent pas une certaine vigilance…

Vigilance vis-à-vis des « services », et, pour le président de la Commission, vigilance vis-à-vis de lui-même !

La vigilance vis-à-vis des services

Il est normal que les services de renseignement, dont c'est le métier, aient tendance à privilégier la sécurité de l'État et des populations par rapport à la protection de la liberté de communication. Ils ne négligent pas cette dernière, mais leur appréciation de l'endroit où il convient de placer le « curseur » peut, dans certaines circonstances, être différente de celle de la Commission. C'est la raison pour laquelle la Commission a inauguré, il y a quelques années le « contrôle continu », consistant à contrôler les interceptions même autorisées, afin de voir, dans la durée, si les conditions de l'autorisation sont toujours réunies, et, si ce n'est pas le cas, de proposer au Premier ministre une suppression anticipée.

Bien entendu, ces initiatives sont le plus souvent précédées d'un contact avec le chef du service intéressé, occasion d'un dialogue empreint de franchise, franchise n'excluant pas une certaine fermeté. L'expérience a prouvé que cette « pédagogie » était efficace et ne minait pas la confiance à long terme.

La vigilance vis-à-vis de soi-même

Comme je l'ai rapporté, le dialogue confiant avec les parlementaires est essentiel.

Il n'empêche qu'entre deux réunions le président est conduit du fait de l'urgence à statuer seul. Or, il n'y a rien de plus dangereux que l'exercice solitaire du pouvoir… Nul n'est à l'abri d'un jugement trop rapide, voire d'une mauvaise appréciation d'un dossier.

Ici, le rôle du délégué général est essentiel. Le président peut en effet confronter son jugement à celui de son délégué général avant de trancher l'affaire. Je dois dire ici, que les deux magistrats de grande qualité qui m'ont successivement assisté dans cette fonction m'ont tous deux beaucoup aidé dans ma tâche, tout en respectant parfaitement mon autonomie de décision.

Que dire, en conclusion ? Si ce n'est qu'il conviendra d'y regarder à deux fois avant d'entreprendre une révision de la loi de 1991, pour l'instant codifiée récemment à droit constant.

En tout état de cause, je conseillerai de conserver les ingrédients de la réussite de ces vingt années : un nombre restreint de membres, la durée de nomination d'un président non renouvelable, et le choix attentif des personnalités qui travaillent en confiance sur ce sujet difficile… mais ce dernier point relève des autorités politiques de nomination !

La jurisprudence de la chambre criminelle relative aux interceptions de correspondances

Isabelle Harel-Dutirou
Conseillère référendaire à la chambre criminelle de la Cour de cassation

Il résulte de l'article 427 du Code de procédure pénale que : « Hors les cas où la loi en dispose autrement, les infractions peuvent être établies par tout mode de preuve ». Cet article pose le principe de la liberté de la preuve qui, en matière pénale, permet de rechercher tous les éléments nécessaires à la manifestation de la vérité et de les produire devant le juge pénal.

Pour autant, la preuve ne saurait être recherchée sans que soit assuré le respect des principes énoncés par La Convention européenne des droits de l'homme, notamment des articles 3 relatif au respect de la dignité humaine, 6 § 1 relatif au procès équitable et 8 relatif à la protection de la vie privée et familiale, du domicile et de la correspondance. Les moyens de preuve produits devant le juge pénal ne sauraient procéder d'une méconnaissance des règles de procédure et avoir pour effet de porter atteinte aux droits de la défense.

Ces principes ont donné lieu à une importante jurisprudence de la part de la Cour européenne qui, conformément à l'article 19 de la Convention, en contrôle le respect par les États et en précise le sens, ainsi qu'à de nombreuses décisions de la Cour de cassation témoignant d'un souci de concilier efficacité et célérité de l'action et respect des droits des individus dans des sociétés démocratiques.

Ces décisions ont porté notamment sur ces éléments de preuve que constituent les données fournies par l'interception des correspondances qui constituent des atteintes à la liberté individuelle, à l'intimité de la vie privée et au respect du domicile, permettant d'apporter d'importantes précisions à une législation très encadrée et de rappeler les limites à respecter.

Une procédure très encadrée

L'article 8 de la Convention européenne des droits de l'homme et les interceptions de correspondance

Il résulte de l'article 8 de la Convention européenne des droits de l'homme que «Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance et qu'il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une

mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. »

Pour la Cour européenne, l'interception des correspondances s'analyse en « une ingérence d'une autorité publique » qui méconnaît l'article 8 de la Convention sauf si, « prévue par la loi », elle est nécessaire à la poursuite d'un ou plusieurs des buts légitimes énoncés. Si les États jouissent d'une certaine marge d'appréciation pour juger du caractère nécessaire de l'ingérence, il n'en demeure pas moins qu'il existe un contrôle européen sur la loi et les décisions qui l'appliquent.

La pertinence de ce contrôle s'est manifestée avec les changements législatifs intervenus en Grande-Bretagne et en France après la condamnation de ces États par la Cour dans les célèbres arrêts *Malone* et *Kruslin*.

Déjà, dans son arrêt *Klass et autres c/Allemagne* du 6 septembre 1978, la Cour avait énoncé que « Quel que soit le système de surveillance retenu, la Cour doit se convaincre de l'existence de garanties adéquates et suffisantes contre les abus. Cette appréciation ne revêt qu'un caractère relatif : elle dépend [entre autres, du] type de recours fourni par le droit interne. Par conséquent, il y a lieu de rechercher si les procédures destinées au contrôle de l'adoption et de l'application des mesures restrictives sont aptes à limiter à ce qui est "nécessaire dans une société démocratique" l'"ingérence" résultant de la législation incriminée. Il faut de surcroît, pour ne pas dépasser les bornes de la nécessité au sens de l'article 8 § 2, respecter aussi fidèlement que possible, dans les procédures de contrôle, les valeurs d'une société démocratique. Parmi les principes fondamentaux de pareille société figure la prééminence du droit, à laquelle se réfère expressément le préambule de la Convention [...]. Elle implique, entre autres, qu'une ingérence de l'exécutif dans les droits d'un individu soit soumise à un contrôle efficace [...] » (CEDH *Klass et autres c/Allemagne* 6 septembre 1978 requête n°5029/71).

Saisie par requête d'un ressortissant britannique qui estimait que l'interception, la surveillance et l'enregistrement de ses conversations téléphoniques dans le cadre d'une procédure suivie contre lui du chef de recel de biens volés étaient illicites en ce qu'elle se fondaient sur un mandat du ministre de l'Intérieur, la Cour a fait application de ces principes et considéré que le droit anglais et gallois relatif à l'interception de communications pour les besoins de la police était obscur, peu accessible et qu'il existait un risque d'abus. Elle a alors condamné le Royaume-Uni pour violation de l'article 8 et, dès 1985, le législateur a tiré les leçons de cette condamnation avec *The Interception of Communication Act* (CEDH *Malone c/RU* 2 août 1984, requête n°8691/79).

De la même façon, saisie de la requête d'un ressortissant français qui s'était vu refuser l'annulation de l'enregistrement d'une communication, la Cour a condamné l'État français en raison de l'absence d'une législation spécifique applicable aux interceptions de correspondances (CEDH *Kruslin c/France* 24 avril 1990, requête n°11801/85).

Le dispositif législatif français

La France a alors modifié son dispositif juridique en la matière, et ce en deux temps, d'une part en posant des règles générales issues de la loi n° 91- 646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques et insérées dans les articles 100 et suivants du Code de procédure pénale (avec une compétence unique du juge d'instruction qui peut prescrire, lorsque les nécessités de l'information l'exigent, l'interception, l'enregistrement et la transcription des correspondances pour une durée de quatre mois maximum, renouvelable), d'autre part en prévoyant dans la loi n° 2004-204 du 9 mars 2004 relative aux adaptations de la justice aux évolutions de la criminalité, un régime spécial en matière de criminalité organisée, prévu à l'article 706-95 du Code de procédure pénale avec l'extension de la possibilité de procéder à des écoutes dans le cadre des enquêtes préliminaire ou de flagrance mais sous le contrôle d'un magistrat du siège.

Il convient de signaler que la loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure a modifié cet article 706-95 en prévoyant que l'autorisation est donnée par le juge des libertés et de la détention non plus pour une durée de quinze jours mais d'un mois et que ce juge est informé sans délai des procès-verbaux dressés en exécution de son autorisation.

La Cour européenne a pris acte de la nouvelle législation adoptée en relevant que « les articles 100 et suivants du Code de procédure pénale, créés par la loi du 10 juillet 1991 sur le secret des correspondances émises par la voie des télécommunications, posent des règles claires et détaillées et précisent, *a priori*, avec suffisamment de clarté l'étendue et les modalités d'exercice du pouvoir d'appréciation des autorités dans le domaine considéré » (CEDH *Lambert c/France* 24 août 1998, requête 88/1997/872/1084).

La jurisprudence de la Cour de cassation

– Faisant application du dispositif législatif ainsi posé par la loi de 1991, la chambre criminelle a énoncé de façon très constante que les interceptions doivent être impérativement placées sous le contrôle d'un juge en énonçant que « les écoutes et enregistrements téléphoniques, qui trouvent leur base légale dans les articles 81 et 151 du Code de procédure pénale, peuvent être effectués à l'insu des personnes intéressées, qui ne sont pas seulement celles sur qui pèsent les indices de culpabilité, s'ils sont opérés pendant une durée limitée, sur l'ordre d'un juge et sous son contrôle en vue d'établir la preuve d'un crime ou de toute

autre infraction portant gravement atteinte à l'ordre public, et d'en identifier les auteurs ; il faut en outre que les écoutes soient obtenues sans artifice ni stratagème, et que leur transcription puisse être contradictoirement discutée par les parties concernées, le tout dans le respect des droits de la défense ; ces prescriptions répondent aux exigences de l'article 8 alinéa 2 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (Crim. 26 novembre 1990, pourvoi n° 90-84.594 ; Crim. 5 novembre 1991, pourvoi n° 91-84.134).

Ce principe énoncé, elle en a logiquement déduit que l'omission d'informer le juge des libertés et de la détention des interceptions qu'il a autorisées, à la requête du procureur de la République, dans la stricte application des articles 706-95 et 100 du Code de procédure pénale, ne porte pas atteinte aux intérêts de la personne mise en examen lorsque la poursuite de ces interceptions a été ordonnée par le juge d'instruction à l'expiration du délai imparti et opérée sous son contrôle ou lorsque ces interceptions ont été portées à la connaissance du magistrat instructeur qui avait pu s'assurer de leur régularité (Crim. 20 mars 2007, pourvoi nn 07-82.625, Crim. 26 juin 2007 Bull. n° 172, Crim. 20 juillet 2011, pourvoi n° 11-81.823).

– S'agissant de la durée de la mesure, elle a indiqué que les interceptions téléphoniques, pour ne pas porter une atteinte injustifiée aux droits fondamentaux de la personne, doivent être effectuées « pendant une durée n'excédant pas le temps nécessaire à la manifestation de la vérité », l'appréciation de cette durée relevant de l'appréciation souveraine des juges du fond (Crim. 9 décembre 1991 Bull. Crim. n° 465, Crim. 1er février 2011 Bull. Crim. n° 15).

Dans le prolongement de la position retenue en matière de sonorisation (Crim. 13 novembre 2008 Bull. Crim. n° 230), la chambre criminelle a précisé que le point de départ de la mesure d'interception doit être fixé au jour de la mise en place effective des interceptions (Crim. 10 mai 2012, pourvoi n° 11-87.328).

– Selon l'article 100 alinéa 2 du Code de procédure pénale, la décision d'interception est écrite ; elle n'a pas de caractère juridictionnel et n'est susceptible d'aucun recours. Ce texte n'impose pas d'obligation de motivation et la chambre criminelle a considéré que la décision d'autorisation des interceptions n'a pas à être motivée en indiquant que « les dispositions de l'article 706-95 du Code de procédure pénale et des articles 100, 100-1 et 100-3 à 100-7 du même code, auxquels il renvoie, qui ne prévoient pas que la décision du juge des libertés et de la détention autorisant des interceptions de correspondances émises par la voie des télécommunications soit motivée, ne sont pas contraires aux articles 6, 8 et 13 de la Convention européenne des droits de l'homme, dès lors que ces mesures, nécessaires au sens des textes conventionnels invoqués, sont autorisées par un juge qui en contrôle l'exécution et que la personne concernée dispose d'un recours effectif pour faire sanctionner

d'éventuelles irrégularités qui les affecteraient » (Crim. 27 septembre 2011 Bull. Crim. n° 186).

– L'article 100-1 du Code de procédure pénale précise que la décision d'interception doit comporter tous les éléments d'identification de la liaison à intercepter ; l'article c/ 100-1 de la circulaire générale indique qu'il s'agit de tous les éléments dont dispose le juge et qui permettent d'identifier la liaison à intercepter ; il s'agira le plus souvent du numéro de la ligne et, le cas échéant, du nom de son titulaire ; la circulaire ajoute que la loi n'imposant pas de formalisme particulier, la décision du juge pourra revêtir la forme d'une ordonnance ou d'une commission rogatoire. Amenée à se prononcer sur ce point, la chambre criminelle a considéré que justifiait sa décision de rejeter le moyen de nullité soulevé l'arrêt relevant que les mentions relatives au numéro des lignes figuraient sur les commissions rogatoires et que l'identité de leur titulaire ou de leur utilisateur était précisée soit dans ces commissions rogatoires, soit dans le premier acte d'exécution de celles-ci (Crim. 25 février 2003, pourvoi n° 02-87.745, Crim. 21 juin 2011, pourvoi n° 10-88.306).

En outre, si cette décision doit intervenir avant que la réquisition ne soit délivrée à l'opérateur téléphonique, il n'est pas exigé que l'autorisation ait été transmise préalablement à l'officier de police judiciaire (Crim. 26 mars 2008, pourvoi n° 07-88.281).

Les informations données par le procureur de la République au juge des libertés et de la détention, en application de l'article 706-95, alinéa 3, du Code de procédure pénale, portent sur les diligences effectuées et non sur leur contenu (même arrêt).

– S'agissant de la notion d'information « sans délai », elle a précisé que l'article 706-95 du Code de procédure pénale n'exige pas que le juge des libertés et de la détention exerce un contrôle immédiat sur le déroulement de l'écoute qu'il a autorisée au cours d'une enquête préliminaire mais seulement qu'il soit informé sans délai par le procureur de la République, à l'issue des opérations d'interception, d'enregistrement et de transcription prévues par les articles 100-3 à 100-5 du Code de procédure pénale (Crim. 23 mai 2006 Bull. Crim. n° 132, Crim. 20 mars 2007, pourvoi n° 06-89.555).

Elle en déduit que les officiers de police judiciaire qui, à l'occasion de l'exécution d'une commission rogatoire, acquièrent la connaissance de faits nouveaux, peuvent, avant toute communication au juge d'instruction des procès-verbaux qui les constatent, effectuer d'urgence les vérifications sommaires qui s'imposent pour en apprécier la vraisemblance, dès lors qu'elles ne présentent pas un caractère coercitif exigeant la mise en mouvement préalable de l'action publique (Crim. 26 octobre 2010, pourvoi n° 10-82.814, Crim. 27 mars 2012, pourvoi n° 11-88.321).

– S'agissant du contrôle de la régularité des pièces jointes à une procédure d'instruction, la Cour européenne a été saisie de la requête

d'un ressortissant français qui se plaignait du versement à son dossier pénal de la transcription d'écoutes téléphoniques réalisées dans une autre procédure pénale, à laquelle il était étranger et dont il n'avait pu contester la régularité, alors que la chambre criminelle avait approuvé l'irrecevabilité de sa demande en annulation de ces écoutes. Elle a estimé que l'intéressé n'avait pas bénéficié d'un « contrôle efficace » tel que voulu par la prééminence du droit et apte à limiter à ce qui était « nécessaire dans une société démocratique » l'ingérence litigieuse et considéré qu'il y avait eu violation de l'article 8 de la Convention (CEDH *Matheron c/France* 20 mars 2005, requête n° 57752/00).

Dans le prolongement de cet arrêt, la chambre criminelle a opéré un important revirement de jurisprudence.

Ainsi, après avoir considéré qu'il n'appartenait pas à la chambre de l'instruction d'apprécier la régularité formelle d'actes de la procédure accomplis dans le cadre d'une information étrangère au dossier dont elle était saisie (cette jurisprudence s'appliquant notamment dans le cas d'écoutes téléphoniques), elle juge désormais qu'une personne mise en examen est recevable à proposer des moyens de nullité pris de l'irrégularité d'actes accomplis dans une information à laquelle elle n'a pas été partie, lorsqu'elle invoque une atteinte à l'un de ses droits qui aurait été commise dans la procédure distincte, ou que les éléments versés dans l'information dans laquelle elle est mise en examen sont susceptibles d'avoir été illégalement recueillis (Crim. 7 décembre 2005, Bull. Crim. n° 327 ; Crim. 8 juin 2006, Bull. Crim. n° 3166).

C'est ce qu'elle a rappelé ultérieurement en énonçant que « le demandeur à la nullité est recevable à proposer des moyens tirés de l'irrégularité d'actes accomplis dans une information à laquelle il n'est pas partie et qui ont été versés à la procédure lorsqu'il invoque une atteinte à l'un de ses droits qui aurait été commise dans la procédure distincte ou que les pièces versées sont susceptibles d'avoir été illégalement recueillies » (Crim. 16 février 2011 Bull. Crim. n° 29).

– Enfin, la chambre criminelle a énoncé que le juge d'instruction pouvait, en application des articles 100 et suivants du Code de procédure pénale, ordonner l'interception, l'enregistrement et la transcription des correspondances émises par la voie des télécommunications, à destination de lignes téléphoniques localisées à l'étranger, dès lors que les interceptions, réalisées à partir de centres internationaux de transit situés en France, portaient sur des appels émis depuis le territoire français (Crim. 14 juin 2000 Bull. Crim. n° 224).

Elle l'a rappelé récemment en indiquant que « les officiers de police judiciaire peuvent, en enquête préliminaire, requérir d'opérateurs de téléphonie français la liste des appels concernant une ligne étrangère, sans violer les règles de compétence territoriale et de souveraineté des États, dès lors que ces appels sont émis à partir du territoire français, entrent sur le territoire national ou transitent sur le réseau d'un opérateur de

téléphonie français. De même, les officiers de police judiciaire, agissant sur commission rogatoire du juge d'instruction, peuvent intercepter et enregistrer les conversations émises à partir du territoire français à destination d'une ligne étrangère, entrant sur le territoire national en provenance d'une ligne étrangère ou transitant sur le réseau d'un opérateur de téléphonie français » (Crim. 1er février 2011 Bull. Crim. n° 15).

Les limites

Le choix de recourir à des mesures d'interception de communications connaît toutefois des limites.

L'interception des communications entre un avocat et son client

S'agissant des communications entre un avocat et son client, la jurisprudence considère que « si le juge d'instruction est investi, selon l'article 100 du Code de procédure pénale du pouvoir de prescrire, lorsque les nécessités de l'information l'exigent, l'interception, l'enregistrement et la transcription des correspondances émises par la voie des télécommunications, ce pouvoir trouve sa limite dans le respect des droits de la défense, qui commande la confidentialité des correspondances téléphoniques de l'avocat désigné par la personne mise en examen : qu'il ne peut être dérogé à ce principe qu'à titre exceptionnel, s'il existe contre l'avocat des indices de participation à une infraction » (Crim. 15 janvier 1997 Bull. Crim. n° 14).

Après avoir rappelé qu'« il résulte des articles 66-5 de la loi du 31 décembre 1971, 100-5 du Code de procédure pénale, 6.3 et 8 de la Convention européenne des droits de l'homme que, même si elle est surprise à l'occasion d'une mesure d'instruction régulière, la conversation entre un avocat et son client ne peut être transcrite et versée au dossier de la procédure que s'il apparaît que son contenu est de nature à faire présumer la participation de cet avocat à une infraction », la Cour de cassation a censuré une chambre de l'instruction qui avait refusé l'annulation d'une conversation « paraissant codée », en retenant que « si la conversation n'est pas, en l'état, susceptible de constituer la preuve de la commission d'une infraction par l'avocat, elle est éminemment suspecte et qu'étant incompréhensible, sa transcription ne porte pas atteinte aux droits de la défense et à la confidentialité des propos échangés entre un avocat et son client », alors qu'il n'en résultait pas que ladite conversation transcrite était de nature à faire présumer la participation de l'avocat à une infraction (Crim. 8 novembre 2000, Bull. Crim. n° 335).

Elle a également énoncé que « la captation et transcription de conversations téléphoniques échangées entre un avocat et son client sont régulières, dès lors que le contenu de celles-ci est de nature à faire présumer la participation de cet avocat à une infraction, les droits de la défense n'étant pas en cause » (Crim. 14 novembre 2001 Bull. Crim. n° 238 ; Crim. 1er octobre. 2003 Bull. Crim. n° 177).

L'interception des communications entre un avocat et un tiers

S'agissant des communications entre un avocat et une personne autre que son client, la Cour de cassation a jugé que « la liberté de communication entre l'avocat et son client, qui entraîne l'interdiction d'intercepter les correspondances ou les communications téléphoniques qu'ils échangent, ne fait pas obstacle à ce que le juge d'instruction, après avoir placé sous écoutes téléphoniques le domicile d'un proche d'une personne mise en examen, intercepte les communications de ce dernier avec l'avocat de cette personne » (Crim. 10 mai 1994 Bull. Crim. n° 9180, Crim. 8 octobre 1997, pourvoi n° 197-83.903 ; Crim. 30 septembre 1998 Bull. Crim. n° 243).

La transcription

Il résulte de l'article 100-5 du Code de procédure pénale que le juge d'instruction ou l'officier de police judiciaire rogatoirement commis, transcrit la correspondance utile à la manifestation de la vérité, qu'il doit en être dressé procès-verbal et que cette transcription est versée au dossier.

La jurisprudence a précisé que « le principe de la confidentialité des conversations échangées entre une personne mise en examen et son avocat ne saurait s'opposer à la transcription de certaines d'entre elles, dès lors qu'il est établi que leur contenu est de nature à faire présumer la participation de cet avocat à des faits constitutifs d'une infraction, fussent-ils étrangers à la saisine du juge d'instruction » (Crim. 1er octobre 2003 Bull. Crim. n° 177).

Retenant que « la conversation entre un avocat et l'un de ses clients ne peut être transcrite et versée au dossier de la procédure que s'il apparaît que son contenu est de nature à faire présumer la participation de cet avocat à une infraction », la chambre criminelle a rappelé qu'en application des articles 66-5 de la loi du 31 décembre 1971, 100-5, 174, 206 et 8 précités, les juridictions répressives doivent vérifier si l'enregistrement et la transcription critiqués ont « porté atteinte au principe de la confidentialité des conversations téléphoniques entre un avocat et un client » et, éventuellement, relever d'office la violation du principe de confidentialité des conversations téléphoniques entre un avocat et l'un de ses clients (Crim. 18 janvier 2006 Bull. Crim. n° 22).

Dès lors, doivent être annulés, au besoin d'office, les enregistrements et transcriptions de conversations téléphoniques entre un avocat et l'un de ses clients parce qu'elles entrent *ipso facto* dans l'exercice des droits de la défense, à moins que ces conversations ne laissent présumer la commission d'une infraction pénale par cet avocat (Crim. 17 sept. 2008 Bull. Crim. n° 191).

Ainsi, la confidentialité absolue de toute conversation d'un avocat avec l'un de ses clients doit être impérativement respectée dans la mesure où elle entre *ipso facto* dans l'exercice des droits de la défense, sous

la seule réserve de la présomption d'infraction imputable à cet avocat. C'est cette prescription qu'a reprise la loi n° 2005-1549 du 12 décembre 2005 qui, dans son article 38, a complété l'article 100-5 du Code de procédure pénale par un alinéa édictant qu'« à peine de nullité, ne peuvent être transcrites les correspondances avec un avocat relevant de l'exercice des droits de la défense ».

Conclusion

L'analyse de leur jurisprudence fait apparaître que tant la Cour européenne des droits de l'homme que, la Cour de cassation s'efforcent de concilier la recherche efficace des éléments nécessaires à la manifestation de la vérité et les impératifs de protection des droits des individus.

Amenés à recourir dans le cadre de la lutte contre la délinquance et tout particulièrement contre le crime organisé et le terrorisme à des méthodes d'enquête et d'investigation de plus en plus nombreuses et perfectionnées qui leur permettent de recueillir les renseignements conduisant à prévenir ou établir des infractions, les services compétents peuvent disposer ainsi, grâce à ces jurisprudences, d'un cadre d'action de plus en plus affiné.

Les enjeux de la protection du secret des correspondances : (bref) bilan et perspectives

Virginie Peltier
Maître de conférences à l'université Montesquieu-Bordeaux IV
Institut des sciences criminelles et de la justice (EA 4601)

1. Feue la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications vient d'entrer dans sa troisième décennie d'existence car même si elle n'existe plus en tant que telle, ses dispositions dispersées dans le Code de procédure pénale [1] et dans le récent Code de la sécurité intérieure [2] continuent d'en faire vivre la lettre.

2. Cette loi, adoptée après les condamnations de la France par la Cour européenne des droits de l'homme dans les arrêts *Kruslin* et *Huvig* en date du 24 avril 1990 [3], organisa la procédure des interceptions judiciaires – dont le manque antérieur de clarté comme de prévisibilité avait été souligné par les juges de Strasbourg – tandis qu'elle introduisit dans le Code pénal la qualification d'atteinte au secret des correspondances émises, transmises ou reçues par la voie des télécommunications, devenues depuis communications électroniques [4].

En outre, elle coucha également sur le papier les modalités des interceptions dites de sécurité, plus connues sous le nom d'écoutes administratives puisqu'autorisées et centralisées par le Premier ministre [5].

3. Une vingtaine d'années d'application invite à se tourner vers le chemin déjà parcouru. De prime abord, le constat est réjouissant puisque la Cour européenne des droits de l'homme a eu l'occasion d'indiquer que le droit interne présentait toutes les garanties requises [6], à condition

1) Articles 100 et suivants régissant les interceptions judiciaires.
2) Articles L. 241-1 et suivants régissant les interceptions de sécurité.
3) CEDH, 24 avr. 1990, *Huvig c/France* : série A, n° 176-B ; 24 avr. 1990, *Kruslin c/France* : série A ; n° 176-A.
4) L. n° 2004-669 du 9 juillet 2004 relatives aux communications électroniques et aux services de communication audiovisuelle.
5) Respectivement, Code de la sécurité intérieure, art. L. 241-2 et art. L. 242-1, al. 2.
6) « Les dispositions de la loi du 10 juillet 1991 sur les écoutes téléphoniques répondent aux exigences de l'article 8 de la Convention et à celles des arrêts *Kruslin* et *Huvig* » : CEDH, 24 août 1998, *Lambert c/France* (§38) : n° 23618/94.

que la Cour de cassation, par sa jurisprudence, ne prive pas le requérant de la protection effective offerte par le dispositif ainsi créé [1].

Pour autant, s'est peu à peu fait jour une difficulté qui risque de prendre ampleur dans les années à venir, en raison de l'extrême diversification des nouvelles formes de communication. De fait, interceptions judiciaires comme de sécurité requièrent d'être en présence – Lapalisse n'aurait pas dit mieux – d'une correspondance. Or, comment se définit-elle ? Même si les nombreuses définitions proposées comportent toutes des éléments communs – message acheminé entre deux personnes, présence d'un fort *intuitu personae*, confidentialité des informations échangées, entre autres –, certaines communications électroniques posent problème tout comme, d'ailleurs, les données techniques qu'elles produisent. La question est loin d'être anecdotique car elle se répercute, immanquablement, sur l'interception qui les vise.

4. **Correspondances et communications électroniques.** Les possibilités de communiquer par l'Internet sont pléthores. Si le courrier électronique ne suscite plus guère, désormais, de difficultés [2], les listes de diffusion, de discussion, chat, forums et, bien entendu, autres réseaux sociaux relèvent-ils de la qualification de correspondance ? Ce n'est en effet qu'à cette condition qu'ils relèvent du régime des interceptions. La difficulté se révèle bien souvent délicate à résoudre car, en réalité, la diffusion de l'information peut s'effectuer de multiples façons, même au sein d'une forme de communication électronique unique (par exemple, sur un forum ou sur Facebook [3]) de sorte que, souvent, rien n'est véritablement clair ou tranché.

5. Si l'on prend l'exemple des listes de discussion, chaque abonné recevant et envoyant des messages par courrier électronique et ceux-ci étant au surplus envoyés en direct ou en léger différé et éventuellement un par un, une réponse favorable semblerait de prime abord s'imposer, d'autant plus que l'utilisateur peut très bien choisir de ne répondre qu'à un seul abonné, ce qui accroît le caractère *intuitu personae* du message.

---

1) Pour deux condamnations de l'État français ; CEDH, 24 août 1998, *Lambert c/France*, préc., à propos de l'absence de qualité du requérant pour se plaindre de la prolongation d'écoutes ordonnées sur la ligne d'un tiers ; 29 mars 2005, *Matheron c/France* : n° 57752/00, au sujet d'écoutes ordonnées par un magistrat au cours d'une procédure judiciaire et opposées au requérant dans une autre, la qualité de magistrat impliquant *ipso facto*, pour la chambre criminelle, la régularité des interceptions, privant ainsi de la protection de la loi toutes les personnes qui se verraient opposer le résultat d'écoutes téléphoniques réalisées dans des procédures étrangères à la leur.

2) Il s'agit bien d'une correspondance privée selon la jurisprudence : TGI Paris 2 novembre 2000 : D. 2000, IR, 286.

3) La messagerie privée que permet ce réseau peut s'assimiler à de la correspondance, s'agissant d'une forme de courrier électronique, alors que le « mur » suscite davantage de discussion dans la mesure où il constitue parfois un espace public au sein duquel les messages ne sont pas confidentiels puisque son titulaire en choisit le degré d'accessibilité (aux « amis », aux « amis des amis », etc.).

Seulement, l'existence de listes publiques empêche de conclure définitivement en faveur de correspondances car les messages envoyés sont ici consultables par tous, y compris par les non-abonnés, au moyen d'un simple moteur de recherche. Les listes de diffusion, quant à elles, dépourvues de toute interactivité, paraîtraient pourtant s'agréger à la notion, en ce qu'elles sont constituées de messages diffusés par courrier électronique à destination d'abonnés, donc de personnes qui se sont choisies. En revanche, l'impossibilité de répondre aux informations transmises – souvent par un automate – tempère nettement le caractère certain de la réponse.

6. Le forum, version plus évoluée de la liste de discussion, est avant tout un espace public[1] où les internautes échangent sur un thème précis, en direct ou en différé. Les messages sont archivés[2] : les utilisateurs lisent ceux qui sont disponibles et choisissent ou non d'y répondre. Le caractère public des communications, qui peuvent de surcroît être lues par n'importe qui, y compris par des personnes qui ne participeront même pas au forum, éloigne ces dernières de l'idée de correspondance.

7. Le chat[3], qui offre la possibilité de discuter en ligne sur l'Internet en temps réel avec une ou plusieurs personnes, soulève également des difficultés : le fait que les utilisateurs puissent dialoguer instantanément et prendre connaissance immédiatement des messages envoyés par les autres invite à rapprocher le chat du mode de fonctionnement du téléphone, mais le caractère public des échanges et l'absence d'*intuitu personae* – puisqu'on ne connaît pas à l'avance son interlocuteur – introduit un doute sérieux.

8. En conséquence, la captation des données qui seraient diffusées par ces canaux semble échapper à l'application des dispositions sur les interceptions, de quelque nature qu'elles soient, si tant est que l'on puisse véritablement adopter une position tranchée. En revanche, quelle qu'elle soit, la solution retenue doit rester identique lorsque les informations sont récupérées alors qu'elles transitent depuis ou vers un téléphone mobile[4]. En effet, le fait que le support de diffusion du message ne soit pas le même (là, un ordinateur, ici, un téléphone) ne modifie en rien la nature du message envoyé ou reçu, ne faisant peut-être qu'ajouter à la confusion ambiante. En d'autres termes, si l'on estime que la participation à un forum ne constitue pas une correspondance, elle n'en devient pas une au motif que les messages sont émis depuis un téléphone mobile.

---

1) Par l'Internet ou l'Intranet, ce qui restreint l'aspect public de la discussion.
2) Il ne s'agit pas d'une messagerie instantanée.
3) De l'anglais, *to chat*, bavarder.
4) Leur captation peut malgré tout obéir à d'autres règles comme, par exemple, celles régissant la captation des données informatiques, introduites par la LOPPSI II : Code de procédure pénale, art. 706-102-1 en cas de criminalité organisée.

9. **Données techniques de communication.** On regroupera sous cette expression l'ensemble des informations produites à l'occasion de l'émission d'une correspondance : nom de l'abonné de la ligne (fixe ou mobile) depuis laquelle est émis le message, identité et localisation de son interlocuteur, durée de la communication, entre autres exemples. La question a pris un tour renouvelé avec l'affaire dite des « fadettes » des journalistes du *Monde*, du nom des factures détaillées relatives aux appels téléphoniques[1]. Quoique les mises en examen prononcées le fussent, notamment, pour violation du secret des correspondances, il n'est guère concevable de retenir – dans la seule hypothèse d'une récupération de ces données, quelles qu'elles soient – une quelconque infraction à l'article 432-9, alinéa 2 du Code pénal pour la bonne et simple raison qu'elles ne constituent absolument pas de la correspondance. La raison en est simple : une correspondance est avant tout un message acheminé d'un point à un autre par le réseau des communications électroniques. Or, ici, même si l'on sait que X a téléphoné à Y – qui se trouvait à tel endroit –, tel jour, pendant x minutes, on reste en dépit de toutes ces informations extrêmement précises, incapables de connaître le contenu de leur conversation[2].

10. La Cour de cassation est d'ailleurs en ce sens puisqu'elle considère que l'identification des numéros de téléphone « entrants » et « sortants » d'une ligne déterminée n'est pas une interception de correspondance mais une simple mesure technique relevant de l'article 77-1[3] du Code de procédure pénale[4]. La jurisprudence administrative est, elle aussi, à l'unisson puisque la cour administrative d'appel de Paris (CAA) a jugé que le secret de la correspondance ne concerne pas la mention d'une adresse électronique sur un site Internet destiné à la consultation du public[5]. Cette solution se répercute immanquablement sur l'appréhension que l'on doit avoir de l'acte d'interception lui-même.

11. **L'interception de correspondance.** Si n'est pas de la correspondance l'ensemble des données techniques de communications, alors les opérations ayant vocation à les récupérer ne peuvent recevoir la qualification d'interception[6]. Cette solution, relativement évidente, est à cet égard confirmée par deux séries d'éléments. Tout d'abord, la jurisprudence est constante, qui conclut effectivement à l'absence d'interception

1) Mais cette affaire pose surtout la question du secret des sources des journalistes : Cass. Crim. 6 déc. 2011 : Bull. crim. n° 248.
2) Sauf à l'avoir interceptée, ce qui constitue une hypothèse distincte.
3) Alors que les dispositions de l'article 60 du Code de procédure pénale, qui ont pour objet de régir les réquisitions adressées par l'officier de police judiciaire à une personne qualifiée pour qu'elle procède à des examens techniques ou scientifiques, sont étrangères aux interceptions de communications téléphoniques : Cass. Crim. 23 mai 2006, Bull. crim. n° 141.
4) Cass. Crim. 27 juin 2001, n° 01-82578.
5) CAA de Paris, 24 janv. 2002 : D. 2003, somm., 1538.
6) Pas plus que d'enregistrement ou de transcription au sens des articles 100 et suivants du Code pénal.

lorsque des réquisitions adressées aux opérateurs sont uniquement destinées à identifier les usagers de numéros de téléphone, la localisation des relais ou les factures détaillées[1]. Ensuite, le législateur a pris la précaution d'étendre les procédures de réquisitions applicables à la collecte de ce type d'informations[2], preuve qu'il estime ne pas être en présence de correspondances, le Code des postes et des communications électroniques (CPCE) comportant en parallèle des dispositions imposant aux opérateurs de différer l'effacement ou l'anonymisation des données produites et même de les communiquer aux enquêteurs, lorsqu'il s'agit de lutter contre le terrorisme. Les informations pouvant faire l'objet de cette demande sont alors limitées aux données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, aux données relatives à la localisation des équipements terminaux utilisés ainsi qu'aux données techniques relatives aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications[3]. Il est cependant rappelé que les réquisitions 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[4], le législateur faisant là encore nettement la distinction entre données produites lors de la correspondance et correspondance.

12. Dans le même ordre d'idées, il y a lieu de rappeler qu'une interception consistant à « prendre au passage et par surprise ce qui est destiné à autrui »[5], n'en est pas une le fait de lire ou de transcrire les messages parvenus sur un terminal quelconque[6] (ordinateur ou téléphone mobile) ou de se connecter sur un réseau au moyen d'un terminal mis à la disposition du public par l'opérateur, sans en modifier les conditions d'utilisation, afin de lire, comme n'importe quel autre utilisateur les messages délivrés[7].

---

1) Cass. crim., : n° 01-82490 : « Le procédé mis en œuvre n'a pas eu pour objet l'interception des correspondances au sens des articles 100 et suivants du Code de procédure pénale » ; 24 novembre 2010 : la cour d'appel a retenu « à bon droit, que les actes mentionnés [...] n'entraient pas dans la catégorie de ceux prévus par l'article 706-95 du Code de procédure pénale ».
2) CPP, art. 60-1s pour l'enquête de flagrance, art. 77-1-1s lors de l'enquête préliminaire, art. 99-3 s lors de l'instruction.
3) CPCE, art. L. 34-1-1, al. 2.
4) CPCE, art. L. 34-1 VI.
5) *Petit Robert*, Dictionnaire alphabétique de la langue française.
6) Cass. Crim. 14 avr. 1999 : Bull. crim. n° 82, à propos de la lecture et de la transcription des informations envoyées sur un récepteur de messagerie unilatérale, mais la solution est aisément transposable aux SMS.
7) Cass. Crim. 25 octobre 2000 : Bull. crim. n° 317, au sujet d'un policier se connectant à un minitel, mais l'exemple est facilement transposable aux ordinateurs et autres terminaux.

13. En guise de conclusion, on soulignera que l'ensemble des difficultés se cristallise autour de l'absence de définition d'une notion, celle de correspondance, qui, pourtant, conditionne l'applicabilité des procédures d'interception, qu'elles soient administratives ou judiciaires.

Il eût alors peut-être été plus simple de concevoir un dispositif d'appréhension des données uniquement fondé sur le caractère réservé de celles-ci – correspondances, données informatiques, à caractère personnel ou autres – sans qu'il soit besoin de s'interroger sur la nature d'un message dont on ne peut savoir avec précision s'il relève effectivement du régime que l'on souhaite lui appliquer.

Première partie

RAPPORT D'ACTIVITÉ

Chapitre I

Organisation et fonctionnement de la Commission

Composition de la Commission

À la date de rédaction du présent rapport, la composition de la Commission est la suivante :

Membres de la Commission

• Hervé Pelletier, président de chambre honoraire à la Cour de cassation, nommé pour une durée de six ans par le Président de la République – décret du 3 octobre 2009, publié au *Journal officiel* le 4 octobre 2009.

• Membre parlementaire – Sénat : Jean-Jacques Hyest, sénateur (UMP) de la Seine-et-Marne, désigné le 6 décembre 2011 par le président du Sénat.

• Membre parlementaire – Assemblée nationale : Jean-Jacques Urvoas, député (PS) du Finistère, désigné le 23 juillet 2012 par le président de l'Assemblée nationale.

La Commission est assistée de deux magistrats de l'ordre judiciaire :

• Olivier Guérin, délégué général, depuis sa nomination en date du 8 septembre 2011.

• Loïc Abrial, chargé de mission, depuis sa nomination en date du 15 mars 2012.

Le secrétariat est assuré par Nathalie Brucker et Marie-José Masset.

Christophe Germin est l'officier de sécurité du service et conduit le véhicule de la Commission.

Rappel des compositions successives de la Commission

Présidents :

- Paul Bouchet, conseiller d'État, 1er octobre 1991
- Dieudonné Mandelkern, président de section au Conseil d'État, 1er octobre 1997
- Jean-Louis Dewost, président de section au Conseil d'État, 1er octobre 2003
- Hervé Pelletier, président de chambre à la Cour de cassation, 3 octobre 2009

Représentants de l'Assemblée nationale :

- François Massot, député des Alpes-de-Haute-Provence, 19 juillet 1991
- Bernard Derosier, député du Nord, 24 mai 1993
- Jean-Michel Boucheron, député d'Ille-et-Vilaine, 3 juillet 1997
- Henri Cuq, député des Yvelines, 4 juillet 2002
- Bernard Derosier, député du Nord, 20 mars 2003
- Daniel Vaillant, député de Paris, 1er août 2007
- Jean-Jacques Urvoas, député du Finistère, 23 juillet 2012

Représentants du Sénat :

- Marcel Rudloff, sénateur du Bas-Rhin, 17 juillet 1991
- Jacques Thyraud, sénateur du Loir-et-Cher, 26 mars 1992
- Jacques Golliet, sénateur de Haute-Savoie, 22 octobre 1992
- Jean-Paul Amoudry, sénateur de Haute-Savoie, 14 octobre 1995
- Pierre Fauchon, sénateur du Loir-et-Cher, 18 septembre 1998
- André Dulait, sénateur des Deux-Sèvres, 6 novembre 2001
- Jacques Baudot, sénateur de Meurthe-et-Moselle, 26 octobre 2004
- Hubert Haenel, sénateur du Haut-Rhin, 4 juillet 2007, en remplacement du sénateur Jacques Baudot décédé, puis le 15 octobre 2008 en qualité de membre parlementaire de la Commission, à titre personnel
- Jean-Jacques Hyest nommé le 2 juin 2010 en remplacement du sénateur Hubert Haenel, nommé membre du Conseil constitutionnel, puis le 6 décembre 2011, à titre personnel

Missions et fonctionnement

La Commission est chargée de veiller au respect des dispositions du titre IV du Livre II du Code de la sécurité intérieure consacré aux « interceptions de sécurité ». En effet l'ordonnance n° 2012-351 du 12 mars 2012 a abrogé la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques depuis le 1er mai 2012, et rassemblé l'essentiel de ses dispositions à droit constant au sein du nouveau Code de la sécurité intérieure. Ce point fait l'objet de développements dans le chapitre 2 de la présente partie.

Conformément à l'article 1er de son règlement intérieur, « la Commission se réunit à intervalles réguliers à l'initiative de son président ; elle peut également être réunie à la demande d'un de ses membres ».

Entre ces assemblées plénières, le président dispose d'une habilitation permanente à l'effet de formuler les avis, les recommandations et les préconisations, dès lors que les demandes présentées, d'interception ou de recueil de données techniques de communications, ne posent pas de questions nouvelles par rapport aux délibérations et aux décisions précédentes de la Commission dans sa formation plénière.

Elle peut à tout moment adresser au Premier ministre une recommandation tendant à ce qu'une interception soit interrompue. Elle peut également faire une recommandation d'avertissement pour alerter le Premier ministre sur des difficultés, qui en perdurant ou en se développant, pourraient fonder un avis d'interruption de la part de la Commission ou de non-renouvellement de la mesure. Des préconisations sont également adressées aux services titulaires de l'autorisation et en charge de l'exploitation du renseignement, avant la procédure de recommandation.

En application de l'article L. 243-9 du Code de la sécurité intérieure (ancien article 15 de la loi de 1991), la Commission reçoit les réclamations des particuliers, procède aux contrôles et aux enquêtes qui lui paraissent nécessaires à l'accomplissement de sa mission. À la demande des particuliers, la Commission effectue les vérifications dans le cadre du contrôle des interceptions de sécurité ordonnées par le Premier ministre pour les motifs prévues par la loi et réalisées par les services habilités. Les investigations de la Commission portent exclusivement sur l'existence ou non d'interceptions illégales qui auraient été conduites par des services de l'État habilités, et ce en violation des dispositions issues de la loi du 10 juillet 1991 relative au secret des correspondances et de la vie privée.

La Commission ne procède à aucune investigation sur les interceptions ordonnées par l'autorité judiciaire qui relèvent du seul contrôle de cette même autorité, en application des dispositions du Code de procédure pénale. De même, les interceptions qui seraient faites par des particuliers sont de la compétence exclusive des services judiciaires territorialement compétents pour recevoir ces plaintes. En conséquence,

les requêtes des particuliers qui portent sur ces interceptions présumées ou réelles sont déclarées irrecevables pour incompétence par la CNCIS.

La Commission contrôle les conditions d'exécution des mesures autorisées par le Premier ministre. À ce titre, elle se rend auprès des services et des directions titulaires des autorisations et en charge de l'exécution des mesures de renseignement portant sur les communications électroniques. Conformément à l'article L. 243-10 du Code de la sécurité intérieure (ancien article 16 de la loi de 1991), les ministres, autorités publiques et agents publics doivent prendre toutes mesures de nature à faciliter son action.

La Commission est en outre chargée, en application de l'article 6 de la loi n° 2006-64 du 23 janvier 2006 relative à la loi contre le terrorisme, du contrôle des demandes de communication des données prévues par l'article L. 34-1-1 du Code des postes et des communications électroniques. Ce sont les demandes formées, pour la prévention des actes de terrorisme, par les services habilités du ministère de l'Intérieur.

Les autres demandes relatives au recueil des données techniques de communications portant sur tous les autres motifs légaux (criminalité organisée, sécurité nationale, protection du patrimoine scientifique et économique...) sont mises en œuvre par les services habilités des ministères de l'Intérieur, de la Défense et des Finances. Elles relèvent de l'article L. 244-2 du Code de la sécurité intérieure (ancien article 22 de la loi du 10 juillet 1991). Elles sont soumises, dans les mêmes conditions que l'article 6 de la loi du 23 janvier 2006, au contrôle de l'autorité administrative indépendante.

La CNCIS est membre de la Commission consultative créée par le décret n° 97-757 du 10 juillet 1997 qui, sous la présidence du directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), émet des avis sur les demandes de commercialisation, d'importation, d'acquisition, de détention ou d'emploi des matériels susceptibles de porter atteinte au secret des correspondances.

En application de l'article L. 243-7 du Code de la sécurité intérieure, le président remet au Premier ministre, avant publication, un rapport annuel sur les conditions d'exercices et les résultats de l'activité de la Commission. Les présidents des deux assemblées en sont également destinataires.

Financement

Autorité administrative indépendante, la CNCIS dispose de crédits individualisés figurant au budget des services du Premier ministre. Le président est ordonnateur des dépenses (article L. 243-6 du Code de la sécurité intérieure).

Pour l'année 2011 et conformément à la déclinaison en programmes, actions et sous-actions de la loi organique relative aux lois de finances (LOLF), le budget de la CNCIS a été inscrit au sein du programme 308 « Protection des droits et libertés ».

Afin de respecter l'indépendance budgétaire de notre autorité, celle-ci a été dotée d'un budget opérationnel de programme (BOP), référencé 308AIC. Les crédits alloués en 2011 se sont élevés à 619 897 euros dont 523 619 euros pour les dépenses du titre II (dépenses de personnel) et à 96 278 euros pour les dépenses de fonctionnement.

Les crédits du BOP CNCIS sont destinés en priorité à permettre le fonctionnement continu de cette autorité administrative indépendante en toute sécurité. La structure permanente de la Commission comprend à cet effet, outre le président, deux magistrats et deux secrétaires fonctionnant en binômes. La Commission doit pouvoir être jointe et s'entretenir avec ses interlocuteurs de façon sécurisée. Ses locaux sont équipés pour répondre aux normes relatives au traitement des documents classifiés au niveau « secret-défense ». La Commission doit disposer des moyens d'information les plus larges comme les plus spécialisés en source ouverte. Elle doit également disposer de moyens de transport dédiés et sécurisés, notamment pour le transfert des documents classifiés et pour effectuer les visites de contrôle prévues par la loi.

La CNCIS participe aux travaux menés par les services du Premier ministre sur la mesure de la performance en matière de gestion budgétaire. Elle poursuit donc, depuis 2009, des actions de rationalisation financière. Ainsi de nouveaux indicateurs de performance ont été élaborés pour couvrir l'intégralité de ses activités, tant celles portant sur l'expertise fournie pour la prise de décision des autorités publiques, que celles destinées à garantir la protection des droits et libertés des citoyens, attribuées par le législateur à l'autorité administrative indépendante.

Dans le même souci de rationalisation des moyens, d'efficacité et de lisibilité des modalités de son fonctionnement, la Commission a choisi de s'inscrire dans le dispositif d'audit interne des services du Premier ministre prévu par le décret n° 2011-775 du 28 juin 2011 relatif à l'audit interne dans l'administration et mis en place progressivement depuis le début de l'année 2012.

Relations extérieures

Dans le prolongement des travaux avec les autorités bulgares et allemandes, déjà évoqués dans les précédents rapports d'activité, la Commission a poursuivi ses échanges avec les institutions et les structures de pays étrangers dont les compétences rejoignent en partie ou en totalité les attributions de la CNCIS.

Ainsi les agents de la Commission ont participé en 2011 aux conférences annuelles du Comité permanent de contrôle des services de renseignement et de sécurité en Belgique.

Une délégation parlementaire roumaine de la Commission commune permanente de la chambre des députés et du Sénat pour le contrôle parlementaire de l'activité du service roumain des renseignements a été reçue par la CNCIS en juin 2011. À la demande des parlementaires roumains, les travaux ont porté essentiellement sur le cadre légal des interceptions, le traitement judiciaire du renseignement technique, ainsi que sur le régime juridique des données de trafic des communications électroniques, leurs conditions d'accès et les modalités du contrôle de ce recueil.

Une délégation libanaise conduite par le président du Conseil d'État, Monsieur Choucri SADER, a été reçue par la CNCIS en août 2012 pour traiter des évolutions législatives et réglementaires en France en matière de communications électroniques. Le thème principal de ces rencontres a porté sur la réglementation en matière de données techniques de communications, les conditions juridiques de leur recueil et de leur exploitation par les services de renseignement, ainsi que sur les modalités du contrôle de l'autorité administrative indépendante.

Il ressort de ces échanges internationaux que le sujet principal de réflexion et les projets législatifs des délégations étrangères rencontrées par la Commission depuis près de trois ans, portent sur les données techniques de communications ou le contenant de la correspondance électronique, avec la question de leur accès (général ou individualisé, aléatoire ou ciblé) ainsi que la détermination des atteintes pouvant fonder leur recueil et les modalités du contrôle de ces mesures d'investigation.

Les agents de la Commission ont aussi poursuivi les actions de formation et les études conduites avec plusieurs organismes d'enseignement et de recherche, telles que la participation à un groupe de travail sur les pratiques des services de renseignement et les libertés publiques au sein des instituts d'études politiques, les interventions dans le cadre de la formation des magistrats de l'ordre judiciaire sur le traitement judiciaire du renseignement, ou les conférences auprès d'organismes comme l'Institut des hautes études de défense nationale (IHEDN).

Chapitre II

Actualités de la Commission au cours de l'année 2011-2012

L'assemblée plénière de la Commission nationale de contrôle des interceptions de sécurité a souhaité formuler des observations à trois reprises au cours de l'année 2011-2012, sur des questions législative, judiciaire ou médiatique, portant sur ses attributions et son activité.

Dans le cadre des prérogatives dévolues par la loi en sa qualité d'autorité administrative indépendante et dans le respect des dispositions en matière d'informations classifiées et protégées, elle a tenu à développer sa position sur l'abrogation de la loi du 10 juillet 1991 et sur le champ d'application de l'article 20 de cette loi. Mis en cause par des sources anonymes par voie de presse, sur des décisions que la Commission aurait prises dans le cadre de la surveillance de Mohamed Merah, les membres de la CNCIS ont rappelé avec fermeté les principes et les règles gouvernant la matière des interceptions de sécurité.

