Commission nationale de contrôle des interceptions de sécurité

22e rapport d'activité

Années 2013-2014

La documentation Française

22e rapport d'activité
2013-2014

Commission nationale
de contrôle
des interceptions
de sécurité

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

« En application de la loi du 11 mars 1957 (article 41) et du Code de la propriété intellectuelle du 1er juillet 1992, complétés par la loi du 3 janvier 1995, toute reproduction partielle ou totale à usage collectif de la présente publication est strictement interdite sans autorisation expresse de l'éditeur. Il est rappelé à cet égard que l'usage abusif et collectif de la photocopie met en danger l'équilibre économique des circuits du livre. »

© Direction de l'information légale et administrative, Paris, 2015
ISBN : 978-2-11-009866-5

Sommaire

Avant-propos

Le contrôle des interceptions de sécurité est inscrit désormais, en France, dans la durée et dans l'efficacité. En des temps où la situation internationale et nationale place l'activité de renseignement devant des exigences redoutables, il est nécessaire de redire que cette activité a pour contrepartie l'examen minutieux de leurs demandes en matière d'interception ainsi que celui des productions auxquelles elles donnent lieu, lorsqu'une suite positive leur est donnée par l'autorité politique. C'est là une nécessité démocratique dont le développement doit aller de pair avec ce qui doit être mis en œuvre pour la sauvegarde de la sécurité du pays.

Pour exercer ce contrôle, Jean-Louis Dewost, président de la Commission (2003-2009), indiquait qu'il fallait trois qualités : l'indépendance, la confiance et la vigilance[1]. Elles n'ont pas manqué durant les mandats de mes prédécesseurs. Elles ne manqueront pas, j'y veillerai, dans les mois qui viennent. Dans le respect du secret que la loi impose et qui doit être observé pour des raisons évidentes, il convient en outre d'assurer les conditions du dialogue avec l'exécutif, notamment le cabinet du Premier ministre et le Groupement interministériel de contrôle ; avec les services demandeurs, dont l'activité doit être comprise et les délais respectés ; avec les autres autorités qui concourent à donner un contenu concret aux garanties qui entourent l'exercice des libertés. Mais ce dialogue constant ne saurait détourner la Commission des fins pour lesquelles elle a été instituée.

Depuis la création de la Commission, en 1991, les interceptions de sécurité sont désormais mieux encadrées. Mais de grands changements sont intervenus. La nature du dispositif a changé, en raison de la montée progressive d'autres moyens de connaissance en « milieu ouvert » comme en « milieu fermé ». Les interceptions ne sont plus le commencement d'un processus de recherche et d'identification, mais plutôt son aboutissement, après usage d'autres technologies. Celles-ci, en plein développement, doivent être contrôlées, si nécessaire, à leur tour. La loi y a pourvu pour certaines d'entre elles ; pas pour toutes. Dans le même

---

1) Commission nationale de contrôle des interceptions de sécurité, 20e rapport d'activité, Paris, la Documentation française, 2012, 205 p., pages 9 *et sq.*

temps, la configuration des services a changé, encore durant l'année 2014 (création de la Direction générale de la sécurité intérieure d'une part et du service central de renseignement territorial d'autre part) ; on doit se réjouir d'un encadrement plus précis donné à la nature de leurs activités. Mais le désir d'y échapper peut toujours exister : les raisons existent, avec la montée des dangers qu'on a mentionnée.

De ces évolutions, beaucoup d'esprits avisés[1] ont déduit que la loi devait évoluer à son tour, à la fois pour encadrer et légitimer les pratiques des services, pour suivre les évolutions technologiques, enfin pour mieux unifier des approches et des procédures devenues trop diverses sans véritable