L'abrogation de la loi du 10 juillet 1991

L'ordonnance n° 2012-351 du 12 mars 2012, relative à la partie législative du Code de la sécurité intérieure, a abrogé la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques à la date du 1er mai 2012. Ce texte rassemble l'essentiel de ses dispositions, à droit constant, au sein du nouveau Code de la sécurité intérieure.

La CNCIS a appris l'abrogation de la loi du 10 juillet 1991, qui portait création de l'autorité administrative indépendante, lors de la parution de

cette ordonnance au *Journal officiel*, le 13 mars 2012. À aucun moment au cours des travaux d'élaboration de ce texte, elle n'a été sollicitée afin de fournir un avis sur cette perspective de codification.

La Commission nourrit dès lors quatre regrets :

Tout d'abord, l'article 13 de la loi du 10 juillet 1991 (devenu l'article L. 243-1 du Code de la sécurité intérieure), a toujours fondé la saisine de la CNCIS sur tout projet législatif ou réglementaire la concernant ou portant sur les sujets relevant de sa compétence. Bien que le texte soit général et ne contienne pas de dispositions impératives, il a toujours été observé que, par cet article, le législateur a chargé la Commission de veiller au respect des dispositions portant sur les interceptions de sécurité ou le recueil de données techniques de communications. À ce titre, tout projet normatif portant sur son domaine de compétence devait être soumis à son examen.

Au cours des précédentes modifications de la loi du 10 juillet 1991 ou dans le cadre de l'élaboration de textes nouveaux comme la loi du 23 janvier 2006, la Commission a été en mesure de fournir un avis destiné à éclairer le travail d'élaboration de la norme, à tous les stades de la procédure législative ou réglementaire, en qualité d'autorité administrative chargée du contrôle de la mise en œuvre des interceptions et du recueil de données en matière de communications électroniques.

S'agissant de dispositions portant sur la protection des libertés publiques, il résulte des travaux parlementaires ayant conduit à l'adoption, tant de la loi n° 91-646 du 10 juillet 1991 que de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme, que la consécration législative du secret des correspondances électroniques privées, ainsi que les exceptions à ce principe, doivent être prévues par une loi spéciale, comme pour toute liberté publique. Or ces dispositions se retrouvent désormais fondues dans un vaste ensemble normatif couvrant des domaines multiples et variés. Ainsi, le Livre II intitulé « Ordre et sécurité publics », comprend, outre le titre IV relatif aux interceptions de sécurité, sept autres titres portant notamment sur « la sécurité dans les transports collectifs » ou « le gardiennage et la surveillance des immeubles », questions importantes, mais très éloignées de la protection du secret des correspondances.

La loi du 10 juillet 1991 constituait le texte de base en matière d'interceptions administratives et judiciaires, et ce après la condamnation de la France par la Cour européenne des droits de l'homme, en l'absence de textes spécifiques portant sur ces mesures d'investigation. Cette loi générale a permis l'adoption de règles et de principes communs pour des interceptions d'origine différente mais portant atteinte dans les mêmes conditions et pour des motifs légaux similaires, au secret des correspondances privées par voie électronique. Ces mesures sont désormais susceptibles de connaître des régimes distincts alors que la problématique commune est celle de l'équilibre entre, d'une part la protection

des correspondances et de la vie privées, et, d'autre part la préservation des intérêts fondamentaux et de la sécurité nationale.

Ainsi, il ressort du texte récemment discuté au Parlement que le titre relatif aux dispositions communes à ces deux types d'interceptions est intégré à droit constant uniquement dans le Code de la sécurité intérieure. Les articles de la loi du 10 juillet 1991, et notamment ceux portant sur la surveillance et le contrôle des transmissions empruntant la voie hertzienne, effectuées par les pouvoirs publics aux seules fins de défense des intérêts nationaux, ainsi que ceux relatifs aux mesures nécessaires à la préparation et à l'exécution des interceptions, ne sont pas intégrés dans le Code de procédure pénale.

Enfin, ce travail de codification n'est pas de nature à répondre aux préoccupations déjà formulées par la Commission quant aux modifications législatives qui lui paraissent nécessaires au regard non seulement des évolutions technologiques, opérationnelles et juridiques, en matière de communications électroniques, mais également des requêtes que lui font parvenir les services de l'État ou les particuliers.

Au vu de ce constat, la Commission, à défaut d'avoir été consultée lors des travaux d'élaboration de cette ordonnance, a souhaité que le passage de ce texte devant les deux assemblées parlementaires soit l'occasion d'un réexamen de cette démarche de codification pour la partie concernant les interceptions de sécurité. La CNCIS a adressé dès le 2 avril 2012 une recommandation en ce sens au Premier ministre.

Un projet de loi visant à ratifier cette ordonnance a été déposé au Sénat le 9 mai 2012. Mais cette ratification a été examinée par le Parlement dans le cadre du projet de loi sur la sécurité et la lutte contre le terrorisme. Le Sénat n'a pas adopté l'article portant sur la ratification de cette ordonnance, mais l'Assemblée nationale a retenu une autre position, relevant qu'il s'agissait d'une codification à droit constant. Il est vraisemblable que le Code de la sécurité intérieure va ainsi, à l'issue du processus parlementaire, acquérir pleine valeur législative.

Prenant acte de ce vote, la Commission forme le vœu que le débat soit désormais ouvert sur une réforme de la loi n° 91-546 du 10 juillet 1991, au regard des évolutions technologiques en matière de communications électroniques et des nouvelles formes de menaces qui emportent des conséquences importantes dans l'équilibre entre, d'une part les enjeux de protection du secret des correspondances et de la vie privées, et, d'autre part les exigences de sécurité. La question de la pertinence du cadre légal des mesures de surveillance et d'investigation par voie électronique, mises en œuvre par les services habilités, est aussi posée.

La réponse à une demande de déclassification formulée par les magistrats instructeurs en matière de recueil de données techniques de communications

Dans la continuité des questions évoquées dans le rapport public de l'an dernier et du rappel effectué par la CNCIS sur le périmètre de son contrôle en matière de recueil de données techniques de communication par les services de l'État, la Commission a été saisie d'une demande de déclassification par la justice.

Par requête du 24 janvier 2012, dans le cadre de l'information ouverte à leur cabinet des chefs « d'atteinte au secret des correspondances par personne dépositaire de l'autorité publique, de collecte de données à caractère personnel par des moyens frauduleux, déloyaux ou illicites, de violations du secret professionnel et recel de ces délits », les magistrats chargés de l'instruction au tribunal de grande instance de Paris, ont sollicité la déclassification de plusieurs documents émis et classifiés par la CNCIS.

Conformément à la procédure prévue par les articles L. 2312-1 et suivants du Code de la défense, la CNCIS a saisi la Commission consultative du secret de la défense nationale (CCSDN) le 28 février 2012.

Cette autorité administrative indépendante a rendu un avis favorable à la déclassification le 15 mars 2012 (publié au *Journal officiel* du 30 mars 2012 et reproduit ci-dessous).

JORF n° 0077 du 30 mars 2012

Texte n° 108

AVIS

Avis n° 2012-05 du 15 mars 2012

NOR : CSDX1209147V

Vu le Code de la défense et ses articles L. 2312-1 à 8 ;

Vu la lettre de saisine de M. Hervé Pelletier, président de la Commission nationale de contrôle des interceptions de sécurité (CNCIS), en date du 28 février 2012, relative à la requête en déclassification en date du 24 janvier 2012 de Mme Sylvie Zimmermann et M. Alain Nguyen The, vice-présidents chargés de l'instruction au tribunal de grande instance de Paris dans le cadre de l'information ouverte à leur cabinet des chefs « d'atteinte au secret des correspondances par personne dépositaire de l'autorité publique, de collecte de données à caractère personnel par des moyens frauduleux, déloyaux ou illicites, de violations du secret professionnel et recel de ces délits ».

La Commission consultative du secret de la défense nationale, régulièrement convoquée et constituée, en ayant délibéré ;

Émet un avis favorable à la déclassification des documents soumis à son examen, soit :
– note du délégué général de la CNCIS en date du 4 février 1999 ;
– compte-rendu de réunion de la CNCIS en date du 26 janvier 2004 ;
– note du délégué général de la CNCIS en date du 3 mars 2005 ;
– extrait de l'avis de la CNCIS en date du 10 janvier 2006 ;
– note rédigée par le chargé de mission de la CNCIS en date du 3 septembre 2009 ;
– courrier du président de la CNCIS JLD/MJM/116.09 en date du 4 septembre 2009 ;
– note interne à la CNCIS en date du 18 janvier 2010 ;
– point 2 du procès-verbal de l'assemblée plénière de la CNCIS en date du 21 janvier 2010 ;
– courrier du président de la CNCIS – HP/NB/19.10 en date du 26 janvier 2010.

À l'exception, le cas échéant, des mentions à caractère technique ou interne dont la protection paraîtrait nécessaire à la Commission nationale de contrôle des interceptions de sécurité.

Fait à Paris, le 15 mars 2012.

Pour la Commission consultative

du secret de la défense nationale :

La présidente,

E. Ratte

Par décision du 29 mars 2012, l'assemblée plénière de la CNCIS a procédé à la déclassification de la totalité des documents sollicités par les magistrats instructeurs. Elle a fait connaître sa décision par un communiqué de presse diffusé le 3 avril 2012.

Cette communication est l'occasion pour la Commission de réaffirmer sa position quant à l'étendue de son contrôle en matière de données techniques de communications.

• L'utilisation de l'article L. 241-3 du Code de la sécurité intérieure se situe hors du champ de contrôle de la Commission

En effet, la CNCIS n'a pas de compétence pour contrôler les mesures de recueil de données prises par les services de l'État en application de l'article L. 241-3 du Code de la sécurité intérieure (ancien article 20 de la loi du 10 juillet 1991).

Article L. 241-3 du Code de la sécurité intérieure

Les mesures prises par les pouvoirs publics pour assurer, aux seules fins de défense des intérêts nationaux, la surveillance et le contrôle des transmissions empruntant la voie hertzienne ne sont pas soumises aux dispositions du présent titre, ni à celles de la sous-section 2 de la section 3 du chapitre Ier du titre III du Livre Ier du Code de procédure pénale.

Comme le relevait déjà la Commission dans son tout premier rapport d'activité (1991-1992) : « Cet article a pour objet d'exclure du champ d'application de la loi les mesures générales de surveillance et de contrôle des transmissions empruntant la voie hertzienne, effectuées par les pouvoirs publics aux seules fins de défense des intérêts nationaux.

Il a été soutenu que le gouvernement aurait pu considérer, sans qu'il soit nécessaire de la préciser, que ces opérations étaient par leur nature même, exclues du champ d'application de la loi comme constituant l'exercice de la mission générale de police des ondes qui lui incombe. Cependant, il lui est apparu souhaitable dans un souci de transparence que la loi rappelle expressément l'existence de cette mission de surveillance tout en l'excluant du champ d'application des dispositions relatives à l'autorisation et au contrôle des interceptions de sécurité.

Ces dispositions n'ont fait l'objet d'aucun débat particulier devant le parlement. »

L'absence de débats sur cet article, alors que les travaux parlementaires ont par ailleurs donné lieu à d'âpres discussions, témoigne de la clarté de ces dispositions, qui sont parfaitement distinctes des interceptions de sécurité et des procédures de recueil de données techniques de communications entrant dans le champ du contrôle de la CNCIS.

L'article L. 241-3 est relatif aux mesures générales de surveillance des ondes incombant au gouvernement pour la seule défense des intérêts nationaux et ne peut servir de base à la mise en œuvre d'interceptions de communications individualisables et portant sur une menace identifiée.

Pareille utilisation reviendrait en effet à contourner les dispositions encadrant les interceptions de sécurité de l'article L. 241-2 du Code de la sécurité intérieure (article 3 de la loi du 10 juillet 1991) et celles réglementant le recueil de données techniques préalables à la réalisation ou relatives à l'exploitation desdites interceptions (article 6 de la loi du 23 janvier 2006 et article L. 244-2 du Code de la sécurité intérieure).

Cet article L. 241-3 permet des mesures de surveillance hors de tout contrôle de la CNCIS, uniquement sous réserve de trois conditions cumulatives :
• l'objectif poursuivi doit être uniquement la « *défense des intérêts nationaux* » ;
• il s'agit de « *mesures prises pour surveiller et contrôler* » des transmissions, de manière aléatoire et non individualisée ;
• celles-ci doivent utiliser « *la voie hertzienne* » ;

□ **La défense des intérêts nationaux**

La Commission rappelle que la notion « *d'intérêts nationaux* » ne doit pas être confondue avec celle de « *sécurité nationale* » employée dans l'article L. 241-2 du Code de la sécurité intérieure (ancien article 3 de la loi du 10 juillet 1991) qui figure parmi les intérêts fondamentaux de la Nation (article 410-1 du Code pénal).

Il appert que cette notion « d'intérêts nationaux » est très large et générique, incluant l'ensemble des « intérêts » de la communauté nationale, quel que soit le domaine considéré, mais que seuls certains de ces « intérêts nationaux », en ce qu'ils sont considérés comme « fondamentaux », bénéficient, à ce titre, de la protection du Code pénal.

□ **Des mesures prises pour assurer la surveillance et le contrôle des transmissions**

Les « *mesures prises par les pouvoirs publics pour assurer le contrôle et la surveillance* » se distinguent, en droit :
– d'une part, des « *interceptions de sécurité* » au sens du titre IV du Livre II du Code de la sécurité intérieure ;
– d'autre part, des « *communications de données techniques* », au sens des articles L. 34-1-1 du Code des postes et des communications électroniques, créé par l'article 6 de la loi n° 2006-64 du 23 janvier 2006, et L. 244-2 du Code de la sécurité intérieure.

La mission de « *surveillance et de contrôle* » qui justifie ici ces « *mesures »,* dont la nature n'est pas précisée par le législateur, est une notion plus large que les deux précédentes. Surtout, ces « *mesures* » se distinguent de toute recherche « ciblée » de renseignement ou de toute situation de menace avérée et identifiée d'atteinte aux intérêts nationaux. Ces « *mesures* » générales et aléatoires, peuvent le cas échéant révéler une menace potentielle, que des « *communications de données techniques* » ou des « *interceptions de sécurité* » permettront, dans le respect du cadre légal dédié, et donc sous le contrôle de la CNCIS, de préciser.

L'exception ainsi apportée à l'article L. 241-3 du Code de la sécurité intérieure (ancien article 20 de la loi du 10 juillet 1991) par le législateur au dispositif soumis par la loi au contrôle de la CNCIS ne peut s'expliquer que s'il s'agit de mesures par nature non-intrusives non ciblées, prises en « amont » de celles justifiant la mise en œuvre des procédures

relatives aux interceptions de sécurité et au recueil de données techniques préalables à l'interception (article L. 244-2 du Code de la sécurité intérieure et article L. 34-1-1 du Code des postes et des communications électroniques).

□ **Les transmissions empruntant la voie hertzienne**

Les communications électroniques sont définies à l'article L. 32 du Code des postes et des communications électroniques : « On entend par communications électroniques les émissions, transmissions ou réceptions de signes, de signaux, d'écrits, d'images ou de sons, par voie électromagnétique. »

Les « transmissions » sont ainsi, juridiquement, une phase particulière d'une « communication » (entre l'émission et la réception).

La voie hertzienne, quant à elle, est un des modes d'acheminement des ondes électromagnétiques. Elle n'échappe donc pas par nature au contrôle de la CNCIS, sauf dans le cas très restrictif prévu à l'article L. 241-3 aux seules fins de défense des intérêts nationaux.

En effet, selon la directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques (directive cadre), on entend par « réseau de communications électroniques » : « Les systèmes de transmission et, le cas échéant, les équipements de commutation ou de routage et les autres ressources qui permettent l'acheminement de signaux par câble, par voie hertzienne, par moyen optique ou par d'autres moyens électromagnétiques, comprenant les réseaux satellitaires, les réseaux terrestres fixes (avec commutation de circuits ou de paquets, y compris l'Internet) et mobiles, les systèmes utilisant le réseau électrique, pour autant qu'ils servent à la transmission de signaux, les réseaux utilisés pour la radiodiffusion sonore et télévisuelle et les réseaux câblés de télévision, quel que soit le type d'information transmise ».

Au sujet de ce dispositif et au regard de la problématique particulière de l'interception des communications à partir des téléphones portables qui passent par la voie hertzienne, la Commission, dès 1998 (rapport 1998 p. 36), indiquait que l'évolution technologique ne pouvait occulter le but poursuivi par le législateur en 1991, c'est-à-dire la protection du secret de la correspondance en son principe, sans en résumer le support à « l'existant technologique » ou à sa possible évolution.

Dans son rapport d'activité, la Commission rappelait ainsi la primauté du principe de liberté publique sur l'évolution technique en indiquant que l'exception à son contrôle prévue par l'article 20 (désormais L. 241-3) devait s'interpréter strictement : «Toute interception de correspondance échangée par la voie des télécommunications, qui n'entre pas dans le champ de l'article 20, est soumise quel que soit le mode de transmission filaire ou hertzien aux conditions et aux procédures fixées par la loi du 10 juillet 1991 ».

Cette règle a été rappelée dans les avis rendus par la Commission, notamment pour définir les modalités des demandes et du contrôle en matière de recueil des données techniques des communications.

Les démentis apportés aux mises en cause par voie de presse de l'action de la Commission dans le cadre de l'affaire dite « Mohamed Merah »

Dans le cadre de l'affaire dite « Mohamed Merah », consécutive aux faits de nature criminelle commis à Montauban et Toulouse entre le 11 et le 19 mars 2012, des mises en cause anonymes dans les médias ont visé la CNCIS. Certaines sources « proches de l'enquête » auraient assuré que la CNCIS avait refusé des mesures d'interceptions visant des proches de Mohamed Merah.

- **Communiqué de presse du 27 mars 2012**

Dans les limites des règles relatives à la protection du secret de la défense nationale, auxquelles, tout comme les services de renseignement, la CNCIS est soumise, son assemblée plénière, a, par communiqué de presse du 27 mars 2012, apporté un démenti formel aux affirmations alléguées.

Elle a rappelé qu'en vertu des dispositions de la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques (désormais titre IV du Livre II du Code de la sécurité intérieure), elle est chargée de donner un avis au Premier ministre sur chaque demande d'interception de sécurité présentée par les services de renseignement. La décision d'autoriser ou non la mise en place d'une interception appartient au Premier ministre, et non à l'autorité administrative indépendante.

Par ailleurs, la CNCIS a indiqué, s'agissant des demandes relatives à la communication de données techniques de communications, présentées par les services de renseignements au titre de la prévention du terrorisme (dispositif de l'article 6 de la loi du 23 janvier 2006 précité) et qui ne sont pas couvertes par le secret-défense, que les demandes des services ont été validées par la personnalité qualifiée et n'ont pas fait l'objet d'observations de la part de la Commission dans son contrôle *a posteriori*.

- **Communiqué de presse du 29 mars 2012**

À la suite de nouvelles allégations parues dans la presse nationale le 28 mars 2012, aux termes desquelles la CNCIS aurait « interrompu » des interceptions téléphoniques visant Mohamed Merah, l'assemblée

plénière de la CNCIS a réaffirmé, dans un communiqué de presse du 29 mars 2012, le démenti formel apporté deux jours auparavant.

La CNCIS, soucieuse du strict respect des règles relatives à la protection du secret de la défense nationale, a tenu à indiquer qu'elle serait à-même de fournir aux autorités habilitées, dans le respect des procédures prévues par la loi, tout élément utile.

Chapitre III

Le contrôle des interceptions de sécurité (Titre IV du Livre II du Code de la sécurité intérieure)

Le contrôle des autorisations

Il convient ici de décrire la nature et la portée du contrôle pratiqué par la Commission sur les demandes d'interception dont elle est saisie.

Ce contrôle intervient en amont de l'autorisation d'interception, sous la forme d'un avis qui est donné au moment de la présentation et de la transmission au Groupement interministériel de contrôle (GIC) des demandes des services habilités validées par le ministre de tutelle. Il porte tant sur la forme que sur le fond de la requête. La décision d'autorisation relève du pouvoir exclusif du Premier ministre ou de ses délégués (article L. 242-1 du Code de la sécurité intérieure).

Le contrôle de la Commission s'exerce aussi en aval de cette décision, durant toute l'exploitation de l'interception. Il peut fonder l'adoption de recommandations d'avertissement ou d'interruption.

Le contrôle en amont

La mission première de la CNCIS est la vérification de la légalité des autorisations d'interceptions. Elle se traduit par un contrôle systématique et exhaustif de l'ensemble des demandes tant au stade initial qu'à celui de l'éventuel renouvellement de l'interception.

La loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques avait prévu un contrôle *a posteriori*. Toutefois, dès les premiers mois de son fonctionnement, la Commission a instauré, avec l'accord du Premier ministre, la pratique du contrôle préalable à la décision d'autorisation, allant ainsi au-delà de la lettre de l'article L. 243-8 du Code de la sécurité intérieure (ancien article 14 de la loi du 10 juillet 1991).

Ce contrôle *a priori* renforce les modalités de la protection de la correspondance privée. Il constitue une garantie importante en ce que l'avis de la Commission portant sur la légalité et sur la protection du secret des correspondances intervient avant la décision et la mise en œuvre de la mesure d'interception.

Depuis l'instauration de cette procédure d'avis *a priori*, les avis défavorables ont été dans leur grande majorité suivis par l'autorité de décision. En ce sens, cette pratique est plus efficace du point de vue de la protection des libertés publiques que la recommandation prévue par la loi et adressée après la notification de la mise en place d'une interception. Dans ce dernier cas, l'atteinte au secret des correspondances, disproportionnée ou inadaptée, est effective, même si elle est de courte durée et que l'interception est stoppée rapidement après sa mise en œuvre et sa notification à la Commission.

En outre, cette pratique permet un dialogue utile avec les services demandeurs et une meilleure prise en compte par ceux-ci, dès le stade préparatoire, des préconisations de la Commission pour garantir le respect de la loi et l'équilibre entre la défense des intérêts fondamentaux de la Nation et la protection du secret des correspondances. Ce dialogue est enrichi et facilité par le travail de centralisation et d'intermédiation effectué par le GIC.

Cette pratique de l'avis *a priori* a été étendue, par décision de la Commission du 25 mars 2003, aux interceptions demandées en urgence absolue. Elle a été confirmée le 18 février 2008 par une directive du Premier ministre, qui a qualifié ce contrôle *a priori* de « pratique la mieux à même de répondre à l'objectif de protection efficace des libertés poursuivi par le législateur ».

Du fait de cet avis *a priori*, que la demande intervienne selon la procédure « normale » ou en « urgence absolue », les dispositions de l'article L. 243-8 alinéas 1 à 3 du Code de la sécurité intérieure n'ont logiquement plus trouvé à s'appliquer au stade de l'autorisation de l'interception de sécurité.

Elles prévoient en effet que : « La décision motivée du Premier ministre mentionnée à l'article L. 242-1 est communiquée dans un délai de 48 heures au plus tard au président de la Commission nationale de contrôle des interceptions de sécurité.

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 adresse au Premier ministre une recommandation tendant à ce que cette interception soit interrompue ».

La procédure de l'article L. 243-8 conserve néanmoins sa pleine effectivité en ce qui concerne les interceptions déjà en cours et dont la Commission recommande au Premier ministre de décider de les interrompre, ou préconise directement aux services cette interruption.

La Commission sollicite que cette pratique adoptée et reconnue par tous comme une meilleure garantie en termes de droits pour les personnes et d'efficacité soit explicitement prévue par la loi, et ce par ajout d'un alinéa à l'article L. 243-8.

Le contrôle formel des demandes d'interception et le respect des contingents

L'activité de contrôle de chacun des projets d'interception comporte en premier lieu un aspect formel, qui consiste à vérifier que les signataires des demandes d'autorisation ont bien été habilités par les ministres compétents. Devant l'augmentation des demandes urgentes et afin de diminuer les délais de traitement, sur proposition de la Commission, la loi n° 2006-64 du 23 janvier 2006 a introduit à l'article 4 de la loi du 10 juillet 1991 (désormais l'article L. 241-2 du Code de la sécurité intérieure) une disposition autorisant chaque ministre, à l'instar du Premier ministre, à déléguer de façon permanente sa signature à deux personnes.

Les contingents d'interceptions simultanées ne doivent pas être confondus avec le nombre total d'interceptions (demandes initiales et renouvellements) réalisées annuellement au profit des trois ministères concernés : Intérieur, Défense et Budget. Dans son souci de conserver un caractère exceptionnel aux interceptions de sécurité, le législateur de 1991 a en effet opté pour une limitation sous forme d'un encours maximum, protecteur des libertés publiques (article L. 242-2 du Code de la sécurité intérieure).

Ce système, mis en place par la décision du 28 mars 1960 du Premier ministre Michel Debré, résultait à l'époque de contraintes techniques (capacité maximale d'enregistrement sur des magnétophones à bandes ou à cassettes et capacité d'exploitation par le GIC). Il a été confirmé en 1991 dans le but d'« inciter les services concernés à supprimer le plus rapidement possible les interceptions devenues inutiles, avant de pouvoir procéder à de nouvelles écoutes » (CNCIS, 3e rapport – 1994, p. 16).

Le contingentement des interceptions de sécurité implique que leur nombre doive à tout moment respecter un plafond fixé par ministère en vertu d'une décision du Premier ministre. La répartition interne entre services est du ressort de chaque ministère et conduit à ce que le nombre des interceptions à un instant donné soit toujours inférieur au contingent. Les services doivent en effet se réserver la possibilité de répondre en permanence à des circonstances inattendues ou à des besoins nouveaux.

L'augmentation constante du parc de vecteurs de communications électroniques (téléphone fixe, mobile, fax, Internet) a conduit à des relèvements progressifs du contingent (50 % depuis l'origine), qu'il faut rapprocher de l'augmentation exponentielle du nombre d'utilisateurs des outils de communication. À titre d'illustration, le nombre de lignes mobiles est ainsi passé de 280 000 en 1994 à 63,1 millions en 2010 (source : Autorité de régulation des communications électroniques et des postes - ARCEP).

Tableau récapitulatif de l'évolution des contingents d'interceptions prévus par l'article L. 242-2 du Code de la sécurité intérieure

	Initial (1991-1996)	1997	2003	Juin 2005	2009
Ministère de la Défense	232	330	400	450	285
Ministère de l'Intérieur	928	1 190	1 190	1 290	1 455
Ministère du Budget	20	20	80	100	100
Total	1 180	1 540	1 670	1 840	1 840

NB : cette modification de la ventilation des contingents d'interceptions attribués à chaque ministère tient compte de l'intégration, depuis 2009, du sous-contingent de la gendarmerie nationale au sein du contingent du ministère de l'Intérieur.

L'année 2011 a été marquée par le troisième exercice de l'interprétation par la Commission de ce contingent comme se référant à un nombre maximum de « cibles » et non plus de « lignes ». Cette référence, à la « cible » doit permettre de ne pas envisager une augmentation de ce contingent à brève et moyenne échéance.

Contrôle de la motivation et justification de la demande d'interception de sécurité

Le premier et unique objectif des interceptions de sécurité est, comme leur nom l'indique, la protection de la sécurité de la Nation et de ses intérêts fondamentaux.

Les motifs prévus par la loi du 10 juillet 1991, repris à l'article L. 241-2 du Code de la sécurité intérieure, sont directement inspirés du Livre IV du Code pénal qui incrimine les atteintes à ces intérêts fondamentaux. Les cinq motifs légaux de 1991 ne font que décliner les différents aspects de la sécurité de la Nation, mais la référence précise à ceux-ci permet une appréciation plus pertinente du fondement des demandes.

Ces motifs sont : la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous en application de la loi du 10 janvier 1936 sur les groupes de combat et les milices privées.

Les services demandeurs doivent donc faire référence de manière explicite à l'un de ces motifs légaux. Ils doivent en outre justifier leur demande par des explications circonstanciées qui permettront à la Commission d'apprécier l'articulation du fait au droit. À cet effet, la présentation des éléments de fait doit être certes synthétique mais non stéréotypée. Elle doit être sincère et consistante pour permettre à chaque autorité, ministres demandeurs, Commission et Premier ministre, de juger de la pertinence de leur adéquation au motif légal. Ce point, ainsi que les critères d'appréciation des motivations, seront repris dans la partie du rapport consacrée aux « avis et préconisations de la Commission ».

Le cadre des demandes servant à la rédaction des demandes par les différents services habilités a été revu en 2006, en 2008, et à nouveau en 2009. L'objectif est de constituer des trames toujours plus claires et précises pour tendre, à partir de modèles, à une présentation complète, gage d'une plus grande facilité pour les services rédacteurs et d'une plus grande efficacité dans le traitement de la demande par les autorités de consultation et de décision. Ces imprimés permettent un contrôle toujours plus efficient de la Commission, qui est très attentive au caractère exhaustif des mentions.

Ces cadres normalisés ne constituent pas un cadre restreint. En tant que de besoin, les services peuvent communiquer tout élément qui leur parait utile à l'appui de leur demande, en présentant spontanément des informations complémentaires indispensables à une appréhension juste et complète de la situation.

Le contrôle opéré par la Commission s'attache d'une part à une identification aussi précise que possible des cibles, d'autre part aux informations recueillies sur leur activité socioprofessionnelle : il convient en effet de porter une attention particulière aux professions ou activités jugées sensibles en raison du rôle qu'elles jouent dans une société démocratique.

Il importe aussi de s'assurer que le motif légal invoqué ne dissimule pas d'autres préoccupations. Il est nécessaire de rappeler que l'interception doit être sollicitée exclusivement pour les faits décrits dans la demande et non pour une raison autre, qui ne relèverait d'aucun motif légal. Ceci sera également développé dans la partie du rapport consacrée aux « avis et préconisations de la Commission ».

La Commission formule toutes les observations qu'elle juge utiles sur la pertinence du motif invoqué, procédant le cas échéant à des

propositions de requalification, afin de substituer au motif initialement visé, un autre des cinq motifs légaux qui paraît plus adapté.

Elle s'assure que la demande respecte le principe de proportionnalité entre le but recherché et la mesure sollicitée. La gravité du risque pour la sécurité des personnes – physiques comme morales – ou pour la sécurité collective, doit être à la mesure de l'atteinte à la vie privée que constitue la surveillance de la correspondance par voie de communications électroniques, et la justifier pleinement.

La recherche de cette proportionnalité peut se traduire *ab initio* ou lors du renouvellement par une restriction, au cas par cas, de la durée de la mesure dont le maximum légal est de quatre mois. Une différenciation des délais a ainsi été instaurée par voie jurisprudentielle : deux mois pour une cible non encore totalement identifiée, un mois en cas de risque de récidive d'une infraction criminelle déjà commise, ou encore délai *ad hoc*, calé sur un événement prévu à une date déterminée.

Des instructions peuvent être données pour exclure des transcriptions (appelées « productions ») certains aspects privés des conversations ou des questions n'entrant pas dans le champ des motifs légaux. Des avis favorables subordonnent l'exploitation des interceptions à certains objectifs ou fixent les orientations exclusives qui paraissent devoir être retenues pour garantir une exploitation des communications conforme aux dispositions légales. La Commission et l'autorité de décision sollicitent régulièrement des bilans circonstanciés avant d'autoriser une nouvelle prolongation dans le cas d'une interception déjà renouvelée.

La Commission veille par ailleurs à ce que soit respecté le principe de subsidiarité. Par conséquent, lors de ses vérifications, elle s'assure que le but recherché ne puisse être rempli que par ce moyen et non par d'autres investigations plus classiques (enquête de terrain, d'environnement, mise en place de forces de l'ordre, etc.).

La jurisprudence de la CNCIS s'attache également à la protection des libertés de conscience et d'expression. Ainsi maintient-elle que le prosélytisme religieux, comme l'expression d'opinions extrêmes, dès lors qu'elles ne tombent pas sous le coup de la loi, ne justifient pas, en tant que tels, une demande d'interception, s'ils ne comportent aucune menace immédiate pour l'ordre public républicain, matérialisée par exemple par un appel ou un encouragement à la violence. De même, elle veille à ce que les interceptions, en ce qu'elles sont parfois concomitantes d'actions sur le terrain, ne portent pas atteinte à la liberté de manifestation. D'une manière générale, et quel que soit le motif, l'implication personnelle de la cible dans des agissements attentatoires à notre sécurité doit être au moins présumée.

Dans le cadre de son contrôle *a priori*, la Commission dispose d'un moyen d'investigation auquel elle recourt plus souvent depuis quelques années. Elle a la possibilité de demander au service concerné les éléments

d'information complémentaires qui lui sont nécessaires pour fonder son avis. Elle peut, en effet, à réception de ces renseignements additionnels, formuler des observations ou rendre un avis défavorable.

Le Premier ministre – ou son délégué – peut, dans les mêmes conditions, solliciter des éléments d'informations supplémentaires. Cette demande suspend, jusqu'à réception des compléments sollicités, la décision d'autorisation ou de renouvellement. Cette requête ou celle initiée par le Premier ministre ou son délégué constitue un sursis à statuer en ce que l'avis préalable doit être recueilli avant l'autorisation et la mise en place d'une interception.

En effet, les renseignements complémentaires sont destinés à compléter, éclairer ou préciser les demandes d'interceptions de sécurité initiales ou de renouvellement. Ces éléments d'information supplémentaires fondent l'avis de la Commission et la décision du Premier ministre, au même titre que les renseignements figurant dans la demande du service.

Par avis n° 7/2012 du 29 mai 2012, la Commission a rappelé que les demandes de renseignements complémentaires formulées par la CNCIS ne constituent pas un avis, mais relèvent des mesures d'investigations prévues aux articles L. 243-8 à L. 243-10 du Code de la sécurité intérieure. Ces demandes emportent donc sursis à statuer durant le délai de réponse du service demandeur et du traitement de cette réponse par la Commission. Elles peuvent intervenir tant dans le cadre des procédures ordinaires que des urgences absolues, pour les demandes initiales comme pour les renouvellements. La Commission a également rappelé que « les autorisations délivrées par le Premier ministre ou son délégué après une demande de renseignements complémentaires et sans disposer de l'avis de la Commission relèvent des décisions visées par l'article L. 243-8 alinéas 2 et 3 [du Code de la sécurité intérieure]. À ce titre, elles font l'objet d'une recommandation adressée au Premier ministre et au ministre ayant proposé l'interception ».

Données chiffrées et commentaires

- *Évolutions 2010-2011*

6396 interceptions de sécurité ont été sollicitées en 2011 (4156 interceptions initiales et 2240 renouvellements).

S'agissant des interceptions initiales, 541 de ces 4156 demandes ont été présentées selon la procédure dite d'urgence absolue (522 en 2010) soit 13 % de ces demandes, ce qui démontre une stabilité par rapport à l'année précédente (13,2 % en 2010).

L'objectif d'un traitement par la Commission de ce type de demande dans un délai inférieur à une heure a toujours été atteint. Le respect de cette contrainte de performance que s'est fixée l'autorité administrative

indépendante nécessite, dans le cadre de l'avis *a priori* donné par la Commission, la mise en œuvre d'une permanence 24h/24, tout au long de l'année, qui peut d'une certaine manière être comparée à celle qui est assurée par chaque parquet près les tribunaux de grande instance.

Au final, si l'on impute à ce chiffre global les cinquante-cinq avis défavorables donnés par la Commission lors des demandes initiales et des demandes de renouvellement, tous suivis par le Premier ministre, ce sont donc 6341 interceptions de sécurité qui ont effectivement été pratiquées au cours de l'année 2011 (5979 en 2010).

Pour ce qui concerne les « motifs légaux » au stade des demandes initiales, la prévention de la criminalité et délinquance organisées reste le premier motif des demandes initiales avec 62 %, suivie de la sécurité nationale avec 21 % et de la prévention du terrorisme 16 %.

Concernant les renouvellements, on note que la sécurité nationale occupe la première place avec 47 % suivie de la prévention du terrorisme 27 % et de la criminalité organisée 25 %. Ces pourcentages de renouvellement rendent compte, de fait, du travail des services en rapport avec les motifs légaux qui supposent une inscription des investigations dans la durée.

La part beaucoup moins importante du motif de la criminalité organisée dans les demandes de renouvellement, alors qu'il constitue plus de la moitié des demandes initiales, est l'application des principes fixés par la loi et repris par le Conseil constitutionnel sur la primauté de l'autorité judiciaire.

Si les projets d'infractions sont confirmés, dans ce cas, les tentatives et la commission des infractions relèvent de la compétence exclusive des autorités judiciaires. Comme tous les agents de l'État, les services exploitant des interceptions et constatant à cette occasion l'existence d'infractions doivent en rendre compte à l'autorité judiciaire en application de l'article 40 du Code de procédure pénale. Le pouvoir judiciaire est la seule autorité en charge de l'opportunité et de la conduite des poursuites pénales. Dans ce cas, de nouvelles interceptions peuvent être réalisées. Elles relèvent des dispositions du Code de procédure pénale et sont conduites dans le cadre d'une enquête ou d'une ouverture d'information.

Si l'interception de sécurité et les autres investigations ne permettent pas de confirmer les présomptions d'implication personnelle et directe de l'objectif dans des projets de commission d'infractions visées par l'article 706-73 du Code de procédure pénale, il n'y a pas lieu, comme pour les autres motifs de poursuivre les écoutes.

Le total cumulé des demandes initiales et des renouvellements confirme que la prévention de la criminalité et de la délinquance organisées se détache nettement avec 49 % des requêtes, suivie de la sécurité nationale 30 % et puis la prévention du terrorisme 20 %. Ces trois motifs représentent quasiment 99 % du total des demandes.

• *Observations*

La Commission a poursuivi sa démarche de dialogue avec les services demandeurs. Cette volonté de privilégier les échanges constructifs s'est traduite par une nette augmentation des réunions bilatérales avec ces mêmes services, tant au niveau central que déconcentré.

Elle s'est également matérialisée, au stade de l'examen des demandes, par des avis ne répondant pas à une logique purement binaire (avis favorable ou défavorable). De fait, le nombre d'observations a encore crû, passant de 2 101 en 2010 dont 79 demandes de renseignements complémentaires et 487 limitations de la durée d'interception sollicitée, à 3 126 en 2011 dont 114 demandes de renseignements complémentaires et 634 limitations de la durée d'interception. Les avis défavorables, comptabilisés dans les observations se sont élevés à 55, 31 concernant les demandes initiales (dont 1 portant sur une procédure d'urgence absolue) et 24 les demandes de renouvellement. À ce chiffre des avis défavorables « bruts », il convient d'ajouter deux techniques d'observation déjà répertoriées dans le rapport d'activité 2008 qui peuvent s'apparenter à « l'avis défavorable » :

• La recommandation adressée au Premier ministre visant à l'interruption de l'interception en cours d'exploitation qui résulte de l'examen exhaustif des « productions » (transcriptions) opérées à partir d'une interception. Il y a été fait recours à une seule reprise en 2011 (contre 7 en 2010). Elle a été immédiatement suivie par le Premier ministre.

• La « préconisation d'interruption » adressée par la Commission au service utilisateur en cours d'exploitation. Elle résulte du même examen des productions et procède d'un dialogue constructif mené directement avec les services utilisateurs à stopper l'exploitation d'interceptions, qui sont susceptibles de présenter des difficultés par rapport aux dispositions légales ou qui s'éloignent du cadre de l'autorisation délivrée par le Premier ministre ou son délégué. 43 préconisations ont été faites en 2011 par la Commission, toutes suivies par les services titulaires de l'autorisation d'interception.

De fait, si l'on additionne avis défavorables, recommandations d'interruption adressées au Premier ministre et « préconisations d'interruption » adressées directement aux services utilisateurs, le nombre de cas où une interception de sécurité n'a pas été réalisée ou poursuivie, conformément au positionnement de la Commission s'établit pour l'année 2011 à 99.

Le contrôle en aval

Force est également de constater que le contrôle en amont des demandes, aussi minutieux et exhaustif soit-il, ne saurait suffire. Le contrôle des « productions » est, en aval, le moyen privilégié pour s'assurer non seulement de la bonne adéquation de la demande au motif

légal invoqué, mais aussi de l'intérêt réel présenté par l'interception, au regard des critères de proportionnalité et de subsidiarité.

Ce « contrôle continu » inauguré en 2005 s'effectue de manière aléatoire ou ciblée. Il permet ainsi à la Commission de rendre des avis plus éclairés au stade du renouvellement de l'interception s'il est demandé par le service, et, le cas échéant, d'effectuer, en cours d'exploitation d'une interception, une recommandation tendant à l'interruption de celle-ci.

Ainsi, les « productions » de 619 interceptions en 2011 (560 en 2010) ont été examinées par la Commission.

La pratique de la « recommandation d'avertissement » décrite dans le rapport 2008 a également été poursuivie : il s'agit d'une lettre annonçant au Premier ministre qu'une recommandation d'interruption de l'écoute pourrait lui être envoyée à bref délai si l'incertitude sur l'adéquation entre le motif invoqué et la réalité des propos échangés devait se poursuivre. Trois recommandations ont été adressées au Premier ministre au cours de l'année 2011. Elles ont entraîné des rappels de la part du délégué du Premier ministre adressés au service exploitant qui a tiré les conséquences des difficultés soulevées par la Commission en demandant à son niveau la suppression des interceptions en question.

Un tel « avertissement » sortant le dossier litigieux de son anonymat administratif, permet au Premier ministre d'interroger le service concerné sur une base concrète, et renforce ainsi, au niveau politique, le dialogue déjà amorcé par la Commission avec les services habilités, au cours de ces dernières années.

Enfin, la Commission procède, en séance plénière, à des auditions de directeurs ou responsables techniques des services de renseignement dans des dossiers où le recueil d'informations complémentaires et le suivi des productions ne suffisent pas à l'éclairer suffisamment avant qu'elle rende ses avis ou formule ses préconisations.

Avec 6 341 interceptions accordées en 2011 par le Premier ministre, rapportées à un nombre de vecteurs de communications électroniques pourtant en constante augmentation, les interceptions de sécurité sont demeurées, comme les années précédentes, la mesure d'exception voulue par la loi.

Tableaux annexes

Les demandes initiales d'interceptions

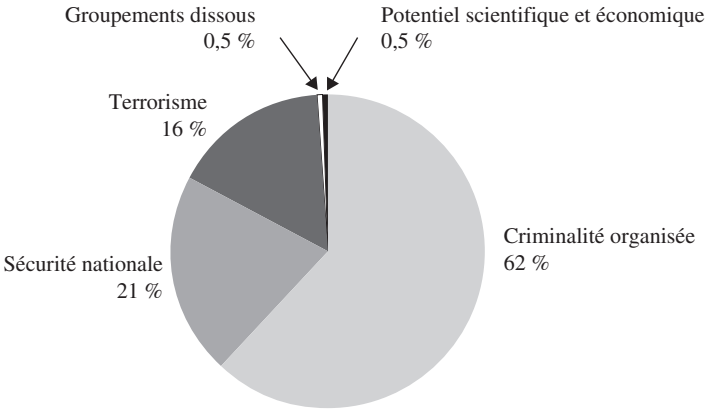
État des demandes initiales d'interceptions (2010 et 2011)

	Demandes initiales		Dont urgence absolue		Accordées	
	2010	2011	2010	2011	2010	2011
Total	3776	4156	522	541	3759	4125

Demandes initiales

Répartition des motifs

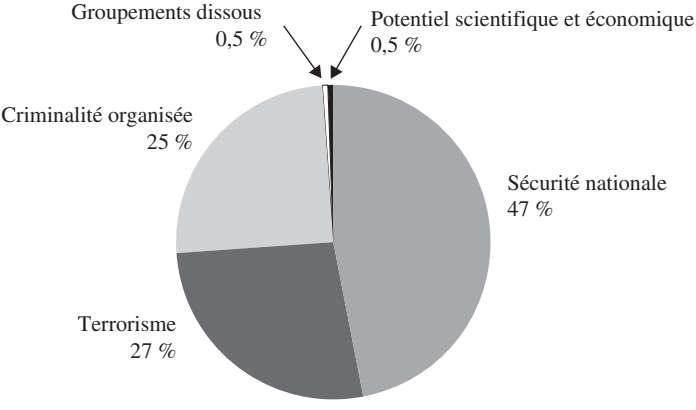
2011



Les renouvellements d'interceptions

Total des renouvellements demandés : 2 240

Répartition des motifs des renouvellements accordés en 2011



Activité globale : demandes initiales et renouvellements

Répartition des demandes entre interceptions et renouvellements d'interceptions

Demandes initiales circuit normal		Demandes initiales en urgence absolue		Demandes de renouvellement	
2010	2011	2010	2011	2010	2011
3 254	3 615	522	541	2 234	2 240

2011

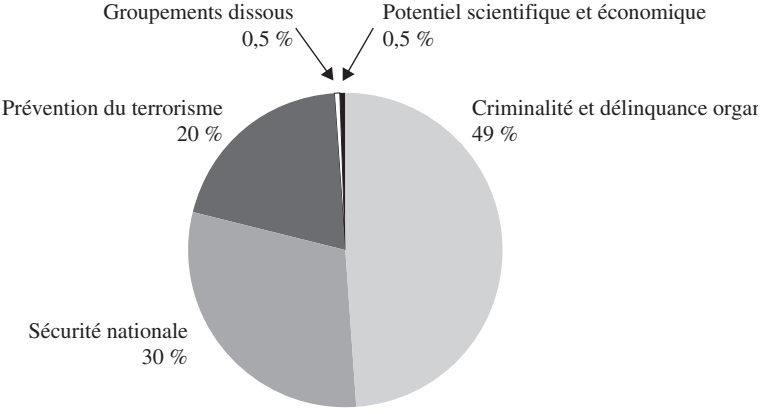
Demandes initiales : 64,99 %. 13 % d'entre elles ont été sollicitées selon la procédure de l'urgence absolue.
Demandes de renouvellements : 35,01 %.

Demandes d'interceptions : tableau récapitulatif global sur six ans (2006 à 2011)

	2006	2007	2008	2009	2010	2011
Demandes initiales d'interceptions	4203	4215	4330	3176	3776	4156
Dont « urgences absolues »	714	964	1095	497	522	541
Demandes de renouvellements	1825	1850	1605	1941	2234	2240
Total	6028	6065	5935	5117	6010	6396

Répartitions des motifs d'interceptions de sécurité accordées

Cumul des demandes initiales et demandes de renouvellements accordés



Répartition entre interceptions et renouvellements accordés

Interceptions accordées en 2011

Interceptions initiales	Renouvellements	Total
4125	2216	6341

Le contrôle de l'exécution

Celui-ci porte sur trois domaines :
– l'enregistrement, la transcription et la durée des interceptions ;

– les visites des centres déconcentrés, des services départementaux et régionaux ainsi que des échelons nationaux qui procèdent aux demandes et à l'exploitation des interceptions de sécurité ;
– l'instruction des réclamations des particuliers et les éventuelles dénonciations à l'autorité judiciaire.

Enregistrement, transcription et destruction

La mise en place en 2002 d'un effacement automatisé de l'enregistrement au plus tard à l'expiration du délai de dix jours, prévu par l'article L. 242-6 du Code de la sécurité intérieure, s'est traduite par un gain de temps appréciable pour les agents chargés de l'exploitation. Cette évolution ne dispense cependant pas de l'accomplissement des formalités prévues par le deuxième alinéa de ce même article : « Il est dressé procès-verbal de cette opération [de destruction des enregistrements à l'expiration d'un délai de dix jours]. » En application de cette disposition, en début d'année civile, le directeur du GIC atteste de la conformité logicielle du parc informatique de tous les établissements placés sous son autorité.

Les transcriptions doivent être détruites, conformément à l'article L. 242-7 du Code de la sécurité intérieure, dès que leur conservation n'est plus « indispensable » à la réalisation des fins mentionnées à l'article L. 241-2, même si cet article L. 242-7 n'édicte pas de délai. Le GIC à la faveur d'une instruction permanente a, conformément aux prescriptions de l'IGI 1300/SGDN/SSD du 30 novembre 2011, imposé aux services destinataires finaux des productions, d'attester auprès de lui de la destruction effective de ces dernières, dès lors que leur conservation ne présentait plus d'utilité pour l'exécution de la mission poursuivie.

Le contrôle du GIC

Service du Premier ministre, consacré comme tel après trente-et-une années d'existence par le décret n° 2002-497 du 12 avril 2002 (CNCIS, 11e rapport – 2002, p. 50) et actuellement dirigé par un officier général, le GIC est l'élément clef du dispositif des interceptions de sécurité. Il en assure la centralisation conformément à l'article L. 242-1 alinéa 2 du Code de la sécurité intérieure (« Le Premier ministre organise la centralisation de l'exécution des interceptions autorisées »).

Cette centralisation des moyens d'écoute, placés sous l'autorité du Premier ministre et confiés à un service technique neutre, en ce qu'il n'est pas en charge de l'exploitation du renseignement et des enquêtes, a été jugée par le législateur comme une garantie fondamentale dans la protection des libertés publiques en ce qu'elle offre une séparation claire et solide entre l'emploi des moyens et les services de renseignement, entre le demandeur et l'autorité de décision. Au regard de ses attributions, la Commission a toujours réaffirmé l'importance de cette organisation et de ce principe comme une garantie essentielle au bon fonctionnement

démocratique des institutions républicaines en charge de ces outils de renseignement et d'investigation.

Ce service s'adapte en permanence aux avancées technologiques incessantes dans le domaine des communications électroniques qui constituent chaque fois autant de défis à relever (citons en l'espace d'une décennie, la téléphonie mobile, le SMS, le mail, l'Internet, le dégroupage et la multiplication des opérateurs).

Conformément à une recommandation prise par la Commission en 1996, le GIC a entrepris dès 1997 la mise en place de centres locaux de regroupement des interceptions, sortes de « GIC déconcentrés » répondant aux normes de sureté souhaitées par la Commission au regard de la protection des personnes mise en cause et des personnels des services chargés de l'exploitation de ces renseignements.

Cette phase est à ce jour achevée. Le maillage du territoire en antennes secondaires se poursuit désormais pour s'adapter aux évolutions des menaces, au redéploiement des services ainsi qu'aux réformes territoriales et des administrations. Après la nécessaire étape de la structuration centralisée voulue par le législateur et le gouvernement, il a été donné aux services enquêteurs la proximité attendue pour une plus grande efficacité de leurs investigations, en créant des centres d'exploitation dans le ressort territorial de leurs missions. Les moyens d'interception et leur contrôle demeurent centralisés. Ce redéploiement des centres d'exploitation, au plus près des utilisateurs, est une garantie d'efficience sur le plan opérationnel, tout en préservant les garanties d'un système centralisé placé sous l'autorité du Premier ministre, contrôlé à la fois par un service du Premier ministre et une autorité administrative indépendante.

Enfin, le GIC répond à toute demande d'information de la Commission qu'il assiste avec célérité et efficacité.

Les visites des centres déconcentrés et des services locaux

En dépit d'une situation de sous-effectif durant près de cinq mois en 2011, la CNCIS a poursuivi les visites inopinées ou programmées des services utilisateurs d'interceptions.

Lors de ces visites, les contrôles portent à la fois sur la sécurisation des locaux, les interceptions en cours, l'examen des relevés d'interception et d'enregistrement (article L. 242-4 du Code de la sécurité intérieure) et des procès-verbaux de destruction des enregistrements et des transcriptions (articles L. 242-5 et L. 242-7 du Code de la sécurité intérieure).

Ces déplacements peuvent être effectués par les membres de la Commission eux-mêmes, le délégué général ou le chargé de mission.

Au total, sous une forme ou sous une autre, seize visites de centres d'exploitation ont été effectuées cette année. À chacune de ces visites, les représentants de la CNCIS dressent un inventaire des pratiques et procédures mises en œuvre par les services pour l'application du Code de la sécurité intérieure, apportent les informations et éclaircissements utiles, notamment sur le rôle et les avis de la CNCIS, recueillent les observations des personnels rencontrés sur les matériels et logiciels mis à leur disposition et s'informent des réalités locales se rapportant aux motifs légaux des interceptions.

Réclamations de particuliers et dénonciation à l'autorité judiciaire

Les saisines de la CNCIS par les particuliers

En 2011, quarante-trois particuliers ont saisi par écrit la CNCIS. Une minorité des courriers concernait des demandes de renseignements sur la législation. La majorité, constituée de réclamations, a donné lieu au contrôle systématique auquel il est procédé lorsque le demandeur justifie d'un intérêt direct et personnel à interroger la Commission sur la légalité d'une éventuelle interception administrative.

Il convient de préciser que les agents de la Commission ont traité un chiffre d'appels téléphoniques bien supérieur à celui des saisines par courrier. Ces contacts préalables ont le plus souvent permis de prévenir des courriers ultérieurs inappropriés lorsqu'il s'agit d'appels malveillants, de problèmes relevant de la saisine de l'autorité judiciaire (soupçons d'écoutes illégales à caractère privé) ou enfin de dysfonctionnements techniques classiques. Les requérants ont pu ainsi être réorientés vers les services compétents ou les autorités en charge de ces questions.

S'agissant des courriers adressés à la CNCIS, il leur est immédiatement donné suite et il est notifié au requérant, conformément à l'article L. 243-11 du Code de la sécurité intérieure, que la Commission a « procédé aux vérifications nécessaires ». On relève à ce propos dans les débats parlementaires précédant l'adoption de la loi du 10 juillet 1991 que « l'imprécision de cette formule reprise à l'identique de l'article 39 de la loi du 6 janvier 1978 [loi informatique et libertés] et reprise à l'article 41 de cette même loi, telle que modifiée par la loi du 6 août 2004 peut sembler insatisfaisante mais il est difficile, notamment au regard des prescriptions de l'article 26 de la loi du 10 juillet 1991 modifiée par la loi du 9 juillet 2004, d'aller plus loin dans la transparence. En effet, à l'occasion de son contrôle, la Commission peut découvrir les situations suivantes :
– existence d'une interception ordonnée par l'autorité judiciaire ;
– existence d'une interception de sécurité décidée et exécutée dans le respect des dispositions légales ;
– existence d'une interception de sécurité autorisée en violation de la loi ;

– existence d'une interception "sauvage", pratiquée en violation de l'article 1er du projet de loi par une personne privée ;
– absence de toute interception.

On comprendra aisément au vu de ces différentes hypothèses que la Commission nationale n'a d'autre possibilité que d'adresser la même notification à l'auteur d'une réclamation, quelle que soit la situation révélée par les opérations de contrôle, et que toute autre disposition conduirait, directement ou indirectement, la Commission à divulguer des informations par nature confidentielles » (Assemblée nationale, rapport n° 2088 de François Massot, 6 juin 1991).

Faut-il en conclure que toute requête est inutile ? Non, car même si le « secret-défense » interdit toute révélation sur l'existence ou l'inexistence d'une interception de sécurité, la CNCIS dispose de deux moyens d'action lorsqu'elle constate une anomalie :
– le pouvoir d'adresser au Premier ministre une recommandation tendant à faire interrompre une interception qui s'avérerait mal fondée ;
– le pouvoir, qui est aussi un devoir, de dénonciation à l'autorité judiciaire de toute infraction à la loi de 1991 (aujourd'hui titre IV du Livre II du Code de la sécurité intérieure) qui pourrait être révélée à l'occasion de ce contrôle (*cf. infra*).

Pour être complet signalons que :
– la Commission d'accès aux documents administratifs (CADA) arguant du secret-défense a émis le 18 décembre 1998 un avis défavorable à la demande de communication d'une copie d'une autorisation du Premier ministre concernant l'interception des communications téléphoniques d'un requérant ;
– le Conseil d'État, dans une décision du 28 juillet 2000, a rejeté le recours d'un requérant contre la décision du président de la CNCIS refusant de procéder à une enquête aux fins, non de vérifier si des lignes identifiées avaient fait l'objet d'une interception comme la loi lui en donne le pouvoir, mais si la surveillance policière dont l'intéressé se disait victime trouvait sa source dans l'interception de lignes de ses relations.

Les avis à l'autorité judiciaire prévus à l'article L. 243-11 du Code de la sécurité intérieure

Au cours de l'année 2011, la CNCIS n'a pas eu à user des dispositions du 2e alinéa de l'article L. 243-11 du Code de la sécurité intérieure qui précisent que « 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 contrôle effectué en application de l'article L. 243-9 ».

Chapitre IV

Le contrôle des opérations portant sur les données techniques de communications

Section 1 – Présentation du dispositif

En matière de police administrative et de prévention des atteintes à la sécurité et aux intérêts fondamentaux de la Nation, le recueil de données techniques de communications repose sur deux cadres légaux. La Commission, assistée des services du Groupement interministériel de contrôle (GIC) et de ceux de la personnalité qualifiée, exerce un strict contrôle sur ces deux modes de réquisitions administratives.

I – Le régime de l'article L. 244-2 du Code de la sécurité intérieure (ex-article 22 de la loi du 10 juillet 1991)

La loi n° 91-646 du 10 juillet 1991 est le premier texte en matière d'exploitation des communications électroniques pour la prévention des atteintes les plus graves à la sécurité nationale et aux intérêts fondamentaux de la Nation. Son article 22 – désormais article L. 244-2 du Code de la sécurité intérieure – constitue la première référence légale relative aux données techniques de communications. Ce texte prévoit que les services, par le biais du GIC, peuvent « recueillir, auprès des personnes physiques ou morales exploitant des réseaux de communications électroniques ou fournisseurs de services de communications électroniques, les informations ou documents qui leur sont nécessaires, chacun en ce

qui le concerne, pour la réalisation et l'exploitation des interceptions autorisées par la loi ».

Sur le fondement de ce texte, les demandes d'identification et de données de trafic auprès du GIC sont faites par les services en vue de l'élaboration d'une interception de sécurité. Ces mesures s'inscrivent dans le cadre de la réalisation visée par la loi, soit l'action de rendre réel et effectif un projet d'interception, ou de l'exclure au terme des résultats de ces investigations préparatoires. S'agissant de mesures moins attentatoires au secret des correspondances, elles constituent ainsi le moyen d'exclure des projets d'interceptions plus intrusives par l'accès qu'elles permettent au contenu des communications.

De même, sur la base de cet article, les prestations annexes, portant sur les communications électroniques de l'objectif visé par l'interception (Fadettes, localisation…), sont transmises par les opérateurs, *via* le GIC, au service exploitant, durant toute la durée de l'écoute. Dans ce cas, les mesures se fondent sur l'exploitation visée explicitement par la loi.

Ce dispositif est mis en œuvre pour tous les motifs légaux (la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous) et par tous les services, hormis, s'agissant de la prévention du terrorisme, les services du ministère de l'Intérieur, qui doivent recourir aux dispositions prévues par l'article L. 34-1-1 du Code des postes et des communications électroniques.

Ces données techniques sont recueillies au terme d'une procédure spécifique, organisée conformément aux recommandations de la CNCIS. La Commission a défini une procédure de contrôle reposant sur les principes de la loi du 10 juillet 1991 et adaptée à la nature du recueil des données :
– la centralisation, le traitement et le contrôle *a priori* des demandes des services par le GIC relevant du Premier ministre ;
– le contrôle *a posteriori* de ces demandes par la CNCIS, qui a accès à l'ensemble de la procédure, à tout instant ;
– la possibilité pour la Commission, de recourir aux mêmes avis et recommandations que ceux adressés au Premier ministre, dans le cadre des interceptions de sécurité.

II – Le dispositif expérimental de l'article 6 de la loi du 23 janvier 2006 (article L. 34-1-1 du Code des postes et des communications électroniques)

À la suite des attentats de Madrid du 11 mars 2004 et de Londres du 7 juillet 2005, le législateur a autorisé les services de police et de gendarmerie spécialisés dans la prévention du terrorisme à se faire

communiquer, sur le fondement d'une réquisition administrative spécifique, certaines données techniques détenues par les opérateurs de communications.

L'article 6 de la loi n° 2006-64 du 23 janvier 2006, relative à la lutte contre le terror[i]sme et portant diverses dispositions relatives la sécurité et aux contrôles frontaliers, autorise les services du ministère de l'Intérieur, chargés de la prévention du terrorisme, à recueillir, sur simple réquisition, des données techniques afférentes à une communication électronique. Il permet d'avoir accès au « contenant » d'une telle communication sans avoir accès au « contenu » de celle-ci, c'est-à-dire la conversation, l'échange de correspondances proprement dit.

Il encadre cet accès en le limitant au seul motif de prévention des actes de terrorisme et en fixant limitativement les prestations qui peuvent être obtenues. Il permet notamment le recueil des données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, le recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, des données relatives à la localisation des équipements terminaux utilisés ainsi que des données techniques relatives aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications.

Quoique moins intrusive dans le secret des correspondances, cette mesure porte atteinte à d'autres droits des citoyens, comme le droit à l'intimité de la vie privée et à la liberté d'aller et venir. C'est la raison pour laquelle le législateur a prévu un certain nombre de garanties au respect desquelles la Commission nationale de contrôle des interceptions de sécurité est associée pleinement.

Ainsi la loi du 23 janvier 2006 a adopté un dispositif original en instituant une personnalité qualifiée auprès du ministre de l'Intérieur, relevant de la Commission nationale de contrôle des interceptions de sécurité pour son activité de contrôle de la légalité des demandes des services habilités en matière de prévention du terrorisme. La Commission est en outre chargée du contrôle a posteriori de toutes les demandes validées par la personnalité qualifiée.

Section 2 – Statistiques de l'activité

I – Concernant l'article L. 244-2 du Code de la sécurité intérieure

Entre le 1er août 2011 et le 31 juillet 2012, le Groupement interministériel de contrôle a traité près de 197 000 demandes. 180 000 demandes portaient sur des mesures d'identification. 3 900 mesures de détails de

trafics ont été examinées. 13 000 autres requêtes avaient pour objet des prestations spécifiques comme l'historique d'un identifiant ou l'identification d'une cellule.

Les services du ministère de l'Intérieur sollicitent par cette procédure des données techniques pour l'ensemble des motifs autres que celui de la prévention du terrorisme. Les services qui dépendent des ministères de la Défense ou du Budget recourent au GIC pour l'ensemble des motifs, y compris en matière de terrorisme, en ce qu'ils ne font pas partie des services habilités au titre de l'article 6 de la loi du 23 janvier 2006.

Les demandes se répartissent entre les différents motifs légaux de la façon suivante : 70 % d'entre elles portent sur la sécurité nationale, 21 % ont trait à la prévention de la délinquance et de la criminalité organisées, 7 % concernent la prévention du terrorisme, 1 % sont relatives à la protection du potentiel scientifique et économique et 1 % visent la reconstitution de groupements dissous.

7 % des mesures sont refusées et 10 % d'entre elles font l'objet de renvoi pour renseignements complémentaires avant validation.

II – Concernant l'article 6 de la loi du 23 janvier 2006

Sur les quatre années pleines (2008, 2009, 2010, et 2011), après une augmentation régulière du nombre de demandes présentées par les services, l'année 2011 a marqué un spectaculaire retournement de tendance, avec 11 635 demandes de moins que l'année précédente.

Cette tendance, qui s'est poursuivie au cours du premier semestre 2012 (13 389 demandes), laisse présager que le total des demandes présentées en 2012 sera inférieur à 30 000.

Année	Nombre de demandes présentées
2008	38 306
2009	43 559
2010	45 716
2011	34 081
Total	161 662

	Demandes présentées	Demandes validées	Demandes renvoyées	Demandes rejetées
2008	38 306	34 911	3 302	93
2009	43 559	39 070	4 459	30
2010	45 716	38 566	7 060	90
2011	34 081	31 637	2 428	16
Total sur 4 ans	161 662	144 184	17 249	229

Les demandes validées ne correspondent pas au nombre d'objectifs et de personnes. Dans la majorité des cas, plusieurs dizaines de

demandes concernent en fait une seule personne soupçonnée de menées terroristes. La recherche d'un renseignement va fonder le recours à plusieurs opérateurs de communications électroniques. Des mesures différentes sont sollicitées pour la même personne au fur et à mesure de l'évolution des investigations et de leur résultat.

Au cours des quatre dernières années, la « personnalité qualifiée » a traité 161 662 demandes, ce qui représente l'examen hebdomadaire de 825 demandes sur la totalité de la période, avec un chiffre moyen de 655 pour l'année 2011.

La diminution du recours au dispositif de l'article 6 par les services en charge de la prévention du terrorisme, déjà évoquée dans le rapport d'activité de l'année 2010, s'est accrue en 2011 avec une baisse de 19,86 % des demandes présentées en 2011 et corrélativement une diminution de 15,67 % des demandes validées.

En dépit de la constance des menaces terroristes, la baisse des demandes peut s'expliquer, en partie, et pour les explications que peut fournir la Commission au regard de ses attributions en matière de contrôle de la légalité, par une meilleure utilisation par les services demandeurs du dispositif. Cette analyse se déduit de l'examen exhaustif des demandes et de la baisse de 50,85 % du pourcentage des demandes renvoyées en raison d'une motivation insuffisante ainsi que des décisions de rejet définitif qui ont diminué de 77, 46 % au cours de l'exercice.

La typologie des mesures sollicitées par les services est identique quelle que soit la période d'exercice, soit près de 75 % de demandes d'identification d'abonnés. Ces mesures sont moins intrusives que les demandes portant sur les données de trafic qui représentent près de 25 % des dossiers traitées.

En 2011, les services de la Direction centrale du renseignement intérieur (DCRI), de la Direction du renseignement de la préfecture de police (DRPP) et de l'Unité de la coordination de la lutte antiterroriste (UCLAT) ont été à l'origine de 97,19 % des 34 081 requêtes présentées dans le cadre du dispositif de l'article 6.

Concernant les services et les unités à vocation judiciaire, qui emploient ce dispositif au titre du renseignement et de la prévention du terrorisme, la direction générale de la gendarmerie nationale a été à l'origine de 73,22 % des 956 demandes.

Les mesures sollicitées visent les moyens de communication électronique suivants :

	2008	2009	2010	2011
Téléphonie fixe	13,81 %	17,96 %	21,02 %	19,58 %
Téléphonie mobile	82,10 %	70,03 %	68,11 %	66,38 %
Internet	4,09 %	12,01 %	10,87 %	14,04 %

Ces chiffres permettent un triple constat :
• la téléphonie mobile reste la technologie qui motive le plus grand nombre de demandes, même si les requêtes s'y rapportant ont été, en 2011, au niveau le plus bas enregistré durant les quatre années de plein exercice de la période expérimentale ;
• le niveau quantitatif des demandes concernant la téléphonie fixe, qui avait suivi une progression à la hausse au cours des trois années précédentes, est en baisse ;
• si les demandes de prestation Internet sont également touchées par la baisse générale des demandes en 2011, leur niveau est supérieur de 22,15 % à leur moyenne sur les trois années précédentes.

Section 3 – Étendue et modalités du contrôle exercé par la CNCIS

Les demandes faites par les services doivent être dûment motivées, et ce au regard des motifs légaux retenus.

Les requêtes fondées sur l'article 6 de la loi du 23 janvier 2006 sont validées préalablement par la « personnalité qualifiée » placée auprès du ministre de l'Intérieur et nommée par la CNCIS pour une durée de trois ans renouvelable, ou par l'un de ses adjoints nommés dans les mêmes conditions. Elles doivent être sollicitées par des « agents individuellement désignés et dûment habilités ».

Les demandes relevant de l'article L. 244-2 du Code la sécurité intérieure sont validées par les personnels de permanence et de direction du GIC.

La loi a conféré à la CNCIS la responsabilité de contrôler *a posteriori* l'activité de ces deux entités, et le devoir corrélatif de saisir le ministre de l'Intérieur ou le Premier ministre d'une « recommandation » quand elle « constate un manquement aux règles… ou une atteinte aux droits et libertés ». La Commission a adressé trois recommandations au ministre de l'Intérieur en 2011.

La « personnalité qualifiée » a privilégié le recours régulier aux demandes de renseignements complémentaires avant validation ou refus. Le nombre de refus a ainsi significativement chuté.

Les motifs principaux de refus et de recommandations, au titre de l'article 6 de la loi du 23 janvier 2006, sont liés à des demandes relatives à des faits déjà commis et/ou faisant l'objet d'enquêtes judiciaires, à des demandes concernant des cibles dont la situation pénale au regard du Code de procédure pénale impose de prendre d'autres mesures et à des requêtes relatives à des faits insusceptibles en l'état de constituer des menées terroristes.

Les motifs essentiels de rejet des demandes au titre de l'article L. 244-2 du Code de la sécurité intérieure portent sur l'insuffisance des présomptions d'implication personnelle et directe de la personne visée par les demandes, le non-respect des principes de proportionnalité et/ou de subsidiarité, la contradiction entre les faits exposés et le motif légal de la demande et l'absence de précisions sur les projets d'atteintes aux intérêts fondamentaux de la Nation et à la sécurité.

La CNCIS a renforcé sa mission de contrôle en poursuivant les réunions avec la personnalité qualifiée et le GIC pour assurer une unicité de traitement des demandes portant sur les mesures référentielles de recueil de données techniques de communications, quel que soit le cadre légal, s'agissant d'investigations et d'atteintes au secret des correspondances identiques.

La Commission a apporté des précisions sur le contrôle gradué des requêtes en fonction du caractère plus ou moins intrusif de la prestation sollicitée au regard des libertés individuelles.

Elle a surtout développé le recours au droit de suite aux fins de connaître dans un nombre plus important de dossiers les résultats des mesures ainsi validées. Il s'agit pour elle de rapprocher le seuil de ce droit de suite et de l'analyse des résultats du recueil de données, de celui fixé pour le suivi des transcriptions en matière d'interceptions de sécurité.

Section 4 – Réflexions sur les perspectives d'évolution des cadres légaux du recueil de données techniques de communications en matière de police administrative

Éléments de droit comparé

Des échanges et des travaux conduits par la CNCIS avec un certain nombre d'organismes en charge du contrôle des interceptions des communications électroniques d'États étrangers (Allemagne, Belgique, Liban, Bulgarie, Roumanie, Italie…), il ressort que certaines législations prévoient un régime unique pour les demandes d'interceptions et celles portant sur le recueil de données techniques (Allemagne). D'autres ont des régimes comparables à celui du système français, avec des dispositions plus explicites et plus précises sur les mesures qui peuvent être sollicitées par les services de renseignement, ainsi que sur la nature des menaces ou des atteintes fondant ces actions administratives préventives (Belgique). D'autres encore ne disposent pas de législation sur les données techniques de communications. Certains pays s'intéressent depuis quelques années aux dispositifs d'interception et de surveillance générale, aléatoire, par balayage ou exhaustif, des communications

électroniques. Ils retiennent alors un contrôle *a posteriori* portant sur l'exploitation du renseignement technique.

Dans tous les cas, les délégations étrangères ont montré un intérêt particulier pour les dispositions françaises, notamment sur le régime différencié de protection et d'autorisation, qui varie selon la nature et l'importance de l'atteinte au secret des correspondances et à la vie privée.

Éléments de l'évaluation faite par la CNCIS

La CNCIS a conduit cette évaluation en qualité qu'organe de contrôle de la légalité chargé de la protection du secret des correspondances privées par voie électronique, et ce depuis la mise en œuvre effective du dispositif en 2007.

Cette évaluation a aussi été conduite au regard des évolutions du dispositif du GIC sur les interceptions de sécurité et sur le recueil des données techniques de communications, pour tous les motifs prévus par la loi du 10 juillet 1991, y compris la prévention du terrorisme conduite par les services habilités des ministères de la Défense et des Finances.

La Commission, dans sa formation plénière le 14 septembre 2005, rappelait que « le recueil de données techniques générées par les communications électroniques ou par Internet, appelées prestations annexes, fait l'objet de l'article 22 de la loi du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques […] Le droit positif relatif au recueil de données techniques prévoit un régime unique pour l'ensemble des motifs légaux et autorise l'atteinte au secret des correspondances, justifiée par l'intérêt supérieur de la sécurité nationale et la protection de la vie des populations. Dès lors, l'adoption d'une procédure spécifique et d'un dispositif spécial pour le seul motif de la prévention du terrorisme ne parait pas pertinente. Ce régime est même contraire à la volonté du législateur de centraliser les outils relatifs aux interceptions des communications électroniques et de les placer sous une autorité de décision distincte des services utilisateurs et des ministères demandeurs. »

Depuis cet avis et après six années d'une expérimentation du dispositif de l'article 6 de la loi du 23 janvier 2006, voulue par le législateur, la Commission constate que la juxtaposition de deux régimes qui offrent les mêmes prestations, mais selon des modalités de fonctionnement et de protection différentes, paraît source de confusion pour les services utilisateurs, d'erreurs dans le choix du cadre procédural, voire dans certains cas de tentations éventuelles d'utiliser successivement l'un et l'autre des cadres en cas de refus d'une des autorités décisionnaires.

Alors que les menaces sont de plus en plus transversales et que les enquêteurs travaillent sur des objectifs « multi-cartes » (criminalité organisée, atteintes à la sécurité nationale ou terrorisme par exemple), la coexistence de deux dispositifs cloisonnés par la différence de leur

niveau de classification (l'un n'étant pas protégé, l'autre relevant du régime du « secret-défense »), peut entrainer des difficultés dans le travail d'investigation et de renseignement ainsi que dans la mise en œuvre d'un régime unique de protection des correspondances privées par voie des communications électroniques.

Le rattachement au ministère de l'Intérieur du dispositif UCLAT de recueil de données techniques de communications pour la prévention du terrorisme, effectué par les services de ce même ministère, déroge aux principes fondamentaux du système mis en œuvre depuis la loi du 10 juillet 1991. Ces principes visent à garantir la légalité et le respect des libertés publiques par l'existence :
– d'une autorité de décision distincte des services habilités et des ministères demandeurs garantissant le recours à titre exceptionnel à ces investigations, et ce par une analyse partagée et contradictoire ;
– d'une autorité de décision disposant d'un outil centralisé de mise en œuvre et de contrôle technique des mesures, structure ne relevant pas des services utilisateurs ;
– d'une autorité de contrôle, dont l'indépendance statutaire renforce les garanties de protection des libertés publiques définies par le législateur.

La loi du 10 juillet 1991 garantit l'équilibre entre, d'une part, les impératifs de sécurité et de préservation des intérêts fondamentaux de la Nation, et, d'autre part, la protection des droits et des libertés individuelles, en consacrant la séparation entre les services habilités relevant de ministères demandeurs et l'autorité de décision. Le Premier ministre dispose d'un service technique autonome (le GIC) et recourt à une autorité administrative indépendante.

Elle offre un cadre légal pertinent et fondé juridiquement pour le recueil des données techniques de communications en matière de prévention du terrorisme. Ce motif est explicitement prévu par la loi pour autoriser les autorités administratives à déroger au respect du secret des correspondances privées par voie électronique. Il est mis en œuvre pour les interceptions de sécurité pour tous les services habilités et pour le recueil de données techniques pour les services ne relevant du champ d'application de la loi du 23 janvier 2006.

Une seule procédure, comme pour toutes les autres atteintes graves à la sécurité et aux intérêts fondamentaux de la Nation, permettrait de disposer d'une seule base de données, commune à tous les motifs légaux, à tous les services habilités des différents ministères, alimentée par les informations recueillies tant au niveau des interceptions que de l'exploitation des données techniques de communications. Elle faciliterait le travail de recueil et d'exploitation et permettrait des recoupements.

En outre, face aux menaces et aux objectifs précités, la réponse paraît plus pertinente en matière de sécurité juridique si elle consiste dans un dispositif global, cohérent, sécurisé, parfaitement contrôlé, et prenant en compte l'ensemble des motifs légaux.

Il apparaît plus efficient de s'orienter vers un dispositif renforcé et interministériel de recueil de données techniques portant sur la prévention de l'ensemble des atteintes à la sécurité de l'État et aux intérêts fondamentaux de la Nation, placé sous le contrôle d'une seule autorité indépendante dédiée à l'ensemble de la problématique du renseignement technique par la voie des communications électroniques.

Il semble que le projet de loi, récemment examiné par le Parlement et comportant entre autres mesures, la prolongation de la période d'expérimentation du dispositif UCLAT, s'inscrit dans la perspective d'une convergence des procédures et des plates-formes de recueil des données techniques. La CNCIS souhaite que ces travaux soient conduits dès le début de cette nouvelle période d'expérimentation souhaitée par le législateur et y être associée en qualité d'autorité administrative indépendante en charge de la protection du secret des correspondances privées et du contrôle des exceptions à ce principe en matière de prévention des atteintes aux intérêts fondamentaux de la Nation.

Chapitre V

Le contrôle portant sur les matériels d'interception

En vertu des articles R. 226-1 à R. 226-12 du Code pénal, le Premier ministre est compétent pour accorder les autorisations de fabrication, d'importation, d'exposition, d'offre, de location, de vente, d'acquisition ou de détention de matériels permettant de porter atteinte à l'intimité de la vie privée ou au secret des correspondances. Ces autorisations interviennent après avis d'une commission consultative à laquelle participe la CNCIS. La structure de cette commission consultative a été modifiée à la faveur de deux décrets publiés durant l'année 2009. Ainsi, le décret n° 2009-834 du 7 juillet 2009 puis le décret n° 2009-1657 du 24 décembre 2009 ont confié la présidence de cette commission au directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), lui-même rattaché au secrétaire général de la défense et de la sécurité nationale. Cette mutation structurelle n'a en revanche emporté aucune modification dans l'économie juridique du dispositif existant.

Le régime de contrôle, issu de l'arrêté du 29 juillet 2004, participe d'une évolution de l'appréhension de ce secteur d'activité sensible par la puissance publique (*cf.* rapport 2004, p. 34-38 ; rapport 2005, p. 31-33). Il traduit une vision libérale quant à la mise sur le marché d'appareils dont la liste initiale a été réduite, vision assortie d'une logique de vigilance quant à l'utilisation finale de ces appareils (*cf.* rapport 2004, p. 38).

Si les règles de commercialisation ont été allégées par rapport au dispositif réglementaire antérieur à 2004, cette facilitation de l'accès au marché n'a pas induit une inflexion dans la qualification du caractère « sensible » de ce type de matériel par les pouvoirs publics.

Ainsi, le décret 1739 du 30 décembre 2005 réglementant les relations financières avec l'étranger et portant application de l'article L. 151-3 du Code monétaire et financier (présenté par la doctrine comme aménageant le contrôle des investissements étrangers dans les secteurs stratégiques en France – *Recueil* Dalloz 2006, p. 218) soumet au principe de l'autorisation préalable l'investissement d'un État (intra ou extracommunautaire) portant sur « les matériels conçus pour l'interception des correspondances et la détection à distance des conversations autorisés au titre de l'article 226-3 du Code pénal ».

La commission consultative prévue à l'article R. 226-2 du Code pénal s'est réunie six fois en 2011. Sa composition est la suivante :
– le directeur de l'Agence nationale de sécurité des systèmes d'information ou son représentant, président ;
– un représentant du ministre de la Justice ;
– un représentant du ministre de l'Intérieur ;
– un représentant du ministre de la Défense ;
– un représentant du ministre chargé des Douanes ;
– un représentant du ministre chargé de l'Industrie ;
– un représentant de la CNCIS ;
– un représentant de l'Agence nationale des fréquences ;
– deux personnalités désignées en raison de leur compétence par le Premier ministre.

En 2011, la Commission a connu, comme les années précédentes, une nette augmentation de son activité. Elle a ainsi rendu 881 décisions (contre 558 en 2009 et 643 en 2010) ventilées comme suit :
• 437 décisions d'autorisation initiale (275 concernant la commercialisation, 162 l'acquisition d'équipements soumis à autorisation) ;
• 121 décisions de renouvellement d'autorisation ;
• 257 décisions d'ajournement ;
• 28 décisions de refus ou de retrait ;
• 26 décisions de radiation ou d'annulation ;
• 8 décisions de mise « hors champ » de l'examen pour autorisation ;
• 4 décisions de mise en attente de la demande.

L'année 2011 a confirmé la tendance nouvelle observée en 2010 : le nombre de décisions de mise « hors champ » de l'examen de la commission a continué à nettement diminuer, pour ne finalement concerner que 8 dossiers (contre 53 en 2009 et 15 en 2010).

Cette évolution est vraisemblablement le résultat d'une meilleure connaissance et mise en application des dispositions de l'arrêté du 29 juillet 2004, qui emportent l'exclusion de certains types d'appareils, qui étaient auparavant soumis à autorisation.

La CNCIS est également membre de la commission d'examen des demandes émanant des services de l'État pouvant solliciter une « autorisation de plein droit », conformément aux dispositions de l'article R. 226-9 du Code pénal.

Les administrations concernées sont invitées, selon le régime mis en place en 2001 (*cf.* rapport 2001, p. 27), à produire leurs registres et à décrire leurs règles internes de gestion des matériels sensibles. L'examen de ces demandes permet aux représentants de la CNCIS de s'assurer du respect des règles adoptées et de l'adéquation des matériels détenus avec les missions confiées à ces services.

Au cours des derniers mois, l'analyse de la CNCIS a été sollicitée par les membres de la commission consultative sur plusieurs points juridiques. Le degré de protection attaché aux travaux de cette commission ne permet pas d'en détailler le contenu, mais la CNCIS a, lors de l'élaboration de ces avis, eu le souci constant de protéger les citoyens contre tout enregistrement à leur insu de communications téléphoniques, qui aurait pu être la conséquence d'une mauvaise utilisation des fonctions offertes par certains matériels.

Deuxième partie

AVIS ET PRÉCONISATIONS DE LA COMMISSION

Chapitre I

Avis et préconisations de la Commission portant sur les motifs légaux en matière d'interceptions de sécurité et de recueil des données techniques de communications

Le rapport public est le moyen de faire une présentation générale et développée de chacun des motifs retenus par la loi et appliqués par la Commission dans ses avis. Ces critères sont repris intégralement par les autorités qui sont chargées d'autoriser ou non ces mesures de renseignement et de police administrative en matière de communications électroniques. S'agissant de mesures classifiées « secret-défense » ou « confidentiel-défense », seuls les principes généraux de la qualification juridique peuvent être exposés dans ce rapport public.

Sécurité nationale

« Sécurité nationale », « sécurité intérieure et extérieure », « sûreté de l'État », « intérêts fondamentaux de la Nation » sont des concepts voisins souvent employés indistinctement. Pour autant, le concept de « sécurité nationale » est apparu comme une nouveauté en 1991 et son usage est spécifique à la loi du 10 juillet 1991.

On relève ainsi dans les travaux parlementaires (rapport de la Commission des lois du Sénat) que « la notion de sécurité nationale est préférée à celle d'atteinte à la sûreté intérieure et extérieure de l'État […]. La sécurité nationale, notion qui n'existe pas en tant que telle dans le droit français est directement empruntée à l'article 8 de la Convention européenne des droits de l'homme. Elle recouvre la défense nationale ainsi que les autres atteintes à la sûreté et à l'autorité de l'État qui figurent au début du titre premier du Livre troisième du Code pénal ».

Pour mémoire, on rappellera que l'article 8 § 2 de la Convention européenne des droits de l'homme dispose : « Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit (droit au respect de la vie privée et familiale) que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. »

Les anciens articles 70 à 103 auxquels se référait le législateur en 1991 sont les incriminations visées désormais dans le Livre IV du Code pénal en vigueur 1994 et dénommées « atteintes aux intérêts fondamentaux de la Nation ».

Les intérêts fondamentaux de la Nation constituent depuis 1994 un concept destiné à remplacer celui de sûreté de l'État qui avait lui-même succédé, dans l'ordonnance du 4 juin 1960, à celui de sécurité intérieure et extérieure.

Selon l'article 410-1 du Code pénal : « Les intérêts fondamentaux de la Nation s'entendent au sens du présent titre de son indépendance, de l'intégrité de son territoire, de sa sécurité, de la forme républicaine de ses institutions, de ses moyens de défense et de sa diplomatie, de la sauvegarde de sa population en France et à l'étranger, de l'équilibre de son milieu naturel et de son environnement et des éléments essentiels de son potentiel scientifique et économique et de son patrimoine naturel. »

On notera que la sauvegarde des éléments essentiels du potentiel scientifique et économique constitue un motif d'interception autonome dans la loi de 1991.

Dès l'entrée en vigueur du nouveau Code pénal en 1994, la CNCIS a estimé que la notion de sécurité nationale devait être définie par référence à ces dispositions pénales (article 410-1 du Code pénal) portant sur les intérêts fondamentaux de la Nation en intégrant les notions d'intégrité du territoire, de forme républicaine des institutions ou des moyens de la défense.

S'il s'agit là d'un élargissement notable de la notion antérieure de sûreté de l'État, on ne saurait y voir pour autant une extension par assimilation aux atteintes les plus courantes à la sécurité des personnes ou des

biens. La Commission a toujours rappelé qu'il ne suffit pas d'invoquer la crainte générale d'un trouble à l'ordre public, comme y expose plus ou moins toute manifestation, pour répondre aux exigences de motivation résultant de la loi. Pour ce faire, il doit être justifié, avec la précision nécessaire, d'une menace particulièrement grave à la sécurité nationale.

Ainsi des demandes motivées par la crainte d'un trouble à l'ordre public ne peuvent fonder le recours à une interception qu'en cas de menace particulièrement grave à la sécurité. Le risque d'attenter à la forme républicaine des institutions ou de déboucher sur un mouvement insurrectionnel est fondamental. Si des manifestations sont susceptibles de dégénérer, le droit de manifester étant constitutionnellement reconnu, il s'agit là, d'un problème d'ordre public et non d'une atteinte à la sécurité nationale. On peut cependant admettre que dans certaines hypothèses, l'ampleur des troubles ou les atteintes aux institutions voulues par leurs auteurs affectant le lieu et le temps des manifestations, la qualité des autorités ou des symboles républicains visés, sont tels que la sécurité nationale peut être menacée.

Les interceptions de sécurité ne sauraient être utilisées comme moyen de pénétrer un milieu syndical ou politique ou de pratiquer la surveillance d'opposants étrangers, si la sécurité de l'État français lui-même n'est pas en cause. S'agissant de la recherche de renseignements, la personne dont il est envisagé d'intercepter les correspondances doit être suspectée d'attenter par ses agissements personnels aux intérêts fondamentaux de la Nation. Si les services de renseignements ont, par nature, une mission de collecte de renseignements qu'ils remplissent en utilisant divers moyens, intrusifs ou non dans le champ des libertés publiques, le recours aux interceptions de sécurité connaît certaines limites. En effet, l'atteinte exceptionnelle à la vie privée qu'autorise la loi ne peut être justifiée même dans ce domaine que par la menace directe ou indirecte, actuelle ou future que la personne écoutée est susceptible de représenter pour la sécurité nationale. En l'absence de menace, et quel que soit l'intérêt que représente la cible comme source de renseignement pour le domaine considéré, l'atteinte à la vie privée serait contraire aux principes de proportionnalité et de subsidiarité.

Enfin, la Commission opère une appréciation *in concreto* de la notion « d'intérêts fondamentaux de la Nation », la notion de sécurité étant appréhendée en un instant donné et dans un contexte géopolitique donné par rapport aux besoins vitaux du pays. Ainsi la Commission considère depuis plusieurs années que la sécurité énergétique fait désormais intégralement partie de la sécurité nationale.

Sauvegarde des éléments essentiels du potentiel scientifique et économique de la Nation

La sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, est, avec la reconstitution de ligues dissoutes, le motif d'interception le plus faible en volume, bien qu'il connaisse un certain développement avec les enjeux en lien avec « l'intelligence économique », la contre-ingérence, ainsi qu'avec les questions d'espionnage industriel et scientifique.

C'est cependant celui qui, lors de la discussion parlementaire de la loi du 10 juillet 1991, a suscité le plus de réserves.

La rédaction initiale n'était d'ailleurs pas celle adoptée. Le projet de loi visait « la protection des intérêts économiques et scientifiques fondamentaux de la France ».

Certains parlementaires, dénonçant le caractère trop général de ces notions d'intérêts fondamentaux, ont privilégié une rédaction s'inspirant de celle du Livre IV du Code pénal et notamment de son article 410-1 qui vise explicitement la « sauvegarde des éléments essentiels du potentiel scientifique et économique [de la Nation] » (Assemblée nationale, 2e séance, 13 juin 1991 ; Sénat du 25 juin 1991).

D'autres parlementaires ont fait valoir que « la possibilité d'interceptions de sécurité pour la protection des intérêts économiques et scientifiques fondamentaux d'un État est reconnue par la Convention européenne des droits de l'homme, dont le texte est d'ailleurs moins restrictif que le projet de loi, puisqu'il se réfère à la notion de "bien-être économique" » ; « […] il est nécessaire que l'État dispose de moyens d'information et d'action adaptés aux menaces résultant de l'internationalisation des activités économiques » (François Massot, rapport de la Commission des lois de l'Assemblée nationale, 6 juin 1991).

« L'article 410-1 susvisé 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 ».

L'article 410-1 du Code pénal est suivi des articles 411-1 à 411-11 qui incriminent les différentes atteintes à ces intérêts au titre desquelles on relève plus particulièrement les infractions des articles 411-5 à 411-8 relatives aux différentes formes d'intelligence avec une puissance étrangère (article 411-5) et à la livraison d'informations à celle-ci (articles 411-6 à 411-8).

Toute forme d'espionnage, y compris économique comme le transfert illicite de technologie, est clairement incriminée par ces articles, où est effectivement visée, la fourniture de procédés.

Cette fourniture peut être le fait d'auteurs divers (ingénieurs, agents de renseignement de pays tiers, « honorables correspondants », officines « spécialisées » dans l'espionnage économique) et être destinée non seulement à des services de renseignements de pays tiers (« puissances étrangères ») mais également à des entreprises ou des organisations étrangères.

Ce transfert illicite d'un procédé de fabrication, détenu exclusivement par un groupe national leader dans sa spécialité, est bien de nature à porter gravement atteinte aux éléments essentiels du potentiel scientifique et économique de la France. Il constitue sans aucun doute une atteinte aux intérêts fondamentaux de la Nation. Les éléments constitutifs d'une suspicion de commission du délit visé à l'article 411-7 du Code pénal, dont on remarquera qu'il constitue un mode original de répression de la tentative (le recueil des informations sans livraison de celles-ci est en soi punissable), sont réunis. En ce cas, l'interception de sécurité est parfaitement fondée en droit.

Il résulte de ces incriminations pénales qu'en dépit de la définition extensive donnée au concept d'intelligence économique, les interceptions sollicitées sous le motif « sauvegarde des éléments essentiels du potentiel scientifique et économique de la France », dont la formulation est directement reprise du Code pénal, correspondent à des faits précis et à des infractions prévues par le législateur.

La jurisprudence de la Commission, pour ce qui concerne ce motif, s'efforce à une synthèse :
– du dispositif normatif pénal ;
– du principe fondamental posé par la loi du 10 juillet 1991 de ce que les interceptions de sécurité relèvent exclusivement de la police administrative, et en conséquence des actions de prévention, et non des démarches actives préconisées par une partie de la doctrine née de l'intelligence économique ;
– de la conciliation entre la protection de notre patrimoine scientifique et économique et la nécessaire préservation de la « vie des affaires », protégée juridiquement dans une zone européenne où le libre-échange représente une valeur constitutive.

Ainsi la CNCIS retient les critères suivants : les interceptions de sécurité sollicitées sous le motif « sauvegarde des éléments essentiels du potentiel scientifique et économique de la France », doivent, d'une part répondre à une menace (infraction issue du dispositif 411-1 à 411-11 du Code pénal) vérifiable traduisant une intention de nuire aux intérêts d'une entreprise française, d'autre part, la personne dont il est demandé d'intercepter les communications doit être clairement impliquée dans cette menace. L'activité de l'entreprise menacée doit enfin être liée à la défense de notre indépendance nationale au sens de l'article 5 de la Constitution de la V^{e} République ou à la sécurité nationale.

Le décret 2005-1739 du 30 décembre 2005 réglementant les relations financières avec l'étranger […] est venu ainsi définir en ses articles 2 et 3 des secteurs d'activité dont l'intérêt justifie la surveillance de leur financement au moyen d'investissements étrangers. Une telle définition peut, par analogie, représenter un travail d'approche qualitative des secteurs constituant les « éléments essentiels du potentiel scientifique et économique de la France ».

Prévention du terrorisme

Les textes en matière de police administrative renvoient pour ce motif au Livre IV du Code pénal et à l'article 421-1 qui incrimine spécialement certaines infractions quand celles-ci sont commises « intentionnellement en relation avec une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur ».

Quand l'infraction commise répond aux conditions posées par cet article, il en découle d'importantes conséquences au plan de la procédure et de la répression. Ainsi sont modifiés les régimes de la garde à vue et des perquisitions, les règles de compétence des juridictions et de composition du tribunal, les régimes de prescription de l'action publique et de la peine, le quantum des peines principales et complémentaires encourues. Compte tenu de l'ensemble des dispositions dérogatoires figurant notamment aux articles 421-1 et suivants du Code pénal, la qualification d'une infraction d'acte de terrorisme, au sens de l'article 421-1 du Code pénal, revêt une particulière gravité et doit correspondre à toutes les conditions posées dans la définition légale de l'incrimination.

Les infractions ne peuvent être qualifiées d'actes de terrorisme que si elles ont bien été commises intentionnellement en relation avec une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur. S'il est admis que l'acte peut être commis par un homme seul, il doit avoir été entrepris dans le but d'intimider ou de terroriser tout ou partie de la population.

Les termes de cette définition ont été précisés dans une circulaire du garde des Sceaux du 10 octobre 1986 (Crim. 86-21-F. 1) et reprise par la doctrine (*cf. Jurisclasseur pénal* rubrique «Terrorisme »).

Cette « entreprise », selon cette circulaire, qui reprend les interventions du garde des Sceaux à l'Assemblée nationale (*JO* du 8 août 1986, p. 4125) et au Sénat (*JO* du 8 août 1986, p. 3795 et 3796), suppose « l'existence d'un dessein formé ou d'un plan concerté se traduisant par des efforts coordonnés en vue de l'objectif à atteindre. La notion d'entreprise exclut l'improvisation ; elle suppose des préparatifs et un minimum d'organisation (établissement d'un plan d'action, rassemblement de moyens

matériels, mise en place d'un dispositif de repli, rédaction de communiqué de revendication) ».

Un certain nombre d'actes relevant de l'expression politique violente pourraient répondre à cette définition comme l'organisation d'incidents en fin de manifestations, le démontage ou le sac symbolique de locaux publics ou privés. Toutefois, pour recevoir la qualification de terroristes, ces actes doivent avoir été commis avec la volonté de troubler gravement l'ordre public par l'intimidation ou la terreur, la gravité du trouble consistant dans la peur collective que l'on cherche à répandre dans la population ou partie de celle-ci afin de promouvoir une cause ou faciliter le succès d'une revendication.

Force est de constater que n'importe quelle action d'expression ou de revendication politique extrême, même violente et susceptible de troubler l'ordre public, ne saurait être qualifiée de terroriste. À la limite, la menace qu'elle peut faire peser sur les personnes et les biens, s'agissant d'une entreprise organisée et planifiée utilisant des moyens virulents peut relever dans certaines circonstances précises de la « criminalité organisée ». Ainsi les « casseurs » qui profitent d'une manifestation politique relèvent-ils de la criminalité organisée dès lors qu'ils constituent un groupe structuré. En revanche, même ce dernier motif ne peut être invoqué pour justifier des interceptions de sécurité à l'encontre de personnes impliquées dans des mouvements politiques extrêmes, pour la seule raison qu'ils contestent radicalement les fondements de notre organisation politique ou économique. Les agissements de ces mouvements relèvent, en effet soit de poursuites pénales (provocations fondées sur des motivations raciales ou religieuses), soit du maintien de l'ordre public.

L'article L. 241-2 du Code de la sécurité intérieure (ancien article 3 de la loi du 10 juillet 1991) dispose que les interceptions de sécurité peuvent être autorisées pour la « prévention du terrorisme ». Les interceptions vont donc se situer en amont du passage à l'acte afin d'en empêcher la commission.

Il est possible d'autoriser la surveillance ciblée des individus les plus radicalisés afin de détecter à temps par exemple une dérive de type « brigadiste » sans entrer pour autant dans une police de l'opinion. Il faut caractériser une association de malfaiteurs en relation avec une entreprise terroriste en accumulant les indices sur la logistique mise en place (réseaux de financement fondés sur le don plus ou moins librement consenti, exploitation de commerces ne respectant pas la législation du travail, voire le crime organisé ; réseaux d'hébergement clandestin, d'infiltration ou d'exfiltration, caches d'armes, communauté de vie à caractère conspiratif) avant que celle-ci ne soit activée pour planifier un ou plusieurs attentats ou que ces faits ne relèvent de l'autorité judiciaire, seule compétente pour poursuivre ces faits. Il faut pouvoir autoriser la surveillance de terreaux ciblés, sur lesquels la pensée terroriste peut éclore (dérive communautariste à caractère sectaire et vindicatif,

endoctrinement de mineurs) sans porter atteinte à la liberté d'opinion telle que protégée par les articles 10 et 11 de la Déclaration des droits de l'homme de 1789.

La frontière est délicate à tracer *a priori*, alors que certains mouvements sont énumérés par les décisions du Conseil de l'Union européenne en la matière (15 juillet 2008 *JOCE* du 16 juillet), et repris par la position commune 2008/959 PESC du Conseil du 16 décembre 2008 (*JOCE* du 17 décembre).

Enfin la préparation en France d'actes à caractère terroriste devant être commis à l'étranger est susceptible comme telle de recevoir une qualification pénale (*cf.* article 113-2 al. 2 du Code pénal : « […] l'infraction est réputée commise sur le territoire de la République dès lors qu'un de ses faits constitutifs a eu lieu sur ce territoire ») et entre naturellement dans le champ de ce motif légal d'interception.

Prévention de la criminalité et de la délinquance organisées

Comme les chiffres le montrent depuis de nombreuses années, en dépit de l'acuité de la menace terroriste, le premier motif de demandes initiales d'interceptions de sécurité reste la prévention de la criminalité et de la délinquance organisées.

L'essentiel des dossiers concerne les grands trafics tels que la livraison attendue par mer, terre ou air de stupéfiants, l'escroquerie à travers la contrebande d'objets contrefaits ou le repérage en vue d'attaques d'établissements bancaires ou de transport de fonds, ou plus récemment encore l'économie souterraine.

Il apparaît aussi de plus en plus nettement que certains groupes activistes recourent volontiers à la criminalité de profit pour financer leurs filières et les attentats projetés. La Commission retient alors la finalité terroriste quand celle-ci est connue.

Ce concept, il y a peu, n'existait pas strictement à l'identique dans le Code pénal. Celui-ci traitait des infractions « commises en bande organisée ». La loi du 9 mars 2004 cependant a consacré dans le Livre quatrième du Code de procédure pénale un titre vingt-cinquième à la « procédure applicable à criminalité et à la délinquance organisée », concernant l'ensemble des infractions aggravées par la circonstance de commission en bande organisée (*cf.* article 706-73 du Code de procédure pénale).

Il est donc permis de dire que le champ couvert aujourd'hui par l'article 706-73 du Code de procédure pénale recouvre désormais totalement celui couvert par l'article L. 241-2 du Code la sécurité intérieure (ancien article 3 de la loi du 10 juillet 1991).

La CNCIS a très tôt apporté dans son rapport public une définition de ce motif au regard des interceptions de sécurité (*cf.* rapport 1994, p. 18 ; rapport 1995, p. 30). Elle a rappelé que cette définition résultait de celle retenue par la Commission Schmelck chargée de proposer un cadre légal aux interceptions de sécurité, et par le Code pénal, notamment dans son article 132-71.

La Commission Schmelck, dont les travaux sont à l'origine de la loi du 10 juillet 1991, envisageait de légaliser les interceptions de sécurité pour « la prévention du grand banditisme et du crime organisé ». Elle entendait par là se référer à des infractions qui avaient justifié, au plan administratif, la création d'offices spécialisés tels que l'Office central pour la répression du banditisme (OCRB). La Commission entendait par là faciliter la lutte en amont contre la grande criminalité.

L'article 132-71 du Code pénal, en définissant les circonstances aggravantes de certains crimes et délits, caractérise la bande organisée comme « tout groupement formé ou toute entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou plusieurs infractions ». Cette définition est également celle de l'association de malfaiteurs.

À l'entrée en vigueur du nouveau Code pénal, les infractions pour lesquelles pouvait être retenue la circonstance aggravante de commission en bande organisée étaient relativement réduites et concernaient les formes graves du banditisme (trafic de stupéfiants, proxénétisme, enlèvement, racket, etc.).

Depuis le 1er mars 1994, la liste s'est allongée, spécialement avec l'entrée en vigueur de la loi n° 2004-204 du 9 mars 2004 (dite Perben II) et des lois qui, depuis, sont venues la compléter.

« La plus redoutable menace – disait en 2004 le garde des Sceaux de l'époque – est celle du crime organisé dans ses formes diverses. À ceux qui choisissent délibérément de s'organiser dans le crime, la société doit répondre par une vigoureuse fermeté pénale. » Criminalité et délinquance organisées et infractions aggravées par la circonstance de commission en bande organisée sont donc bien des notions similaires.

La bande organisée est le groupement, la réunion de plusieurs malfaiteurs. L'élément constitutif qui, au plan pénal, va permettre de distinguer la commission en bande organisée de la simple réunion, c'est, précisément, l'organisation. Dans la simple réunion, il n'y a ni hiérarchie, ni distribution des rôles, ni entente préalable en vue de commettre des infractions. La réunion est fortuite, elle est une action collective inorganisée.

La commission en bande organisée suppose au contraire la préméditation. Elle suppose également un nombre de personnes supérieur à deux, chiffre qui suffit en revanche à caractériser la réunion.

Cette définition correspond à l'approche internationale du phénomène criminel organisé.

Ainsi, la convention des Nations unies contre la criminalité transnationale dite « convention de Palerme » du 15 novembre 2000, signée par la France le 12 décembre 2000 et ratifiée le 29 octobre 2002 stipule que :
– l'expression « groupe criminel organisé » désigne un groupe structuré de trois personnes ou plus existant depuis un certain temps et agissant de concert dans le but de commettre une ou plusieurs infractions graves pour en tirer directement ou indirectement un avantage financier ou un autre avantage matériel ;
– l'expression « infraction grave » désigne un acte constituant une infraction passible d'une peine privative de liberté dont le maximum ne doit pas être inférieur à quatre ans ou d'une peine plus lourde ;
– l'expression « groupe structuré » désigne un groupe qui ne s'est pas constitué au hasard pour commettre immédiatement une infraction et qui n'a pas nécessairement de rôles formellement définis pour ses membres, de continuité dans sa composition ou de structure élaborée.

Cette intégration de critères internationaux retenus dans la définition de la criminalité organisée (et notamment le nombre minimal de participants fixé à trois) a fait l'objet d'une « validation » par le Conseil constitutionnel lors de sa décision du 2 mars 2004 (considérants 13 et 14) relative à l'examen de la notion de criminalité organisée dans la loi du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité.

Pénalement, la circonstance de commission en bande organisée aggrave sensiblement plus les faits que la circonstance de simple réunion. Ainsi, le vol en réunion est puni de sept ans d'emprisonnement et le vol en bande organisée de quinze ans de réclusion criminelle (article 311-9 du Code pénal).

Ce qui caractérise par conséquent la « criminalité et la délinquance organisées », c'est à la fois la gravité des peines encourues et le degré d'organisation, notamment le nombre de personnes sciemment impliquées dans le processus criminel.

La majeure partie des projets d'interceptions soumis à la Commission répond effectivement à ces critères. Marginalement toutefois, la Commission note que quelques demandes ne relèvent pas d'une gravité manifeste. Dans ces hypothèses, le caractère organisé au sens de l'article 132-71 du Code pénal n'est pas avéré et relève plus, tant par le faible degré d'entente que par le faible nombre de participants – au titre desquels on ne saurait ranger les « clients » dans, par exemple, l'hypothèse d'une revente de produits stupéfiants – d'une qualification de commission en réunion. En revanche, le nombre de clients estimés ou les quantités vendues sont un bon indice de la gravité des faits supposés.

L'organisation ne doit pas cependant être nécessairement totalement « professionnelle ». Le réseau constitué d'un fournisseur, de plusieurs « dealers », chacun responsable de son territoire, et de petits guetteurs bénévoles, entre bien dans la qualification de groupe criminel organisé au même titre que le cartel international de type mafieux.

La Commission a toujours réservé le recours à ce motif légal à des agissements d'une gravité certaine, souvent tendus par la recherche d'un avantage financier ou matériel et menés par de véritables structures organisées composées de plus de deux acteurs, participant d'une entente préalable caractérisant une préméditation criminelle et écartant de fait la commission fortuite d'une infraction à la faveur de la circonstance aggravante de réunion.

Ici encore, la position de la Commission représente une synthèse des dispositifs pénaux qui sont venus constituer le droit positif applicable à cette matière :
– notion de bande organisée au sens de l'article 132-71 du Code pénal ;
– notion d'association de malfaiteurs au sens de l'article 450-1 du Code pénal ;
– notion de « criminalité organisée » au sens de la loi du 9 mars 2004 précitée.

Sur le fondement de ces définitions de la bande organisée et de l'association de malfaiteurs, constatant le caractère exceptionnel de certains projets criminels ainsi que la gravité des atteintes aux intérêts fondamentaux de la Nation, la Commission plénière a émis un avis favorable pour les demandes portant sur des objectifs susceptibles de commettre des infractions dont la nature et les conditions de leur commission, pouvaient porter atteinte à la vie et à la santé publique, alors que ces infractions ne sont explicitement visées par l'article 706-73 du Code de procédure pénale.

L'ampleur du trafic, les modalités de commission des infractions projetées (notamment leur aspect international) les intérêts mis en cause par ces infractions, strictement identiques à ceux protégés par les incriminations de l'article 706-73, ont fondé cet avis de la Commission, en ce que les faits revêtent un caractère exceptionnel visé par la loi pour autoriser une interception de sécurité. S'agissant d'une menace particulièrement grave, et en l'absence d'autres moyens de recueil de renseignements, ces demandes sont conformes aux principes de proportionnalité et de subsidiarité régissant les mesures d'investigation spéciales comme l'interception de sécurité, définies par la loi.

Chapitre II

Avis et préconisations de la Commission portant sur les demandes en matière d'interceptions de sécurité et de recueil des données techniques de communications

♦ Préalablement, il convient de rappeler le champ des demandes relevant du régime de protection des lois du 10 juillet 1991 et du 23 janvier 2006. À ce titre, elles relèvent des avis et du contrôle de la CNCIS.

Concernant ce champ d'application, la commission en a régulièrement rappelé les limites par référence aux dispositions de l'article 20 de la loi du 10 juillet 1991 devenu l'article L. 241-3 du Code de la sécurité intérieure.

Par cet article, le législateur a entendu réserver une exception au principe du contrôle des interceptions de sécurité et du recueil des données techniques de communication par la CNCIS, en ce que les mesures mises en œuvre sur le fondement de cet article, s'inscrivent dans le cadre de la mission de surveillance générale du domaine radio électrique, par opérations aléatoires de balayage des fréquences, pour la défense des intérêts nationaux. « Ces techniques réalisées dans le cadre de la mission générale de défense et ne visant pas de communications individualisables ne peuvent être considérées comme des ingérences de l'autorité

publique dans l'exercice par toute personne de son droit au respect de sa correspondance au sens de l'article 8 de la CEDH » (Commission des lois du Sénat 19 juin 1991).

La Commission a rappelé la primauté du principe de libertés publiques sur l'évolution technique en indiquant que l'exception à son contrôle prévue par l'article 20 devait s'interpréter strictement : «Toute interception de correspondance échangée par la voie des télécommunications, qui n'entre pas dans le champ de l'article 20, est soumise quel que soit le mode de transmission filaire ou hertzien aux conditions et aux procédures fixées par la loi du 10 juillet 1991 ».

♦ Le contenu et la forme des demandes ainsi que la nature des contrôles varient selon qu'il s'agit d'interceptions du contenu des communications électroniques ou de recueillir les données techniques de ces correspondances, soit le contenant ou l'accessoire de la communication.

Les données techniques ne relèvent pas du même régime de protection en ce qu'elles ne permettent pas d'accéder et de connaître le contenu des correspondances et sont, à ce titre, moins attentatoires au secret des correspondances privées.

Pour ce qui concerne la Commission et le contrôle qu'elle exerce sur ce type de données, deux cadres légaux distincts sont mis en œuvre :
– l'article L. 244-2 du Code de la sécurité intérieure (ancien article 22 de la loi du 10 juillet 1991) pour l'ensemble des atteintes à la sécurité et aux intérêts fondamentaux prévus par la loi ;
– l'article 6 de la loi du 23 janvier 2006 permettant l'accès à ce type de mesure pour la seule prévention des actes de terrorisme et pour les services du ministère de l'Intérieur.

La CNCIS a, sur le fondement des dispositions de ces articles, défini une procédure de contrôle reposant sur les principes suivants :
– la centralisation, le traitement et la validation, par le groupement interministériel de contrôle pour les demandes fondées sur l'article L. 244-2 du Code de la sécurité intérieure, par la personnalité qualifiée pour les demandes relevant de l'article 6 de la loi du 23 janvier 2006 ;
– le contrôle *a posteriori* hebdomadaire de l'intégralité de ces demandes par la CNCIS ;
– la possibilité pour le GIC comme pour la personnalité qualifiée de solliciter des renseignements complémentaires, et pour la Commission de recourir aux avis, aux recommandations, et aux droits de suite comme en matière d'interceptions de sécurité.

Les mesures sont classées selon la nature des informations qu'elles permettent de recueillir et l'importance de leur caractère intrusif dans la correspondance et la vie privées. Les exigences de rédaction, d'informations et de motivation des demandes sont déclinées en fonction de cette classification. Elles sont graduées en fonction de la catégorie des données concernées, selon qu'il s'agit de simples mesures d'identification ou de recueillir l'historique la localisation des cellules ou le détail du trafic.

La nature des contrôles exercés par la Commission pour chaque requête portant sur les données techniques de communication, est définie par rapport à cette classification et selon l'étendue de l'intrusion dans le contenant et les accessoires de la communication électronique.

Néanmoins, les principes généraux retenus pour les demandes d'interceptions de sécurité sont appliqués au recueil des données techniques de communication, tant en ce qui concerne la forme que le fond de la requête.

Les critères de la motivation de la demande

Chaque semaine, la Commission est amenée à donner son avis sur plus d'une centaine de demandes de construction et de renouvellement d'interceptions de sécurité. En outre, et comme cela a déjà été indiqué dans les éléments chiffrés relatant son activité, elle statue quotidiennement sur des demandes présentées sous la forme de l'urgence absolue.

Dans le cadre de l'élaboration de ses avis, la Commission examine plus particulièrement au niveau des motivations les critères principaux suivants :
– la qualification juridique des faits au regard des motifs légaux ;
– les présomptions d'implication directe et personnelle de l'objectif dans les projets d'atteintes et d'infractions ou les menaces ;
– la proportionnalité qui permet de mesurer le rapport entre le but recherché et l'action sollicitée. La gravité du risque et l'importance des intérêts en jeu doivent être à la mesure de l'atteinte à la vie privée que constitue la surveillance de la correspondance par voie de communications électroniques ou l'exploitation des données de correspondances électroniques, et la justifier pleinement ;
– la subsidiarité qui permet de s'assurer de l'absolue nécessité de recourir matériellement à l'interception ou au recueil de données techniques de communication, et de vérifier que le but recherché ne peut pas être aussi bien atteint par d'autres moyens.

Il résulte de l'application de ces critères que la motivation doit être suffisante, pertinente et sincère.

Une motivation suffisante

La motivation doit être suffisante en quantité, mais aussi en qualité :

- En quantité

Quelques lignes ne sauraient suffire. Les développements doivent permettre de cerner la personnalité de la cible, de développer un minimum les soupçons qui pèsent sur elle, et d'expliquer la nature et la gravité du danger qu'elle fait courir à la sécurité de l'État et aux citoyens.

Ces informations permettent également à la Commission d'opérer un contrôle sur l'articulation juridique entre des éléments factuels relevant du comportement de la cible et le motif légal d'interception invoqué par le service.

Dans la majorité des cas, les « renseignements complémentaires » fournis à la demande de la Commission emporteront la conviction de cette dernière qui déplore dès lors une information initiale insuffisante.

• En qualité

La motivation doit absolument :
– faire ressortir les présomptions d'implication directe et personnelle de la cible. Quel que soit le motif, l'implication directe et personnelle de l'objectif dans des agissements attentatoires à notre sécurité, doit être présumée ;
– ne pas se référer à un comportement purement hypothétique de celle-ci ou à des comportements généraux de groupements auxquels appartiendrait l'objectif.

Ainsi une demande trop éloignée d'une implication directe et personnelle de la cible dans des faits participant du motif invoqué peut recevoir un avis négatif comme par exemple une demande où la démonstration de cette implication ne repose que sur un « relationnel » avec d'autres individus.

Une motivation pertinente

L'examen de cette pertinence porte sur trois points :
– la motivation doit être exclusivement tournée vers la vocation préventive voulue par le législateur de 1991 pour les interceptions de sécurité. Outil de renseignement, ces mêmes interceptions ne peuvent être utilisées pour l'élucidation de faits passés relevant de l'autorité judiciaire ;
– corrélativement, la motivation doit exclusivement se référer à des investigations participant de l'activité de renseignement et en aucun cas pouvoir générer un « risque d'interférence » avec une action judiciaire déjà déclenchée ;
– enfin, les soupçons qui pèsent sur la cible doivent nécessairement être en relation directe avec le motif. Ainsi un comportement dont la description reste floue, vague, imprécise et non « rattachable » au travail d'articulation juridique déjà décrit prive la demande de toute pertinence.

La Commission a poursuivi son inscription dans une volonté de dialogue avec les services demandeurs. Cette démarche s'est traduite par une nette augmentation des réunions bilatérales avec ces mêmes services. Elle s'est également matérialisée, au stade de l'examen de leurs demandes, par une logique d'avis moins binaire (avis favorable/défavorable). De fait, le nombre d'observations a encore crû, comme les demandes de renseignements complémentaires et les limitations de la durée d'interception sollicitée. Les avis défavorables sont stabilisés à

une cinquantaine par an. À ce chiffre des avis défavorables « bruts », il convient d'ajouter deux techniques d'observation déjà répertoriées dans le rapport d'activité 2008 qui peuvent s'apparenter à « l'avis négatif » :

• La recommandation adressée au Premier ministre visant à l'interruption de l'interception en cours d'exploitation qui résulte de l'examen exhaustif des « productions » (transcriptions) opérées à partir d'une interception. Il y est fait recours une dizaine de fois par an. Elles ont toutes été suivies par le Premier ministre.

• La « préconisation d'interruption » adressée par la Commission au service utilisateur en cours d'exploitation. Elle résulte du même examen des productions et procède d'un dialogue constructif mené directement avec les services utilisateurs à « abandonner ». Cela concerne une soixantaine de mesures par an.

Une motivation sincère

Il importe aussi de s'assurer que le motif légal invoqué ne dissimule pas d'autres préoccupations ou des objectifs non visés par la loi. L'interception doit être sollicitée exclusivement pour les faits articulés, et non pour une raison autre qui ne relèverait d'aucun motif légal, quelle que soit par ailleurs la véracité des faits rapportés. C'est la notion de demande sincère.

Le mensonge caractérisé et délibéré dans la présentation des motifs de la demande entraîne l'illégalité de l'interception qui serait autorisée par le Premier ministre à la suite de l'avis rendu par la Commission sur le fondement d'informations mensongères et dont les véritables objectifs seraient dissimulés.

Le caractère illégal de l'interception et les suites pénales qui sont susceptibles d'en découler en matière d'atteintes au secret des correspondances sont identiques lorsque certaines informations soutenant la demande sont partiellement exactes, sont amplifiées, ou lorsque des hypothèses ou des soupçons sont présentées comme des faits établis. La Commission rappelle que s'agissant de police administrative préventive, la loi exige des présomptions d'implication. Quand les atteintes sont certaines et établies, le recours au dispositif administratif est exclu. Les poursuites pénales sont exclusives, tel que le rappelle le Conseil constitutionnel lorsqu'il souligne « la primauté de l'autorité judiciaire ».

Troisième partie

ÉTUDES ET DOCUMENTS

Chapitre I

Présentation ordonnée des textes relatifs aux missions de la Commission

Première mission : les interceptions de communications

Avant de reproduire certaines dispositions spécifiques ou communes aux différents types d'interception, il convient de rappeler le principe du secret des correspondances émises par la voie des « communications électroniques » posé par l'article 1er de la loi n° 91-646 du 10 juillet 1991, devenu depuis l'entrée en vigueur du Code de la sécurité intérieure l'article L. 241-1 : « Le secret des correspondances émises par la voie des communications électroniques est garanti par la loi. Il ne peut être porté atteinte à ce secret que par l'autorité publique, dans les seuls cas de nécessité d'intérêt public prévus par la loi et dans les limites fixées par celle-ci. »

Les interceptions légales de correspondances émises par la voie des « communications électroniques » sont de deux types, judiciaires et de sécurité.

S'agissant des interceptions judiciaires, le pluriel est employé à dessein depuis l'entrée en vigueur des lois n° 2002-1138 du 9 septembre 2002 et 2004-204 du 9 mars 2004, modifiée dernièrement par la loi n° 2011-267 du 11 mars 2011.

En effet, aux interceptions en matière criminelle et correctionnelle prévues par les articles 100 à 100-7 du Code de procédure pénale, s'ajoutent celles prévues par les dispositions suivantes du même code :
– article 74-2 (recherche d'une personne en fuite) ;
– article 80-4 (recherche des causes de la mort ou d'une disparition présentant un caractère inquiétant) ;
– article 706-95 (criminalité et délinquance organisées) ;
– article 727-1 (écoute, enregistrement et interruption des conversations téléphoniques des détenus).

Pour des raisons de clarté de présentation les dispositions relatives à ces interceptions seront présentées à la suite de celles des articles 100 à 107 du Code de procédure pénale auxquels elles renvoient même si elles ne faisaient pas explicitement partie du titre Ier de la loi de 1991, et ne figurent pas dans le Code de la sécurité intérieure.

La loi n° 91-646 du 10 juillet 1991 (abrogée depuis le 1er mai 2012 conformément à l'article 19, *20°*, de l'ordonnance n° 2012-351 du 12 mars 2012)

Il s'agit d'une loi fondatrice en matière de protection de secret des correspondances. Elle a créé la Commission nationale de contrôle des interceptions de sécurité.

Titre I (de la loi n° 91-646 du 10 juillet 1991 consolidée) :
DES INTERCEPTIONS ORDONNÉES PAR L'AUTORITÉ JUDICIAIRE

Les interceptions ordonnées en matière criminelle et correctionnelle

Code de procédure pénale

Livre Ier : De l'exercice de l'action publique et de l'instruction

Titre III : Des juridictions d'instruction

Chapitre Ier : Du juge d'instruction : juridiction d'instruction du premier degré

Section III : Des transports, des perquisitions, des saisies et des interceptions de correspondances émises par la voie des télécommunications

Sous-section II : Des interceptions de correspondances émises par la voie des télécommunications

Article 100 – « En matière criminelle et en matière correctionnelle, si la peine encourue est égale ou supérieure à deux ans d'emprisonnement, le juge d'instruction peut, lorsque les nécessités de l'information l'exigent, prescrire l'interception, l'enregistrement et la transcription de correspondances émises par la voie des télécommunications. Ces opérations sont effectuées sous son autorité et son contrôle.

La décision d'interception est écrite. Elle n'a pas de caractère juridictionnel et n'est susceptible d'aucun recours. »

Article 100-1 – « La décision prise en application de l'article 100 doit comporter tous les éléments d'identification de la liaison à intercepter, l'infraction qui motive le recours à l'interception ainsi que la durée de celle-ci. »

Article 100-2 – « Cette décision est prise pour une durée maximum de quatre mois. Elle ne peut être renouvelée que dans les mêmes conditions de forme et de durée. »

Article 100-3 – « Le juge d'instruction ou l'officier de police judiciaire commis par lui peut requérir tout agent qualifié d'un service ou organisme placé sous l'autorité ou la tutelle du ministre chargé des Télécommunications ou tout agent qualifié d'un exploitant de réseau ou fournisseur de services de télécommunications autorisé, en vue de procéder à l'installation d'un dispositif d'interception. »

Article 100-4 – « Le juge d'instruction ou l'officier de police judiciaire commis par lui dresse procès-verbal de chacune des opérations d'interception et d'enregistrement. Ce procès-verbal mentionne la date et l'heure auxquelles l'opération a commencé et celles auxquelles elle s'est terminée.

Les enregistrements sont placés sous scellés fermés. »

Article 100-5 – « Le juge d'instruction ou l'officier de police judiciaire commis par lui transcrit la correspondance utile à la manifestation de la vérité. Il en est dressé procès-verbal. Cette transcription est versée au dossier.

Les correspondances en langue étrangère sont transcrites en français avec l'assistance d'un interprète requis à cette fin.

À peine de nullité, ne peuvent être transcrites les correspondances avec un avocat relevant de l'exercice des droits de la défense.

À peine de nullité, ne peuvent être transcrites les correspondances avec un journaliste permettant d'identifier une source en violation de l'article 2 de la loi du 29 juillet 1881 sur la liberté de la presse. »

Article 100-6 – « Les enregistrements sont détruits, à la diligence du procureur de la République ou du procureur général, à l'expiration du délai de prescription de l'action publique.

Il est dressé procès-verbal de l'opération de destruction. »

Article 100-7 – (*loi n° 95-125 du 8 février 1995)* – « Aucune interception ne peut avoir lieu sur la ligne d'un député ou d'un sénateur sans que le président de l'assemblée à laquelle il appartient en soit informé par le juge d'instruction.

Aucune interception ne peut avoir lieu sur une ligne dépendant du cabinet d'un avocat ou de son domicile sans que le bâtonnier en soit informé par le juge d'instruction. »

• Loi n° 93-1013 du 24 août 1993. « Les formalités prévues par le présent article sont prescrites à peine de nullité. »

Les interceptions ordonnées pour recherche d'une personne en fuite

Code de procédure pénale

Livre Ier : De l'exercice de l'action publique et de l'instruction

Titre II : Des enquêtes de contrôle d'identité

Chapitre Ier : Des crimes et des délits flagrants

Article 74-2 – « Les officiers de police judiciaire, assistés le cas échéant des agents de police judiciaire, peuvent, sur instructions du procureur de la République, procéder aux actes prévus par les articles 56 à 62 aux fins de rechercher et de découvrir une personne en fuite dans les cas suivants :

1) Personne faisant l'objet d'un mandat d'arrêt délivré par le juge d'instruction, le juge des libertés et de la détention, la chambre de l'instruction ou son président ou le président de la cour d'assises, alors qu'elle est renvoyée devant une juridiction de jugement.

2) Personne faisant l'objet d'un mandat d'arrêt délivré par une juridiction de jugement ou par le juge de l'application des peines.

3) Personne condamnée à une peine privative de liberté sans sursis supérieure ou égale à un an, lorsque cette condamnation est exécutoire ou passée en force de chose jugée. »

Si les nécessités de l'enquête pour rechercher la personne en fuite l'exigent, le juge des libertés et de la détention du tribunal de grande instance peut, à la requête du procureur de la République, autoriser l'interception, l'enregistrement et la transcription de correspondances émises par la voie des télécommunications selon les modalités prévues par les articles 100, 100-1 et 100-3 à 100-7, pour une durée maximale de deux mois renouvelable dans les mêmes conditions de forme et de durée, dans la limite de six mois en matière correctionnelle. Ces opérations sont faites sous l'autorité et le contrôle du juge des libertés et de la détention […]. »

NB : les articles 695-36 et 696-21 du Code de procédure pénale étendent respectivement les dispositions de l'article 74-2 du même code au mandat d'arrêt européen et à la procédure d'extraction (*cf.* article 39 V et VI de la loi 2005-1549 du 12 décembre 2005 relative au traitement de la récidive des infractions pénales).

Les interceptions ordonnées pendant le déroulement de l'information pour recherche des causes de la mort ou d'une disparition de mineur, de majeur protégé ou présentant un caractère inquiétant

Code de procédure pénale (loi n° 2002-1138 du 9 septembre 2002, article 66)

Livre Ier : De l'exercice de l'action publique et de l'instruction

Titre III : Des juridictions d'instruction

Chapitre Ier : Du juge d'instruction : juridiction d'instruction du premier degré

Section I : Dispositions générales

Article 80-4 – « Pendant le déroulement de l'information pour recherche des causes de la mort ou des causes d'une disparition mentionnée aux articles 74 et 74-1, le juge d'instruction procède conformément aux dispositions du chapitre 1er du titre III du Livre Ier. Les interceptions de correspondances émises par la voie des télécommunications sont effectuées sous son autorité et son contrôle dans les conditions prévues au deuxième alinéa de l'article 100 et aux articles 100-1 à 100-7. Les interceptions ne peuvent excéder une durée de deux mois renouvelable.

Les membres de la famille ou les proches de la personne décédée ou disparue peuvent se constituer partie civile à titre incident. Toutefois, en cas de découverte de la personne disparue, l'adresse de cette dernière et les pièces permettant d'avoir directement ou indirectement connaissance de cette adresse ne peuvent être communiquées à la partie civile qu'avec l'accord de l'intéressé s'il s'agit d'un majeur et qu'avec l'accord du juge d'instruction s'il s'agit d'un mineur ou d'un majeur protégé. »

Les interceptions ordonnées en matière de criminalité et délinquance organisées

Code de procédure pénale

Livre IV : De quelques procédures particulières

Titre XXV : De la procédure applicable à la criminalité et à la délinquance organisées

Chapitre II : Procédure

Section V : Des interceptions de correspondances émises par la voie des télécommunications

Article 706-95 – « Si les nécessités de l'enquête de flagrance ou de l'enquête préliminaire relative à l'une des infractions entrant dans le champ d'application de l'article 706-73 l'exigent, le juge des libertés et

de la détention du tribunal de grande instance peut, à la requête du procureur de la République, autoriser l'interception, l'enregistrement et la transcription de correspondances émises par la voie des télécommunications selon les modalités prévues par les articles 100 deuxième alinéa, 100-1 et 100-3 à 100-7, pour une durée maximum d'un mois (*), renouvelable une fois dans les mêmes conditions de forme et de durée.

Ces opérations sont faites sous le contrôle du juge des libertés et de la détention […]. »

(*) La loi n° 2011-267 du 11 mars 2011 a fait passer la durée légale de quinze jours à un mois, renouvelable une fois.

Les interceptions prévues par l'article 727-1 du Code de procédure pénale

Code de procédure pénale

Livre V : Des procédures d'exécution

Titre II : De la détention

Chapitre III : Des dispositions communes aux différents établissements pénitentiaires

Article 727-1 – Créé par la loi n° 2007-297 du 5 mars 2007 – article 72 *JORF* du 7 mars 2007

« Aux fins de prévenir les évasions et d'assurer la sécurité et le bon ordre des établissements pénitentiaires ou des établissements de santé habilités à recevoir des détenus, les communications téléphoniques que les personnes détenues ont été autorisées à passer peuvent, à l'exception de celles avec leur avocat, être écoutées, enregistrées et interrompues par l'administration pénitentiaire sous le contrôle du procureur de la République territorialement compétent, dans des conditions et selon des modalités qui sont précisées par décret.

Les détenus ainsi que leurs correspondants sont informés du fait que les conversations téléphoniques peuvent être écoutées, enregistrées et interrompues.

Les enregistrements qui ne sont suivis d'aucune transmission à l'autorité judiciaire en application de l'article 40 ne peuvent être conservés au-delà d'un délai de trois mois. »

Article D. 419-3 – Créé par le décret n° 2007-699 du 3 mai 2007 – article 11 *JORF* du 5 mai 2007

« Conformément aux dispositions de l'article 727-1, les conversations téléphoniques, à l'exception de celles avec les avocats, peuvent, sous la responsabilité du chef d'établissement, être écoutées, enregistrées et interrompues par le personnel de surveillance désigné à cet effet.

Dans les maisons centrales, les conversations téléphoniques peuvent être enregistrées de façon systématique.

L'information du détenu et de son correspondant relative à ces contrôles est faite au début de la conversation, le cas échéant par un message préenregistré.

Les conversations téléphoniques peuvent faire l'objet d'une interruption lorsque leur contenu est de nature à compromettre l'un des impératifs énoncé au troisième alinéa de l'article D. 419-1.

Les conversations en langue étrangère peuvent être traduites aux fins de contrôle.

La transmission au procureur de la République des conversations susceptibles de constituer ou de faciliter la commission d'un crime ou d'un délit est effectuée immédiatement, au moyen d'une retranscription sur support papier. Si les communications concernent une personne mise en examen, copie en est adressée au juge d'instruction saisi.

Les enregistrements sont conservés pour une durée maximum de trois mois.

Pendant cette durée, seuls le chef d'établissement et les membres du personnel de surveillance qu'il habilite à cet effet peuvent avoir accès à ces enregistrements, sous réserve des dispositions du dernier alinéa.

La destruction des enregistrements qui n'ont pas été transmis à l'autorité judiciaire est effectuée à l'expiration du délai de trois mois sous la responsabilité du chef d'établissement.

Le procureur de la République peut procéder sur place, à tout moment, au contrôle du contenu des enregistrements conservés. Il peut ordonner leur destruction si leur conservation ne lui paraît plus nécessaire, après en avoir informé le chef d'établissement. »

Titre II (de la loi n° 91-646 du 10 juillet 1991 consolidée) :
DES INTERCEPTIONS DE SÉCURITÉ

Article 3 – « Peuvent être autorisées, à titre exceptionnel, dans les conditions prévues par l'article 4, les interceptions de correspondances émises par la voie des "communications électroniques" (loi n° 2004-669 du 9 juillet 2004) ayant pour objet de rechercher des renseignements intéressant la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, ou la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous en application de la loi du 10 janvier 1936 sur les groupes de combat et les milices privées. »

Article 4 – *modifié par l'article 6 II de la loi n° 2006-64 du 23 janvier 2006* –

« L'autorisation est accordée par décision écrite et motivée du Premier ministre ou de l'une des deux personnes spécialement déléguées par lui. Elle est donnée sur proposition écrite et motivée du ministre de la Défense, du ministre de l'Intérieur ou du ministre chargé des Douanes, ou de l'une des deux personnes que chacun d'eux aura spécialement déléguée.

Le Premier ministre organise la centralisation de l'exécution des interceptions autorisées. »

Article 5 – « Le nombre maximum des interceptions susceptibles d'être pratiquées simultanément en application de l'article 4 est arrêté par le Premier ministre.

La décision fixant ce contingent et sa répartition entre les ministères mentionnés à l'article 4 est portée sans délai à la connaissance de la Commission nationale de contrôle des interceptions de sécurité. »

Article 6 – « L'autorisation mentionnée à l'article 3 est donnée pour une durée maximum de quatre mois. Elle cesse de plein droit de produire effet à l'expiration de ce délai. Elle ne peut être renouvelée que dans les mêmes conditions de forme et de durée. »

Article 7 – « Dans les correspondances interceptées, seuls les renseignements en relation avec l'un des objectifs énumérés à l'article 3 peuvent faire l'objet d'une transcription.

Cette transcription est effectuée par les personnels habilités. »

Article 8 – « Il est établi, sous l'autorité du Premier ministre, un relevé de chacune des opérations d'interception et d'enregistrement. Ce relevé mentionne la date et l'heure auxquelles elle a commencé et celles auxquelles elle s'est terminée. »

Article 9 – « L'enregistrement est détruit sous l'autorité du Premier ministre, à l'expiration d'un délai de dix jours au plus tard à compter de la date à laquelle il a été effectué. Il est dressé procès-verbal de cette opération. »

Article 10 – « Sans préjudice de l'application du deuxième alinéa de l'article 40 du Code de procédure pénale, les renseignements recueillis ne peuvent servir à d'autres fins que celles mentionnées à l'article 3. »

Article 11 – « Les opérations matérielles nécessaires à la mise en place des interceptions dans les locaux et installations des services ou organismes placés sous l'autorité ou la tutelle du ministre chargé des "Communications électroniques" ou des exploitants de réseaux ou fournisseurs de services de "communications électroniques" ne peuvent être effectuées que sur ordre du ministre chargé des "Communications électroniques" ou sur ordre de la personne spécialement déléguée par

lui, par des agents qualifiés de ces services, organismes, exploitants ou fournisseurs dans leurs installations respectives. »

Article 11-1 – *(introduit par l'article 31 de la loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne)* – « Les personnes physiques ou morales qui fournissent des prestations de cryptologie visant à assurer une fonction de confidentialité sont tenues de remettre aux agents autorisés dans les conditions prévues à l'article 4, sur leur demande, les conventions permettant le déchiffrement des données transformées au moyen des prestations qu'elles ont fournies. Les agents autorisés peuvent demander aux fournisseurs de prestations susmentionnés de mettre eux-mêmes en œuvre ces conventions, sauf si ceux-ci démontrent qu'ils ne sont pas en mesure de satisfaire à ces réquisitions.

Le fait de ne pas déférer, dans ces conditions, aux demandes des autorités habilitées est puni de deux ans d'emprisonnement et de 30 000 euros d'amende.

Un décret en Conseil d'État précise les procédures suivant lesquelles cette obligation est mise en œuvre ainsi que les conditions dans lesquelles la prise en charge financière de cette mise en œuvre est assurée par l'État. »

Article 12 – « Les transcriptions d'interceptions doivent être détruites dès que leur conservation n'est pas indispensable à la réalisation des fins mentionnées à l'article 3.

Il est dressé procès-verbal de l'opération de destruction.

Les opérations mentionnées aux alinéas précédents sont effectuées sous l'autorité du Premier ministre. »

Article 13 – « Il est institué une Commission nationale de contrôle des interceptions de sécurité. Cette Commission est une autorité administrative indépendante. Elle est chargée de veiller au respect des dispositions du présent titre. Elle 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'État et le premier président de la Cour de cassation.

Elle comprend, en outre :
– un député désigné pour la durée de la législature par le président de l'Assemblée nationale ;
– un sénateur désigné après chaque renouvellement partiel du Sénat par le président du Sénat.

La qualité de membre de la Commission est incompatible avec celle de membre du Gouvernement. Sauf démission, il ne peut être mis fin aux fonctions de membre de la Commission qu'en cas d'empêchement constaté par celle-ci. Le mandat des membres de la Commission n'est pas renouvelable. En cas de partage des voix, la voix du président est prépondérante. Les agents de la Commission sont nommés par le président.

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. À l'expiration de ce mandat, par dérogation au septième alinéa ci-dessus, ils peuvent être nommés comme membre de la Commission s'ils ont occupé ces fonctions de remplacement pendant moins de deux ans.

Les membres de la Commission sont astreints au respect des secrets protégés par les articles 226-13, 226-14 et 413-10 du Code pénal pour les faits, actes ou renseignements dont ils ont pu avoir connaissance en raison de leurs fonctions. La Commission établit son règlement intérieur. »

Article 14 – « 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 Commission nationale de contrôle des interceptions de sécurité.

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 adresse au Premier ministre une recommandation tendant à ce que cette interception soit interrompue.

Elle porte également cette recommandation à la connaissance du ministre ayant proposé l'interception et du ministre chargé des "Communications électroniques".

La Commission peut adresser au Premier ministre une recommandation relative au contingent et à sa répartition visée à l'article 5.

Le Premier ministre informe sans délai la Commission des suites données à ses recommandations. »

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.

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 cette interception soit interrompue.

Il est alors procédé ainsi qu'il est indiqué aux quatrième et sixième alinéas de l'article 14. »

Article 16 – « Les ministres, les autorités publiques, les agents publics doivent prendre toutes mesures utiles pour faciliter l'action de la Commission. »

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.

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 contrôle effectué en application de l'article 15. »

Article 18 – « Les crédits nécessaires à la Commission nationale de contrôle des interceptions de sécurité pour l'accomplissement de sa mission sont inscrits au budget des services du Premier ministre. »

Article 19 – *modifié par l'article 6 de la loi n° 2006-64 du 23 janvier 2006* – « La Commission remet chaque année au Premier ministre un rapport sur les conditions d'exercice et les résultats de son activité, qui précise notamment le nombre de recommandations qu'elle a adressées au Premier ministre en application de l'article 14 de la présente loi et au ministre de l'Intérieur en application de l'article L. 34-1-1 du Code des postes et des communications électroniques et de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, ainsi que les suites qui leur ont été données. Ce rapport est rendu public.

Elle adresse, à tout moment, au Premier ministre les observations qu'elle juge utile. »

Titre III (de la loi n° 91-646 du 10 juillet 1991 consolidée) :

DISPOSITIONS COMMUNES AUX INTERCEPTIONS JUDICIAIRES ET DE SÉCURITÉ

Article 20 – « Les mesures prises par les pouvoirs publics pour assurer, aux seules fins de défense des intérêts nationaux, la surveillance et le contrôle des transmissions empruntant la voie hertzienne ne sont pas soumises aux dispositions des titres I et II de la présente loi. »

Article 21 – « Dans le cadre des attributions qui lui sont conférées par le Livre II du Code des postes et des "communications électroniques", le ministre chargé des "Communications électroniques" veille notamment à ce que l'exploitant public, les autres exploitants de réseaux publics de "Communications électroniques" et les autres fournisseurs de services de "communications électroniques" autorisés prennent les mesures nécessaires pour assurer l'application des dispositions de la présente loi. »

Article 22 – *(modifié par l'article 18 de la loi n° 96-659 du 26 juillet 1996 sur la réglementation des télécommunications)* – « Les juridictions compétentes pour ordonner des interceptions en application du Code de procédure pénale ainsi que le Premier ministre ou, en ce qui concerne l'exécution des mesures prévues à l'article 20, le ministre de la Défense ou le ministre de l'Intérieur, peuvent recueillir, auprès des personnes physiques ou morales exploitant des réseaux de "communications électroniques" ou fournisseurs de services de "communications électroniques", les informations ou documents qui leur sont nécessaires, chacun en ce qui le concerne, pour la réalisation et l'exploitation des interceptions autorisées par la loi.

La fourniture des informations ou documents visés à l'alinéa précédent ne constitue pas un détournement de leur finalité au sens de l'article 226-21 du Code pénal.

Le fait, en violation du premier alinéa, de refuser de communiquer les informations ou documents, ou de communiquer des renseignements erronés est puni de six mois d'emprisonnement et de 7 500 euros d'amende. Les personnes morales peuvent être déclarées responsables pénalement dans les conditions prévues par l'article 121-2 du code pénal de l'infraction définie au présent alinéa. Les peines encourues par les personnes morales sont l'amende, suivant les modalités prévues par l'article 131-38 du Code pénal. »

Article 23 – « Les exigences essentielles définies au 12° de l'article L. 32 du Code des postes et des "communications électroniques" et le secret des correspondances mentionné à l'article L. 32-3 du même code ne sont opposables ni aux juridictions compétentes pour ordonner des interceptions en application de l'article 100 du Code de procédure pénale, ni au ministre chargé des "Communications électroniques" dans l'exercice des prérogatives qui leur sont dévolues par la présente loi. »

Article 24 – *cf.* article 226-3 du Code pénal (ex-article 371 du même code)

Article 226-3 – « Est puni des mêmes peines [un an d'emprisonnement et 45 000 euros d'amende] la fabrication, l'importation, la détention, l'exposition, l'offre, la location ou la vente, en l'absence d'autorisation ministérielle dont les conditions d'octroi sont fixées par décret en Conseil d'État, d'appareils conçus pour réaliser les opérations pouvant constituer l'infraction prévue par le deuxième alinéa de l'article 226-15 ou qui, conçus pour la détection à distance des conversations, permettent de réaliser l'infraction prévue par l'article 226-1 et figurant sur une liste dressée dans des conditions fixées par ce même décret. Est également puni des mêmes peines le fait de réaliser une publicité en faveur d'un appareil susceptible de permettre la réalisation des infractions prévues par l'article 226-1 et le second alinéa de l'article 226-15 du Code pénal lorsque cette publicité constitue une incitation à commettre cette infraction. »

Article 25 – *cf.* article 432-9 du Code pénal (ex-article 186-1 du même code)

Article 432-9 – « Le fait, par une personne dépositaire de l'autorité publique ou chargée d'une mission de service public, agissant dans l'exercice ou à l'occasion de l'exercice de ses fonctions ou de sa mission, d'ordonner, de commettre ou de faciliter, hors les cas prévus par la loi, le détournement, la suppression ou l'ouverture de correspondances ou la révélation du contenu de ces correspondances, est puni de trois ans d'emprisonnement et de 45 000 euros d'amende.

Est puni des mêmes peines le fait, par une personne visée à l'alinéa précédent ou un agent d'un exploitant de réseau "ouvert au public de communications électroniques" ou d'un fournisseur de services de "communications électroniques", agissant dans l'exercice de ses fonctions, d'ordonner, de commettre ou de faciliter, hors les cas prévus par la loi, l'interception ou le détournement des correspondances émises, transmises ou reçues par la voie des télécommunications, l'utilisation ou la divulgation de leur contenu. »

Article 26 – « Sera punie des peines mentionnées à l'article 226-13[1] du Code pénal toute personne qui, concourant dans les cas prévus par la loi à l'exécution d'une décision d'interception de sécurité, révélera l'existence de l'interception. »

Titre IV (de la loi n° 91-646 du 10 juillet 1991 consolidée) :

COMMUNICATION DES DONNÉES TECHNIQUES RELATIVES À DES COMMUNICATIONS ÉLECTRONIQUES

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 à l'article L. 34-1 du Code précité ainsi que des prestataires mentionnés aux 1 et 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 précitée. »

Titre V (de la loi n° 91-646 du 10 juillet 1991 consolidée) :

DISPOSITIONS FINALES

1) Substitué dans le Nouveau Code pénal à l'article 378, mentionné dans la loi du 10 juillet 1991.

Article 28 – « La présente loi entrera en vigueur le 1er octobre 1991. »

1.2 Le titre IV « Interceptions de sécurité » du Livre II « Ordre et sécurité publics » du Code de la sécurité intérieure

Il s'agit du texte applicable depuis le 1er mai 2012, date de l'abrogation de la loi du 10 juillet 1991, après la ratification, par le Parlement, de l'ordonnance n° 2012-351 du 12 mars 2012.

TITRE IV Interceptions de sécurité

Chapitre Ier : Dispositions générales

Article L. 241-1

Le secret des correspondances émises par la voie des communications électroniques est garanti par la loi.

Il ne peut être porté atteinte à ce secret que par l'autorité publique, dans les seuls cas de nécessité d'intérêt public prévus par la loi et dans les limites fixées par celle-ci.

Article L. 241-2

Peuvent être autorisées, à titre exceptionnel, dans les conditions prévues par l'article L. 242-1, les interceptions de correspondances émises par la voie des communications électroniques ayant pour objet de rechercher des renseignements intéressant la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, ou la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous en application de l'article L. 212-1.

Article L. 241-3

Les mesures prises par les pouvoirs publics pour assurer, aux seules fins de défense des intérêts nationaux, la surveillance et le contrôle des transmissions empruntant la voie hertzienne ne sont pas soumises aux dispositions du présent titre, ni à celles de la sous-section 2 de la section 3 du chapitre Ier du titre III du Livre Ier du Code de procédure pénale.

Article L. 241-4

Les exigences essentielles définies au 12° de l'article L. 32 du Code des postes et communications électroniques et le secret des correspondances mentionné à l'article L. 32-3 du même code ne sont opposables ni aux juridictions compétentes pour ordonner des interceptions en application de l'article 100 du Code de procédure pénale, ni au ministre chargé des « Communications électroniques » dans l'exercice des prérogatives qui leur sont dévolues par le présent titre.

Chapitre II : Conditions des interceptions

Article L. 242-1

L'autorisation prévue à l'article L. 241-2 est accordée par décision écrite et motivée du Premier ministre ou de l'une des deux personnes spécialement déléguées par lui. Elle est donnée sur proposition écrite et motivée du ministre de la Défense, du ministre de l'Intérieur ou du ministre chargé des Douanes, ou de l'une des deux personnes que chacun d'eux aura spécialement déléguées.

Le Premier ministre organise la centralisation de l'exécution des interceptions autorisées.

Article L. 242-2

Le nombre maximum des interceptions susceptibles d'être pratiquées simultanément en application de l'article L. 242-1 est arrêté par le Premier ministre.

La décision fixant ce contingent et sa répartition entre les ministères mentionnés à l'article L. 242-1 est portée sans délai à la connaissance de la Commission nationale de contrôle des interceptions de sécurité.

Article L. 242-3

L'autorisation mentionnée à l'article L. 241-2 est donnée pour une durée maximum de quatre mois. Elle cesse de plein droit de produire effet à l'expiration de ce délai. Elle ne peut être renouvelée que dans les mêmes conditions de forme et de durée.

Article L. 242-4

Il est établi, sous l'autorité du Premier ministre, un relevé de chacune des opérations d'interception et d'enregistrement. Ce relevé mentionne la date et l'heure auxquelles elle a commencé et celles auxquelles elle s'est terminée.

Article L. 242-5

Dans les correspondances interceptées, seuls les renseignements en relation avec l'un des objectifs énumérés à l'article L. 241-2 peuvent faire l'objet d'une transcription. Cette transcription est effectuée par les personnels habilités.

Article L. 242-6

L'enregistrement est détruit sous l'autorité du Premier ministre, à l'expiration d'un délai de dix jours au plus tard à compter de la date à laquelle il a été effectué. Il est dressé procès-verbal de cette opération.

Article L. 242-7

Les transcriptions d'interceptions doivent être détruites dès que leur conservation n'est plus indispensable à la réalisation des fins

mentionnées à l'article L. 241-2. Il est dressé procès-verbal de l'opération de destruction. Les opérations mentionnées aux alinéas précédents sont effectuées sous l'autorité du Premier ministre.

Article L. 242-8

Sans préjudice de l'application du deuxième alinéa de l'article 40 du Code de procédure pénale, les renseignements recueillis ne peuvent servir à d'autres fins que celles mentionnées à l'article L. 241-2.

Article L. 242-9

Les opérations matérielles nécessaires à la mise en place des interceptions dans les locaux et installations des services ou organismes placés sous l'autorité ou la tutelle du ministre chargé des « Communications électroniques » ou des exploitants de réseaux ou fournisseurs de services de télécommunications ne peuvent être effectuées que sur ordre du ministre chargé des « Communications électroniques » ou sur ordre de la personne spécialement déléguée par lui, par des agents qualifiés de ces services, organismes, exploitants ou fournisseurs, dans leurs installations respectives.

Chapitre III : Commission nationale de contrôle des interceptions de sécurité

Section 1 : Composition et fonctionnement

Article L. 243-1

La Commission nationale de contrôle des interceptions de sécurité est une autorité administrative indépendante chargée de veiller au respect des dispositions du présent titre.

Article L. 243-2

La Commission nationale de contrôle des interceptions de sécurité 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'État et le premier président de la Cour de cassation.

Elle comprend, en outre, un député désigné pour la durée de la législature par le président de l'Assemblée nationale et un sénateur désigné après chaque renouvellement partiel du Sénat par le président du Sénat.

La qualité de membre de la commission est incompatible avec celle de membre du Gouvernement.

Article L. 243-3

Sauf démission, il ne peut être mis fin aux fonctions de membre de la Commission qu'en cas d'empêchement constaté par celle-ci. Le mandat des membres de la Commission n'est pas renouvelable.

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. À l'expiration de ce mandat, par dérogation au précédent alinéa, ils peuvent être nommés comme membre de la Commission s'ils ont occupé ces fonctions de remplacement pendant moins de deux ans.

Article L. 243-4

Les membres de la Commission sont astreints au respect des secrets protégés par les articles 413-10, 226-13 et 226-14 du Code pénal pour les faits, actes ou renseignements dont ils ont pu avoir connaissance en raison de leurs fonctions.

Article L. 243-5

La Commission établit son règlement intérieur. En cas de partage des voix, la voix du président est prépondérante. Les agents de la Commission sont nommés par le président.

Article L. 243-6

La Commission dispose des crédits nécessaires à l'accomplissement de sa mission dans les conditions fixées par la loi de finances. Le président est ordonnateur des dépenses de la Commission.

Article L. 243-7

La Commission remet chaque année au Premier ministre un rapport sur les conditions d'exercice et les résultats de son activité, qui précise notamment le nombre de recommandations qu'elle a adressées au Premier ministre en application de l'article L. 243-8 et au ministre de l'Intérieur en application de l'article L. 34-1-1 du Code des postes et des communications électroniques et de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, ainsi que les suites qui leur ont été données. Ce rapport est rendu public. La Commission adresse, à tout moment, au Premier ministre les observations qu'elle juge utiles.

Section 2 : Missions

Article L. 243-8

La décision motivée du Premier ministre mentionnée à l'article L. 242-1 est communiquée dans un délai de 48 heures au plus tard au président de la Commission nationale de contrôle des interceptions de sécurité. 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 Commission 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 adresse au Premier ministre une recommandation tendant à ce que cette interception soit

interrompue. Elle porte également cette recommandation à la connaissance du ministre ayant proposé l'interception et du ministre chargé des « Communications électroniques ». La Commission peut adresser au Premier ministre une recommandation, relative au contingent et à sa répartition, mentionnée à l'article L. 242-2. Le Premier ministre informe sans délai la Commission des suites données à ses recommandations.

Article L. 243-9

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. 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 cette interception soit interrompue. Il est alors procédé ainsi qu'il est indiqué aux quatrième et sixième alinéas de l'article L. 243-8.

Article L. 243-10

Les ministres, les autorités publiques, les agents publics doivent prendre toutes mesures utiles pour faciliter l'action de la Commission.

Article L. 243-11

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. 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 du présent titre dont elle a pu avoir connaissance à l'occasion du contrôle effectué en application de l'article L. 243-9.

Article L. 243-12

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 à l'article L. 34-1 du Code précité ainsi que des prestataires mentionnés aux 1 et 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 précitée.

Chapitre IV : Obligations des opérateurs et prestataires de services

Article L. 244-1

Les personnes physiques ou morales qui fournissent des prestations de cryptologie visant à assurer une fonction de confidentialité sont tenues de remettre aux agents autorisés dans les conditions prévues à l'article L. 242-1, sur leur demande, les conventions permettant

le déchiffrement des données transformées au moyen des prestations qu'elles ont fournies. Les agents autorisés peuvent demander aux fournisseurs de prestations susmentionnés de mettre eux-mêmes en œuvre ces conventions, sauf si ceux-ci démontrent qu'ils ne sont pas en mesure de satisfaire à ces réquisitions.

Un décret en Conseil d'État précise les procédures suivant lesquelles cette obligation est mise en œuvre ainsi que les conditions dans lesquelles la prise en charge financière de cette mise en œuvre est assurée par l'État.

Article L. 244-2

Les juridictions compétentes pour ordonner des interceptions en application du Code de procédure pénale ainsi que le Premier ministre ou, en ce qui concerne l'exécution des mesures prévues à l'article L. 241-3, le ministre de la Défense ou le ministre de l'Intérieur peuvent recueillir, auprès des personnes physiques ou morales exploitant des réseaux de communications électroniques ou fournisseurs de services de communications électroniques, les informations ou documents qui leur sont nécessaires, chacun en ce qui le concerne, pour la réalisation et l'exploitation des interceptions autorisées par la loi. La fourniture des informations ou documents visés à l'alinéa précédent ne constitue pas un détournement de leur finalité au sens de l'article 226-21 du Code pénal.

Article L. 244-3

Dans le cadre des attributions qui lui sont conférées par le Livre II du Code des postes et des « Communications électroniques », le ministre chargé des communications électroniques veille notamment à ce que l'exploitant public, les autres exploitants de réseaux publics de communications électroniques et les autres fournisseurs de services de communications électroniques autorisés prennent les mesures nécessaires pour assurer l'application des dispositions du présent titre et de la section 3 du chapitre I^{er} du titre III du Livre I^{er} du Code de procédure pénale relatives aux interceptions de correspondances émises par la voie des télécommunications ordonnées par l'autorité judiciaire.

Chapitre V : Dispositions pénales

Article L. 245-1

Le fait par une personne concourant, dans les cas prévus par la loi, à l'exécution d'une décision d'interception de sécurité, de révéler l'existence de l'interception est puni des peines mentionnées aux articles 226-13, 226-14 et 226-31 du Code pénal.

Article L. 245-2

Le fait de ne pas déférer, dans les conditions prévues au premier alinéa de l'article L. 244-1, aux demandes des autorités habilitées est puni de deux ans d'emprisonnement et de 30 000 euros d'amende.

Article L. 245-3

Le fait par une personne exploitant un réseau de communications électroniques ou fournissant des services de communications électroniques de refuser, en violation du premier alinéa de l'article L. 244-2, de communiquer les informations ou documents ou de communiquer des renseignements erronés est puni de six mois d'emprisonnement et de 7 500 euros d'amende.

1.3 Les textes réglementaires récents visant la loi du 10 juillet 1991

Décret n° 2002-497 du 12 avril 2002 relatif au groupement interministériel de contrôle (*JO* du 13 avril 2002)

« […] Vu la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des "communications électroniques", modifiée par la loi n° 92-1336 du 16 décembre 1992, l'ordonnance n° 2000-916 du 19 septembre 2000 et la loi n° 2001-1062 du 15 novembre 2001 […]. »

Article 1er – « Le Groupement interministériel de contrôle est un service du Premier ministre chargé des interceptions de sécurité. »

Article 2 – « Le Groupement interministériel de contrôle a pour mission :
1) de soumettre au Premier ministre les propositions d'interception présentées dans les conditions fixées par l'article 4 de la loi du 10 juillet 1991 susvisée ;
2) d'assurer la centralisation de l'exécution des interceptions de sécurité autorisées ;
3) de veiller à l'établissement du relevé d'opération prévu par l'article 8 de la loi du 10 juillet 1991 susvisée, ainsi qu'à la destruction des enregistrements effectués, dans les conditions fixées par l'article 9 de la même loi. »

Article 3 – « Le directeur du Groupement interministériel de contrôle est nommé par arrêté du Premier ministre. »

Article 4 – « Le ministre de la Fonction publique et de la Réforme de l'État est chargé de l'exécution du présent décret, qui sera publié au *Journal officiel de la République française*. »

Décret n° 2002-997 du 16 juillet 2002 relatif à l'obligation mise à la charge des fournisseurs de prestations de cryptologie en application de l'article 11-1 de la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des « communications électroniques » (*JO* du 18 juillet 2002)

Article 1 – « L'obligation mise à la charge des fournisseurs de prestations de cryptologie par l'article 11-1 de la loi du 10 juillet 1991 susvisée résulte d'une décision écrite et motivée, émanant du Premier ministre,

ou de l'une des deux personnes spécialement déléguées par lui en application des dispositions de l'article 4 de la même loi.

La décision qui suspend cette obligation est prise dans les mêmes formes. »

Article 2 – « Les décisions prises en application de l'article 1er sont notifiées au fournisseur de prestations de cryptologie et communiquées sans délai au président de la Commission nationale de contrôle des interceptions de sécurité. »

Article 3 – « Les conventions mentionnées dans le présent décret permettant le déchiffrement des données s'entendent des clés cryptographiques ainsi que de tout moyen logiciel ou de toute autre information permettant la mise au clair de ces données. »

Article 4 – « La décision mentionnée au premier alinéa de l'article 1er :
a) indique la qualité des agents habilités à demander au fournisseur de prestations de cryptologie la mise en œuvre ou la remise des conventions, ainsi que les modalités selon lesquelles les données à déchiffrer lui sont, le cas échéant, transmises ;
b) fixe le délai dans lequel les opérations doivent être réalisées, les modalités selon lesquelles, dès leur achèvement, le fournisseur remet aux agents visés au a) du présent article les résultats obtenus ainsi que les pièces qui lui ont été éventuellement transmises ;
c) prévoit, dès qu'il apparaît que les opérations sont techniquement impossibles, que le fournisseur remet aux agents visés au a) les pièces qui lui ont été éventuellement transmises. »

Article 5 – « Les fournisseurs prennent toutes dispositions, notamment d'ordre contractuel, afin que soit respectée la confidentialité des informations dont ils ont connaissance relativement à la mise en œuvre ou à la remise de ces conventions. »

Article 6 – « L'intégralité des frais liés à la mise en œuvre de l'obligation prévue par l'article 11-1 de la loi du 10 juillet 1991 susvisée est prise en charge, sur la base des frais réellement exposés par le fournisseur et dûment justifiés par celui-ci, par le budget des services du Premier ministre. »

Article 7 – « Le présent décret est applicable en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna. »

Article 8 – « Le ministre de l'Intérieur, de la Sécurité intérieure et des Libertés locales, la ministre de la Défense, le ministre de l'Économie, des Finances et de l'Industrie, la ministre de l'Outre-mer et le ministre délégué au Budget et à la Réforme budgétaire sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret, qui sera publié au *Journal officiel de la République française*. »

Deuxième mission : les opérations de recueil de données techniques de communications

Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers

Au sein de ce texte, l'article 6 concerne directement la Commission :

Article 6

I. – Après l'article L. 34-1 du Code des postes et des communications électroniques, il est inséré un article L. 34-1-1 ainsi rédigé :

Article L. 34-1-1 – « Afin de prévenir [Dispositions déclarées non conformes à la Constitution par la décision du Conseil constitutionnel n° 2005-532 DC du 19 janvier 2006] les actes de terrorisme, les agents individuellement désignés et dûment habilités des services de police et de gendarmerie nationales spécialement chargés de ces missions peuvent exiger des opérateurs et personnes mentionnés au I de l'article L. 34-1 la communication des données conservées et traitées par ces derniers en application dudit article.

Les données pouvant faire l'objet de cette demande sont limitées aux données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, aux données relatives à la localisation des équipements terminaux utilisés ainsi qu'aux données techniques relatives aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications.

Les surcoûts identifiables et spécifiques éventuellement exposés par les opérateurs et personnes mentionnés au premier alinéa pour répondre à ces demandes 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 Commission nationale de contrôle des interceptions de sécurité sur proposition du ministre de l'Intérieur qui lui présente une liste d'au moins trois noms. Des adjoints pouvant la suppléer sont désignés dans les mêmes conditions. La personnalité qualifiée établit un rapport d'activité annuel adressé à la Commission nationale de contrôle des interceptions de sécurité. Les demandes, accompagnées de leur motif, font l'objet d'un enregistrement et sont communiquées à la Commission nationale de contrôle des interceptions de sécurité.

Cette instance peut à tout moment procéder à des contrôles relatifs aux opérations de communication des données techniques. Lorsqu'elle

constate un manquement aux règles définies par le présent article ou une atteinte aux droits et libertés, elle saisit le ministre de l'Intérieur d'une recommandation. Celui-ci lui fait connaître dans un délai de quinze jours les mesures qu'il a prises pour remédier aux manquements constatés. Les modalités d'application des dispositions du présent article sont fixées par décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés et de la Commission nationale de contrôle des interceptions de sécurité, qui précise notamment la procédure de suivi des demandes et les conditions et durée de conservation des données transmises. »

II. – Après le II de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, il est inséré un II bis ainsi rédigé :

II bis – « Afin de prévenir [Dispositions déclarées non conformes à la Constitution par la décision du Conseil constitutionnel n° 2005-532 DC du 19 janvier 2006] les actes de terrorisme, les agents individuellement désignés et dûment habilités des services de police et de gendarmerie nationales spécialement chargés de ces missions peuvent exiger des prestataires mentionnés aux 1 et 2 du I la communication des données conservées et traitées par ces derniers en application du présent article.

Les demandes des agents sont motivées et soumises à la décision de la personnalité qualifiée instituée par l'article L. 34-1-1 du Code des postes et des communications électroniques selon les modalités prévues par le même article. La Commission nationale de contrôle des interceptions de sécurité exerce son contrôle selon les modalités prévues par ce même article.

Les modalités d'application des dispositions du présent II bis sont fixées par décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés et de la Commission nationale de contrôle des interceptions de sécurité, qui précise notamment la procédure de suivi des demandes et les conditions et durée de conservation des données transmises. »

III. – 1. À la fin de la seconde phrase du premier alinéa de l'article 4 de la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques, les mots : « Ou de la personne que chacun d'eux aura spécialement déléguée » sont remplacés par les mots : « Ou de l'une des deux personnes que chacun d'eux aura spécialement déléguées ».

2. Dans la première phrase du premier alinéa de l'article 19 de la même loi, les mots : « De l'article 14 et » sont remplacés par les mots : « De l'article 14 de la présente loi et au ministre de l'Intérieur en application de l'article L. 34-1-1 du Code des postes et des communications électroniques et de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, ainsi que ».

3. La même loi est complétée par un titre V intitulé : « Dispositions finales » comprenant l'article 27 qui devient l'article 28.

4. Il est inséré, dans la même loi, un titre IV ainsi rédigé :

Titre IV (de la loi n° 91-646 du 10 juillet 1991 consolidée) :

COMMUNICATION DES DONNÉES TECHNIQUES RELATIVES À DES COMMUNICATIONS ÉLECTRONIQUES

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 à l'article L. 34-1 du Code précité ainsi que des prestataires mentionnés aux 1 et 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 précitée. »

Cet article appelle les commentaires suivants :

– Sur la « personnalité qualifiée » :

Les demandes relatives à ces données sont soumises à l'appréciation d'une personnalité qualifiée désignée par la Commission pour une durée de trois ans renouvelable, à partir d'une liste de trois noms proposée par le ministre de l'Intérieur. La même procédure est prévue pour la désignation des adjoints de cette personnalité.

– Sur le champ d'application de cet article :

Le Conseil constitutionnel a censuré au nom du principe de séparation des pouvoirs la disposition liminaire de l'article 6 consistant non seulement à prévenir mais également à réprimer le terrorisme (décision n° 2002-532 DC du 19 janvier 2006). Cette séparation entre réquisitions judiciaires (*cf.* notamment l'article 77-1-1 du Code de procédure pénale) et réquisitions administratives (les articles 22 de la loi du 10 juillet 1991 et 6 de la loi n° 2006-64 du 23 janvier 2006) est ainsi conforme à celle entre interceptions judiciaires (les articles 100 à 100-7 du Code de procédure pénale) et interceptions administratives rappelée régulièrement par la CNCIS dans ses avis et rapports publics (3e rapport 1994, p. 19 ; 7e rapport 1998, p. 23 ; 8e rapport 1999, p. 14).

Loi n° 2008-1245 du 1er décembre 2008 visant à prolonger l'application des articles 3, 6 et 9 de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.

Article unique

Les dispositions des articles 3, 6 et 9 sont applicables jusqu'au 31 décembre 2012.

Le Gouvernement remet chaque année au Parlement un rapport sur l'application de la présente loi.

Le texte définitivement adopté stipule que par parallélisme avec les procédures de demandes d'interceptions, les demandes soumises à la Commission seront enregistrées, accompagnées de leur motivation et communiquées à la Commission. Le décret du 22 décembre 2006 précise que celle-ci peut à tout moment avoir accès aux données enregistrées et demander des éclaircissements sur la motivation des demandes.

Décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne

CHAPITRE I : DISPOSITIONS RELATIVES AUX RÉQUISITIONS JUDICIAIRES PRÉVUES PAR LE II DE L'ARTICLE 6 DE LA LOI n° 2004575 DU 21 JUIN 2004

Article 1

Les données mentionnées au II de l'article 6 de la loi du 21 juin 2004 susvisée, que les personnes sont tenues de conserver en vertu de cette disposition, sont les suivantes :

1° Pour les personnes mentionnées au 1 du I du même article et pour chaque connexion de leurs abonnés :
a) l'identifiant de la connexion ;
b) l'identifiant attribué par ces personnes à l'abonné ;
c) l'identifiant du terminal utilisé pour la connexion lorsqu'elles y ont accès ;
d) les dates et heure de début et de fin de la connexion ;
e) les caractéristiques de la ligne de l'abonné.

2° Pour les personnes mentionnées au 2 du I du même article et pour chaque opération de création :
a) l'identifiant de la connexion à l'origine de la communication ;
b) l'identifiant attribué par le système d'information au contenu, objet de l'opération ;
c) les types de protocoles utilisés pour la connexion au service et pour le transfert des contenus ;
d) la nature de l'opération ;
e) les date et heure de l'opération ;
f) l'identifiant utilisé par l'auteur de l'opération lorsque celui-ci l'a fourni.

3° Pour les personnes mentionnées aux 1 et 2 du I du même article, les informations fournies lors de la souscription d'un contrat par un utilisateur ou lors de la création d'un compte :
a) au moment de la création du compte, l'identifiant de cette connexion ;
b) les nom et prénom ou la raison sociale ;
c) les adresses postales associées ;
d) les pseudonymes utilisés ;
e) les adresses de courrier électronique ou de compte associées ;
f) les numéros de téléphone ;
g) le mot de passe ainsi que les données permettant de le vérifier ou de le modifier, dans leur dernière version mise à jour.

4° Pour les personnes mentionnées aux 1 et 2 du I du même article, lorsque la souscription du contrat ou du compte est payante, les informations suivantes relatives au paiement, pour chaque opération de paiement :
a) le type de paiement utilisé ;
b) la référence du paiement ;
c) le montant ;
d) la date et l'heure de la transaction.

Les données mentionnées aux 3° et 4° ne doivent être conservées que dans la mesure où les personnes les collectent habituellement.

Article 2

La contribution à une création de contenu comprend les opérations portant sur :
a) des créations initiales de contenus ;
b) des modifications des contenus et de données liées aux contenus ;
c) des suppressions de contenus.

Article 3

La durée de conservation des données mentionnées à l'article 1er est d'un an :
a) s'agissant des données mentionnées aux 1° et 2°, à compter du jour de la création des contenus, pour chaque opération contribuant à la création d'un contenu telle que définie à l'article 2 ;
b) s'agissant des données mentionnées au 3°, à compter du jour de la résiliation du contrat ou de la fermeture du compte ;
c) s'agissant des données mentionnées au 4°, à compter de la date d'émission de la facture ou de l'opération de paiement, pour chaque facture ou opération de paiement.

Article 4

La conservation des données mentionnées à l'article 1er est soumise aux prescriptions de la loi du 6 janvier 1978 susvisée, notamment les prescriptions prévues à l'article 34, relatives à la sécurité des informations.

Les conditions de la conservation doivent permettre une extraction dans les meilleurs délais pour répondre à une demande des autorités judiciaires.

CHAPITRE II : DISPOSITIONS RELATIVES AUX DEMANDES ADMINISTRATIVES PRÉVUES PAR LE II BIS DE L'ARTICLE 6 DE LA LOI n° 2004575 DU 21 JUIN 2004

Article 5

Les agents mentionnés au premier alinéa du II bis de l'article 6 de la loi du 21 juin 2004 susvisée sont désignés par les chefs des services de police et de gendarmerie nationales chargés des missions de prévention des actes de terrorisme, dont la liste est fixée par l'arrêté prévu à l'article 33 de la loi du 23 janvier 2006 susvisée. Ils sont habilités par le directeur général ou central dont ils relèvent.

Article 6

Les demandes de communication de données d'identification, conservées et traitées en application du II bis de l'article 6 de la loi du 21 juin 2004 susvisée, comportent les informations suivantes :
a) le nom, le prénom et la qualité du demandeur, ainsi que son service d'affectation et l'adresse de celui-ci ;
b) la nature des données dont la communication est demandée et, le cas échéant, la période intéressée ;
c) la motivation de la demande.

Article 7

Les demandes sont transmises à la personnalité qualifiée instituée à l'article L. 34-1-1 du Code des postes et des communications électroniques.

Ces demandes ainsi que les décisions de la personnalité qualifiée sont enregistrées et conservées pendant une durée maximale d'un an dans un traitement automatisé mis en œuvre par le ministère de l'Intérieur.

Article 8

Les demandes approuvées par la personnalité qualifiée sont adressées, sans les éléments mentionnés aux a) et c) de l'article 6, par un agent désigné dans les conditions prévues à l'article 5 aux personnes mentionnées aux 1 et 2 du I de l'article 6 de la loi du 21 juin 2004 susvisée, lesquelles transmettent sans délai les données demandées à l'auteur de la demande.

Les transmissions prévues à l'alinéa précédent sont effectuées selon des modalités assurant leur sécurité, leur intégrité et leur suivi, définies par

une convention conclue avec le prestataire concerné ou, à défaut, par un arrêté conjoint du ministre de l'Intérieur et du ministre chargé de l'Industrie.

Les données fournies par les personnes mentionnées aux 1 et 2 du I de l'article 6 de la loi du 21 juin 2004 susvisée sont enregistrées et conservées pendant une durée maximale de trois ans dans des traitements automatisés mis en œuvre par le ministère de l'Intérieur et le ministère de la Défense.

Article 9

Une copie de chaque demande est transmise, dans un délai de sept jours à compter de l'approbation de la personnalité qualifiée, à la Commission nationale de contrôle des interceptions de sécurité. Un arrêté du ministre de l'Intérieur, pris après avis de celle-ci, définit les modalités de cette transmission.

La Commission peut, en outre, à tout moment, avoir accès aux données enregistrées dans les traitements automatisés mentionnés aux articles 7 et 8. Elle peut également demander des éclaircissements sur la motivation des demandes approuvées par la personnalité qualifiée.

Article 10

Les surcoûts identifiables et spécifiques supportés par les personnes mentionnées aux 1 et 2 du I de l'article 6 de la loi du 21 juin 2004 susvisée pour la fourniture des données prévue par l'article II bis du même article font l'objet d'un remboursement par l'État par référence aux tarifs et selon des modalités fixés par un arrêté conjoint du ministre de l'Intérieur et du ministre chargé du Budget.

CHAPITRE III : DISPOSITIONS DIVERSES

Article 11

À l'article R. 10-19 du Code des postes et des communications électroniques, les mots : « Sans leur motivation » sont remplacés par les mots : « Sans les éléments mentionnés aux a et c de l'article R. 10-17 ».

Article 12

Les dispositions du présent décret sont applicables sur tout le territoire de la République à l'exception des dispositions des articles 1er à 4, 10 et 11 qui ne sont pas applicables dans les Terres australes et antarctiques françaises.

Article 13

Le garde des Sceaux, ministre de la Justice et des Libertés, le ministre de l'Intérieur, de l'Outre-mer, des Collectivités territoriales et de l'Immigration, la ministre de l'Économie, des Finances et de l'Industrie et le ministre du Budget, des Comptes publics, de la Fonction publique

et de la Réforme de l'État, porte-parole du Gouvernement, sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret, qui sera publié au *Journal officiel de la République française*.

Troisième mission : le contrôle des matériels d'interception

Cette activité de « contrôle du matériel » s'inscrit dans un cadre juridique qu'il convient de rappeler ici :

• **Les dispositions législatives qui définissent et répriment les infractions d'atteinte à la vie privée et au secret des correspondances :**
– article 226-1 du Code pénal : réprimant les atteintes à la vie privée ;
– article 226-15 du Code pénal : réprimant le détournement de correspondance.

Ce texte inclut, dans cette notion de détournement, le fait, de mauvaise foi : « D'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions » ;

– article 226-3 du Code pénal : réprimant la fabrication, l'importation, la détention, l'exposition, l'offre, la location ou la vente, en l'absence d'autorisation ministérielle dont les conditions sont fixées par décret en Conseil d'État, d'appareils conçus pour réaliser les opérations pouvant constituer l'infraction prévue par l'article 226-15 du Code pénal.

• **Le décret 97-757 du 10 juillet 1997** qui met en œuvre, à la faveur des articles R. 226-1 à R. 226-12 du Code pénal, la procédure d'« autorisation ministérielle » prévue par l'article 226-3 du Code pénal. L'organisation de la commission consultative placée sous la présidence du directeur général de l'Agence nationale de sécurité des systèmes d'information, pièce de la procédure d'autorisation est décrite par ce dispositif (article R. 226-2 du Code pénal).

• **Les dispositions réglementaires portant sur l'organisation et le fonctionnement des entités chargées de l'examen des demandes des services de l'État et des sociétés privées :**

• Le décret 2009-619 du 6 juin 2009 relatif à certaines commissions administratives à caractère consultatif relevant du Premier ministre.

• Le décret 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information » : ce texte confie la présidence de la commission dite « R226 » au directeur général de l'Agence nationale de la sécurité, lui-même rattaché au Secrétariat général de la défense et de la sécurité nationale :

– article 4 : l'Agence nationale de la sécurité des systèmes d'information se prononce sur la sécurité des dispositifs et des services, offerts par les prestataires, nécessaires à la protection des systèmes d'information.

L'Agence est en particulier chargée, par délégation du Premier ministre :
– de la certification de sécurité des dispositifs de création et de vérification de signature électronique prévue par le décret du 30 mars 2001 susvisé ;
– de l'agrément des centres d'évaluation et de la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information prévus par le décret du 18 avril 2002 susvisé ;
– de la délivrance des autorisations et de la gestion des déclarations relatives aux moyens et aux prestations de cryptologie prévues par le décret du 2 mai 2007 susvisé.

L'Agence instruit les demandes d'autorisation présentées en application de l'article 226-3 du Code pénal.

• Le décret 2009-1657 du 24 décembre 2009 relatif au conseil de défense et de sécurité nationale et au Secrétariat général de la défense et de la sécurité nationale :
– article 5.
– I. : À l'article 2 du décret du 7 juillet 2009 susvisé, la référence : « l'article D. 1132-10 » est remplacée par la référence « le 7° de l'article R. 1132-3 ».
– II. : Dans les articles R. 226-2, R. 226-4 et R. 226-8 du Code pénal, les mots : « Le Secrétariat général de la défense nationale » sont remplacés par les mots : « L'Agence nationale de la sécurité des systèmes d'information ».
– III. : Dans toutes les dispositions à caractère réglementaire, sous réserve des dispositions du II du présent article, les références au conseil de défense, au Secrétariat général de la défense nationale et au secrétaire général de la défense nationale sont remplacés respectivement par les références au conseil de défense et de sécurité nationale, au Secrétariat général de la défense et de la sécurité nationale et au Secrétaire général de la défense et de la sécurité nationale.

• L'arrêté du 29 juillet 2004 (*cf.* rapport d'activité 2004, p. 35-38) fixant la liste des appareils soumis à autorisation ministérielle pour application de l'article 226-3 du Code pénal.

• L'arrêté du 16 août 2006 mettant en œuvrant de manière spécifique le régime relatif au « registre » prévu par l'article R. 226-10 du Code pénal (registre retraçant la gestion des matériels soumis à autorisation). Cet arrêté a emporté l'abrogation de l'arrêté du 15 janvier 1998 qui constituait jusqu'alors le siège de cette matière.

• L'instruction du 5 septembre 2006, véritable documentation pédagogique à l'attention des « usagers » de la réglementation relative au matériel. Elle constitue un guide pratique efficace offrant une présentation claire des modalités procédurales d'examen des demandes, ainsi que des règles de compétence de la commission consultative dite « R. 226 ».

Chapitre II

Actualité législative et réglementaire

Ordonnance n° 2011-1069 du 8 septembre 2011 transposant la décision-cadre 2006/960/JAI du Conseil du 18 décembre 2006 relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des États membres de l'Union européenne

Article 1

Il est ajouté au chapitre II du titre X du Livre IV du Code de procédure pénale une section 6 ainsi rédigée :

« Section 6

« De l'échange simplifié d'informations entre services en application de la décision-cadre du Conseil de l'Union européenne du 18 décembre 2006

« Paragraphe 1

« Dispositions générales

« Art. 695-9-31. - Pour l'application de la décision-cadre 2006/960/JAI du Conseil du 18 décembre 2006, les services ou unités de la police nationale, de la gendarmerie nationale et de la direction des douanes et droits indirects désignés par arrêté du ministre de la Justice et, selon le cas, du ministre de l'Intérieur ou du ministre chargé du Budget peuvent, dans les conditions prévues à la présente section, aux fins de prévenir une infraction, d'en rassembler les preuves ou d'en rechercher les auteurs, échanger avec les services compétents d'un autre État membre de l'Union européenne des informations qui sont à leur disposition, soit qu'ils les détiennent, soit qu'ils puissent y accéder, notamment par consultation

d'un traitement automatisé de données, sans qu'il soit nécessaire de prendre ou solliciter une réquisition ou toute autre mesure coercitive.

« Art. 695-9-32. - Sans préjudice des dispositions de l'article 11 relatives au secret de l'enquête et de l'instruction, les informations ou données échangées sont confidentielles. Les modalités de leur transmission et de leur conservation garantissent le respect de ce principe.

« Paragraphe 2

« Dispositions applicables aux demandes d'informations émises par les services français

« Art. 695-9-33. - S'il existe des raisons de supposer qu'un État membre détient des informations entrant dans les prévisions de l'article 695-9-31 utiles à la prévention d'une infraction ou aux investigations tendant à en établir la preuve ou à en rechercher les auteurs, les services et unités mentionnés au même article peuvent en solliciter la transmission auprès des services compétents de cet État.

« La demande de transmission expose les raisons laissant supposer que les informations sont détenues par ces services. Elle précise à quelles fins les informations sont demandées et, lorsque les informations sont relatives à une personne déterminée, le lien entre cette personne et les fins de la demande.

« Art. 695-9-34. - Les informations obtenues ne peuvent être utilisées à titre de preuve qu'avec l'accord de l'État membre qui les a transmises.

« Art. 695-9-35. - Les informations obtenues ne peuvent être utilisées à d'autres fins que celles pour lesquelles elles ont été communiquées qu'avec l'accord de l'État membre qui les a transmises.

«Toutefois, même en l'absence d'accord, elles peuvent être utilisées pour prévenir un danger grave et immédiat pour la sécurité publique.

« En outre, les dispositions du premier alinéa ne font pas obstacle à l'exercice, par les autorités judiciaires, du pouvoir qu'elles tiennent des articles 12 et 13. Elles ne font pas davantage obstacle à l'exercice de leur mission par les autorités chargées par la loi de contrôler les modalités de traitement et de conservation des informations transmises.

« Art. 695-9-36. - À la demande de l'État membre qui a transmis l'information, le service ou l'unité qui l'a obtenue informe le service compétent de cet État de l'utilisation qui en a été faite.

« Paragraphe 3

« Dispositions applicables aux demandes d'informations reçues par les services français

« Art. 695-9-37. - Les services et unités mentionnés à l'article 695-9-31 transmettent, à leur demande, aux services compétents des États membres les informations, mentionnées au même article, utiles à la

prévention d'une infraction ou aux investigations tendant à en établir la preuve ou à en rechercher les auteurs.

« Art. 695-9-38. - Si des faits permettent de penser que des informations mentionnées à l'article 695-9-31 pourraient être utiles à un autre État membre soit pour prévenir une infraction entrant dans l'une des catégories énumérées à l'article 695-23 et punie en France d'une peine privative de liberté d'une durée égale ou supérieure à trois ans d'emprisonnement, soit pour conduire les investigations tendant à établir la preuve ou à rechercher les auteurs d'une telle infraction, le service ou l'unité qui détient ces informations les transmet, sans demande préalable, aux services compétents de cet État.

« Art. 695-9-39. - Lorsque les informations détenues par les services et unités mentionnés à l'article 695-9-31 leur ont été transmises par un État membre sur le fondement des dispositions de la décision-cadre 2006/960/JAI, elles ne peuvent être transmises à un autre État membre qu'avec l'accord de l'État qui les avait transmises et dans les conditions fixées par lui.

« Lorsque les informations détenues par ces mêmes services ou unités avaient été transmises à la France par un État membre sur un autre fondement que la décision-cadre 2006/960/JAI ou par un État tiers, elles ne peuvent être transmises à un autre État membre qu'avec l'accord de l'État qui les avait transmises et dans les conditions fixées par lui chaque fois que la France y est tenue par ses engagements internationaux.

« Art. 695-9-40. - Les informations ne peuvent être transmises aux services compétents de l'État membre qui les a demandées qu'avec l'autorisation préalable d'un magistrat chaque fois que cette autorisation est requise en France pour accéder à ces mêmes informations ou les transmettre à un service ou à une unité de police judiciaire.

« Lorsque cette autorisation est nécessaire, le service ou l'unité à laquelle les informations sont demandées la sollicite auprès du magistrat compétent.

« Les pièces d'une procédure pénale en cours ne peuvent être transmises, selon le cas, qu'avec l'accord de la juridiction d'instruction ou, lorsqu'une enquête est en cours ou que la juridiction de jugement est saisie, du ministère public.

« Art. 695-9-41. - Les services et unités mentionnés à l'article 695-9-31 ne peuvent refuser de communiquer les informations demandées par un État membre que s'il existe des motifs laissant supposer que leur communication :
« 1° porterait atteinte aux intérêts fondamentaux de l'État en matière de sécurité nationale ;
« 2° nuirait au déroulement d'investigations en matière pénale ou compromettrait la sécurité des personnes ;

« 3° ou serait manifestement disproportionnée ou sans objet au regard des finalités pour lesquelles elle a été demandée.

« Art. 695-9-42. - Les services et unités mentionnés à l'article 695-9-31 peuvent refuser de transmettre les informations demandées lorsqu'elles se rapportent à une infraction punie en France d'une peine d'emprisonnement inférieure ou égale à un an et qu'elles ne leur paraissent pas présenter un intérêt suffisant pour justifier les contraintes attachées à leur transmission.

« Art. 695-9-43. - Lors de la transmission de l'information, le service ou l'unité mentionnée à l'article 695-9-31 indique au service destinataire les conditions d'utilisation de celle-ci.

« Chaque fois qu'il l'estime utile, il peut demander au service destinataire de l'informer de l'utilisation qui a été faite de l'information transmise.

« Art. 695-9-44. - Lorsqu'une information a été transmise par un service ou une unité mentionné à l'article 695-9-31 au service compétent d'un État membre et que celui-ci envisage de la communiquer à un autre État ou d'en faire une utilisation différente de celle pour laquelle la transmission avait été décidée, le service ou l'unité qui avait procédé à la transmission initiale est compétent pour apprécier s'il y a lieu d'autoriser, à la demande de l'État destinataire, la retransmission ou la nouvelle utilisation de l'information et, le cas échéant, pour fixer les conditions de celle-ci.

« Art. 695-9-45. - Les informations transmises par les services et unités mentionnés à l'article 695-9-31 peuvent être utilisées par le service destinataire à titre de preuve, sauf mention contraire lors de leur transmission.

« Art. 695-9-46. - Les informations transmises par les services ou unités mentionnés à l'article 695-9-31 aux services compétents d'un État membre sont également transmises aux unités EUROJUST et EUROPOL dans la mesure où elles portent sur une infraction relevant de leur mandat.

« Art. 695-9-47. - Un arrêté du ministre de la Justice, du ministre de l'Intérieur et du ministre chargé du Budget désigne les points de contact auxquels les demandes de transmission d'informations peuvent être adressées par les services compétents des États membres.

« Paragraphe 4

« Application à certains États non membres de l'Union européenne

« Art. 695-9-48. - Les dispositions de la présente section sont applicables à l'échange des informations mentionnées à l'article 695-9-31 entre les services ou unités mentionnés au même article et les services compétents des États non membres de l'Union européenne associés à

la mise en œuvre, à l'application et au développement de l'acquis de Schengen.

« Art. 695-9-49. - Les modalités d'application des dispositions de la présente section sont déterminées par décret en Conseil d'État. Ce décret fixe, notamment, les modalités et délais dans lesquels les informations sont transmises aux services qui les ont sollicitées. »

Article 2

La présente ordonnance est applicable sur l'ensemble du territoire de la République.

Article 3

Le Premier ministre, le garde des Sceaux, ministre de la Justice et des Libertés, le ministre de l'Intérieur, de l'Outre-mer, des Collectivités territoriales et de l'Immigration et la ministre du Budget, des Comptes publics et de la Réforme de l'État, porte-parole du Gouvernement, sont responsables, chacun en ce qui le concerne, de l'application de la présente ordonnance, qui sera publiée au *Journal officiel de la République française*.

* * *

Article 706-25-2 créé par la loi n° 2011-267 du 14 mars 2011 – art. 34

Dans le but de constater les infractions mentionnées au sixième alinéa de l'article 24 de la loi du 29 juillet 1881 sur la liberté de la presse et lorsque celles-ci sont commises par un moyen de communication électronique, d'en rassembler les preuves et d'en rechercher les auteurs, les officiers ou agents de police judiciaire agissant au cours de l'enquête ou sur commission rogatoire peuvent, s'ils sont affectés dans un service spécialisé désigné par arrêté du ministre de l'Intérieur et spécialement habilités à cette fin, procéder aux actes suivants sans en être pénalement responsables :
1° participer sous un pseudonyme aux échanges électroniques ;
2° être en contact par ce moyen avec les personnes susceptibles d'être les auteurs de ces infractions ;
3° extraire, acquérir ou conserver par ce moyen les éléments de preuve et les données sur les personnes susceptibles d'être les auteurs de ces infractions.

À peine de nullité, ces actes ne peuvent constituer une incitation à commettre ces infractions.

* * *

ARRÊTÉ

Arrêté du 19 septembre 2011 pris pour l'application de l'article 706-25-2 du Code de procédure pénale relatif à la mise en œuvre des techniques d'enquêtes sous pseudonyme au cours d'enquêtes portant sur les infractions mentionnées au sixième alinéa de l'article 24 de la loi du 29 juillet 1881 sur la liberté de la presse lorsque celles-ci sont commises par un moyen de communication électronique

Article 1

Sont autorisés à procéder aux actes définis par l'article 706-25-2 du Code de procédure pénale les officiers et agents de police judiciaire spécialement habilités à cette fin, affectés à l'un des services ou unités suivants :

1. Services et unités relevant de la direction centrale de la police judiciaire :
– la sous-direction antiterroriste ;
– le service interministériel d'assistance technique ;
– l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication ;
– l'Office central pour la répression de la grande délinquance financière ;
– les directions régionales et interrégionales de police judiciaire.

2. La direction centrale du renseignement intérieur.

3. La direction du renseignement de la préfecture de police.

4. Services et unités relevant de la direction générale de la gendarmerie nationale :
– le bureau de la lutte antiterroriste de la sous-direction de la police judiciaire ;
– le service technique de recherches judiciaires et de documentation ;
– l'Office central de lutte contre les atteintes à l'environnement et à la santé publique ;
– les sections de recherches ;
– les sections d'appui judiciaire.

Article 2

Le directeur général de la police nationale et le directeur général de la gendarmerie nationale sont chargés, chacun en ce qui le concerne, de l'exécution du présent arrêté, qui sera publié au *Journal officiel de la République française*.

* * *

DÉCRET

Décret n° 2011-1425 du 2 novembre 2011 portant application de l'article 413-7 du Code pénal et relatif à la protection du potentiel scientifique et technique de la Nation

Article 1 La section 1 du chapitre III du titre Ier du Livre IV de la partie réglementaire du Code pénal est complétée par un article ainsi rédigé :

« Art. R. 413-5-1. – I. – Sont dites "zones à régime restrictif" celles des zones, mentionnées à l'article R. 413-1, dont le besoin de protection tient à l'impératif qui s'attache à empêcher que des éléments essentiels du potentiel scientifique ou technique de la Nation :

« 1° fassent l'objet d'une captation de nature à affaiblir ses moyens de défense, à compromettre sa sécurité ou à porter préjudice à ses autres intérêts fondamentaux ;

« 2° ou soient détournés à des fins de terrorisme, de prolifération d'armes de destruction massive et de leurs vecteurs ou de contribution à l'accroissement d'arsenaux militaires.

« Les zones à régime restrictif peuvent inclure, dans leur périmètre, des locaux dont la protection renforcée est justifiée par l'entreposage de produits ou par l'exécution d'activités comportant des risques particuliers au regard des impératifs mentionnés aux trois premiers alinéas.

« II. – Par dérogation aux deux premiers alinéas de l'article R. 413-5, l'accès à une zone à régime restrictif pour y effectuer un stage, y préparer un doctorat, y participer à une activité de recherche, y suivre une formation, y effectuer une prestation de service ou y exercer une activité professionnelle est soumis à l'autorisation du chef du service, d'établissement ou d'entreprise, après avis favorable du ministre chargé d'en exercer la tutelle ou, à défaut de ministre de tutelle, du ministre qui a déterminé le besoin de protection en application de l'article R. 413-2.

« La demande d'avis est adressée par le chef de service, d'établissement ou d'entreprise au ministre mentionné au précédent alinéa. Le silence gardé par le ministre au cours des deux mois suivant la réception de la demande vaut avis favorable.

« Le refus d'autorisation d'accès n'est pas motivé.

« III. – Toute personne bénéficiant d'une habilitation au titre de la protection du secret de la défense nationale est réputée avoir obtenu l'avis ministériel favorable mentionné au II.

« Les prestataires extérieurs de services relevant de catégories précisées par arrêté du Premier ministre et exerçant leur activité habituelle dans une zone à régime restrictif sont réputés avoir obtenu l'avis ministériel favorable mentionné au II pour accéder, dans les conditions prévues par un contrat de prestation de service, à la zone à régime restrictif.

« IV. – Dans tous les cas, le chef du service, de l'établissement ou de l'entreprise informe le ministre mentionné au premier alinéa du II de sa décision relative à l'autorisation d'accès. »

Article 2 I. – La protection du potentiel scientifique et technique de la Nation est assurée par concertation entre les pouvoirs publics et les chefs des services, établissements ou entreprises dans lesquels :

1° ont été délimitées une ou plusieurs zones à régime restrictif, en application de l'article R. 413-5-1 du Code pénal ;

2° ou qui abritent une activité exposée aux risques définis au I du même article.

II. – À cet effet, les informations nécessaires à la protection du potentiel scientifique et technique de la Nation sont fournies au ministre dont relève l'activité en cause dans des conditions fixées, selon les caractéristiques du service, établissement ou entreprise intéressé :

1° par ce ministre ;

2° ou par convention entre ce ministre et les organes compétents du service, établissement ou entreprise intéressé.

III. – Pour l'application des dispositions qui précèdent, un arrêté du Premier ministre détermine :

1° la liste des secteurs scientifiques et techniques et des unités de recherche exposés aux risques définis au I de l'article R. 413-5-1 du Code pénal ;

2° la liste des catégories d'informations nécessaires à la protection du potentiel scientifique et technique de la Nation ainsi que de leurs modalités de transmission, compte tenu des caractéristiques du service, établissement ou entreprise, du secteur et de la spécialité.

IV. – Un arrêté non publié du Premier ministre détermine, au sein des secteurs scientifiques et techniques mentionnés au 1° du III, la liste des spécialités dont les savoir-faire sont susceptibles d'être détournés à des fins de terrorisme ou de prolifération d'armes de destruction massive et de leurs vecteurs.

Article 3 Le présent décret est applicable sur l'ensemble du territoire de la République.

Article 4 Le ministre de la Défense et des Anciens combattants, la ministre de l'Écologie, du Développement durable, des Transports et du Logement, le garde des Sceaux, ministre de la Justice et des Libertés, le ministre de l'Intérieur, de l'Outre-mer, des Collectivités territoriales et de l'Immigration, le ministre de l'Économie, des Finances et de l'Industrie, le ministre du Travail, de l'Emploi et de la Santé, le ministre de l'Agriculture, de l'Alimentation, de la Pêche, de la Ruralité et de l'Aménagement du territoire et le ministre de l'Enseignement supérieur et de la Recherche sont

chargés, chacun en ce qui le concerne, de l'exécution du présent décret, qui sera publié au *Journal officiel de la République française*.

* * *

DÉCRET

Décret n° 2011-1431 du 3 novembre 2011 portant modification du Code de procédure pénale (partie réglementaire : Décrets simples) pris pour l'application de l'article 706-102-6 de ce Code relatif à la captation des données informatiques

Article 1 Il est ajouté au chapitre Ier du titre Ier du Livre Ier du Code de procédure pénale (partie réglementaire : Décrets simples) une section 5 ainsi rédigée :

« Section 5

« De la captation des données informatiques

« Art. D. 15-1-6. - Les services, unités et organismes, visés à l'article 706-102-6, pouvant procéder aux opérations d'installation des dispositifs techniques mentionnés à l'article 706-102-1 sont :
« – la direction centrale de la police judiciaire et ses directions interrégionales et régionales ;
« – la direction centrale du renseignement intérieur ;
« – les offices centraux de police judiciaire ;
« – l'unité de recherche, assistance, intervention et dissuasion ;
« – les groupes d'intervention de la police nationale ;
« – la sous-direction de la police judiciaire de la gendarmerie nationale ;
« – les sections de recherches de la gendarmerie nationale ;
« – les sections d'appui judiciaire de la gendarmerie nationale ;
« – le groupe d'intervention de la gendarmerie nationale. »

Article 2

Le garde des Sceaux, ministre de la Justice et des Libertés, et le ministre de l'Intérieur, de l'Outre-mer, des Collectivités territoriales et de l'Immigration sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret, qui sera publié au *Journal officiel de la République française*.

Chapitre III

Jurisprudence et actualités parlementaires

1) Décision du Conseil constitutionnel du 10 novembre 2011, n° 2011-192 QPC

LE CONSEIL CONSTITUTIONNEL,

Vu les pièces produites et jointes au dossier ;

Le rapporteur ayant été entendu ;

1. Considérant qu'aux termes de l'article 413-9 du Code pénal : « Présentent un caractère de secret de la défense nationale au sens de la présente section les procédés, objets, documents, informations, réseaux informatiques, données informatisées ou fichiers intéressant la défense nationale qui ont fait l'objet de mesures de classification destinées à restreindre leur diffusion ou leur accès.

« Peuvent faire l'objet de telles mesures les procédés, objets, documents, informations, réseaux informatiques, données informatisées ou fichiers dont la divulgation ou auxquels l'accès est de nature à nuire à la défense nationale ou pourrait conduire à la découverte d'un secret de la défense nationale.

« Les niveaux de classification des procédés, objets, documents, informations, réseaux informatiques, données informatisées ou fichiers présentant un caractère de secret de la défense nationale et les autorités chargées de définir les modalités selon lesquelles est organisée leur protection sont déterminés par décret en Conseil d'État » ;

2. Considérant qu'aux termes de l'article 413-9-1 du même code : « Seuls peuvent faire l'objet d'une classification au titre du secret de la

défense nationale les lieux auxquels il ne peut être accédé sans que, à raison des installations ou des activités qu'ils abritent, cet accès donne par lui-même connaissance d'un secret de la défense nationale.

« La décision de classification est prise pour une durée de cinq ans par arrêté du Premier ministre, publié au *Journal officie*l, après avis de la Commission consultative du secret de la défense nationale.

« Les conditions d'application du présent article, notamment les conditions de classification des lieux, sont déterminées par décret en Conseil d'État » ;

3. Considérant qu'aux termes de l'article 413-10 du même code : « Est puni de sept ans d'emprisonnement et de 100 000 euros d'amende le fait, par toute personne dépositaire, soit par état ou profession, soit en raison d'une fonction ou d'une mission temporaire ou permanente, d'un procédé, objet, document, information, réseau informatique, donnée informatisée ou fichier qui a un caractère de secret de la défense nationale, soit de le détruire, détourner, soustraire ou de le reproduire, soit d'en donner l'accès à une personne non qualifiée ou de le porter à la connaissance du public ou d'une personne non qualifiée.

« Est puni des mêmes peines le fait, par la personne dépositaire, d'avoir laissé accéder à, détruire, détourner, soustraire, reproduire ou divulguer le procédé, objet, document, information, réseau informatique, donnée informatisée ou fichier visé à l'alinéa précédent.

« Lorsque la personne dépositaire a agi par imprudence ou négligence, l'infraction est punie de trois ans d'emprisonnement et de 45 000 euros d'amende » ;

4. Considérant qu'aux termes de l'article 413-10-1 du même code : « Est puni de sept ans d'emprisonnement et de 100 000 euros d'amende le fait, par toute personne responsable, soit par état ou profession, soit en raison d'une fonction ou d'une mission temporaire ou permanente, d'un lieu classifié au titre du secret de la défense nationale d'en avoir permis l'accès à une personne non qualifiée.

« Est puni des mêmes peines le fait, par toute personne qualifiée, de porter à la connaissance du public ou d'une personne non qualifiée un élément relatif à la nature des installations ou des activités qu'un tel lieu abrite.

« Lorsque la personne responsable a agi par imprudence ou négligence, l'infraction est punie de trois ans d'emprisonnement et de 45 000 euros d'amende » ;

5. Considérant qu'aux termes de l'article 413-11 du Code pénal : « Est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende le fait, par toute personne non visée à l'article 413-10 de :
« 1° s'assurer la possession, accéder à, ou prendre connaissance d'un procédé, objet, document, information, réseau informatique, donnée

informatisée ou fichier qui présente le caractère d'un secret de la défense nationale ;
« 2° détruire, soustraire ou reproduire, de quelque manière que ce soit, un tel procédé, objet, document, information, réseau informatique, donnée informatisée ou fichier ;
« 3° porter à la connaissance du public ou d'une personne non qualifiée un tel procédé, objet, document, information, réseau informatique, donnée informatisée ou fichier » ;

6. Considérant qu'aux termes de l'article 413-11-1 du même code : « Est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende le fait, par toute personne non qualifiée :
« 1° d'accéder à un lieu classifié au titre du secret de la défense nationale ;
« 2° de porter à la connaissance du public ou d'une personne non qualifiée un élément relatif à la nature des installations ou des activités qu'un tel lieu abrite » ;

7. Considérant qu'aux termes de l'article 413-12 du même code : « La tentative des délits prévus au premier alinéa de l'article 413-10 et à l'article 413-11 est punie des mêmes peines ».

8. Considérant qu'aux termes de l'article L. 2311-1 du Code de la défense : « Les règles relatives à la définition des informations concernées par les dispositions du présent chapitre sont définies par l'article 413-9 du Code pénal » ;

9. Considérant qu'aux termes de l'article L. 2312-1 du même code : « La Commission consultative du secret de la défense nationale est une autorité administrative indépendante. Elle est chargée de donner un avis sur la déclassification et la communication d'informations ayant fait l'objet d'une classification en application des dispositions de l'article 413-9 du Code pénal, à l'exclusion des informations dont les règles de classification ne relèvent pas des seules autorités françaises.

« L'avis de la Commission consultative du secret de la défense nationale est rendu à la suite de la demande d'une juridiction française.

« Le président de la Commission consultative du secret de la défense nationale, ou son représentant, membre de la Commission, est chargé de donner, à la suite d'une demande d'un magistrat, un avis sur la déclassification temporaire aux fins de perquisition de lieux ayant fait l'objet d'une classification » ;

10. Considérant qu'aux termes de l'article L. 2312-2 du même code : « La Commission consultative du secret de la défense nationale comprend cinq membres :
« 1° un président, un vice-président qui le supplée en cas d'absence ou d'empêchement et un membre choisis par le Président de la République sur une liste de six membres du Conseil d'État, de la Cour de cassation ou de la Cour des comptes, établie conjointement par le vice-président

du Conseil d'État, le premier président de la Cour de cassation et le premier président de la Cour des comptes ;
« 2° un député, désigné pour la durée de la législature par le président de l'Assemblée nationale ;
« 3° un sénateur, désigné après chaque renouvellement partiel du Sénat par le président du Sénat.

« Le mandat des membres de la Commission n'est pas renouvelable.

« Le mandat des membres non parlementaires de la Commission est de six ans.

« Sauf démission, il ne peut être mis fin aux fonctions de membre de la Commission qu'en cas d'empêchement constaté par celle-ci. Les membres de la Commission désignés en remplacement de ceux dont le mandat a pris fin avant son terme normal sont nommés pour la durée restant à courir dudit mandat. Par dérogation au cinquième alinéa, lorsque leur nomination est intervenue moins de deux ans avant l'expiration du mandat de leur prédécesseur, ils peuvent être renouvelés en qualité de membre de la Commission » ;

11. Considérant qu'aux termes de l'article L. 2312-3 du même code : « Les crédits nécessaires à la Commission pour l'accomplissement de sa mission sont inscrits au programme de la mission « Direction de l'action du Gouvernement » relatif à la protection des droits et des libertés fondamentales.

« Le président est ordonnateur des dépenses de la Commission. Il nomme les agents de la Commission » ;

12. Considérant qu'aux termes de l'article L. 2312-4 du même code : « Une juridiction française dans le cadre d'une procédure engagée devant elle peut demander la déclassification et la communication d'informations, protégées au titre du secret de la défense nationale, à l'autorité administrative en charge de la classification.

« Cette demande est motivée.

« L'autorité administrative saisit sans délai la Commission consultative du secret de la défense nationale.

« Un magistrat, dans le cadre d'une procédure engagée devant lui, peut demander la déclassification temporaire aux fins de perquisition de lieux protégés au titre du secret de la défense nationale au président de la Commission. Celui-ci est saisi et fait connaître son avis à l'autorité administrative en charge de la classification dans les conditions prévues par l'article 56-4 du Code de procédure pénale » ;

13. Considérant qu'aux termes de l'article L. 2312-5 du même code : « Le président de la Commission peut mener toutes investigations utiles.

« Les membres de la Commission sont autorisés à connaître de toute information classifiée et d'accéder à tout lieu classifié dans le cadre de leur mission.

« Ils sont astreints au respect du secret de la défense nationale protégé en application des articles 413-9 et suivants du Code pénal pour les faits, actes ou renseignements dont ils ont pu avoir connaissance à raison de leurs fonctions.

« Pour l'accomplissement de sa mission, la Commission, ou sur délégation de celle-ci son président, est habilitée, nonobstant les dispositions des articles 56 et 97 du Code de procédure pénale, à procéder à l'ouverture des scellés des éléments classifiés qui lui sont remis. La Commission en fait mention dans son procès-verbal de séance. Les documents sont restitués à l'autorité administrative par la Commission lors de la transmission de son avis.

« La Commission établit son règlement intérieur » ;

14. Considérant qu'aux termes de l'article L. 2312-6 du même code : « Les ministres, les autorités publiques, les agents publics ne peuvent s'opposer à l'action de la Commission pour quelque motif que ce soit et prennent toutes mesures utiles pour la faciliter » ;

15. Considérant qu'aux termes de l'article L. 2312-7 du même code : « La Commission émet un avis dans un délai de deux mois à compter de sa saisine. Cet avis prend en considération les missions du service public de la justice, le respect de la présomption d'innocence et les droits de la défense, le respect des engagements internationaux de la France ainsi que la nécessité de préserver les capacités de défense et la sécurité des personnels.

« En cas de partage égal des voix, celle du président est prépondérante.

« Le sens de l'avis peut être favorable, favorable à une déclassification partielle ou défavorable.

« L'avis de la Commission est transmis à l'autorité administrative ayant procédé à la classification » ;

16. Considérant qu'aux termes de l'article L. 2312-7-1 du même code : « L'avis du président de la Commission consultative du secret de la défense nationale sur la déclassification d'un lieu aux fins de perquisition, dont le sens peut être favorable, favorable à la déclassification partielle ou défavorable, prend en considération les éléments mentionnés au premier alinéa de l'article L. 2312-7 » ;

17. Considérant qu'aux termes de l'article L. 2312-8 du même code : « Dans le délai de quinze jours francs à compter de la réception de l'avis de la Commission, ou à l'expiration du délai de deux mois mentionné à l'article L. 2312-7, l'autorité administrative notifie sa décision, assortie

du sens de l'avis, à la juridiction ayant demandé la déclassification et la communication d'informations classifiées.

« Le sens de l'avis de la Commission est publié au *Journal officiel de la République française* » ;

18. Considérant qu'aux termes de l'article 56-4 du Code de procédure pénale : « I. Lorsqu'une perquisition est envisagée dans un lieu précisément identifié, abritant des éléments couverts par le secret de la défense nationale, la perquisition ne peut être réalisée que par un magistrat en présence du président de la Commission consultative du secret de la défense nationale. Ce dernier peut être représenté par un membre de la Commission ou par des délégués, dûment habilités au secret de la défense nationale, qu'il désigne selon des modalités déterminées par décret en Conseil d'État. Le président ou son représentant peut être assisté de toute personne habilitée à cet effet.

« La liste des lieux visés au premier alinéa est établie de façon précise et limitative par arrêté du Premier ministre. Cette liste, régulièrement actualisée, est communiquée à la Commission consultative du secret de la défense nationale ainsi qu'au ministre de la Justice, qui la rende accessible aux magistrats de façon sécurisée. Le magistrat vérifie si le lieu dans lequel il souhaite effectuer une perquisition figure sur cette liste.

« Les conditions de délimitation des lieux abritant des éléments couverts par le secret de la défense nationale sont déterminées par décret en Conseil d'État.

« Le fait de dissimuler dans les lieux visés à l'alinéa précédent des procédés, objets, documents, informations, réseaux informatiques, données informatisées ou fichiers non classifiés, en tentant de les faire bénéficier de la protection attachée au secret de la défense nationale, expose son auteur aux sanctions prévues à l'article 434-4 du Code pénal.

« La perquisition ne peut être effectuée qu'en vertu d'une décision écrite du magistrat qui indique au président de la Commission consultative du secret de la défense nationale les informations utiles à l'accomplissement de sa mission. Le président de la Commission ou son représentant se transporte sur les lieux sans délai. Au commencement de la perquisition, le magistrat porte à la connaissance du président de la Commission ou de son représentant, ainsi qu'à celle du chef d'établissement ou de son délégué, ou du responsable du lieu, la nature de l'infraction ou des infractions sur lesquelles portent les investigations, les raisons justifiant la perquisition, son objet et les lieux visés par cette perquisition.

« Seul le président de la Commission consultative du secret de la défense nationale, son représentant et, s'il y a lieu, les personnes qui l'assistent peuvent prendre connaissance d'éléments classifiés découverts sur les lieux. Le magistrat ne peut saisir, parmi les éléments classifiés, que ceux relatifs aux infractions sur lesquelles portent les investigations.

Si les nécessités de l'enquête justifient que les éléments classifiés soient saisis en original, des copies sont laissées à leur détenteur.

« Chaque élément classifié saisi est, après inventaire par le président de la Commission consultative, placé sous scellé. Les scellés sont remis au président de la Commission consultative du secret de la défense nationale qui en devient le gardien. Les opérations relatives aux éléments classifiés saisis ainsi que l'inventaire de ces éléments font l'objet d'un procès-verbal qui n'est pas joint au dossier de la procédure et qui est conservé par le président de la Commission consultative.

« La déclassification et la communication des éléments mentionnés dans l'inventaire relèvent de la procédure prévue par les articles L. 2312-4 et suivants du Code de la défense.

« II. Lorsqu'à l'occasion d'une perquisition un lieu se révèle abriter des éléments couverts par le secret de la défense nationale, le magistrat présent sur le lieu ou immédiatement avisé par l'officier de police judiciaire en informe le président de la Commission consultative du secret de la défense nationale. Les éléments classifiés sont placés sous scellés, sans en prendre connaissance, par le magistrat ou l'officier de police judiciaire qui les a découverts, puis sont remis ou transmis, par tout moyen en conformité avec la réglementation applicable aux secrets de la défense nationale, au président de la Commission afin qu'il en assure la garde. Les opérations relatives aux éléments classifiés font l'objet d'un procès-verbal qui n'est pas joint au dossier de la procédure. La déclassification et la communication des éléments ainsi placés sous scellés relèvent de la procédure prévue par les articles L. 2312-4 et suivants du Code de la défense.

« III. Lorsqu'une perquisition est envisagée dans un lieu classifié au titre du secret de la défense nationale dans les conditions définies à l'article 413-9-1 du Code pénal, elle ne peut être réalisée que par un magistrat en présence du président de la Commission consultative du secret de la défense nationale. Ce dernier peut être représenté par un membre de la Commission et être assisté de toute personne habilitée à cet effet.

« Le magistrat vérifie auprès de la Commission consultative du secret de la défense nationale si le lieu dans lequel il souhaite effectuer une perquisition fait l'objet d'une mesure de classification.

« La perquisition ne peut être effectuée qu'en vertu d'une décision écrite et motivée qui indique la nature de l'infraction ou des infractions sur lesquelles portent les investigations, les raisons justifiant la perquisition et l'objet de celle-ci, ainsi que le lieu visé par la perquisition. Le magistrat transmet cette décision au président de la Commission consultative du secret de la défense nationale. Il la porte, au commencement de la perquisition, à la connaissance du chef d'établissement ou de son délégué, ou du responsable du lieu.

« La perquisition doit être précédée d'une décision de déclassification temporaire du lieu aux fins de perquisition et ne peut être entreprise que dans les limites de la déclassification ainsi décidée. À cette fin, le président de la Commission consultative du secret de la défense nationale, saisi par la décision du magistrat mentionnée à l'alinéa précédent, fait connaître sans délai son avis à l'autorité administrative compétente sur la déclassification temporaire, totale ou partielle, du lieu aux fins de perquisition. L'autorité administrative fait connaître sa décision sans délai. La déclassification prononcée par l'autorité administrative ne vaut que pour le temps des opérations. En cas de déclassification partielle, la perquisition ne peut être réalisée que dans la partie des lieux qui fait l'objet de la décision de déclassification de l'autorité administrative.

« La perquisition se poursuit dans les conditions prévues au sixième alinéa et suivants du I.

« IV. Les dispositions du présent article sont édictées à peine de nullité » ;

19. Considérant que, selon les requérants, ces dispositions, qui sont relatives tant aux informations qu'aux lieux classifiés au titre du secret de la défense nationale, méconnaissent le droit à un procès équitable et le principe de la séparation des pouvoirs figurant à l'article 16 de la Déclaration des droits de l'homme et du citoyen de 1789 ;

– SUR LES NORMES CONSTITUTIONNELLES APPLICABLES :

20. Considérant, d'une part, qu'aux termes de l'article 16 de la Déclaration de 1789 : «Toute société dans laquelle la garantie des droits n'est pas assurée, ni la séparation des pouvoirs déterminée, n'a point de Constitution » ; qu'en vertu de l'article 5 de la Constitution, le Président de la République est le garant de l'indépendance nationale et de l'intégrité du territoire ; qu'aux termes du premier alinéa de l'article 20 : « Le Gouvernement détermine et conduit la politique de la Nation » ; que le principe de la séparation des pouvoirs s'applique à l'égard du Président de la République et du Gouvernement ; que le secret de la défense nationale participe de la sauvegarde des intérêts fondamentaux de la Nation, réaffirmés par la charte de l'environnement, au nombre desquels figurent l'indépendance de la Nation et l'intégrité du territoire ;

21. Considérant, d'autre part, que l'article 16 de la Déclaration de 1789 implique le respect du caractère spécifique des fonctions juridictionnelles, sur lesquelles ne peuvent empiéter ni le législateur ni le Gouvernement, ainsi que le droit des personnes intéressées à exercer un recours juridictionnel effectif et le droit à un procès équitable ; qu'en outre, la recherche des auteurs d'infractions constitue un objectif de valeur constitutionnelle nécessaire à la sauvegarde de droits et de principes de valeur constitutionnelle ;

22. Considérant qu'en vertu de l'article 34 de la Constitution, le législateur est compétent pour fixer les règles concernant les

garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques, les sujétions imposées par la défense nationale aux citoyens en leur personne et en leurs biens, la détermination des crimes et délits, ainsi que les peines qui leur sont applicables et la procédure pénale ; que tant le principe de la séparation des pouvoirs que l'existence d'autres exigences constitutionnelles lui imposent d'assurer une conciliation qui ne soit pas déséquilibrée entre le droit des personnes intéressées à exercer un recours juridictionnel effectif, le droit à un procès équitable ainsi que la recherche des auteurs d'infractions et les exigences constitutionnelles inhérentes à la sauvegarde des intérêts fondamentaux de la Nation ;

– SUR LES INFORMATIONS CLASSIFIÉES AU TITRE DU SECRET DE LA DÉFENSE NATIONALE :

23. Considérant que l'article 413-9 du Code pénal définit les informations qui peuvent être classifiées au titre du secret de la défense nationale ; que les articles 413-10, 413-11 et 413-12 du même code répriment la violation de ce secret ; que les articles L. 2311-1, L. 2312-1, alinéas 1er et 2, L. 2312-2, L. 2312-3, L. 2312-4, alinéas 1er à 3, L. 2312-5, L. 2312-6, L. 2312-7 et L. 2312-8 du Code de la défense déterminent le rôle de la Commission consultative du secret de la défense nationale dans la procédure de déclassification et de communication des informations classifiées ; que les paragraphes I et II de l'article 56-4 du Code de procédure pénale fixent les conditions d'accès aux informations classifiées à l'occasion des perquisitions dans les lieux précisément identifiés comme abritant des éléments couverts par le secret de la défense nationale et dans les lieux se révélant abriter des éléments couverts par ce secret ;

24. Considérant que, selon les requérants, en privant le juge du pouvoir et des moyens d'apprécier l'intégralité des éléments déterminants pour l'issue du procès et en ne prévoyant pas de recours juridictionnel permettant à un juge de porter une appréciation sur la nature des informations classifiées, le législateur a méconnu l'article 16 de la Déclaration de 1789 ;

– En ce qui concerne la procédure de déclassification et de communication des informations classifiées :

25. Considérant qu'en vertu de l'article 413-9 du Code pénal, peuvent faire l'objet d'une mesure de classification les procédés, objets, documents, informations, réseaux informatiques, données informatisées ou fichiers dont la divulgation ou auxquels l'accès est de nature à nuire à la défense nationale ou pourrait conduire à la découverte d'un secret de la défense nationale ; que les niveaux de classification et les autorités chargées de définir les modalités selon lesquelles est organisée la protection desdites informations sont déterminés par décret en Conseil d'État ; qu'en outre, les articles 413-10, 413-11 et 413-12 du même code répriment la violation du secret de la défense nationale ;

26. Considérant, en premier lieu, que, lorsqu'une juridiction présente une demande motivée tendant à la déclassification et à la communication d'informations protégées à l'autorité administrative en charge de la classification, cette dernière saisit sans délai la Commission consultative du secret de la défense nationale ; que cette Commission émet un avis dans les deux mois à compter de sa saisine en prenant en considération les missions du service public de la justice, le respect de la présomption d'innocence et les droits de la défense, le respect des engagements internationaux de la France, ainsi que la nécessité de préserver les capacités de défense et la sécurité des personnels ; qu'à cette fin, le président de la Commission peut mener toutes investigations utiles et les membres de cette même Commission peuvent accéder à l'ensemble des informations classifiées ; que l'avis dont le sens peut être favorable, favorable à une déclassification partielle ou défavorable est adressé à l'autorité administrative ; que, dans un délai de quinze jours à compter de la réception de l'avis ou à l'expiration d'un délai de deux mois à compter de la saisine de la Commission, l'autorité administrative notifie sa décision, assortie du sens de l'avis, à la juridiction intéressée ; qu'en outre, le sens de cet avis est publié au *Journal officiel de la République française* ;

27. Considérant, en second lieu, qu'aux termes de l'article L. 2312-1 du Code de la défense, la Commission consultative du secret de la défense nationale est une « autorité administrative indépendante » ; qu'elle est composée de cinq membres, dont un président, un vice-président et un membre, tous trois choisis par le Président de la République sur une liste de six membres du Conseil d'État, de la Cour de cassation ou de la Cour des comptes, établie conjointement par le vice-président du Conseil d'État, le premier président de la Cour de cassation et le premier président de la Cour des comptes, un député désigné par le président de l'Assemblée nationale pour la durée de la législature et un sénateur désigné par le président du Sénat après chaque renouvellement partiel de cette assemblée ; que la durée du mandat des membres non parlementaires est fixée à six ans ; que leur mandat n'est pas renouvelable ; qu'il ne peut être mis fin à leurs fonctions qu'en cas d'empêchement constaté par la Commission ; qu'est garantie son autonomie de gestion administrative et financière ; que les ministres, autorités publiques et agents publics ne peuvent s'opposer à son action pour quel que motif que ce soit et prennent toutes mesures utiles pour la faciliter ;

28. Considérant qu'en raison des garanties d'indépendance conférées à la Commission ainsi que des conditions et de la procédure de déclassification et de communication des informations classifiées, le législateur a opéré, entre les exigences constitutionnelles précitées, une conciliation qui n'est pas déséquilibrée ; que, par suite, les dispositions de l'article L. 2311-1, des premier et deuxième alinéas de l'article L. 2312-1, des articles L. 2312-2 et L. 2312-3, des premier au troisième alinéas de l'article L. 2312-4, de l'article L. 2312-5 et des articles L. 2312-6, L. 2312 7 et L. 2312-8 du Code de la défense, ainsi que les dispositions

des articles 413-9, 413-10, 413-11 et 413-12 du Code pénal ne sont pas contraires à la Constitution ;

– En ce qui concerne l'accès aux informations classifiées à l'occasion de perquisitions ;

– Quant aux perquisitions dans les lieux précisément identifiés comme abritant des éléments couverts par le secret de la défense nationale ;

29. Considérant que les dispositions du paragraphe I de l'article 56-4 du Code de procédure pénale prévoient que le Premier ministre détermine de façon limitative les lieux précisément identifiés abritant des éléments couverts par le secret de la défense nationale ; que cette liste, régulièrement actualisée, est communiquée à la Commission consultative du secret de la défense nationale ainsi qu'au ministre chargé de la Justice ; qu'elle est rendue accessible de façon sécurisée à tout magistrat intéressé ; qu'il ressort des travaux parlementaires que, par l'expression « lieu précisément identifié », le législateur a entendu que ne soit pas désigné un bâtiment dans son ensemble ou une catégorie de locaux mais une pièce clairement déterminée ; que la perquisition envisagée dans un lieu précisément identifié, abritant des éléments couverts par le secret de la défense nationale, n'est subordonnée à aucune autorisation préalable ; que le fait de dissimuler des informations non classifiées, en tentant de les faire bénéficier de la protection attachée au secret de la défense nationale, est pénalement réprimé ;

30. Considérant que, dans ces conditions, si le législateur a subordonné la perquisition d'un magistrat dans un lieu précisément identifié comme abritant des éléments couverts par le secret de la défense nationale à la présence du président de la Commission ou de son représentant et a écarté la possibilité pour ce magistrat de prendre connaissance des éléments classifiés découverts sur les lieux, il a assorti la procédure de perquisition de garanties de nature à assurer, entre les exigences constitutionnelles précitées, une conciliation qui n'est pas déséquilibrée ; que, par suite, les dispositions du paragraphe I de l'article 56-4 du Code de procédure pénale sont conformes à la Constitution ;

– Quant aux perquisitions dans les lieux se révélant abriter des éléments couverts par le secret de la défense nationale :

31. Considérant que les dispositions du paragraphe II de l'article 56-4 du Code de procédure pénale définissent le régime juridique des perquisitions au cours desquelles des éléments protégés par le secret de la défense nationale sont incidemment découverts ; qu'en pareille hypothèse, le magistrat présent ou immédiatement avisé par l'officier de police judiciaire en informe le président de la Commission ; que, sans en prendre connaissance, le magistrat ou l'officier de police judiciaire qui les a découverts place sous scellés les éléments classifiés et les remet ou les transmet, par tout moyen, au président de la Commission chargé

d'en assurer la garde ; qu'un procès-verbal, qui n'est pas joint à la procédure, est rédigé pour rendre compte des opérations relatives aux éléments classifiés ; que seule la Commission, ou sur délégation de celle-ci son président, est habilitée à procéder à l'ouverture des scellés des éléments classifiés qui lui sont remis ; qu'en pareil cas, la Commission en fait mention dans son procès-verbal de séance ; qu'enfin, les documents sont restitués à l'autorité administrative par la Commission lors de la transmission de son avis ;

32. Considérant qu'il résulte de l'ensemble de ces dispositions que les perquisitions dans les lieux se révélant abriter des éléments couverts par le secret de la défense nationale s'accompagnent des garanties appropriées permettant d'assurer, entre les exigences constitutionnelles précitées, une conciliation qui n'est pas déséquilibrée ; que, par suite, les dispositions du paragraphe II de l'article 56-4 du Code de procédure pénale sont conformes à la Constitution ;

– SUR LES LIEUX CLASSIFIÉS AUTITRE DU SECRET DE LA DÉFENSE NATIONALE :

33. Considérant, d'une part, que l'article 413-9-1 du Code pénal autorise la classification des lieux auxquels il ne peut être accédé sans que, à raison des installations ou des activités qu'ils abritent, cet accès donne par lui-même connaissance d'un secret de la défense nationale ; qu'il prévoit que la décision de classification est prise pour une durée de cinq ans par arrêté du Premier ministre, publié au *Journal officiel*, après avis de la Commission consultative du secret de la défense nationale ; qu'en outre, les articles 413-10-1 et 413-11-1 du Code pénal répriment la violation de ces dispositions relatives aux lieux classifiés ;

34. Considérant, d'autre part, qu'il ressort des dispositions du paragraphe III de l'article 56-4 du Code de procédure pénale qu'une perquisition dans un lieu classifié ne peut être réalisée que par un magistrat et en présence du président de la Commission ; que ce dernier peut être représenté par un membre de la Commission et être assisté de toute personne habilitée à cet effet ; que le magistrat vérifie auprès de la Commission si le lieu dans lequel il souhaite effectuer une perquisition fait l'objet d'une mesure de classification ; qu'en pareil cas, ce magistrat indique, de manière écrite et motivée, la nature de l'infraction ou des infractions sur lesquelles portent les investigations, les raisons justifiant la perquisition et l'objet de celle-ci, ainsi que le lieu visé par la perquisition ;

35. Considérant que la perquisition dans un lieu classifié est subordonnée à une décision de déclassification temporaire du lieu ; que, lorsqu'il est saisi par un magistrat d'une demande de déclassification temporaire, le président de la Commission donne un avis sur cette demande à l'autorité administrative compétente ; que cette dernière fait connaître sa décision sans délai ; que la déclassification prononcée par cette autorité ne vaut que pour le temps des opérations ; qu'en cas de déclassification partielle, la perquisition ne peut être réalisée que dans

la partie des lieux qui fait l'objet de la décision de déclassification de l'autorité administrative ;

36. Considérant que, selon les requérants, en admettant que tous les éléments de preuve qui se trouvent dans les lieux classifiés bénéficient de la protection du secret de la défense nationale et en subordonnant les perquisitions dans ces lieux à une autorisation de l'autorité administrative sans qu'aucun contrôle juridictionnel ne puisse s'exercer sur la décision refusant au magistrat d'accéder à ces lieux, le législateur a méconnu l'article 16 de la Déclaration de 1789 ;

37. Considérant que la classification d'un lieu a pour effet de soustraire une zone géographique définie aux pouvoirs d'investigation de l'autorité judiciaire ; qu'elle subordonne l'exercice de ces pouvoirs d'investigation à une décision administrative ; qu'elle conduit à ce que tous les éléments de preuve, quels qu'ils soient, présents dans ces lieux lui soient inaccessibles tant que cette autorisation n'a pas été délivrée ; que, par suite, en autorisant la classification de certains lieux au titre du secret de la défense nationale et en subordonnant l'accès du magistrat aux fins de perquisition de ces mêmes lieux à une déclassification temporaire, le législateur a opéré, entre les exigences constitutionnelles précitées, une conciliation qui est déséquilibrée ; qu'ainsi, les dispositions du paragraphe III de l'article 56-4 du Code de procédure pénale, celles des articles 413 9 1, 413-10-1 et 413-11-1 du Code pénal, celles du troisième alinéa de l'article L. 2312-1, du quatrième alinéa de l'article L. 2312-4, celles de l'article L. 2312-7-1 du Code de la défense, ainsi que, par voie de conséquence, les mots : « Et d'accéder à tout lieu classifié » figurant au deuxième alinéa de l'article L. 2312-5 du même code doivent être déclarées contraires à la Constitution ;

38. Considérant qu'aux termes du deuxième alinéa de l'article 62 de la Constitution : « Une disposition déclarée inconstitutionnelle sur le fondement de l'article 61-1 est abrogée à compter de la publication de la décision du Conseil constitutionnel ou d'une date ultérieure fixée par cette décision. Le Conseil constitutionnel détermine les conditions et limites dans lesquelles les effets que la disposition a produits sont susceptibles d'être remis en cause » ; que, si, en principe, la déclaration d'inconstitutionnalité doit bénéficier à l'auteur de la question prioritaire de constitutionnalité et la disposition déclarée contraire à la Constitution ne peut être appliquée dans les instances en cours à la date de la publication de la décision du Conseil constitutionnel, les dispositions de l'article 62 de la Constitution réservent à ce dernier le pouvoir tant de fixer la date de l'abrogation et reporter dans le temps ses effets que de prévoir la remise en cause des effets que la disposition a produits avant l'intervention de cette déclaration ; qu'afin de permettre à l'autorité administrative de tirer les conséquences de cette inconstitutionnalité, il y a lieu de reporter la date de cette déclaration d'inconstitutionnalité au 1er décembre 2011 ;

D É C I D E :

Article 1er. – Sont contraires à la Constitution les dispositions suivantes :
– le paragraphe III de l'article 56-4 du Code de procédure pénale ;
– les articles L. 2312-1, alinéa 3, L. 2312-4, alinéa 4, et l'article L. 2312-7-1 du Code de la défense ;
– au deuxième alinéa de l'article L. 2312-5 du Code de la défense, les mots : « Et d'accéder à tout lieu classifié » ;
– les articles 413-9-1, 413-10-1 et 413-11-1 du Code pénal.

Article 2. – La déclaration d'inconstitutionnalité de l'article 1er prend effet le 1er décembre 2011 dans les conditions fixées au considérant 38.

Article 3. – Sont conformes à la Constitution les dispositions suivantes :
– les paragraphes I et II de l'article 56-4 du Code de procédure pénale ;
– les articles 413-9, 413-10, 413-11 et 413-12 du Code pénal ;
– le surplus des articles L. 2312-1, L. 2312-4 et L. 2312-5 du Code de la défense ;
– les articles L. 2311-1, L. 2312-2, L. 2312-3, L. 2312-6, L. 2312-7 et L. 2312-8 du Code de la défense.

Article 4. – La présente décision sera publiée au *Journal officiel de la République française* et notifiée dans les conditions prévues à l'article 23 11 de l'ordonnance du 7 novembre 1958 susvisée.

2) Cour européenne des droits de l'homme – *UZUN contre Allemagne* – 2 septembre 2010

En l'affaire *UZUN c/Allemagne*

PROCÉDURE

1. À l'origine de l'affaire se trouve une requête (no 35623/05) dirigée contre la République fédérale d'Allemagne et dont un ressortissant de cet État, M. Bernhard Uzun (« le requérant »), a saisi la Cour le 24 septembre 2005 en vertu de l'article 34 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales (« la Convention »). Le requérant, qui avait abandonné le nom de Falk pour celui de Uzun au cours de la procédure devant les juridictions internes, a repris le premier en 2009.

2. Le requérant, qui a été admis au bénéfice de l'assistance judiciaire, est représenté par Me H. Comes, avocat au barreau de Cologne. Le gouvernement allemand (« le Gouvernement ») est représenté par son agent, Mme A. Wittling-Vogel, *Ministerialdirigentin*, du ministère fédéral de la Justice.

3. Le requérant allègue que les mesures de surveillance dont il a fait l'objet, en particulier par GPS, et l'utilisation des informations ainsi obtenues dans le cadre de la procédure pénale dirigée contre lui ont emporté violation de son droit au respect de sa vie privée garanti par l'article 8 de la Convention et de son droit à un procès équitable protégé par l'article 6 de la Convention.

4. Le 21 avril 2008, le président de la cinquième section a décidé de communiquer la requête au Gouvernement. Se prévalant de l'article 29 § 3 de la Convention, il a en outre résolu que seraient examinés en même temps la recevabilité et le fond de l'affaire.

EN FAIT

I. LES CIRCONSTANCES DE L'ESPÈCE

5. Le requérant est né en 1967 et réside à Mönchengladbach.

A. Le contexte

6. Au printemps 1993, le ministère de la Protection de la Constitution (*Verfassungsschutz*) de la Rhénanie-du-Nord-Westphalie entama une surveillance de longue durée du requérant. Celui-ci était soupçonné d'avoir participé aux infractions commises par la cellule anti-impérialiste (*Antiimperialistische Zelle*), une organisation qui poursuivait la lutte armée abandonnée en 1992 par la Fraction armée rouge (*Rote Armee Fraktion*), mouvement terroriste d'extrême gauche.

7. En conséquence, le requérant fit occasionnellement l'objet d'une surveillance visuelle d'agents du ministère de la Protection de la Constitution et les entrées dans ses appartements furent filmées au moyen de caméras vidéo. En outre, les téléphones du domicile où il vivait avec sa mère (du 26 avril 1993 au 4 avril 1996) et celui d'une cabine téléphonique située à proximité (du 11 janvier 1995 au 25 février 1996) furent mis sur écoute par le ministère, et son courrier fut ouvert et vérifié (du 29 avril 1993 au 29 mars 1996).

8. De même, S., un complice présumé du requérant, fut soumis à des mesures de surveillance à partir de 1993. L'Office de protection de la Constitution de Hambourg intercepta les communications téléphoniques du domicile de ses parents ainsi que son courrier. De surcroît, des agents de l'Office le surveillèrent occasionnellement.

9. En octobre 1995, le procureur général près la Cour fédérale de justice ouvrit une instruction contre le requérant et S. pour participation à des attentats à la bombe revendiqués par la cellule anti-impérialiste. L'Office fédéral de la police judiciaire fut chargé des investigations.

10. Le requérant et S. firent alors l'objet d'une surveillance visuelle d'agents de l'Office fédéral de la police judiciaire, essentiellement pendant les week-ends, du 30 septembre 1995 au 25 février 1996, date de leur arrestation. En outre, les entrées dans la maison où il vivait avec sa mère

furent surveillées au moyen d'une caméra vidéo supplémentaire installée par l'Office fédéral de la police judiciaire (d'octobre 1995 à février 1996). Les téléphones dans cette maison, dans une cabine téléphonique située à proximité et dans l'appartement de S. à Hambourg furent placés sur écoute sur l'ordre du juge d'instruction près la Cour fédérale de justice (du 13 octobre 1995 au 27 février 1996). Celui-ci ordonna également à la police de surveiller le requérant et S. ainsi que les véhicules utilisés par eux. L'Office fédéral de la police judiciaire surveilla également l'entrée de l'appartement de S. au moyen de caméras vidéo (d'octobre 1995 à février 1996). En outre, il intercepta les radiocommunications professionnelles de S.

11. En octobre 1995, l'Office fédéral de la police judiciaire installa également deux émetteurs (*Peilsender)* dans la voiture de S., que celui-ci et le requérant utilisaient souvent ensemble. Toutefois, les intéressés découvrirent les dispositifs et les détruisirent. Soupçonnant que leurs télécommunications étaient interceptées et qu'ils étaient surveillés, ils ne se parlèrent plus jamais au téléphone et réussirent à plusieurs occasions à se dérober à la surveillance visuelle des autorités d'enquête.

12. Cela étant, sur l'ordre du procureur général près la Cour fédérale de justice, l'Office fédéral de la police judiciaire installa un récepteur GPS (système de géolocalisation par satellite) dans le véhicule de S. en décembre 1995. Il fut ainsi en mesure de localiser la voiture et d'établir sa vitesse toutes les minutes. Toutefois, pour éviter que le récepteur ne fût détecté, les données ne furent collectées que tous les deux jours. Cette surveillance dura jusqu'à l'arrestation du requérant et de S., le 25 février 1996.

13. Le GPS est un système de radionavigation fonctionnant à l'aide de satellites. Il permet la localisation continue et en temps réel des objets équipés d'un récepteur GPS en n'importe quel endroit sur terre, avec une précision maximale de 50 mètres à l'époque. Il n'implique aucune surveillance visuelle ou acoustique. Contrairement aux émetteurs, son utilisation n'exige pas de savoir où la personne à localiser se trouve approximativement.

B. La procédure devant la cour d'appel de Düsseldorf

14. Dans le cadre de la procédure pénale ouverte contre le requérant et S., la cour d'appel de Düsseldorf, par une décision du 12 décembre 1997, rejeta l'objection du requérant à l'utilisation en tant que preuve des informations obtenues grâce à la surveillance par GPS. Elle estima que le recours au GPS en l'espèce était autorisé par l'article 100c § 1.1. b) du Code de procédure pénale (paragraphe 29 ci-dessous). Les renseignements fiables ainsi recueillis pouvaient donc être utilisés au procès. Ils étaient confirmés par les éléments obtenus au moyen de la surveillance personnelle et vidéo – légale – des accusés. En outre, contrairement à ce que soutenait le requérant, aucune décision judiciaire n'était nécessaire pour la localisation par GPS, cette mesure ayant été associée à d'autres

méthodes de surveillance légales. Le Code de procédure pénale n'exigeait pas que la surveillance par GPS fût ordonnée par un juge, contrairement aux mesures portant plus profondément atteinte au droit à l'autodétermination dans la sphère de l'information (*Recht auf informationnelle Selbstbestimmung*).

La possibilité d'ordonner une mesure de surveillance en plus des mesures déjà en place tenait à la proportionnalité de la mesure supplémentaire en question.

15. Le 1er septembre 1999, la cour d'appel de Düsseldorf condamna le requérant à une peine de treize ans d'emprisonnement, notamment pour tentative de meurtre et pour quatre attentats à la bombe. Elle conclut que l'intéressé et S., qui étaient les seuls membres de la cellule anti-impérialiste depuis le printemps 1995, avaient posé des bombes devant le domicile de députés et d'anciens députés et devant le consulat honoraire du Pérou entre janvier et décembre 1995.

16. La cour d'appel releva que le requérant s'était prévalu de son droit de garder le silence sur les accusations portées contre lui et que S. avait seulement avoué de manière générale avoir participé aux attentats à la bombe, sans donner de précisions. Or, les preuves indirectes recueillies grâce aux mesures mises en œuvre pour surveiller les intéressés prouvaient que ceux-ci avaient commis les infractions dont ils avaient été reconnus coupables.

17. En particulier, s'agissant de l'attentat à la bombe commis après la surveillance par GPS de la voiture de S., la cour d'appel releva qu'il était démontré que la voiture avait stationné à proximité du lieu de l'infraction le jour où celle-ci avait été commise et quelques jours auparavant. De plus, la voiture avait été localisée près des lieux où les accusés avaient photocopié, caché puis posté des lettres revendiquant l'attentat et à proximité de sites dans la forêt où les enquêteurs avaient par la suite découvert des endroits où étaient cachés les matériaux nécessaires à la construction de la bombe. Ces éléments étaient corroborés par les renseignements obtenus grâce à d'autres moyens de surveillance, en particulier la surveillance vidéo de l'entrée du domicile du requérant et la surveillance visuelle des accusés par des agents de l'Office fédéral de la police judiciaire. La participation des accusés à des attentats à la bombe perpétrés avant leur surveillance par GPS était prouvée par la similitude des méthodes employées ainsi que par les informations obtenues par la surveillance vidéo des domiciles des intéressés et par l'interception de leurs télécommunications.

C. La procédure devant la Cour fédérale de justice

18. Le requérant se pourvut en cassation, se plaignant en particulier de l'utilisation au procès d'éléments de preuve obtenus grâce à sa surveillance effectuée de façon prétendument illégale, notamment par GPS.

19. Par un arrêt du 24 janvier 2001, la Cour fédérale de justice rejeta le pourvoi en cassation pour défaut de fondement. Elle considéra que la collecte de données au moyen du GPS avait une base légale, notamment l'article 100c § 1.1. b) du Code de procédure pénale. Dès lors, les renseignements ainsi obtenus pouvaient être employés dans le cadre de la procédure pénale dirigée contre le requérant.

20. En particulier, le recours à des dispositifs techniques de localisation, tels que le GPS, ne constituait pas une immixtion dans le domicile du requérant. Étant donné que celui-ci était soupçonné d'infractions extrêmement graves, notamment de participation à des attentats à la bombe commis par une organisation terroriste, le recours au GPS représentait une ingérence proportionnée dans l'exercice par l'intéressé de son droit au respect de sa vie privée (tel que protégé également par l'article 8 de la Convention) et de son droit à l'autodétermination dans la sphère de l'information. D'autres méthodes d'enquête auraient donné moins de résultats puisque le requérant et S. avaient souvent réussi à se dérober à certaines mesures de surveillance.

21. Souscrivant aux motifs exposés par la cour d'appel, la Cour fédérale de justice estima en outre qu'en cas de recours à plusieurs mesures d'enquête simultanément il n'y avait aucune obligation de fournir une base légale supplémentaire ni d'obtenir une décision judiciaire. Cependant, les autorités d'enquête devaient examiner s'il était proportionné ou non d'ordonner la mise en œuvre d'une autre mesure de surveillance, en plus de celles qui étaient déjà prises. Quoi qu'il en soit, le requérant n'avait pas fait l'objet d'une surveillance totale qui, à elle seule, était de nature à enfreindre le principe de proportionnalité et le droit au respect de la vie privée, et soulever la question de l'exclusion, dans le cadre de la procédure pénale, d'éléments ainsi obtenus.

22. La Cour fédérale de justice concéda que, depuis l'introduction de modifications législatives en 2000, l'article 163f § 4 du Code de procédure pénale (paragraphe 32 ci-dessous) énonçait que toute observation de longue durée supérieure à un mois devait être ordonnée par un juge, que des moyens techniques de surveillance fussent utilisés ou non. Cependant, la nécessité d'obtenir une décision judiciaire ne ressortait ni du Code de procédure pénale, ni du droit constitutionnel, ni de l'article 8 de la Convention.

D. La procédure devant la Cour constitutionnelle fédérale

23. Le requérant saisit ensuite la Cour constitutionnelle fédérale, alléguant en particulier que sa surveillance d'octobre 1995 à février 1996 par les offices de protection de la Constitution de la Rhénanie-du-Nord-Westphalie et de Hambourg et par l'Office fédéral de la police judiciaire ainsi que les arrêts de la cour d'appel et de la Cour fédérale de justice emportaient violation de son droit au respect de sa vie privée. Il soutenait que l'article 100c § 1.1. b) du Code de procédure pénale ne pouvait passer pour offrir une base légale suffisamment précise pour sa surveillance par

GPS. Cette mesure n'avait pas fait l'objet d'un contrôle judiciaire effectif et le recours simultané à plusieurs moyens de surveillance aurait exigé une base légale distincte pour chacun d'eux. En outre, le requérant alléguait que l'utilisation au procès des informations obtenues au moyen de ces mesures, qui étaient dépourvues de base légale, avait porté atteinte à son droit à un procès équitable.

24. Le 12 avril 2005, après avoir tenu une audience, la Cour constitutionnelle fédérale écarta le recours (dossier n° 2 BvR 581/01). Elle le jugea mal fondé pour autant que le requérant se plaignait de l'utilisation dans le cadre de la procédure d'éléments obtenus au moyen de sa surveillance par GPS en plus d'autres mesures de surveillance et que ces mesures étaient illégales.

25. L'article 100c § 1.1. b) du Code de procédure pénale pouvait constituer la base légale de la surveillance par GPS du requérant. Cette disposition était constitutionnelle. En particulier, l'expression « moyens techniques spéciaux destinés à la surveillance » était suffisamment précise. À la différence de la surveillance visuelle ou acoustique, les moyens englobaient la localisation d'une personne et l'établissement de ses déplacements à l'aide de moyens techniques tels que le GPS. Le législateur n'était pas tenu de définir les méthodes de surveillance de telle manière que l'application de nouvelles techniques scientifiques soit exclue. Toutefois, il y avait un risque d'atteinte au droit à l'autodétermination dans la sphère de l'information, c'est-à-dire le droit pour la personne de décider de l'utilisation de données la concernant. Dès lors, le législateur devait suivre les progrès techniques et, le cas échéant, garantir le respect par les autorités d'enquête des droits fondamentaux en édictant de nouvelles dispositions législatives.

26. En outre, la mesure n'avait pas porté atteinte de manière disproportionnée au droit du requérant au respect de sa vie privée. La surveillance de l'intéressé n'avait pas touché à la substance même de sa vie privée. Au contraire, une telle surveillance par des moyens techniques permettait dans certains cas d'éviter des atteintes graves, par exemple l'interception des communications. Dès lors, il n'était pas disproportionné d'ordonner cette mesure de surveillance lorsqu'il existait seulement un début de soupçon de commission d'une infraction (extrêmement grave) et lorsque d'autres méthodes d'enquête avaient moins de chance d'aboutir. De plus, le législateur n'était pas tenu de prévoir des garanties supplémentaires pour une surveillance de longue durée – il le fit par la suite en adoptant l'article 163 f § 4 du Code de procédure pénale – mais était en droit d'observer d'abord l'évolution dans ce domaine.

27. Par ailleurs, le législateur n'était pas obligé de réglementer le recours à plusieurs mesures de surveillance simultanément. La surveillance totale d'une personne permettant de dresser un profil personnel exhaustif serait inconstitutionnelle, mais elle pouvait en principe être évitée grâce aux garanties procédurales en place. Toutefois, lorsqu'il

ordonnait une mesure de surveillance, le parquet devait s'assurer sur la base des pièces pertinentes figurant dans le dossier et dans les registres fédéraux qu'il avait connaissance de l'ensemble des autres mesures de surveillance dont l'intéressé faisait simultanément l'objet. En outre, le législateur devait examiner si, eu égard à l'évolution future, les garanties procédurales existantes étaient suffisantes pour fournir une protection effective des droits fondamentaux et éviter la mise en œuvre non coordonnée de mesures d'enquête par différentes autorités.

28. En l'espèce, l'atteinte causée aux droits du requérant par sa surveillance par GPS était proportionnée, notamment eu égard à la gravité des infractions dont il était soupçonné et le fait qu'il s'était dérobé à d'autres mesures de surveillance. Le recours à plusieurs mesures d'observation simultanément n'avait pas donné lieu à une surveillance totale. Le requérant avait été géolocalisé uniquement lorsqu'il s'était déplacé dans la voiture de S. D'autres mesures de surveillance avaient essentiellement été appliquées durant les week-ends exclusivement et avaient englobé, dans une moindre mesure seulement, l'interception de communications.

II. LE DROIT INTERNE PERTINENT

29. L'article 100c § 1.1 fut inséré dans le Code de procédure pénale par la loi sur la lutte contre le trafic de stupéfiants et d'autres formes de crime organisé (*Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität*) du 15 juillet 1992. Tel qu'en vigueur à l'époque des faits, l'article 100c du Code de procédure pénale, en ses passages pertinents en l'espèce, se lisait ainsi :

« (1) Il est possible, à l'insu de l'intéressé,

1.
a) de prendre des photographies et de réaliser des films ;
b) de recourir à d'autres moyens techniques spéciaux destinés à la surveillance aux fins d'enquêter sur les faits de la cause ou de localiser l'auteur d'une infraction lorsque l'enquête concerne une infraction extrêmement grave, et lorsque d'autres moyens d'enquête sur les faits de l'affaire ou de localisation de l'auteur de l'infraction ont moins de chance d'aboutir ou sont plus difficiles à mettre en œuvre […].

2.

D'écouter et d'enregistrer à l'aide de moyens techniques des propos tenus en privé […].

(2) Les mesures prévues par le premier paragraphe ne peuvent être prises que contre l'accusé […]. Celles prévues par le premier paragraphe 1 b) […] ne peuvent être ordonnées contre des tiers que si des faits précis permettent de présumer qu'ils sont ou seront en rapport avec l'auteur de l'infraction et que la mesure permettra d'établir les faits ou de

localiser l'auteur de l'infraction ou lorsque d'autres moyens ont moins de chances d'aboutir ou sont considérablement plus difficiles à mettre en œuvre. »

30. En vertu de l'article 100d § 1 du Code de procédure pénale, dans sa version en vigueur à l'époque des faits, le recours, sur le fondement de l'article 100c § 1.2 dudit code, à des dispositifs techniques d'écoute ou d'enregistrement de conversations tenues en privé était subordonné à l'obtention d'une décision judiciaire – tout comme l'était le placement du téléphone d'une personne sur écoute (article 100b § 1 du Code de procédure pénale). Toutefois, cette disposition ne faisait pas obligation d'obtenir une telle décision pour les mesures d'enquête prises sur la base de l'article 100c § 1.1.

31. D'après l'article 101 § 1 du Code de procédure pénale, la personne faisant l'objet d'une mesure prise en vertu de l'article 100c § 1.1. b) de ce Code devait être informée de cette mesure dès que la notification pouvait se faire sans compromettre l'enquête, la sécurité publique, la vie et l'intégrité physique d'autrui ou le recours futur éventuel à un agent infiltré intervenant dans la mise en œuvre de la mesure.

32. Le 1er novembre 2000 entra en vigueur l'article 163f du Code de procédure pénale sur la surveillance systématique de longue durée de suspects. D'après le premier paragraphe de cette disposition, une telle surveillance durant plus de 24 heures d'affilée ou opérée plus de deux jours au total, ne peut être ordonnée qu'à l'égard de personnes soupçonnées d'infractions extrêmement graves et lorsque d'autres moyens d'enquête destinés à établir les faits de l'affaire ou à localiser le suspect ont nettement moins de chances d'aboutir ou sont considérablement plus difficiles à mettre en œuvre. La mesure doit être ordonnée par le parquet (paragraphe 3). Selon le paragraphe 4, sa mise en œuvre ne peut dépasser un mois ; toute prolongation doit être ordonnée par un juge.

EN DROIT

I. SUR LA VIOLATION ALLÉGUÉE DE L'ARTICLE 8 DE LA CONVENTION

33. Le requérant se plaint que sa surveillance par GPS et le recours à plusieurs autres mesures de surveillance simultanément ainsi que l'utilisation des données ainsi obtenues dans le cadre de la procédure pénale dirigée contre lui ont emporté violation de son droit au respect de sa vie privée garanti par l'article 8 de la Convention, lequel, en ses passages pertinents en l'espèce, est ainsi libellé :

« 1. Toute personne a droit au respect de sa vie privée […].

2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions

pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. »

34. Le Gouvernement conteste cet argument.

A. Sur la recevabilité

1. Thèses des parties

a) Le Gouvernement

35. Le Gouvernement soutient que le requérant n'a pas épuisé les voies de recours internes, contrairement à ce qu'exige l'article 35 de la Convention. Dans la procédure devant les juridictions internes, l'intéressé ne se serait pas plaint de sa surveillance visuelle en tant que telle, qui à elle seule aurait établi un lien entre lui-même et les données obtenues par sa surveillance par GPS puisqu'elle aurait révélé sa présence dans la voiture de S. En outre, hormis sa surveillance par GPS, le requérant n'aurait pas contesté devant les juridictions internes la légalité de l'ensemble des autres mesures de surveillance, en particulier l'interception de ses télécommunications.

36. Le Gouvernement estime également que le requérant ne saurait se prétendre victime d'une violation de son droit au respect de sa vie privée aux fins de l'article 34 de la Convention. D'après lui, la surveillance par GPS de la voiture du complice S. n'a pas directement visé le requérant en personne.

b) Le requérant

37. Le requérant combat cette thèse. Il soutient en particulier avoir épuisé les voies de recours internes. Il aurait dénoncé tant devant les juridictions internes que devant la Cour la surveillance par GPS à laquelle il a été soumis simultanément à d'autres méthodes de surveillance et aurait objecté à l'utilisation des éléments de preuve obtenus au moyen du GPS et pas seulement à l'emploi des indications fournies par le GPS en tant que telles. En outre, tout au long de la procédure, il se serait également plaint d'avoir été placé sous une totale surveillance, eu égard au recours à différentes mesures de surveillance simultanément en plus du GPS, ce que confirmeraient les motifs des décisions rendues par les juridictions internes, qui ont examiné – et rejeté – les arguments à cet égard.

2. Appréciation de la Cour

38. En ce qui concerne l'objet du litige dont elle se trouve saisie, la Cour note que le requérant se plaint sous l'angle de l'article 8 de sa surveillance par GPS. L'intéressé soutient que cette mesure, considérée isolément, porte atteinte à son droit au respect de sa vie privée et, quoi qu'il en soit, enfreint l'article 8 en ce qu'elle a été associée à plusieurs autres mesures de surveillance. L'intéressé dénonce également l'utilisation dans le cadre de la procédure pénale dirigée contre lui des données ainsi réunies. Outre sa surveillance par GPS, le requérant n'a contesté la légalité

d'aucune des autres mesures de surveillance. La Cour observe que l'intéressé a soulevé son grief, tel que défini ci-dessus, devant la cour d'appel de Düsseldorf, la Cour fédérale de justice et la Cour constitutionnelle fédérale, qui l'ont toutes examiné et rejeté sur le fond (paragraphes 14, 18-22 et 23-28 ci-dessus). L'exception préliminaire de non-épuisement des voies de recours soulevée par le Gouvernement doit donc être rejetée.

39. Quant à la question de savoir si le requérant peut se prétendre victime d'une violation de son droit au respect de sa vie privée aux fins de l'article 34 de la Convention, étant donné que ce n'est pas lui-même mais la voiture de son complice qui était l'objet de la surveillance par GPS, la Cour estime que ce point est étroitement lié au fond du grief tiré de l'article 8. Dès lors, elle joint au fond l'exception préliminaire soulevée par le Gouvernement à cet égard.

40. Enfin, la Cour note que ce grief n'est pas manifestement mal fondé au sens de l'article 35 § 3 de la Convention. Elle estime de surcroît qu'il ne se heurte à aucun autre motif d'irrecevabilité. Partant, elle doit le déclarer recevable.

B. Sur le fond

1. Sur l'existence d'une ingérence dans la vie privée

a) Thèses des parties

41. Le requérant estime que le fait qu'il ait été intégralement surveillé par GPS a constitué une ingérence dans l'exercice de son droit au respect de sa vie privée. Bien que le récepteur GPS ait été posé sur un objet (la voiture de S.), il aurait été utilisé pour observer ses déplacements (et ceux de S.). Il aurait permis aux autorités d'enquête de suivre tous ses déplacements en public pendant des mois au moyen d'une mesure de très grande précision et difficile à repérer. Des tiers auraient été au courant de tous ses déplacements, alors qu'il n'avait pas donné son consentement. Les renseignements réunis grâce à la surveillance par GPS auraient permis aux autorités de procéder à d'autres investigations, notamment dans les lieux où il s'était rendu.

42. D'après le Gouvernement, la surveillance par GPS n'a pas constitué une ingérence dans l'exercice par le requérant de son droit au respect de sa vie privée garanti par l'article 8. Cette surveillance n'aurait pas directement visé le requérant en personne, le récepteur GPS ayant été posé sur la voiture de son complice S. et les données ainsi réunies ayant uniquement révélé où se trouvait le récepteur à un moment précis et non qui se trouvait dans la voiture de S.

b) Appréciation de la Cour

i. Rappel des principes pertinents :

43. La Cour rappelle que la « vie privée » est une notion large, qui ne se prête pas à une définition exhaustive. L'article 8 protège notamment le

droit à l'identité et au développement personnel ainsi que le droit pour tout individu de nouer et de développer des relations avec ses semblables et le monde extérieur. Il existe donc une zone d'interaction entre l'individu et autrui qui, même dans un contexte public, peut relever de la « vie privée » (*P.G. et J.H. c/ Royaume-Uni*, n° 44787/98, § 56, CEDH 2001-IX, *Peck c/ Royaume-Uni*, n° 44647/98, § 57, CEDH 2003-I, et *Perry c/ Royaume-Uni*, n° 63737/00, § 36, CEDH 2003-IX).

44. Un certain nombre d'éléments entrent en ligne de compte lorsqu'il s'agit de déterminer si la vie privée d'une personne est touchée par des mesures prises en dehors de son domicile ou de ses locaux privés. Puisqu'à certaines occasions les gens se livrent sciemment ou intentionnellement à des activités qui sont ou peuvent être enregistrées ou rapportées publiquement, ce qu'un individu est raisonnablement en droit d'attendre quant au respect de sa vie privée peut constituer un facteur significatif, quoique pas nécessairement décisif (*Perry*, précité, § 37). Une personne marchant dans la rue sera forcément vue par toute autre personne qui s'y trouve aussi. Le fait d'observer cette scène publique par des moyens techniques (par exemple un agent de sécurité exerçant une surveillance au moyen d'un système de télévision en circuit fermé) revêt un caractère similaire (voir également *Herbecq et Association « Ligue des droits de l'homme » c/ Belgique*, nos 32200/96 et 32201/96, décision de la Commission du 14 janvier 1998, décisions et rapports (DR) 92-B, p. 92, concernant l'utilisation de systèmes de prise de vue sans enregistrement des données visuelles recueillies). En revanche, la création d'un enregistrement systématique ou permanent de tels éléments appartenant au domaine public peut donner lieu à des considérations liées à la vie privée. (*P.G. et J.H. c/ Royaume-Uni*, précité, § 57, *Peck*, précité, §§ 58-59, et *Perry*, précité, § 38).

45. Parmi les autres éléments, la Cour a pris en considération à cet égard si des informations avaient été recueillies sur une personne bien précise, si des données à caractère personnel avaient été traitées ou utilisées et si les éléments en question avaient été rendus publics d'une manière ou dans une mesure excédant ce à quoi les intéressés pouvaient raisonnablement s'attendre.

46. Aussi la Cour a-t-elle estimé que la collecte et la conservation systématiques d'informations par des services de sécurité sur certains individus, même sans recours à des méthodes de surveillance secrète, constituaient une ingérence dans la vie privée de ces personnes (*Rotaru c/ Roumanie* [GC], n° 28341/95, §§ 43-44, CEDH 2000-V, *P.G. et J.H. c/ Royaume-Uni*, précité, § 57, *Peck*, précité, § 59, et *Perry*, précité, § 38, comparer aussi avec *Amann c/ Suisse* [GC], n° 27798/95, §§ 65-67, CEDH 2000-II, arrêt dans lequel la Cour a estimé que la conservation d'informations relatives au requérant sur une fiche dans un dossier constituait une ingérence dans la vie privée de l'intéressé, même si cette fiche ne contenait aucun élément sensible et n'avait probablement jamais été consultée). La Cour a également invoqué à cet égard la Convention du 28 janvier 1981, élaborée au sein du Conseil de l'Europe, pour la protection des

personnes à l'égard du traitement automatisé des données à caractère personnel, entrée en vigueur le 1er octobre 1985 – notamment à l'égard de l'Allemagne –, dont le but est « de garantir, sur le territoire de chaque partie, à toute personne physique […] le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant » (article 1), ces données étant définies comme « toute information concernant une personne physique identifiée ou identifiable » (article 2) (*P.G. et J.H. c/ Royaume-Uni*, précité, § 57).

47. La Cour a en outre examiné si la mesure litigieuse s'analysait en un traitement ou en une utilisation de données personnelles propres à porter atteinte au respect de la vie privée (voir, en particulier, *Perry*, précité, §§ 40-41). Ainsi, la Cour a estimé, par exemple, que l'enregistrement sur un support permanent des images du requérant délibérément prises au poste de police par une caméra de surveillance et l'utilisation de cette séquence dans une vidéo pour une procédure d'identification de témoins s'analysaient en un traitement de données personnelles sur le requérant portant atteinte à son droit au respect de sa vie privée (*ibidem*, §§ 39-43). De même, l'enregistrement en secret des voix des requérants au poste de police sur un support permanent aux fins d'un processus d'analyse directement destiné à identifier ces personnes à la lumière d'autres données personnelles a été considéré comme le traitement de données personnelles les concernant révélant une ingérence dans leur droit au respect de leur vie privée (*P.G. et J.H. c/ Royaume-Uni*, précité, §§ 59-60, et *Perry*, précité, § 38).

48. Enfin, les données ou éléments enregistrés peuvent également tomber sous le coup de l'article 8 § 1 de la Convention lorsqu'ils sont rendus publics d'une manière ou dans une mesure excédant ce que les intéressés peuvent normalement prévoir (*Peck*, précité, §§ 60-63, concernant la communication aux médias, pour diffusion, d'une séquence vidéo du requérant prise dans un lieu public, et *Perry*, précité, § 38).

ii. Application des principes susmentionnés au cas d'espèce :

49. Pour déterminer si la surveillance par GPS effectuée par les autorités d'enquête a constitué une ingérence dans l'exercice par le requérant de son droit au respect de sa vie privée, la Cour, eu égard aux principes susmentionnés, examinera d'abord si cette mesure a consisté à recueillir des données sur le requérant. Elle note que le Gouvernement soutient que tel n'a pas été le cas, le récepteur GPS ayant été intégré sur un objet (une voiture) appartenant à un tiers (le complice du requérant). Toutefois, en procédant de la sorte, les autorités d'enquête avaient manifestement l'intention de recueillir des informations sur les déplacements du requérant et de son complice, étant donné que leurs précédentes investigations leur avaient révélé que les deux suspects avaient utilisé ensemble la voiture de S. au cours des week-ends où des attentats à la bombe antérieurs avaient été commis (paragraphes 11 et 17 ci-dessus ;

voir également, *mutatis mutandis, Lambert c/ France*, 24 août 1998, § 21, *Recueil des arrêts et décisions* 1998-V, affaire dans laquelle la Cour a estimé qu'il importait peu pour le constat d'une ingérence dans la vie privée du requérant que les écoutes téléphoniques litigieuses aient été opérées sur la ligne d'une tierce personne).

50. De plus, il ne fait aucun doute que l'on doit considérer que le requérant, tout comme S., a fait l'objet de la surveillance par GPS puisque l'on n'a pu faire le lien entre les déplacements de la voiture de S. et le requérant qu'en soumettant celui-ci à une surveillance visuelle supplémentaire pour confirmer qu'il se trouvait bien dans ce véhicule. En fait, aucune des juridictions internes n'a contesté que le requérant avait été soumis à une surveillance par GPS (voir, en particulier, les paragraphes 14, 17, 20 et 26 ci-dessus).

51. La Cour relève en outre qu'en procédant à la surveillance du requérant par GPS, les autorités d'enquête ont, pendant quelque trois mois, systématiquement recueilli et conservé des données indiquant l'endroit où se trouvait l'intéressé et les déplacements de celui-ci en public. Elles ont de surcroît enregistré les données personnelles et les ont utilisées pour suivre tous les déplacements du requérant, pour effectuer des investigations complémentaires et pour recueillir d'autres éléments de preuve dans les endroits où le requérant s'était rendu, éléments qui ont ensuite été utilisés dans le cadre du procès pénal de l'intéressé (paragraphe 17 ci-dessus).

52. De l'avis de la Cour, il y a lieu de distinguer, de par sa nature même, la surveillance par GPS d'autres méthodes de surveillance par des moyens visuels ou acoustiques qui, en règle générale, sont davantage susceptibles de porter atteinte au droit d'une personne au respect de sa vie privée car elles révèlent plus d'informations sur la conduite, les opinions ou les sentiments de la personne qui en fait l'objet. Eu égard au principe consacré par sa jurisprudence, la Cour estime toutefois que les aspects susmentionnés suffisent pour conclure qu'en l'occurrence la surveillance du requérant par GPS ainsi que le traitement et l'utilisation des données ainsi obtenues dans les conditions décrites ci-dessus s'analysent en une ingérence dans la vie privée de l'intéressé, telle que protégée par l'article 8 § 1.

53. Par conséquent, l'exception préliminaire du Gouvernement selon laquelle le requérant ne peut se prétendre victime d'une violation de son droit au respect de sa vie privée au sens de l'article 34 de la Convention doit également être rejetée.

2. Sur la justification de l'ingérence

a) L'ingérence était-elle « prévue par la loi » ?

i. Thèses des parties

– Le requérant

54. Le requérant soutient que l'ingérence en question n'était pas justifiée au regard de l'article 8 § 2. L'article 100c § 1.1. b) du Code de procédure pénale n'aurait pas fourni une base légale suffisante à l'ingérence. Le législateur n'aurait pas eu l'intention d'englober dans cette disposition les mesures de surveillance non connues au moment de son adoption. En outre, l'expression « autres moyens techniques spéciaux destinés à la surveillance » figurant dans ladite disposition ne serait pas suffisamment claire et, eu égard aux progrès techniques possibles, son contenu n'aurait pas été prévisible pour les personnes éventuellement concernées. C'est ce que la Cour constitutionnelle fédérale aurait implicitement confirmé en déclarant que l'utilisation de nouvelles techniques scientifiques risquait d'entraîner des atteintes aux droits fondamentaux et que le législateur devait garantir le respect de ces droits par l'adoption, le cas échéant, de nouvelles dispositions législatives (paragraphe 25 ci-dessus).

55. En outre, d'après le requérant, les dispositions juridiques sur le fondement desquelles la surveillance par GPS a été ordonnée ne satisfont pas aux exigences qualitatives développées dans la jurisprudence de la Cour sur les mesures de surveillance secrète (le requérant renvoie en particulier à l'affaire *Weber et Saravia c/ Allemagne* (déc.), n° 54934/00, CEDH 2006-XI et à l'affaire *Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev c/ Bulgarie*, n° 62540/00, 28 juin 2007). En particulier, la loi ne fixerait aucune limite à la durée d'une telle surveillance. De plus, eu égard au degré d'ingérence, le fait que ce soient les autorités de poursuite, et non le juge d'instruction, qui aient ordonné ce type de surveillance n'aurait pas offert une protection suffisante contre l'arbitraire.

56. Le requérant estime en outre que le recours à de nombreuses autres mesures de surveillance, en plus de sa géolocalisation, a abouti à sa totale surveillance par les autorités de l'État et a emporté violation de ses droits garantis par l'article 8, la loi ne renfermant pas de garanties suffisantes contre les abus, en particulier du fait que l'autorisation et la supervision des mesures de surveillance dans leur ensemble n'étaient pas subordonnées à la délivrance d'une ordonnance par un tribunal indépendant. Un contrôle judiciaire ultérieur des mesures de surveillance ne suffirait pas à lui seul à protéger les personnes concernées. Il ne serait effectué qu'en cas d'ouverture d'une procédure pénale à la suite de la mise en œuvre d'une telle mesure et que si cette mesure avait permis aux autorités de poursuite d'obtenir des éléments de preuve destinés à être utilisés au procès. L'article 163f du Code de procédure pénale (paragraphe 32 ci-dessus) n'aurait pas été en vigueur à l'époque des faits et, quoi qu'il en soit, ne renfermerait pas de garanties suffisantes contre les abus.

– Le Gouvernement

57. Quand bien même la surveillance du requérant par GPS constituerait une ingérence dans l'exercice par l'intéressé de son droit au respect de sa vie privée, le Gouvernement soutient que cette ingérence était justifiée sous l'angle du paragraphe 2 de l'article 8. Elle aurait été fondée sur l'article 100c § 1.1. b) du Code de procédure pénale, disposition juridique qui aurait satisfait aux exigences qualitatives nécessaires, en particulier à celles de prévisibilité. D'après le Gouvernement, les principes développés dans la jurisprudence de la Cour sur la prévisibilité de la loi dans le contexte d'affaires se rapportant à l'interception de télécommunications ne peuvent pas être appliqués à la présente affaire concernant la surveillance par GPS, cette mesure constituant une ingérence moins importante que les écoutes téléphoniques dans la vie privée de la personne qui en fait l'objet. Comme l'auraient confirmé les juridictions internes, il aurait été suffisamment clair que l'expression « autres moyens techniques spéciaux destinés à la surveillance » figurant à l'article 100c § 1b) du Code de procédure pénale, par laquelle le législateur entendait autoriser l'utilisation de techniques de surveillance futures, couvrait la surveillance par GPS.

58. Le Gouvernement soutient en outre que les dispositions juridiques litigieuses renfermaient des garanties suffisantes contre une ingérence arbitraire des autorités dans les droits des citoyens. Une surveillance par des moyens techniques tels que le GPS n'aurait été autorisée par l'article 100c § 1.1. b) du Code de procédure pénale que dans le cadre d'une enquête portant sur une infraction extrêmement grave. En vertu de l'article 100c § 2 du Code de procédure pénale (paragraphe 29 ci-dessus), une telle mesure n'aurait en principe pu être ordonnée que contre des personnes accusées d'une infraction. Les dispositions juridiques en vigueur à l'époque des faits auraient autorisé le parquet à délivrer un mandat de surveillance. Il n'aurait pas été nécessaire de conférer ce pouvoir à un juge. Quoi qu'il en soit, les mesures en question auraient fait l'objet d'un contrôle judiciaire dans la procédure pénale qui s'en était suivie. De plus, comme les juridictions internes l'auraient conclu de manière convaincante, un mandat judiciaire aux fins de la surveillance par GPS n'aurait pas été nécessaire puisque cette mesure venait s'ajouter à plusieurs autres mesures de surveillance.

59. Par ailleurs, le Gouvernement souligne qu'il fallait informer l'intéressé de la surveillance dont il faisait l'objet dès que cela était possible sans compromettre le but de l'enquête (article 101 § 1 du Code de procédure pénale, paragraphe 31 ci-dessus). En outre, le principe de proportionnalité aurait été respecté puisque, en vertu de l'article 100c § 1.1. b) du Code de procédure pénale, il n'aurait été possible de recourir aux méthodes de surveillance en question que lorsque d'autres moyens d'enquête avaient moins de chances d'aboutir ou étaient plus difficiles à mettre en œuvre. Enfin, la durée d'une surveillance par GPS devrait être proportionnée au but visé.

ii. Appréciation de la Cour

– Principes pertinents

60. Conformément à la jurisprudence de la Cour, les mots « prévue par la loi » veulent d'abord que la mesure contestée ait une base en droit interne, mais ils ont trait aussi à la qualité de la loi en cause : ils exigent l'accessibilité de celle-ci à la personne concernée, qui doit de surcroît pouvoir en prévoir les conséquences pour elle, et sa compatibilité avec la prééminence du droit (voir, entre autres, *Kruslin c/ France*, 24 avril 1990, § 27, série A n° 176-A, *Lambert*, décision précitée, § 23, et *Perry*, arrêt précité, § 45).

61. Quant à l'exigence de « prévisibilité » de la loi dans ce domaine, la Cour rappelle que dans le contexte de mesures de surveillance secrète la loi doit user de termes assez clairs pour indiquer à tous de manière suffisante en quelles circonstances et sous quelles conditions elle habilite la puissance publique à recourir à de telles mesures (voir, entre autres, *Malone c/ Royaume-Uni*, 2 août 1984, § 67, série A n° 82, *Valenzuela Contreras c/ Espagne*, 30 juillet 1998, § 46 iii), *Recueil* 1998-V, et *Bykov c/ Russie* [GC], n° 4378/02, § 76, CEDH 2009 –…). Eu égard au risque d'abus inhérent à tout système de surveillance secrète, de telles mesures doivent se fonder sur une loi particulièrement précise, en particulier compte tenu de ce que la technologie disponible devient de plus en plus sophistiquée (*Weber et Saravia c/ Allemagne* (déc.), n° 54934/00, § 93, CEDH 2006-XI, *Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev*, précitée, § 75, *Liberty et autres c/ Royaume-Uni*, n° 58243/00, § 62, 1 juillet 2008, et *Iordachi et autres c/ Moldova*, n° 25198/02, § 39, 10 février 2009).

62. En outre, la Cour a déclaré sous l'angle de l'article 7 de la Convention que aussi clair que le libellé d'une disposition légale puisse être, dans quelque système juridique que ce soit, y compris le droit pénal, il existe immanquablement un élément d'interprétation judiciaire. Il faudra toujours élucider les points douteux et s'adapter aux changements de situation. D'ailleurs, il est solidement établi dans la tradition juridique des États parties à la Convention que la jurisprudence, en tant que source du droit, contribue nécessairement à l'évolution progressive du droit pénal. On ne saurait interpréter la Convention comme proscrivant la clarification graduelle des règles de la responsabilité pénale par l'interprétation judiciaire d'une affaire à l'autre, à condition que le résultat soit cohérent avec la substance de l'infraction et raisonnablement prévisible (voir, entre autres, *S.W. c/ Royaume-Uni*, 22 novembre 1995, § 36, série A n° 335-B, et *Streletz, Kessler et Krenz c/ Allemagne* [GC], n^{os} 34044/96, 35532/97 et 44801/98, § 50, CEDH 2001-II). La Cour estime que ces principes, développés sous l'angle de l'article 7, s'appliquent également au contexte examiné.

63. En outre, lorsqu'il s'agit de mesures de surveillance secrète par les autorités publiques, l'absence de contrôle public et le risque d'abus de pouvoir impliquent que le droit interne offre une protection contre

les ingérences arbitraires dans l'exercice des droits garantis par l'article 8 (voir, *mutatis mutandis*, *Amann*, précité, §§ 76-77, *Bykov*, précité, § 76, voir également *Weber et Saravia* (déc.), précitée, § 94, et *Liberty et autres*, précité, § 62). La Cour doit se convaincre de l'existence de garanties adéquates et suffisantes contre les abus. Cette appréciation dépend de l'ensemble des circonstances de la cause, par exemple la nature, l'étendue et la durée des mesures éventuelles, les raisons requises pour les ordonner, les autorités compétentes pour les permettre, exécuter et contrôler, le type de recours fourni par le droit interne (*Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev*, précitée, § 77, avec renvoi à *Klass et autres c/ Allemagne*, 6 septembre 1978, § 50, série A n° 28).

– Application des principes susmentionnés au cas d'espèce

64. La Cour a recherché si l'ingérence dans l'exercice par le requérant de son droit au respect de sa vie privée résultant de sa surveillance par GPS était « prévue par la loi » au sens de l'article 8 § 2. Elle estime que cette ingérence avait une base dans la législation allemande, à savoir l'article 100c § 1.1. b) du Code de procédure pénale, disposition qui était accessible au requérant.

65. Quant à la prévisibilité de la loi et à sa compatibilité avec la prééminence du droit, la Cour note d'emblée que dans ses observations le requérant s'appuie fortement sur les garanties minimales contre les abus que la loi doit renfermer d'après sa jurisprudence relative à l'interception de télécommunications. Conformément à ces critères, la loi doit définir la nature des infractions susceptibles de donner lieu à un mandat d'interception, les catégories de personnes susceptibles d'être mises sur écoute, la durée maximale de l'exécution de la mesure, la procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies, les précautions à prendre pour la communication des données à d'autres parties, et les circonstances dans lesquelles peut ou doit s'opérer l'effacement ou la destruction des enregistrements (*Weber et Saravia*, décision précitée, § 95, avec d'autres références).

66. La Cour peut certes s'inspirer de ces principes, mais elle estime que ces critères relativement stricts, établis et suivis dans le contexte spécifique de la surveillance des télécommunications (voir également *Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev*, précitée, § 76, *Liberty et autres*, précitée, § 62, et *Iordachi et autres*, précitée, § 39), ne sont pas applicables en tant que tels aux affaires comme le cas d'espèce qui a trait à la surveillance par GPS de déplacements en public et donc à une mesure qui, par rapport à l'interception de conversations téléphoniques, doit passer pour constituer une ingérence moins importante dans la vie privée de la personne concernée (paragraphe 52 ci-dessus). Elle suivra donc les principes plus généraux, tels que résumés ci-dessus (paragraphe 63), à observer pour qu'il y ait

une protection adéquate contre une ingérence arbitraire dans l'exercice des droits protégés par l'article 8.

67. Sur le point de savoir si les dispositions appliquées pour la surveillance du requérant par GPS satisfont à l'exigence de « prévisibilité », la Cour relève l'argument du requérant selon lequel l'expression « autres moyens techniques spéciaux destinés à la surveillance » figurant à l'article 100c § 1.1. b) du Code de procédure pénale n'est pas suffisamment clair et ne saurait passer pour couvrir la géolocalisation. En revanche, les juridictions internes, auxquelles il incombe au premier chef d'interpréter et d'appliquer le droit interne (voir, parmi beaucoup d'autres, *Kopp c/ Suisse*, 25 mars 1998, § 59, *Recueil* 1998-II), ont conclu à l'unanimité que ladite disposition s'étendait à ce moyen de surveillance (paragraphes 14, 19 et 25 ci-dessus).

68. La Cour considère qu'il ressortait clairement du libellé de l'article 100c § 1.1. b), lu à la lumière de l'article 100c § 1.1. a) et § 1.2, que les moyens techniques en question s'étendaient aux méthodes de surveillance qui n'étaient ni visuelles ni acoustiques et qui étaient utilisées en particulier « pour localiser l'auteur d'une infraction ». Le recours au GPS ne constituant une surveillance ni visuelle ni acoustique et permettant la localisation d'objets équipés d'un récepteur GPS et donc de personnes se déplaçant avec ou dans ces objets, la Cour estime que la conclusion des juridictions internes selon laquelle cette surveillance était couverte par l'article 100c § 1.1. b) a constitué une évolution raisonnablement prévisible et une clarification de ladite disposition du Code de procédure pénale par l'interprétation judiciaire.

69. Sur le point de savoir si le droit interne renfermait des garanties suffisantes et effectives contre les abus, la Cour observe que, par sa nature, la surveillance d'une personne par la pose d'un récepteur GPS dans la voiture qu'elle utilise, associée à d'autres mesures de surveillance visuelle de cette personne, permet aux autorités, chaque fois que l'intéressé emprunte cette voiture, de suivre ses déplacements dans les lieux publics. Il est vrai, comme le requérant le fait remarquer, que la loi ne fixait aucune limite à la durée d'une telle surveillance. Une durée précise n'a été adoptée que par la suite, le nouvel article 163f § 4 du Code de procédure pénale prévoyant que la surveillance systématique d'un suspect, lorsqu'elle est ordonnée par un procureur, ne peut dépasser un mois et que toute prolongation doit être ordonnée par un juge (paragraphe 32 ci-dessus). Toutefois, la durée de cette surveillance devait être proportionnée à la situation et la Cour considère que les juridictions internes ont examiné si le principe de proportionnalité avait été respecté à cet égard (voir, par exemple, le paragraphe 28 ci-dessus). Elle estime que le droit allemand fournissait donc des garanties suffisantes contre des abus à cet égard.

70. Quant aux motifs requis pour ordonner la surveillance d'une personne par GPS, la Cour note que d'après l'article 100c § 1.1. b) et § 2 du

Code de procédure pénale une telle surveillance ne pouvait être ordonnée qu'à l'égard d'une personne soupçonnée d'une infraction extrêmement grave ou, dans des circonstances très limitées, à l'égard d'un tiers soupçonné d'être en rapport avec l'accusé, et lorsque d'autres moyens de localiser l'accusé avaient moins de chances d'aboutir ou étaient plus difficiles à mettre en œuvre. La Cour est d'avis que le droit interne subordonnait donc l'autorisation de la mesure de surveillance litigieuse à des conditions très strictes.

71. La Cour observe en outre que le droit interne permet aux autorités de poursuite d'ordonner la surveillance d'un suspect par GPS, laquelle est effectuée par la police. Elle relève que d'après le requérant c'est seulement en octroyant le pouvoir d'ordonner une surveillance par GPS à un juge d'instruction qu'on aurait offert une protection contre l'arbitraire. La Cour constate que d'après l'article 163f § 4 du Code de procédure pénale, entré en vigueur après la surveillance par GPS du requérant, lorsque la surveillance systématique d'un suspect dépasse une durée d'un mois, elle doit en fait être ordonnée par un juge. Elle se félicite de ce renforcement de la protection du droit d'un suspect au respect de sa vie privée. Elle note toutefois que déjà en vertu des dispositions en vigueur à l'époque des faits la surveillance d'un individu par GPS était susceptible d'un contrôle judiciaire. Dans la procédure pénale ultérieure menée contre la personne concernée, les juridictions pénales pouvaient contrôler la légalité d'une telle mesure de surveillance et, si celle-ci était jugée illégale, elles avaient la faculté d'exclure les éléments ainsi obtenus du procès (un tel contrôle a été effectué en l'espèce ; voir en particulier les paragraphes 14, 19 et 21 ci-dessus).

72. La Cour estime qu'un tel contrôle judiciaire ainsi que la possibilité d'exclure les éléments de preuve obtenus au moyen d'une surveillance illégale par GPS constituaient une garantie importante, en ce qu'elle décourageait les autorités d'enquête de recueillir des preuves par des moyens illégaux. La surveillance par GPS devant être considérée comme étant moins attentatoire à la vie privée d'une personne que, par exemple, des écoutes téléphoniques, mesure pour laquelle tant le droit interne (voir l'article 100b § 1 du Code de procédure pénale, paragraphe 30 ci-dessus) que l'article 8 de la Convention (voir, en particulier, *Dumitru Popescu c/ Roumanie (no 2)*, n° 71525/01, §§ 70-71, 26 avril 2007, et *Iordachi et autres*, précitée, § 40) requièrent la délivrance d'un mandat par un organe indépendant, la Cour estime que le contrôle judiciaire ultérieur de la surveillance d'une personne par GPS offre une protection suffisante contre l'arbitraire. En outre, l'article 101 § 1 du Code de procédure pénale renfermait une garantie supplémentaire contre les abus en ce qu'il énonçait que la personne faisant l'objet de la surveillance devait être informée de la mesure dans certaines circonstances (paragraphe 31 ci-dessus).

73. Enfin, la Cour ne perd pas de vue que le Code de procédure pénale n'exigeait pas qu'un tribunal autorisât et supervisât la surveillance

par GPS lorsque celle-ci était associée à d'autres moyens de surveillance, et donc qu'il autorisât et supervisât les mesures de surveillance dans leur ensemble. Elle est d'avis que, pour que les garanties contre les abus soient suffisantes, il faut en particulier que les mesures d'investigation prises par différentes autorités soient coordonnées et que, en conséquence, avant d'ordonner la surveillance d'un suspect par GPS, le parquet s'assure que l'intéressé est au courant des autres mesures de surveillance déjà en place. Toutefois, vu les conclusions de la Cour constitutionnelle fédérale sur ce point (paragraphe 27 ci-dessus), elle estime que les garanties existant à l'époque des faits pour empêcher la surveillance totale d'une personne, y compris celles relevant du principe de proportionnalité, étaient suffisantes pour prévenir les abus.

74. Eu égard à ce qui précède, la Cour estime que l'ingérence dans l'exercice par le requérant de son droit au respect de sa vie privée était « prévue par la loi » au sens de l'article 8 § 2.

b) But et nécessité de l'ingérence

i. Thèses des parties

75. Le requérant soutient que l'ingérence litigieuse n'était pas nécessaire dans une société démocratique au sens de l'article 8 § 2 car, comme il l'a exposé ci-dessus (paragraphes 54-56), le droit applicable ne le protégeait pas suffisamment contre une ingérence arbitraire des autorités de l'État.

76. De l'avis du Gouvernement, la mesure de surveillance poursuivait des buts légitimes en ce qu'elle était nécessaire à la sécurité nationale, à la sûreté publique, à la prévention des infractions pénales et à la protection des droits d'autrui. La mesure aurait également été nécessaire dans une société démocratique. Ainsi qu'il a été exposé ci-dessus, il y aurait eu des garanties effectives contre les abus. Certes, en adoptant l'article 163f § 4 du Code de procédure pénale, le législateur aurait par la suite renforcé les droits des personnes concernées en soumettant la mesure de surveillance à la délivrance d'un mandat judiciaire et à une durée maximale. Toutefois, cela n'autoriserait pas à conclure que la mesure ne respectait pas auparavant les normes minimales fixées par la Convention. La surveillance du requérant par GPS pendant plus de deux mois et demi ne pourrait passer pour disproportionnée. De même, le recours à différentes méthodes de surveillance simultanément n'aurait pas rendu l'ingérence dans les droits du requérant disproportionnée. La surveillance visuelle en particulier aurait été conduite presque exclusivement pendant les week-ends et la gravité de l'infraction dont le requérant était soupçonné et le danger pour le public auraient justifié cette forme de surveillance.

ii. Appréciation de la Cour

77. La surveillance du requérant par GPS, ordonnée par le procureur général près la Cour fédérale de justice, aux fins d'enquêter sur

plusieurs accusations de tentatives de meurtre revendiquées par un mouvement terroriste et de prévenir d'autres attentats à la bombe était dans l'intérêt de la sécurité nationale, de la sûreté publique, de la prévention des infractions pénales et de la protection des droits des victimes.

78. Sur le point de savoir si la surveillance du requérant par GPS, telle qu'elle a été conduite en l'espèce, était « nécessaire dans une société démocratique », la Cour rappelle que la notion de nécessité implique que l'ingérence corresponde à un besoin social impérieux et, en particulier, qu'elle soit proportionnée au but légitime poursuivi (*Leander c/ Suède*, 26 mars 1987, § 58, série A n° 116, et *Messina c/ Italie (no 2)*, n° 25498/94, § 65, CEDH 2000-X). Sur la question de savoir si, à la lumière de l'affaire dans son ensemble, la mesure prise était proportionnée au but légitime poursuivi, la Cour relève que la surveillance du requérant par GPS n'a pas été ordonnée d'emblée. Les autorités d'enquête ont d'abord tenté d'établir si le requérant était en cause dans les attentats à la bombe en question au moyen de mesures portant moins atteinte à son droit au respect de sa vie privée. Elles ont notamment essayé de le localiser en installant des transmetteurs dans la voiture de S., dont l'utilisation (à la différence du GPS) exigeait de savoir où la personne concernée se trouvait approximativement. Toutefois, le requérant et son complice avaient repéré et détruit les transmetteurs et s'étaient également soustraits avec succès à la surveillance visuelle des agents de l'État à plusieurs occasions. Dès lors, il est clair que les autres mesures d'investigation, qui étaient moins attentatoires à la vie privée du requérant que la surveillance de celui-ci par GPS, s'étaient révélées moins efficaces.

79. La Cour note en outre qu'en l'espèce la surveillance du requérant par GPS s'est ajoutée à une multitude d'autres mesures d'observation, faisant en partie double emploi, qui avaient été ordonnées précédemment, dont la surveillance visuelle du requérant par des agents du ministère de la Protection de la Constitution de la Rhénanie-du-Nord-Westphalie et par des fonctionnaires de l'Office fédéral de la police judiciaire, la surveillance vidéo de l'entrée de la maison où vivait le requérant et la mise sur écoute des téléphones dans cette maison et dans une cabine téléphonique située à proximité par les agents des deux organes séparément. En outre, le ministère de la Protection de la Constitution de la Rhénanie-du-Nord-Westphalie a intercepté les communications postales de l'intéressé à l'époque des faits.

80. La Cour estime dans ces conditions que la surveillance du requérant par GPS a entraîné une observation relativement approfondie de la conduite de l'intéressé par différentes autorités de l'État. En particulier, le fait que le requérant ait été soumis aux mêmes mesures de surveillance par différentes autorités a entraîné une ingérence plus grave dans sa vie privée, puisque cela a accru le nombre de personnes ayant eu connaissance des informations sur sa conduite. Cela étant, l'ingérence constituée par la surveillance supplémentaire du requérant par GPS devait donc être justifiée par des raisons encore plus impérieuses.

Cependant, cette mesure a été mise en œuvre pendant une période relativement courte (quelque trois mois), et, tout comme la surveillance visuelle par des agents de l'État, n'a guère touché l'intéressé que pendant les week-ends et lorsqu'il se déplaçait dans la voiture de S. Dès lors, on ne saurait dire que le requérant a été soumis à une surveillance totale et exhaustive. En outre, l'enquête dans le cadre de laquelle la surveillance a été conduite portait sur des infractions très graves, à savoir plusieurs tentatives de meurtre d'hommes politiques et de fonctionnaires par des attentats à la bombe. Ainsi qu'il a été démontré ci-dessus, l'enquête sur ces infractions et, notamment, la prévention d'autres actes similaires par le recours auparavant à des méthodes de surveillance moins attentatoires à la vie privée, ne s'étaient pas révélées efficaces. Dès lors, la Cour estime que la surveillance du requérant par GPS, telle qu'elle a été effectuée dans les circonstances de l'espèce, était proportionnée aux buts légitimes poursuivis et donc « nécessaire dans une société démocratique », au sens de l'article 8 § 2.

81. Partant, il n'y a pas eu violation de l'article 8 de la Convention.

II. SUR LA VIOLATION ALLÉGUÉE DE L'ARTICLE 6 DE LA CONVENTION

82. Le requérant allègue la violation de son droit à un procès équitable en raison de l'utilisation dans le cadre de la procédure pénale d'informations qui ont été recueillies grâce à sa surveillance effectuée en violation de l'article 8 et qui ont constitué la base de sa condamnation. Il invoque l'article 6 § 1 de la Convention, lequel est ainsi libellé en ses passages pertinents en l'espèce :

«Toute personne a droit à ce que sa cause soit entendue équitablement [...] par un tribunal [...] qui décidera [...] du bien-fondé de toute accusation en matière pénale dirigée contre elle. »

83. Le Gouvernement conteste cet argument.

A. Sur la recevabilité

84. La Cour relève que ce grief est lié à celui qu'elle vient d'examiner ci-dessus et qu'il doit donc également être déclaré recevable.

B. Sur le fond

85. Eu égard à sa conclusion ci-dessus selon laquelle la surveillance du requérant par GPS n'a pas emporté violation de l'article 8 de la Convention, la Cour estime que l'utilisation dans le cadre de la procédure pénale dirigée contre l'intéressé d'informations et d'éléments de preuve ainsi obtenus ne soulève dans les circonstances de l'espèce aucune question distincte sous l'angle de l'article 6 § 1 de la Convention.

PAR CES MOTIFS, LA COUR, À L'UNANIMITÉ,

1. *Joint au fond* l'exception préliminaire du Gouvernement selon laquelle le requérant ne saurait se prétendre victime d'une violation de ses droits garantis par l'article 8 et la *rejette*;

2. *Déclare* la requête recevable ;

3. Dit qu'il n'y a pas eu violation de l'article 8 de la Convention ;

4. Dit qu'aucune question distincte ne se pose sous l'angle de l'article 6 § 1 de la Convention.

Fait en anglais et en français, puis communiqué par écrit le 2 septembre 2010, en application de l'article 77 §§ 2 et 3 du règlement.

3) Arrêt du 22 novembre 2011 de la chambre criminelle de la Cour de cassation

LA COUR DE CASSATION, CHAMBRE CRIMINELLE, a rendu l'arrêt suivant :

Statuant sur les pourvois formés par :
– *M. Mohamed X...,*
– *M. Mohamed Y...,*
– *M. Ouaihid Y...,*
– *M. Salah Y...,*

contre l'arrêt de la chambre de l'instruction de la cour d'appel de Paris, 4e section, en date du 6 mai 2011, qui, dans l'information suivie, notamment, contre les trois premiers des chefs d'importation de stupéfiants, infractions à la législation sur les stupéfiants, association de malfaiteurs et non-justification de ressources et, contre le quatrième, du chef de ces trois derniers délits, a prononcé sur des demandes d'annulation d'actes de la procédure ;

Vu l'ordonnance du président de la chambre criminelle, en date du 20 juillet 2011, joignant les pourvois en raison de la connexité et prescrivant leur examen immédiat ;

Vu le mémoire, commun aux demandeurs, et les observations complémentaires produits ;

Attendu qu'il résulte des énonciations de l'arrêt et des pièces de la procédure que, lors d'une enquête portant sur un trafic de stupéfiants, les officiers de police judiciaire ont délivré, avec l'autorisation du procureur de la République, le 24 juillet 2009, une réquisition judiciaire à un opérateur de téléphonie aux fins d'identifier les appels entrants et sortants sur trois lignes téléphoniques ainsi que les cellules activées par ces lignes ; que, dans le même temps, le juge des libertés et de la détention, sur réquisitions du ministère public, a autorisé, par ordonnances des 6 août et 20 août 2009, et ce jusqu'au 4 septembre 2009, l'interception des correspondances téléphoniques sur la ligne utilisée par M. Sofiane Y... ; qu'il a été mis fin à l'exécution de cette dernière mesure le 3 septembre 2009 ; que, le 4 septembre 2009, le procureur de la République

a ouvert une information contre personnes non dénommées des chefs d'importation de stupéfiants, infractions à la législation sur les stupéfiants, association de malfaiteurs et blanchiment ; que, le 8 septembre 2009, le juge d'instruction a délivré une commission rogatoire aux fins qu'il soit procédé à de nouvelles interceptions de correspondances sur la ligne téléphonique susvisée ;

Attendu que, par commissions rogatoires distinctes, en date des 18 mai et 3 juin 2010, le magistrat instructeur a prescrit, d'une part, la mise en place d'un dispositif technique, dit de "géolocalisation", sur un véhicule Renault Laguna utilisé par les suspects aux fins d'en déterminer les déplacements, et, d'autre part, l'installation, dans ce même véhicule et dans le parking souterrain d'un immeuble d'habitation, d'un système de captation des conversations, et, dans ce dernier lieu, d'images des personnes concernées ;

Attendu qu'à la suite de la communication qui lui a été faite, par le magistrat instructeur, d'éléments provenant de ces investigations, le procureur de la République a délivré, les 27 mai et 11 juin 2010, des réquisitoires portant, notamment, sur des faits d'importation de stupéfiants survenus postérieurement à la saisine initiale du juge d'instruction ;

Attendu que MM. Mohamed Y..., Ouahid Y... et Mohamed X..., notamment, ont été mis en examen des chefs susvisés, le 14 juin 2010 et que M. Salah Y... l'a été, le 7 décembre 2010 ;

Attendu que, par requêtes déposées, respectivement les 9 décembre, 10 décembre et 14 décembre 2010, MM. Mohamed Y..., Mohamed X... et Ouahid Y... ont saisi la chambre de l'instruction aux fins d'annulation de nombreux actes de la procédure ; que cette juridiction n'a fait droit que partiellement à leurs demandes ;

En cet état ;

Sur le premier moyen de cassation, pris de la violation des articles 16 de la Déclaration des droits de l'homme et du citoyen, 16 et 66 de la Constitution, 8 de la Convention européenne des droits de l'homme, préliminaire, 40, 41, 60-1, 60-2, 77-1, 77-1-1, 592, 593 du Code de procédure pénale ;

« en ce que l'arrêt attaqué a refusé d'annuler la réquisition judiciaire du 24 juillet 2009 adressée, sur la seule autorisation du procureur de la République, par les officiers de police judiciaire dans le cadre de l'enquête préliminaire aux opérateurs de téléphonie pour avoir la localisation et la liste des appels entrants et sortants de trois lignes téléphoniques pour lesquelles le juge des libertés et de la détention avait refusé d'autoriser la mise sous écoute ;

« aux motifs que la réquisition du 24 juillet 2009 a été régulièrement délivrée conformément aux dispositions de l'article 77-1-1 ; que cette réquisition ne portait que sur l'identification des titulaires de quatre

lignes téléphoniques et la liste des appels entrants et sortants sur trois d'entre elles ; que ces opérations sont de simples mesures techniques relevant dudit article et ne sont pas des interceptions de correspondance qui seules sont susceptibles de porter atteinte à la vie privée et au secret de correspondances ; qu'ainsi, l'autorisation du juge des libertés et de la détention n'était pas nécessaire ;

« 1°) alors que l'article 77-1-1 du Code de procédure pénale ne permet à l'officier de police judiciaire, sur autorisation du procureur de la République, de ne requérir un opérateur privé qu'aux fins de lui remettre des documents intéressant l'enquête et non de procéder à des mesures techniques ; qu'en l'espèce, par la réquisition litigieuse, l'officier de police judiciaire demandait également à la société Cegetel de "procéder à l'identification des cellules déclenchées par ces lignes" ; que cette mesure, qui n'est pas une remise de documents et comporte des investigations attentatoires à la vie privée et à la liberté d'aller et venir dès lors qu'elle permet de connaître les déplacements des titulaires des abonnements, ne pouvait être ordonnée par l'officier de police judiciaire sur la seule autorisation du procureur de la République, dans le cadre de l'article 77-1-1 du Code de procédure pénale ; qu'ainsi, l'arrêt attaqué, en affirmant que ces "mesures techniques" relevaient de l'article 77-1-1 du Code de procédure pénale, a violé ce texte par fausse application ainsi que l'ensemble des textes visés au moyen ;

« 2°) alors que, le ministère public, partie poursuivante, ne présente pas les garanties d'indépendance et d'impartialité et n'est pas une autorité judiciaire habilitée comme telle à garantir la liberté ; que les renseignements concernant non seulement la liste des appels entrants et sortants de lignes téléphoniques mais aussi "l'identification des cellules déclenchées par ces lignes", c'est à dire la localisation des titulaires de ces lignes, portent atteinte à la vie privée et la liberté d'aller et venir ; que tel était le cas en l'espèce des renseignements demandés à la société Cegetel par la réquisition du 24 juillet 2009 ; que, dès lors, ces mesures ne pouvaient être valablement autorisées par le seul procureur de la république, sans l'accord ou l'autorisation du juge des libertés et de la détention qui, le même jour, avait refusé d'autoriser l'interception des mêmes lignes téléphoniques faute d'existence de soupçons suffisants pour justifier une mesure portant atteinte aux libertés individuelles ; qu'en refusant d'annuler ladite réquisition ainsi que toute la procédure subséquente, l'arrêt attaqué a violé les textes susvisés » ;

Attendu que, pour rejeter le moyen de nullité pris de l'absence de simple caractère technique de la réquisition judiciaire adressée à un opérateur de téléphonie et du défaut de qualité du procureur de la République pour autoriser une telle investigation, l'arrêt prononce par les motifs repris au moyen ;

Attendu qu'en se déterminant ainsi, les juges ont fait une exacte application de l'article 77-1-1 du Code de procédure pénale et du texte

conventionnel invoqué, dès lors que la remise de documents au sens du premier de ces textes s'entend également de la communication, sans recours à un moyen coercitif, de documents issus d'un système informatique ou d'un traitement de données nominatives, tels ceux détenus par un opérateur de téléphonie et qu'une telle mesure n'entre pas dans le champ d'application de l'article 5 § 3 de la Convention européenne des droits de l'homme relatif au contrôle de la privation de liberté ;

D'où il suit que le moyen ne saurait être accueilli ;

Sur le deuxième moyen de cassation, pris de la violation des articles 706-95, préliminaire, 171, 592, 593, 802 du Code de procédure pénale, 8 de la Convention européenne des droits de l'homme ;

« en ce que l'arrêt attaqué a refusé d'annuler les écoutes téléphoniques de la ligne n°…, ordonnées le 6 août 2009 ainsi que celle du réquisitoire introductif et de toute la procédure subséquente ;

« aux motifs que les interceptions de correspondances téléphoniques de la ligne utilisée par M. Sofiane Y… ont été effectuées dans les délais impartis par le juge des libertés et de la détention et n'ont porté que sur les conversations en relation avec les faits recherchés, ce que les requérants ne contestent pas ; que, si à l'issue des opérations d'interception qui ont pris fin le 3 septembre 2009, le juge des libertés et de la détention n'a pas été informé dans les termes de l'article 706-95 du Code de procédure pénale, néanmoins ces écoutes téléphoniques ont fait l'objet d'un contrôle par le juge d'instruction saisi le 4 septembre 2009, qui, d'ailleurs, en a ordonné le renouvellement le 8 septembre 2009 ; qu'ainsi, l'omission de la formalité prévue par la loi, n'a pas porté atteinte aux intérêts des requérants ;

« alors que, s'il n'est pas nécessaire de communiquer au juge des libertés et de la détention qui l'a autorisée les procès-verbaux de transcription de l'écoute téléphonique, le procureur de la République doit le tenir informé des diligences effectuées ; que cette règle qui touche à la compétence et à l'ordre des juridictions doit être observée à peine de nullité de la procédure et indépendamment de la démonstration d'un grief ; que l'arrêt attaqué, qui constate que le juge des libertés et de la détention n'a pas été tenu informé des diligences effectuées sur l'autorisation qu'il avait donnée et refuse de prononcer la nullité des écoutes téléphoniques ainsi pratiquées ainsi que de toute la procédure subséquente, a violé les textes visés au moyen » ;

Attendu que la Cour de cassation est en mesure de s'assurer que l'interception de communications téléphoniques autorisée, à la demande du procureur de la République, par le juge des libertés et de la détention, a pris fin avant la date fixée par ce magistrat pour son exécution et que, dans le même délai, les procès-verbaux en résultant, joints au réquisitoire introductif, ont été soumis au contrôle du juge d'instruction, en sorte que l'irrégularité résultant de la méconnaissance des formalités

substantielles prévues par l'alinéa 3 de l'article 706-95 du Code de procédure pénale n'a pas eu pour effet de porter atteinte aux intérêts des requérants ;

D'où il suit que le moyen doit être écarté ;

Sur le troisième moyen de cassation, pris de la violation des articles 8 de la Convention européenne des droits de l'homme, préliminaire, 81, 170, 171, 592, 593, 802 du Code de procédure pénale, ensemble violation des droits de la défense ;

« en ce que l'arrêt attaqué a refusé d'annuler les mesures de surveillance par géolocalisation effectuées grâce à la mise en place d'un dispositif technique placé sur le véhicule utilisé par M. Mohamed Y..., ainsi que toute la procédure subséquente ;

« aux motifs que la surveillance à distance du déplacement d'un véhicule par un dispositif de géolocalisation par satellite (GPS) n'est pas prévue expressément par le Code de procédure pénale ; que, cependant, le recours à ce type de surveillance est justifié par l'article 81 dudit Code qui permet au juge d'instruction de procéder à tous les actes d'information qu'il juge utiles à la manifestation de la vérité ; que la mise en place du dispositif de surveillance par GPS du véhicule Renault Laguna immatriculé... (sic) *a été autorisée le 3 juin 2010 par une ordonnance motivée du juge d'instruction, pour une durée limitée d'un mois ; que cette surveillance a été ordonnée dans le cadre de l'information ouverte contre X du chef d'importation de produits stupéfiants, l'existence d'un vaste trafic de ces produits ayant été constatée dans une cité de la Courneuve ; qu'elle a été réalisée sous le contrôle du juge et qu'un procès-verbal de transcription de ladite surveillance a été versé au dossier et peut être contradictoirement discuté par les requérants ; que cette surveillance des requérants, telle qu'elle a été effectuée, sous le contrôle d'un juge constituant une garantie suffisante contre l'arbitraire, était proportionnée au but poursuivi, s'agissant d'un important trafic de stupéfiants en bande organisée portant gravement atteinte à l'ordre public et à la santé publique et nécessaire au sens de l'article 8, alinéa 2, de la Convention européenne des droits de l'homme ; que l'ordonnance du 3 juin 2010 autorisait les enquêteurs à s'introduire dans le parking dans le véhicule Renault Laguna immatriculé...,* (sic) *y compris en dehors des heures prévues à l'article 59 du Code de procédure pénale, non seulement pour la pose d'un dispositif technique de sonorisation et de captation d'images mais aussi pour celui du dispositif de géolocalisation ; que, contrairement à ce qui est affirmé, la loi française n'interdit pas le procédé de géolocalisation ; qu'en effet, l'article 15 de la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité dispose simplement que s'il peut être fait obligation aux constructeurs et importateurs de véhicules, en vue de prévenir les infractions contre les véhicules et leurs équipements, d'installer sur ces biens des dispositifs de sécurité ou leur marquage, y compris par des procédés électroniques,*

*il ne peut, en revanche, leur être fait obligation d'installer des dispositifs ou procédés permettant de localiser à distance des véhicules non signalés comme volés ; qu'il ne ressort pas des pièces de la procédure que les officiers de police judiciaire ont procédé à des actes d'enquêtes sur les territoires belge et hollandais ; que les opérations de géolocalisation du véhicule réalisées le 4 juin 2010 en application de l'ordonnance du 3 juin 2010 sont régulières ; que le moyen pris de leur annulation ne peut être admis ; qu'en conséquence, l'interpellation de M. Mohamed Y… (*sic*, il s'agit en réalité de M. Mohamed X…) alors qu'il vient de pénétrer dans le véhicule Laguna contenant 111 kg de cannabis, n'encourt aucune nullité ;*

« alors que toute ingérence dans la vie privée et familiale doit être prévue par une loi suffisamment claire et précise pour indiquer à tous de manière suffisante en quelles circonstances et sous quelles conditions elle habilite la puissance publique à recourir à de telles mesures ; que la mise en place d'un GPS sur un véhicule privé à l'insu de son utilisateur constitue une ingérence dans la vie privée et familiale qui n'est donc compatible avec les exigences de l'article 8 de la Convention européenne des droits de l'homme qu'à la condition d'être prévue par une loi suffisamment claire et précise ; qu'en affirmant que l'article 81 du Code de procédure pénale, qui ne prévoit ni les circonstances ni les conditions dans lesquelles un tel dispositif peut être placé sur un véhicule privé, constituait une base légale suffisante à cette ingérence, l'arrêt attaqué a violé l'article 8 de la Convention européenne des droits de l'homme ;

Attendu que, pour écarter le moyen de nullité pris du défaut de fondement légal de l'apposition sur un véhicule automobile Renault Laguna d'un dispositif technique, dit de « géolocalisation », permettant d'en suivre et relever les déplacements, l'arrêt retient que, d'une part, cette mesure a pour fondement l'article 81 du Code de procédure pénale et que, d'autre part, en l'espèce, cette surveillance a été effectuée sous le contrôle d'un juge constituant une garantie suffisante contre l'arbitraire, qu'elle était proportionnée au but poursuivi, s'agissant d'un important trafic de stupéfiants en bande organisée portant gravement atteinte à l'ordre public et à la santé publique et nécessaire au sens de l'article 8 § 2 de la Convention européenne des droits de l'homme ;

Attendu qu'en l'état de ces énonciations, les juges, qui ont caractérisé la prévisibilité et l'accessibilité de la loi, et la proportionnalité de l'ingérence ainsi réalisée dans l'exercice, par les requérants, du droit au respect de leur vie privée, ont fait une exacte application du texte conventionnel invoqué ;

D'où il suit que le moyen n'est pas fondé ;

Sur le quatrième moyen de cassation, pris de la violation des articles 706-96, 592 et 593 du Code de procédure pénale, ensemble violation des droits de la défense ;

« en ce que l'arrêt attaqué a refusé d'annuler les opérations de sonorisation et de captation d'images du parking souterrain de l'immeuble situé 34/38 rue d'Aubervilliers à Paris et du véhicule Renault Laguna stationné dans ce même lieu ainsi que toute la procédure subséquente ;

« aux motifs, d'une part, que, par ordonnances motivées des 18 mai et 3 juin 2010, le juge d'instruction a autorisé des opérations de sonorisation et de captation d'images des deux niveaux du parking souterrain de l'immeuble situé 34/38 rue de la commune de Paris à Aubervilliers, et des opérations de sonorisation du véhicule Renault Laguna immatriculé... stationné en ce même lieu ; que le même jour, le juge d'instruction a délivré deux commissions rogatoires spéciales pour la réalisation de ces opérations autorisant les officiers de police judiciaire à pénétrer dans le parking et dans le véhicule ; qu'un parking, partie commune d'une copropriété, n'est pas un lieu d'habitation au sens de l'article 706-96 du Code de procédure pénale mais un lieu privé ; que, par application des dispositions de l'article 706-96 précité, le juge d'instruction peut autoriser les officiers de police judiciaire à y pénétrer pour la mise en place des dispositifs techniques de sonorisation et de fixations d'images, y compris hors des heures prévues par l'article 59 du Code de procédure pénale sans avoir à saisir le juge des libertés et de la détention ;

« alors que les parties communes d'un immeuble d'habitation, y compris le parking, sont parties intégrantes de ce lieu d'habitation en sorte que seul le juge des libertés et de la détention est compétent pour autoriser les enquêteurs à y pénétrer afin de mettre en place des dispositifs de sonorisation et captation d'images ;

« et aux motifs, d'autre part, que l'article 706-96 ne prévoit pas d'autorisation spéciale à donner aux policiers qui doivent dans le cadre des opérations précitées, et pendant la durée fixée pour celles-ci, pénétrer à nouveau dans ces lieux pour effectuer une réparation du dispositif ou récupérer des données enregistrées ;

« alors que l'article 706-96 qui prévoit que le juge d'instruction doit autoriser les enquêteurs à pénétrer dans les lieux privés pour l'installation du dispositif de sonorisation et de captation d'images, qu'il doit également les autoriser pour pénétrer à nouveau dans lesdits lieux afin de désinstaller le dispositif technique et que les opérations effectuées ne peuvent avoir d'autres fins que la mise en place du dispositif technique exige nécessairement que chaque visite des lieux soient préalablement autorisée par le juge ; que l'arrêt attaqué a violé l'article 706-96 susvisé » ;

Attendu que, pour rejeter le grief de nullité tenant aux opérations de sonorisation et de captation d'images dans un parking souterrain, l'arrêt prononce par les motifs repris au moyen ;

Attendu qu'en se déterminant ainsi, les juges ont justifié leur décision dès lors que, d'une part, le parking souterrain d'un immeuble d'habitation constitue un lieu privé et non un lieu d'habitation, au sens

de l'article 706-96 du Code de procédure pénale et que, d'autre part, l'ordonnance et la commission rogatoire par lesquelles le juge d'instruction prescrit la mise en place du dispositif de captation et le placement sous scellés des enregistrements incluent l'autorisation donnée aux officiers de police judiciaire de pénétrer dans les lieux aux seules fins de contrôler le fonctionnement du système et de recueillir les données, chaque fois qu'il est nécessaire, obligation leur étant faite d'en rendre compte par procès-verbal au magistrat, lequel exerce le contrôle effectif de ces opérations ; que tel est le cas en l'espèce ;

D'où il suit que le moyen doit être écarté ;

Sur le cinquième moyen de cassation, pris de la violation des articles 19, 80, 81, 1er alinéa, 171, 802 du Code de procédure pénale, ensemble violation des droits de la défense ;

« en ce que l'arrêt attaqué a refusé d'annuler les actes coercitifs (géolocalisation, écoutes téléphoniques, sonorisation et captation d'images) effectués entre le 30 avril et le 7 mai 2010 et entre le 1er juin et le 11 juin 2010, relatifs à des faits non compris dans la saisine du juge d'instruction, ainsi que toute la procédure subséquente, notamment les interpellations et mises en examen de MM. Mohamed, Ouaihid Y... et M. Mohamed X... et a refusé de prononcer leur mise en liberté ;

« aux motifs que les procès-verbaux de surveillance et d'interrogatoire des vendeurs depuis 2008 figurant dans l'enquête préliminaire décrivaient un trafic très important de cannabis en cours par un réseau composé de plusieurs individus ; qu'il résultait des modalités de l'approvisionnement du point de vente par les frères Y..., de la recherche de cartes bleues pour louer des voitures et de la présence de véhicules immatriculés à l'étranger des indices apparents d'importation du cannabis dont la vente était organisée ; qu'en outre, le cannabis étant classé parmi les stupéfiants et sa production, son emploi pour des usages aux fins de recherche ou d'opérations industrielles ou commerciales étant très réglementés sur le territoire national, les ventes de grandes quantités constatées lors de l'enquête préliminaire impliquaient nécessairement que le cannabis vendu était importé ; qu'en conséquence, il appartenait au juge d'instruction saisi par le réquisitoire introductif du 4 septembre 2009 de faits d'importation et de trafic de stupéfiants de vérifier l'ampleur du réseau, d'identifier ses membres, d'en rechercher son organisation et de déterminer le périmètre de son territoire d'activité ; que, pour opérer ces vérifications, le juge d'instruction, après des avis favorables du parquet, a rendu des ordonnances et délivré des commissions rogatoires techniques autorisant les officiers de police judiciaire à procéder à des écoutes téléphoniques et à des captations d'images ; que les enquêteurs ont opéré des surveillances physiques sur le terrain ; que, rapidement, l'ensemble de ces surveillances a révélé que le trafic perdurait et que des importations se poursuivaient ; que les infractions dont il était saisi continuant à être commises par les personnes surveillées selon un

mode opératoire identique à celui révélé au cours de l'enquête préliminaire, le juge d'instruction pouvait ordonner de nouvelles mesures de surveillance et d'investigations ; que, dès que le magistrat instructeur a eu connaissance par l'étude judiciaire du n° 06.. 32. 52, de la vraisemblance des présomptions relatives à des importations imminentes de stupéfiants en provenance des Pays-Bas, il a immédiatement saisi le parquet qui, par réquisitoires supplétifs des 27 mai et 11 juin 2011 a étendu sa saisine ; que le juge ayant instruit dans les limites de sa saisine, le moyen doit être rejeté ;

« alors que le juge d'instruction, qui doit instruire à charge et à décharge, ne peut ordonner de mesures d'investigation et de surveillance coercitives que sur des faits dont il est déjà saisi et n'a pas compétence pour diriger une enquête sur des faits non encore commis ; que chaque importation constitue un fait nouveau même si elle est commise selon un mode opératoire identique ; qu'en affirmant que le juge d'instruction pouvait autoriser des écoutes téléphoniques et des captations d'images et ordonner de nouvelles mesures de surveillances et d'investigations sans se limiter à de simples vérifications sur les importations qui se poursuivaient après sa saisine et dont il n'était par conséquent pas saisi, la chambre de l'instruction a violé les textes visés au moyen et les règles d'ordre public régissant la compétence du juge d'instruction » ;

Attendu que, pour décider que le juge d'instruction, saisi initialement, non seulement de faits d'importation de stupéfiants, mais également d'autres infractions à la législation sur les stupéfiants, d'association de malfaiteurs et de blanchiment, n'avait pas excédé sa saisine en poursuivant la mise en œuvre des mesures coercitives exécutées sur commission rogatoire lorsque des faits nouveaux d'importation étaient apparus, l'arrêt retient, notamment, que, dès que la réalité de ces nouvelles importations en provenance des Pays-Bas a été confirmée par les investigations, le magistrat instructeur a communiqué ces éléments au procureur de la République qui a étendu sa saisine par les réquisitoires supplétifs susvisés ;

Attendu qu'en l'état de ces énonciations, fondées sur l'appréciation souveraine des éléments de fait qui lui étaient soumis, la chambre de l'instruction a justifié sa décision ;

D'où il suit que le moyen doit être écarté ;

Et attendu que l'arrêt est régulier en la forme ;

REJETTE les pourvois ;

* * *

4) Arrêt n° 3570 du 15 juin 2011 (09-87.135) – Cour de cassation – chambre criminelle

Rejet

Joignant les pourvois en raison de la connexité ;

Sur le pourvoi formé le 15 octobre 2009 en ce qu'il porte sur des dispositions civiles :

Attendu que les arrêts civils n'ont été rendus que le 29 octobre 2009 ; que, dès lors, le pourvoi formé le 15 octobre 2009 contre des dispositions civiles inexistantes est sans objet ;

Sur la recevabilité du pourvoi formé le 16 octobre 2009 ;

Attendu que le demandeur, ayant épuisé, par l'exercice qu'il en avait fait le 15 octobre 2009 le droit de se pourvoir contre l'arrêt attaqué, était irrecevable à se pourvoir à nouveau contre la même décision ; que seul est recevable le pourvoi formé le 15 octobre 2009 ;

Vu les mémoires produits en demande et en défense ;

Sur le premier moyen de cassation, pris de la violation des articles 6 de la Convention européenne des droits de l'homme, 327, 378, 591 et 593 du Code de procédure pénale, défaut de motifs, ensemble violation des droits de la défense ;

« en ce que le procès-verbal des débats ne précise pas quelles décisions de mise en accusation ont été lues préalablement aux débats ;

« alors que la lecture de la décision de renvoi est une formalité indispensable, essentielle au procès équitable, devant la cour d'assises, que le procès-verbal doit constater et que les mentions du procès-verbal des débats ne permettent pas à la Cour de cassation de s'assurer que les trois arrêts de mise en accusation, en date respectivement des 13 février 2001, 3 août 2001 et 27 novembre 2001, qui fixaient l'étendue de l'accusation portée contre M. X... aient été effectivement lus, en sorte que la cassation est encourue » ;

Attendu que le procès-verbal des débats constate, d'une part, que M. X... a été renvoyé devant la cour d'assises de Paris, spécialement composée, par décisions de mise en accusation des 13 février 2001, 3 août 2001 et 27 novembre 2001, ainsi que par arrêt rectificatif du 22 juin 2001 et, d'autre part, que le président a invité l'accusé et les magistrats composant la cour à écouter avec attention la lecture des décisions de mise en accusation et de l'arrêt en rectification d'erreur matérielle rendu par la chambre de l'instruction de la cour d'appel de Paris le 22 juin 2001 ;

Attendu qu'en cet état, et dès lors que le procès-verbal des débats relate, dans le même contexte, que les greffiers ont procédé alternativement à ces lectures à haute et intelligible voix, la Cour de cassation est en

mesure de s'assurer qu'il a été satisfait aux dispositions de l'article 327 du Code de procédure pénale ;

D'où il suit que le moyen doit être écarté ;

Sur le deuxième moyen de cassation, pris de la violation des articles 6 de la Convention européenne des droits de l'homme, 327, 378, 591 et 593 du Code de procédure pénale, défaut de motifs, ensemble violation des droits de la défense ;

« en ce que le procès-verbal des débats mentionne : – page 7 : "Le président a alors invité l'accusé et les magistrats composant la cour à écouter avec attention la lecture des décisions de mise en accusation, de l'arrêt en rectification d'erreur matérielle rendu par la chambre d'instruction de la cour d'appel de Paris, en date du 22 juin 2001, et des ordonnances de jonction et disjonction rendues par le président de la cour d'assises de Paris, en date des 6 juin 2002 et 1er octobre 2002, des questions posées à la cour d'assises ayant statué en premier ressort, des réponses faites à ces questions, de la décision et de la condamnation prononcée, conformément aux dispositions de l'article 327 du Code de procédure pénale ; qu'à cet instant, Mme Y..., greffier, physiquement empêchée (extinction de voix) a été remplacée par Mme Z..., greffier, pour procéder auxdites lectures ; qu'à la demande du président, les greffiers ont procédé alternativement à ces lectures à haute et intelligible voix ; qu'au cours de l'audience, les interprètes ont prêté leur concours chaque fois que cela a été nécessaire" et reprend les mêmes énonciations page 8 ;

« alors qu'aux termes de l'article 6 § 3 a) de la Convention européenne des droits de l'homme, tout accusé a droit à être informé, dans le plus court délai, dans une langue qu'il comprend et d'une manière détaillée, de la nature et de la cause de l'accusation portée contre lui ; que la lecture des décisions de renvoi est une formalité indispensable pour que l'accusé ait une connaissance détaillée de l'accusation et que, dès lors, cette lecture doit être complète ; qu'il résulte de la procédure que M. X... est de langue arabe, ce qui a justifié la désignation d'interprètes et que la Cour de cassation n'est pas en mesure de s'assurer, au vu des énonciations susvisées du procès-verbal des débats, qu'une traduction complète des arrêts de mise en accusation a été lue à l'audience dans la langue de l'accusé en sorte que la cassation est encourue » ;

Attendu que le procès-verbal des débats mentionne qu'au cours de l'audience durant laquelle ont été lus les trois arrêts de renvoi, les interprètes ont prêté leur concours chaque fois que cela a été nécessaire ;

Qu'il en résulte, en l'absence d'un donné acte qu'il appartenait à l'accusé ou à ses avocats de solliciter, que les interprètes ont traduit les pièces dont la lecture a été donnée à l'audience ;

D'où il suit que le moyen n'est pas fondé ;

Sur le troisième moyen de cassation, pris de la violation des articles 6 de la Convention européenne des droits de l'homme, 4 du Protocole n° 7 annexé à cette Convention, 50 de la Charte des droits fondamentaux de l'Union européenne, 14 du Pacte international relatif aux droits civils et politiques, 6, 316, 591 et 593 du Code de procédure pénale, défaut et contradiction de motifs, manque de base légale, ensemble violation de la règle *non bis in idem*;

« en ce que, par arrêt en date du 17 septembre 2009, la cour d'assises a rejeté l'exception non bis in idem tirée de ce que M. X... avait, en substance, été jugé par un arrêt définitif de la cour d'appel de Paris, en date du 18 décembre 2006, pour des faits identiques à ceux visés dans les trois arrêts de mise en accusation ;

« aux motifs que, si la défense de M. X... fait à bon droit observer que l'article 4 du Protocole n° 7 doit être compris comme interdisant de poursuivre ou de juger une personne pour une seconde infraction, pour autant que celle-ci a pour origine des faits identiques ou des faits qui sont en substance les mêmes, il impose cependant de considérer en l'espèce que les faits sur lesquels se sont fondées les juridictions correctionnelles, comporteraient-ils l'évocation d'actes criminels visés aux présentes poursuites, ne se limitent aucunement à ces derniers pour asseoir la culpabilité de M. X... ; que, pour caractériser en effet le délit d'association de malfaiteurs, infraction autonome prévue et réprimée par l'article 450-1 du Code pénal, celles-ci ont analysé l'ensemble des éléments de nature à caractériser l'implication de l'accusé en son sein et dont le but consistait à organiser, développer et pérenniser un mouvement déterminé à imposer sa cause, notamment par le recours à la clandestinité et à la mise en œuvre de moyens matériels et intellectuels (recrutement et contacts réguliers avec des activistes, diffusion d'informations sur les activités et les thèses du GIA, recherche de fonds, d'armes et matériels divers...), sans se donner nécessairement et exclusivement pour objectif la commission des attentats visés aux poursuites ; que les faits dont se trouve saisie la cour diffèrent substantiellement des précédents en ce qu'ils visent un comportement criminel dirigé vers la réalisation d'objectifs ponctuels, précisément déterminés et non indissociablement liés entre eux, et animés par une motivation spécifique consistant en particulier à fournir, en connaissance de cause, à autrui, les moyens de porter délibérément atteinte à la vie humaine ou à l'intégrité physique ou psychique de l'individu par le recours à des charges explosives ; que, dans ces conditions, la déclaration de culpabilité et la condamnation prononcées par la cour d'appel de Paris ne sauraient conduire la cour d'assises à considérer que l'action publique dirigée contre M. X... se trouve éteinte et à déclarer nulles les poursuites criminelles dont il fait l'objet ; qu'il appartiendra dès lors à cette dernière, à l'issue des débats et à la lumière de ceux-ci, de dire, par ses réponses aux questions qui lui seront posées, si M. X... est coupable ou non des actes de complicité qui lui sont imputés ;

« 1) alors que les arrêts incidents des cours d'assises doivent, à peine de nullité, s'expliquer sur les chefs péremptoires des conclusions déposées au nom de l'accusé ; que, dans ses conclusions régulièrement déposées aux fins de constatation de l'extinction de l'action publique et de nullité des poursuites, M. X… faisait valoir que l'intégralité des faits matériels – transfert de fonds à destination des auteurs des attentats – transmission d'instructions aux mêmes auteurs – suivi de la préparation et de la commission des attentats – fondant les trois actes d'accusation à l'encontre de M. X… avaient déjà servi de fondement à sa condamnation définitive par la cour d'appel de Paris du chef de participation à une association de malfaiteurs en vue de la commission d'actes de terrorisme et qu'en ne s'expliquant pas sur ce chef péremptoire de conclusions, la cour d'assises a méconnu les textes susvisés ;

« 2) alors qu'un même fait autrement qualifié ne peut donner lieu à une double déclaration de culpabilité et que la circonstance que le délit d'association de malfaiteurs soit un délit autonome ne saurait faire échec à ce principe qui est à la fois un principe de droit interne et de droit conventionnel ;

« 3) alors qu'un même fait autrement qualifié ne saurait donner lieu à une double déclaration de culpabilité et que la cour d'assises, qui constatait implicitement mais nécessairement que la décision correctionnelle définitive que M. X… invoquait au soutien de son exception évoquait expressément les faits criminels dont elle était saisie, ne pouvait, sans méconnaître le principe fondamental susvisé, refuser de faire droit à cette exception au motif erroné que le périmètre des faits sur lesquels ladite décision correctionnelle avait statué était plus large que celui des faits soumis à la cour d'assises ;

« 4) alors que la cour d'assises ne pouvait, sans contredire les actes de la procédure, affirmer que les faits dont elle se trouvait saisie différaient substantiellement de ceux ayant fait l'objet de l'arrêt de la cour d'appel de Paris, en date du 18 décembre 2006, en ce qu'ils visaient un comportement criminel dirigé vers la réalisation d'objectifs ponctuels précisément déterminés et non indissociablement liés entre eux dès lors, qu'ainsi que la Cour de cassation est en mesure de s'en assurer, chacun des trois arrêts de mise en accusation affirmait, dans un motif qui servait de soutien nécessaire à sa décision, que l'attentat particulier dont il traitait, s'inscrivait dans une série d'attentats du même type, tous commis entre le 11 juillet 1995 et le 17 octobre 1995, dont il rappelait les lieux et les circonstances, précisant notamment dans l'arrêt du 27 novembre 2001 et qu'il résultait des expertises réalisées dans chacune des affaires concernées que les engins utilisés lors des attentats étaient de même facture et les insérant explicitement dans l'action du GIA, organisation considérée comme une association à but criminel par l'arrêt de la cour d'appel du 18 décembre 2006 ;

« 5) alors que la cour d'assises ne pouvait, sans contredire les pièces de la procédure, affirmer que les faits dont elle était saisie différaient substantiellement des précédents en ce qu'ils visaient un comportement criminel animé par une motivation spécifique consistant en particulier à fournir en connaissance de cause, à autrui, les moyens de porter délibérément atteinte à la vie humaine ou à l'intégrité physique ou psychique de l'individu par le recours à des charges explosives alors qu'il résulte sans ambiguïté des motifs qui servent de soutien nécessaire au jugement du tribunal correctionnel de Paris, en date du 29 mars 2006, dont la cour d'appel de Paris s'est expressément appropriée les motifs dans son arrêt du 18 décembre 2006 qu'en imputant à M. X... la participation, consciente et volontaire, à une entente destinée à accomplir des actes de terrorisme sur le territoire français notamment par des appels téléphoniques qui étaient intervenus dans un contexte d'attentats et plus précisément à la veille de ceux-ci et par l'envoi de fonds destinés au financement des attentats (notamment une somme de 5 000 £ la veille de l'attentat commis le 17 octobre 1995 sur la ligne C du RER à la station Musée d'Orsay), ces décisions correctionnelles lui avaient prêté exactement la même motivation ;

« 6) alors que la cour d'assises a méconnu la portée de l'arrêt de la cour d'appel de Paris du 18 décembre 2006 en affirmant que cette décision concernait l'implication de l'accusé au sein d'une association de malfaiteurs qui ne s'était pas donné nécessairement et exclusivement pour objectif la commission des attentats visés aux poursuites dès lors que la cour d'appel est expressément entrée en voie de condamnation à l'encontre de M. X... pour avoir joué un rôle essentiel au sein du GIA, organisation dont l'objectif était la préparation, l'assistance à la réalisation et l'exploitation médiatique des attentats réalisés » ;

Attendu que, pour rejeter, par arrêt incident, l'exception de chose jugée tirée de ce que l'accusé a déjà été condamné par arrêt de la cour d'appel de Paris du 18 décembre 2006 du chef de participation à une association de malfaiteurs en vue de la commission d'actes de terrorisme, la cour d'assises prononce par les motifs reproduits au moyen ;

Attendu qu'en cet état, et dès lors que l'association de malfaiteurs constitue un délit distinct tant des crimes préparés ou commis par ses membres que des infractions caractérisées par certains faits qui la concrétisent, les griefs invoqués ne sont pas encourus ;

D'où il suit que le moyen ne saurait être accueilli ;

Sur le quatrième moyen de cassation, pris de la violation des articles 6 de la Convention européenne des droits de l'homme, préliminaire et 32 du Code de procédure pénale, ensemble violation des droits de la défense ;

« En ce que, par arrêt en date du 17 septembre 2009, la cour d'assises a rejeté l'exception d'irrecevabilité des poursuites en raison de l'atteinte irréparable portée à la présomption d'innocence de M. X… ;

« aux motifs que, si les propos attribués au garde des Sceaux en exercice à l'époque des faits et dont s'est fait l'écho la presse nationale n'ont pas lieu d'être remis en cause, la cour relèvera toutefois que ceux-ci doivent être replacés dans un contexte marqué par l'inquiétude de la population française dans son ensemble ainsi que celle de ses dirigeants ; que, s'ils ont été tenus par un responsable politique important dont relève directement l'autorité de poursuite, que celui-ci n'a cependant pas concouru de manière directe au déroulement de l'enquête et de l'instruction et se borne d'ailleurs à imputer à M. X… un rôle central sans pour autant le préciser et sans lui attribuer de manière définitive une culpabilité qui reste à démontrer ; qu'en toute hypothèse, de telles déclarations n'apparaissent pas suffisantes pour porter atteinte à l'impartialité et à l'indépendance des magistrats du siège composant la cour et à priver de la sorte M. X… des garanties que lui confèrent les dispositions de l'article 6 de la Convention européenne des droits de l'homme ;

« 1) alors que les propos publiquement tenus avant tout jugement par un garde des Sceaux et relayés par l'ensemble de la presse selon lesquels un "individu nommément désigné a manifestement joué un rôle central dans un ensemble d'attentats commis en France" sont des propos qui attribuent à cet individu une culpabilité certaine relativement à des faits de nature criminelle en violation de la présomption d'innocence et qui pèsent, du fait de l'autorité qui s'attache aux fonctions de garde des Sceaux, irrévocablement sur son jugement ultérieur ;

« 2) alors que la sensibilité de l'opinion publique, loin de justifier de tels propos, en aggrave la portée au regard du principe intangible de la présomption d'innocence ;

« 3) alors que la circonstance que le garde des Sceaux dont relève directement l'autorité de poursuite selon les constatations de l'arrêt n'ait pas concouru de manière directe au déroulement de l'enquête ou de l'instruction est sans influence sur l'appréciation de l'atteinte à la présomption d'innocence dès lors qu'ainsi que la cour européenne des droits de l'homme l'a constaté dans son arrêt Medvedyev et autres c/ France *du 10 juillet 2008 (no 61) que le procureur de la République n'est pas en France une "autorité judiciaire" au sens que la jurisprudence de la cour européenne des droits de l'homme donne à cette notion puisqu'il lui manque en particulier l'indépendance à l'égard du pouvoir exécutif pour pouvoir être ainsi qualifié ;*

« 4) alors que le ministère public étant partie intégrante et nécessaire des juridictions répressives, il ne suffit pas pour que l'impartialité et l'indépendance de la juridiction soient garanties que les magistrats du siège, compte tenu de leur statut, ne puissent pas personnellement être suspectés de manque d'impartialité et d'indépendance » ;

Attendu que, pour écarter, par arrêt incident, l'exception d'irrecevabilité des poursuites en raison de l'atteinte à la présomption d'innocence, la cour d'assises prononce par les motifs reproduits au moyen ;

Attendu qu'en cet état, et dès lors que les expressions d'opinion invoquées par le demandeur n'étaient pas de nature à porter atteinte à l'indépendance des juges ou à remettre en cause leur impartialité, les griefs allégués ne sont pas encourus ;

D'où il suit que le moyen n'est pas fondé ;

Sur le cinquième moyen de cassation, pris de la violation des articles 6 de la Convention européenne des droits de l'homme et 331, alinéa 4, du Code de procédure pénale ;

« en ce qu'il résulte du procès-verbal des débats qu'à l'audience du 6 octobre 2009, après-midi, le témoin M. A... a été interrompu dans sa déposition par l'avocat général sous prétexte d'indiquer à la cour que le témoin M. B... pourrait être entendu par visio-conférence dans le courant de l'après-midi du 7 octobre 2009 ;

« alors qu'aux termes de l'article 331, alinéa 4, du Code de procédure pénale, sous réserve des dispositions de l'article 309, les témoins ne sont pas interrompus en leur déposition et que cette règle, qui doit être strictement observée, s'impose au représentant du ministère public à peine de nullité des débats » ;

Attendu qu'il résulte du procès-verbal des débats qu'à l'audience du 6 octobre 2009, le témoin M. A... a été entendu après avoir prêté serment dans les termes prescrits par l'article 331, alinéa 3, du Code de procédure pénale et après avoir accompli toutes les autres formalités prévues par cet article ; qu'après cette déposition, les dispositions des articles 312 et 332 du même code ont été observées ; qu'au cours de l'audition du témoin, le président, pour faciliter la compréhension des débats, a communiqué aux parties une annexe d'un rapport d'expertise ; qu'aucune observation n'a été faite à ce propos ; qu'à cet instant l'avocat général a indiqué à la cour qu'un témoin pourrait être entendu par visio-conférence dans le courant de l'après-midi du 7 octobre 2009 ; que le procès-verbal ajoute qu'il a ensuite été procédé à l'audition du témoin M^me^ C... ;

Attendu qu'il se déduit de ces énonciations que l'avocat général est intervenu après la déposition du témoin M. A... ;

D'où il suit que le moyen manque en fait ;

Sur le sixième moyen de cassation, pris de la violation des articles 6 de la Convention européenne des droits de l'homme, préliminaire, 315, 316, 591 et 593 du Code de procédure pénale, défaut de motifs, manque de base légale, ensemble violation des droits de la défense ;

« en ce que, par arrêt en date du 8 octobre 2009, la cour d'assises a rejeté les demandes de supplément d'information présentées par M. X... suivant conclusions régulièrement déposées les 24 septembre et 1er octobre 2009 ;

« aux motifs que la défense de M. X... fait en substance valoir que la thèse avancée par l'accusation selon laquelle l'individu surnommé "E..., F..., G..., H...", ou « I... » alias "A... J...," complice de M. K..., ne serait autre que M. X... est formellement contestée par ce dernier ; qu'un individu du nom de M. A... L..., membre du GIA, alias « A... J... » aurait été si impliqué dans des groupes considérés comme terroristes qu'il aurait été condamné à mort par contumace par décision de la cour d'appel d'Alger pour des faits d'attentats terroristes à l'aéroport d'Alger en 1992 ; que d'une manière tout à fait inespérée et à la suite de l'évocation de la personne de M. L... en audience publique, elle aurait été informée que le nommé M. A... J... pourrait s'identifier à un certain M. A... L..., susceptible d'être né le 6 septembre 1952 ou le 9 juin 1952, domicilié au Royaume-Uni depuis approximativement 1988, où il aurait changé de nom pour s'appeler M. F... C... et dont l'un des enfants, né R... L..., aurait été condamné à la prison à vie pour des faits de nature terroriste par un tribunal de Londres ; que l'accusation se fonde notamment sur les relations téléphoniques prétendument échangées par le dénommé G... ou F..., s'identifiant selon elle à M. X..., et M. K... à partir de lignes téléphoniques ouvertes aux noms de MM. M..., N... et O..., sans qu'aucune de ces trois personnes n'ait fait l'objet d'investigations ; que M. X... s'étant trouvé astreint à des mesures de surveillance du mois de mai 1993 au 4 novembre 1995, la communication des registres de signature tenus par les commissariats de Londres où il avait pour obligation de se présenter une fois par semaine permettait de vérifier si les communications téléphoniques incriminées lui sont ou ne lui sont pas imputables et si les alias d'E... et A... J... peuvent s'appliquer à M. C..., ce qui permettrait de l'innocenter ; qu'il est apparu à l'audience du 29 septembre 2009, à l'occasion de la déposition de M. P..., d'une part, que M. N..., titulaire de l'une des lignes téléphoniques prétendument utilisée par M. X..., a fait l'objet d'une enquête de la section antiterroriste de la Metropolitan police *britannique en même temps que MM. Q..., R... et S... ; que, d'autre part, le témoin M. P... a fait état, à la suite d'un fax de* Scotland Yard *reçu le jour même de son audition d'un relevé dactyloscopique qui n'est pas présent au dossier de la cour pourtant relatif aux scellés saisis au 30, Braybrook Street à Londres dont l'un des locataires officiels était M. X... ; que, selon la défense, faute d'ordonner le supplément d'information sollicité, la cour ne pourra que prononcer le renvoi de l'affaire à une autre session ; que les parties civiles, notamment Me T..., Me U... et Me V..., soulignant que les prétendues difficultés invoquées par la défense avaient été contradictoirement débattues à l'audience et qu'en aucune manière n'apparaissent justifiées les mesures d'investigations réclamées, ont demandé que soient rejetées les demandes ; que l'avocat général a, par voie de réquisitions orales, demandé à la cour de rejeter les demandes*

et de passer outre aux débats ; qu'au vu des résultats de l'instruction à l'audience qui vient de prendre fin, la cour est en mesure de s'assurer que les mesures d'investigations sollicitées ne sont pas nécessaires à la manifestation de la vérité ;

« 1) alors que la cour qui, en reproduisant fut-ce de manière tronquée les éléments figurant dans le procès-verbal des débats invoqués par la défense, dont elle ne contestait pas la réalité, constatait implicitement mais nécessairement l'existence d'éléments nouveaux résultant des débats, ne pouvait, sans méconnaître ses pouvoirs et violer ce faisant le principe de la présomption d'innocence, refuser de faire droit aux demandes de supplément d'information sollicitées par l'accusé en se bornant à faire laconiquement état de ce que les mesures d'investigation sollicitées ne sont pas nécessaires à la manifestation de la vérité ;

« 2) alors que, lorsqu'à l'appui de sa demande de supplément d'information la défense verse aux débats une pièce à décharge susceptible d'établir son innocence, la cour a l'obligation de l'examiner et d'en déterminer la portée dans sa décision ; qu'au soutien de sa contestation de la thèse de l'accusation selon laquelle il s'identifierait à M. A... J... alias M. A... L..., complice de M. K..., M. X... produisait en annexe de ses conclusions un extrait de la décision de la chambre de contrôle de la cour spéciale d'Alger, en date du 21 avril 1993, d'où il résultait que M. L... avait été condamné par contumace pour l'attentat de l'aéroport d'Alger du 26 août 1992 et qu'en ne s'expliquant dans sa décision sur la portée de cette pièce à décharge qui était capitale et qu'en ne la visant même pas dans sa décision, la cour d'assises a privé M. X... du procès équitable auquel il avait droit ;

« 3) alors que, dans ses conclusions régulièrement déposées le 24 septembre 2009, M. X... se fondait expressément sur les déclarations de l'avocat général à l'audience du 21 septembre 2009, d'où il résultait que des recherches pourraient être entreprises concernant la personne de M. L... auquel M. X... contestait s'identifier si l'état civil de celui-ci était précisé et notamment sa date de naissance et que dès lors que M. X... fournissait, selon les propres constatations de l'arrêt, la date de naissance de celui-ci, la cour d'assises ne pouvait, compte tenu de cet élément nouveau dont l'accusation avait admis l'importance, refuser de faire droit à la demande de supplément d'information sollicitée en omettant de s'expliquer sur la valeur de cet élément nouveau ;

« 4) alors que, dans ses conclusions régulièrement déposées le 24 septembre 2009, M. X... invoquait à l'appui de sa demande de supplément d'information comme éléments nouveaux les propos tenus par M. W..., directeur adjoint de la direction de la surveillance du territoire à l'audience du 23 septembre 2009 rapportés au procès-verbal des débats et qu'en ne faisant même pas mention dans sa décision de cette audition et en s'abstenant d'en préciser la portée, la cour a privé sa décision de base légale ;

« 5) alors qu'en ne recherchant pas si les élément fournis par M. P… à l'audience du 29 septembre 2009 ne justifiaient pas un supplément d'information, la cour a méconnu ses pouvoirs et violé ce faisant de plus fort la présomption d'innocence » ;

Attendu que, pour rejeter, par arrêt incident du 8 octobre 2009, les demandes de supplément d'information présentées par l'accusé, la cour d'assises prononce par les motifs reproduits au moyen ;

Attendu qu'en l'état de ces motifs exempts d'insuffisance comme de contradiction, d'où il résulte que les mesures d'instruction sollicitées n'étaient pas nécessaires à la manifestation de la vérité, la cour a justifié sa décision sans méconnaître les dispositions conventionnelles et légales invoquées ;

D'où il suit que le moyen doit être écarté ;

Sur le neuvième moyen de cassation, pris de la violation des articles 6 de la Convention européenne des droits de l'homme, préliminaire et 348 du Code de procédure pénale, ensemble violation des droits de la défense ;

« en ce que le président de la cour d'assises a obtenu de la défense qu'elle le dispense de donner lecture des questions motif pris de leur prétendue conformité avec l'acte d'accusation ;

« alors qu'il résulte des dispositions de l'article 348 du Code de procédure pénale que la lecture des questions, formalité essentielle aux droits de la défense, est obligatoire toutes les fois que les questions ne sont pas posées dans les termes de la décision de renvoi et que la défense ne peut y renoncer qu'en connaissance de cause ; qu'en l'espèce, les questions sur la culpabilité de l'accusé qui ont été posées à la cour d'assises s'étant bornées à viser de façon abstraite les différents modes de complicité sans préciser aucun des faits figurant dans le dispositif des actes d'accusation, ces questions ne peuvent être considérées comme ayant reproduit la substance de l'accusation et que, dès lors, la défense ne peut être considérée comme ayant renoncé en connaissance de cause à leur lecture » ;

Attendu que, si les questions critiquées se sont écartées de la formulation des arrêts de renvoi, elles n'en altèrent pas le sens ni n'en modifient la substance ; que, dès lors, l'article 348 du Code de procédure pénale, qui n'exige pas que les questions soient la reproduction littérale du dispositif de l'arrêt de renvoi, dispensait le président d'en donner lecture ;

D'où il suit que le moyen ne peut être admis ;

Sur le septième moyen de cassation, pris de la violation des articles 6 de la Convention européenne des droits de l'homme, préliminaire, 348 et 349 du Code de procédure pénale, ensemble violation des droits de la défense ;

« en ce que la cour d'assises a répondu affirmativement aux questions n° 1, 7, 27 et 45 ;

« 1) alors qu'est entachée de complexité prohibée, la question, formulée de façon abstraite interrogeant la cour d'assises sur le point de savoir si la mort a été volontairement donnée à une pluralité de victimes ou s'il a été tenté de donner volontairement la mort à une pluralité de victimes ;

« 2) alors que la complexité dont s'agit ne saurait d'autant moins être justifiée que la circonstance que les faits poursuivis, à les supposer avérés, seraient susceptible de s'inscrire dans une action terroriste, que précisément, par leur formulation, les questions susvisées présument des réponses aux questions n° 3, 9, 29 et 47 interrogeant la cour d'assises sur le point de savoir si l'action spécifiée dans ses questions a été commise intentionnellement en relation avec une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur » ;

Attendu que la cour d'assises spécialement composée a répondu affirmativement aux questions suivantes :

N° 1 : Est-il constant qu'à Paris, le 25 juillet 1995, la mort a été volontairement donnée à huit personnes dont les noms sont énumérés ?

N° 7 : Est-il constant qu'à Paris, le 25 juillet 1995, il a été tenté de donner volontairement la mort à cent quarante-neuf personnes dont les noms sont énumérés ?

N° 27 : Est-il constant qu'à Paris, le 6 octobre 1995, il a été tenté de donner volontairement la mort à trente-et-une personnes dont les noms sont énumérés ?

N° 45 : Est-il constant qu'à Paris, le 17 octobre 1995, il a été tenté de donner volontairement la mort à vingt-et-une personnes dont les noms sont énumérés ?

Attendu que ces questions n'encourent pas les griefs allégués ;

Que, d'une part, lorsque le complice paraît seul aux débats, l'existence du fait criminel principal est établi par les réponses affirmatives de la cour d'assises aux questions qui lui sont posées dans la forme abstraite, sur la matérialité du crime ;

Que, d'autre part, quel que fût le nombre de victimes, les crimes dont M. X... a été accusé procédaient, pour chacun d'entre eux, d'un acte unique et indivisible accompli par les mêmes moyens dans les mêmes circonstances de temps et de lieu relevant d'une même intention homicide et devant entraîner les mêmes conséquences pénales ;

D'où il suit que le moyen doit être écarté ;

Sur le huitième moyen de cassation, pris de la violation des articles 6 de la Convention européenne des droits de l'homme, 348 et 349 du Code de procédure pénale, ensemble violation des droits de la défense ;

« En ce que la cour d'assises a répondu affirmativement aux questions n° 4, 5, 6, 10, 11, 12, 19, 20, 21, 24, 25, 26, 30, 31, 32, 35, 36, 37, 42, 43, 44, 48, 49, 50, 56, 57, 58, 61, 62 et 63 ;

« 1) alors que les questions doivent être rédigées en fait par référence au dispositif des décisions de mise en accusation et que ces questions, qui se bornent à reproduire les termes de l'article 121-7 du Code pénal relatifs aux modes de complicité sans reproduire, fut-ce succinctement, les termes des dispositifs des arrêts de mise en accusation relatifs aux faits précis de complicité reprochés à M. X..., ne permettent pas de justifier les déclarations de la cour d'assises relatives à la culpabilité de celui-ci et par conséquent l'arrêt de condamnation ;

« 2) alors que, dans la mesure où les réponses aux questions sur la culpabilité servent de base à l'arrêt de condamnation, lesdites questions doivent être rédigées en énonçant, fut-ce de façon résumée, les faits figurant dans le dispositif de l'acte d'accusation faute de quoi l'arrêt de condamnation ne saurait être considéré comme suffisamment motivé ;

« 3) alors que, en s'abstenant de motiver la déclaration de culpabilité, la cour a méconnu les textes susvisés » ;

Attendu que, d'une part, les questions critiquées, posées dans les termes de la loi, caractérisent en tous leurs éléments les actes de complicité dont M. X... a été déclaré coupable ;

Attendu que, d'autre part, sont reprises dans l'arrêt de condamnation les réponses qu'en leur intime conviction, les magistrats composant la cour d'assises d'appel spécialement composée, statuant dans la continuité des débats, à vote secret et à la majorité, ont données aux questions sur la culpabilité posées conformément aux dispositifs des décisions de renvoi et soumises à la discussion des parties ;

Qu'en cet état, et dès lors qu'ont été assurés l'information préalable sur les charges fondant la mise en accusation, le libre exercice des droits de la défense ainsi que le caractère public et contradictoire des débats, il a été satisfait aux exigences conventionnelles et légales invoquées ;

D'où il suit que le moyen ne saurait être accueilli ;

Sur le dixième moyen de cassation, pris de la violation des articles 4 du Protocole n° 7 additionnel à la Convention européenne des droits de l'homme, 593 du Code de procédure pénale, défaut de motifs, manque de base légale ;

« En ce que la cour d'assises a prononcé à l'encontre de M. X..., en violation du texte susvisé, une double peine, en le condamnant à la

fois à la réclusion criminelle à perpétuité et à l'interdiction définitive du territoire français » ;

Attendu que, contrairement à ce qui est allégué, l'article 4 du Protocole n° 7 à la Convention européenne des droits de l'homme n'interdit pas de prononcer, comme en l'espèce, une peine principale et une peine complémentaire dans une même procédure ;

D'où il suit que le moyen est inopérant ;

Et attendu que la procédure est régulière et que la peine a été légalement appliquée aux faits déclarés constants par la cour d'assises spécialement composée ;

Par ces motifs :

I – Sur le pourvoi formé le 15 octobre 2009 en ce qu'il porte sur des dispositions civiles inexistantes :

Le DECLARE SANS OBJET ;

II – Sur le pourvoi formé le 16 octobre 2009 :

Le déclare IRRECEVABLE ;

III – Sur le pourvoi formé le 15 octobre 2009 en ce qu'il porte sur les dispositions pénales :

Le REJETTE

* * *

5) Arrêt du 27 septembre 2011 de la chambre criminelle de la Cour de cassation

LA COUR DE CASSATION, CHAMBRE CRIMINELLE, a rendu l'arrêt suivant :

Statuant sur les pourvois formés par :

– M. Kassoum X...,

contre l'arrêt de la chambre de l'instruction de la cour d'appel de Paris, 1re section, en date du 15 février 2011, qui, dans l'information suivie contre lui des chefs d'infractions à la législation sur les stupéfiants en bande organisée, association de malfaiteurs et blanchiment, a prononcé sur sa demande d'annulation d'actes de la procédure ;

Vu l'ordonnance du président de la chambre criminelle, en date du 24 mai 2011, prescrivant l'examen immédiat ;

Joignant les pourvois en raison de la connexité ;

Vu le mémoire produit ;

Attendu qu'il résulte des énonciations de l'arrêt attaqué et des pièces de la procédure que, le 30 octobre 2008, le juge d'instruction en charge d'une information portant, notamment, sur un trafic de stupéfiants, a transmis au procureur de la République la copie de pièces faisant apparaître des faits dont il n'était pas saisi, à l'égard d'un nommé « X... », en particulier des déclarations de Mme Aissé Y..., entendue sous le régime de la garde à vue ; qu'en suite de cette transmission, le procureur de la République a fait diligenter une enquête au cours de laquelle, d'une part, le juge des libertés et de la détention a autorisé plusieurs interceptions de correspondances téléphoniques et d'autre part, les officiers de police judiciaire se sont transportés aux fins de perquisition au domicile de Mme Hassiba Z..., entendue également sous le régime de la garde à vue ; qu'à l'issue de l'enquête, une information distincte a été ouverte, le 25 novembre 2008, contre personnes non dénommées, pour trafic de stupéfiants en bande organisée, association de malfaiteurs et blanchiment et que, le 9 octobre 2009, M. Kassoum X... a été mis en examen de ces chefs ;

Attendu que, le 8 avril 2010, M. X... a présenté une requête en annulation des actes de procédure susvisés ; que la chambre de l'instruction, par arrêt avant dire droit du 22 juin 2010, a ordonné la production des procès-verbaux relatifs à la garde à vue et aux auditions de Mme Y... puis, par l'arrêt attaqué, a rejeté la requête ;

En cet état ;

Sur le premier moyen de cassation, pris de la violation des articles 6, 8, 13 de la Convention européenne des droits de l'homme, des articles préliminaire, 706-95, 100, 100-1, 100-3 à 100-7, 591 à 593 du Code de procédure pénale, défaut de motifs, manque de base légale, excès de pouvoir ;

« en ce que l'arrêt attaqué a refusé de prononcer l'annulation des procès-verbaux d'écoutes téléphoniques relatifs aux autorisations délivrées par le juge des libertés et de la détention les 10, 13 et 18 novembre 2008 ainsi que tous les actes ultérieurs qui se trouvent dans un lien de dépendance avec eux ;

« aux motifs que, selon les dispositions de l'article 706-95 du Code de procédure pénale, si les nécessités de l'enquête de flagrance ou de l'enquête préliminaire relative à l'une des infractions entrant dans le champ d'application de l'article 706-73 l'exigent, le juge des libertés et de la détention du tribunal de grande instance peut, à la requête du procureur de la République, autoriser l'interception, l'enregistrement et la transcription de correspondances émises par la voie des télécommunications selon les modalités prévues par les articles 100, 2e alinéa, 100-1 et 100-3 à 100-7, pour une durée maximum de quinze jours, renouvelable une fois dans les mêmes conditions de forme et de durée ; ces opérations sont faites sous le contrôle du juge des libertés et de la détention ; selon les dispositions de l'article 100, alinéa 2, dudit code, la décision

d'interception est écrite, elle n'a pas de caractère juridictionnel et elle n'est susceptible d'aucun recours ; dès lors le juge des libertés et de la détention n'avait pas à motiver sa décision ; que les deux conditions à l'ingérence que constitue une écoute téléphonique, c'est-à-dire être "prévue par la loi" et "poursuivre un but légitime nécessaire dans une société démocratique", ont été en l'espèce respectées dès lors que les modalités des articles 100 à 100-7 du Code de procédure pénale ont été respectées et que l'on se trouvait, en présence d'un trafic de stupéfiants, dans le champ d'application de l'article 706 – 73 3° du même code ;

« 1°) alors que la décision par laquelle le juge des libertés et de la détention autorise l'interception des correspondances émises par la voie des télécommunications doit être soumise à un recours efficace ; qu'en rejetant la demande de nullité des autorisations d'interception tirée au motif qu'elles n'ont pas de caractère juridictionnel et ne sont susceptibles d'aucun recours, la chambre de l'instruction a violé les textes et le principe susvisé ;

« 2°) alors que les autorisations d'interception doivent être motivées afin de justifier des nécessités de l'enquête et de leur caractère proportionné ; qu'en relevant que les autorisations critiquées étaient suffisamment motivées par le respect des articles 100 à 100-7 du Code de procédure pénale et 706-73 du même code, qui se bornent à exiger l'obligation de mentionner les éléments permettant d'identifier la ligne téléphonique soumise à l'interception, la durée de celle-ci et l'infraction, objet des investigations, quand ces autorisations ne caractérisaient pas des constatations précises et circonstanciées au regard des faits de l'espèce la nécessité d'effectuer ces actes coercitifs, la chambre de l'instruction a violé les textes et principes susvisés » ;

Attendu que, pour rejeter le moyen de nullité pris du défaut de motivation des décisions d'autorisation des interceptions de correspondances téléphoniques rendues par le juge des libertés et de la détention, l'arrêt prononce par les motifs repris au moyen ;

Attendu qu'en se déterminant ainsi, les juges ont fait une exacte application des textes légaux susvisés, qui ne prévoient pas une telle motivation, lesquels ne sont pas contraires aux dispositions conventionnelles invoquées dès lors que les écoutes téléphoniques constituent une ingérence nécessaire, dans une société démocratique, pour lutter notamment contre la criminalité organisée, que ces mesures sont autorisées par un juge qui doit être tenu informé de leur exécution et qu'elles répondent à des exigences précises, énoncées par les articles 100 à 100-5 du Code de procédure pénale, dont la personne concernée peut faire sanctionner le défaut de respect par une requête en nullité ;

D'où il suit que le moyen doit être écarté ;

Sur le deuxième moyen de cassation, pris de la violation de l'article préliminaire, des articles 56, 56-1, 57, 59, 591 à 593 du Code de procédure

pénale, défaut de motifs, manque de base légale, excès de pouvoirs et dénaturation des pièces de la procédure ;

« en ce que l'arrêt attaqué a refusé d'annuler la perquisition réalisée au domicile de Mme Hassiba Z... ainsi que tous les actes subséquents dont elle constitue le support nécessaire ;

« aux motifs que, selon le procès-verbal de "transport-interpellation" coté D 1202, les enquêteurs se sont transportés... où était domiciliée Mme Hassiba Z... à 5 heures 20 ; rejoints à 5 heures 50 par un équipage du commissariat de l'arrondissement, ils ont constaté que l'accès au numéro 36 se faisait par un portail situé au numéro 40 de la voie considérée ; ils ont ensuite emprunté un escalier au fond d'une cour et se sont portés à hauteur de la porte RDC gauche du logement occupé par l'intéressée puis, après quelques précautions, ont toqué à la porte à 6 heures qui leur a été ouverte par l'occupante des lieux, Mme Hassiba Z... qui a été interpellée ; la perquisition ou visite domiciliaire a été réalisée au seul domicile de Mme Hassiba Z..., lieu où elle habite, à 6 heures ; l'approche dudit domicile par un portail situé à proximité puis le franchissement d'une cour intérieure ne sauraient en l'espèce, dès lors qu'il ne s'agit nullement de parties communes dudit immeuble, être assimilés à un domicile c'est-à-dire un lieu clos à usage privé ;

« alors que l'accès au domicile par un passage protégé par un portail fût-il commun à plusieurs occupants d'un immeuble, constitue le prolongement du domicile de chacun de ces occupants ; qu'ainsi, en pénétrant dans les parties communes de l'immeuble du domicile de Mme Hassiba Z... et en franchissant un portail avant 6 heures du matin en l'absence de l'autorisation prévue par la loi, les officiers de police judiciaire ont excédé leurs pouvoirs ; que, dès lors, en refusant d'annuler cette perquisition et tous les acte dont elle était le support et qui portaient grief à M. Kassoum X..., la chambre de l'instruction a violé les textes et principes susvisés » ;

Attendu que M. X... ne démontre pas en quoi l'irrégularité des opérations de transport au domicile de Mme Z... qu'il allègue, prise de ce que les officiers de police judiciaire se trouvaient, entre cinq heures cinquante et six heures, dans la cour de l'immeuble où est domicilié l'intéressée, a porté atteinte à ses intérêts, dès lors que, dans les lieux et le laps de temps considérés, il n'a été procédé à aucune investigation ;

D'où il suit que le moyen n'est pas fondé ;

Sur le troisième moyen de cassation, pris de la violation des articles 6 de la Convention européenne des droits de l'homme, des articles préliminaire, 63-1, 63-4, 77, 706-73, 706-88, 591 à 593 du Code de procédure pénale, défaut de motifs, manque de base légale ;

« en ce que l'arrêt attaqué a dit n'y avoir lieu à annulation de la garde à vue de Mme Aissé Y... ainsi que l'ensemble des pièces dont elle est le support nécessaire et qui font grief à M. X... ;

« aux motifs qu'il résulte de la procédure, spécialement de tous les procès-verbaux de la garde à vue de Mme AisséY… les éléments suivants : les policiers ont notifié à Mme Aissé Y… en langue française qu'elle comprenait, que pour les nécessités de l'enquête et au vu d'une ou plusieurs raisons plausibles de soupçonner qu'elle avait commis ou tenté de commettre une infraction à la législation sur les stupéfiants, elle était placée en garde à vue à compter du 19 août 2008 à 6 heures 40, heure de son interpellation, pour une durée de 24 heures, qui pourrait éventuellement être prolongée de 24 heures, et après présentation devant un magistrat de deux nouveaux délais de 24 heures ou dérogatoirement d'un seul délai de 48 heures ; informée des articles 63-1 à 63-4 et 706-88 du Code de procédure pénale, l'intéressée a déclaré qu'elle ne voulait pas aviser une tierce personne de la mesure de garde à vue dont elle faisait l'objet, ne désirait pas faire l'objet d'un examen médical, prenait acte de ce qu'elle pourrait solliciter un examen médical en cas de première prolongation, du droit de ce qu'elle serait de droit examinée par un médecin désigné en cas de prolongation supplémentaire et qu'elle pourrait solliciter un autre examen médical à tout moment, de ce qu'elle pouvait bénéficier du droit à s'entretenir avec un avocat à l'issue de la soixante douzième heure de la mesure, répondant alors qu'elle voulait être assistée par un avocat commis d'office ; après l'avoir entendue à deux reprises, les enquêteurs notifiaient à Mme Aissé Y… le 19 août 2008 à 18 heures 45 une première prolongation de sa garde à vue décidée par le magistrat instructeur en ces termes : "Lui notifions, en langue française, qu'elle comprend, que pour les nécessités de l'enquête, et au vu de l'existence d'une ou plusieurs raisons plausibles de soupçonner qu'elle a commis ou tenté de commettre une infraction à la législation sur les stupéfiants, sur notre demande et après autorisation écrite de Mme Goetzmann, juge d'instruction au tribunal de grande instance de Paris, la mesure de garde à vue prise à son encontre ce jour le 19 août 2008 à 06 heures 40, est prolongée d'un nouveau délai de 24 h 00 à compter du 20 août 2008 à 06 heures 40 ; que, rappel effectué des droits mentionnés à l'article 63-3 du Code de procédure pénale, l'intéressée déclare : je souhaite n'être pas examinée par un médecin conformément à ma précédente demande" ; après l'avoir encore entendue à trois reprises, les enquêteurs notifiaient à Mme Y… le 20 août 2008 à 21 heures une seconde prolongation de sa garde à vue décidée par le magistrat instructeur en ces termes : « Lui notifions, en langue française, qu'elle comprend, que pour les nécessités de l'enquête, et après sa présentation, sur requête de Mme Goetzmann, juge d'instruction au tribunal de grande instance de Paris, ce magistrat nous a délivré une autorisation écrite de prolongation de garde à vue d'un nouveau délai de 48 heures ; que cette mesure prend effet à compter du 21 août 2008 à 6 heures 40 ; que rappel effectué des droits mentionnés aux articles 706-88, 63-3 et 63-4 du Code de procédure pénale, l'intéressée nous déclare : je prends acte qu'un médecin, désigné dès le début de la mesure par le magistrat compétent ou l'officier de police judiciaire va m'examiner sans délai ; de droit, je prends acte que je pourrai solliciter un autre examen médical ; vous me rappelez que je peux bénéficier du

droit à m'entretenir avec un avocat à l'issue de la soixante douzième heure de la mesure ; pour le moment, je désire m'entretenir avec un avocat désigné à savoir Me Bremaud, du barreau de Paris, tel : 01 42 21 10 01 ou le 06 20 81 34 04 à l'issue de la soixante douzième heure de la mesure ; après l'avoir enfin entendue à deux reprises, les enquêteurs notifiaient à Mme Aïssé Y… le 22 août 2008 à 10 heures 30 le déroulement et la fin de sa garde à vue intervenue à 10 heures 40, en vue de sa présentation devant le magistrat instructeur ; son conseil désigné, régulièrement avisé le 21 août 2008 à 16 heures 45, ne s'est pas présenté comme invité à le faire à l'issue de la soixante douzième heure soit à compter du 22 août 2008 à 06 heures 40 ; il est spécialement indiqué audit procès-verbal les formalités procédurales suivantes : "Lui notifions, en langue française qu'elle comprend, que sur instructions de Mme Goetzmann, juge d'instruction au tribunal de grande instance de Paris, il est mis fin à la mesure de garde à vue dont elle fait l'objet depuis le 19 août à 06 heure 40, heure de son interpellation, ce jour à l'heure figurant en bas du présent, en vue d'une présentation devant le juge mandant ; mesure prolongée de 24 h 00, sur autorisation de Mme Goetzmann, juge d'instruction au tribunal de grande instance de Paris, depuis le 20 août 2008 à 06 h 40 ; et prolongée d'un nouveau délai de 48 h 00, sur autorisation de Mme Goetzmann juge d'instruction au tribunal de grande instance de Paris et après présentation de l'intéressée, depuis le 21 août 2008 à 06 h 40 ; Lui rappelons, qu'informée de ses droits, conformément aux dispositions des articles 63-1 à 63-4 du Code de procédure pénale : elle n'a pas souhaité faire prévenir un membre de sa famille, elle a fait l'objet d'un examen médical : le 19 août 2008 à 06 h 40 ; annexons au présent le certificat médical établi par ce praticien ; elle a souhaité s'entretenir avec un avocat à l'issue de la soixante douzième heure de garde à vue ; elle a assisté à la perquisition de son domicile le 19 août de 06 heures 50 à 07 heures 30 ; elle a été entendue : le 19 août 2008 de 08 h 20 à 12 h 15, le 19 août 2008 de 15 h 15 à 16 h 30, le 20 août 2008 de 10 h 15 à 12 h 30, le 20 août 2008 de 14 h 30 à 15 h 30, le 21 août 2008 de 17 h 30 à 18 h 50, le 21 août 2008 de 10 h 30 à 12 h 30, le 21 août 2008 de 15 h 00 à 17 h 45 ; elle n'a pu s'entretenir avec Me Bremaud, celui – ci bien que régulièrement avisé, ne s'est pas présenté au service durant le temps de la garde à vue ; elle a été laissée au repos le reste du temps ; elle a pu s'alimenter aux heures habituelles dans les locaux de police ; restituons à l'intéressée ses effets ou documents personnels n'ayant pas fait l'objet d'une mise sous cote ou d'un placement sous scellé pour les besoins de l'enquête ; l'intéressée ne formule aucune observation" ; que si le procès-verbal de la première prolongation de garde à vue en date du 19 août 2008 à 18 heures 40 ne mentionne pas le rappel du droit à bénéficier de l'assistance d'un conseil à l'issue de la soixante douzième heure, qui avait été notifié lors du placement en garde à vue et qui a été rappelé lors de la deuxième prolongation de la mesure coercitive en vertu du procès-verbal en date du 20 août à 21 heures 30, le procès-verbal récapitulatif du déroulement de la garde à vue et de notification de la fin de la mesure, tel que décrit intégralement ci-avant, énonce notamment que les droits des articles 63-1 à 63-4

du Code de procédure pénale ont bien été notifiés ; selon la cote D 950/2 devenue D 1729/62, les enquêteurs ont régulièrement avisé Me Bremaud d'avoir à se présenter au service de police à compter du 22 août 2008 à compter de 06 heures 40 ; aucune atteinte n'a été portée aux droits de Mme Y... puisque elle a été utilement informée du droit et qu'il a été régulièrement mis à exécution par les enquêteurs ; la chambre n'a relevé aucune cause de nullité jusqu'à la cote D 1734 ;

« 1°) alors qu'en vertu de l'article 706-88 du Code de procédure pénale la personne dont la garde à vue est prolongée doit être avisée de son droit à s'entretenir avec un avocat à chaque notification de prolongation ; qu'en l'espèce, il ressort du procès-verbal de prolongation de garde à vue que le droit à l'assistance d'un avocat n'a pas été rappelé à Mme Y... lors de la première prolongation, ce qui lui a nécessairement porté atteinte ; qu'en refusant d'annuler cette garde à vue, en relevant que cette notification résulterait du procès-verbal récapitulatif du déroulement de la garde à vue et de notification de la fin de la mesure, la chambre de l'instruction a dénaturé les pièces de la procédure et privé sa décision de base légale ;

« 2°) alors, qu'en vertu de l'article 6 § 3 de la Convention européenne des droits de l'homme, toute personne, placée en garde à vue, doit, dès le début de cette mesure, être informée de son droit de se taire et, sauf exceptions justifiées par des raisons impérieuses tenant aux circonstances particulières de l'espèce pouvoir bénéficier, en l'absence de renonciation non équivoque, de l'assistance d'un avocat ; qu'en l'espèce, dès lors que la chambre de l'instruction a refusé d'annuler la garde à vue de Mme Y..., bien qu'il ressort des pièces de la procédure qu'elle n'a pas été informée de son droit au silence et qu'elle n'a pas bénéficié de l'assistance d'un avocat dans les conditions précitées, la chambre de l'instruction a violé les textes et le principe susvisés » ;

Sur le moyen pris en sa première branche :

Attendu que M. X... ne démontre pas en quoi l'irrégularité de la garde à vue de Mme Y... qu'il allègue, prise du défaut de notification à celle-ci, lors de la première prolongation de cette mesure, de son droit à l'assistance d'un avocat, a porté atteinte à ses intérêts dès lors que l'intéressée, informée de ce droit dès son placement en garde à vue, avait déclaré vouloir en bénéficier et que, cette assistance ne pouvant être mise en œuvre légalement qu'à partir de la soixante douzième heure, cet élément est indifférent au contenu des déclarations, faites antérieurement, par lesquelles Mme Y... a mis en cause le demandeur ;

Sur le moyen pris en sa seconde branche :

Attendu que M. X..., qui n'est plus recevable, en application des articles 173-1 et 174 du Code de procédure pénale, à faire état auprès de la chambre de l'instruction, fût-ce en se prévalant d'une évolution de la jurisprudence, d'un moyen de nullité des auditions en garde à vue de Mme Y..., ne saurait être admis à invoquer devant la Cour de cassation un

tel moyen pour faire grief à l'arrêt d'avoir rejeté sa requête en annulation d'actes de la procédure ;

D'où il suit que le moyen, irrecevable en sa seconde branche, ne saurait être accueilli ;

Et attendu que l'arrêt est régulier en la forme ;

REJETTE les pourvois ;

Table des matières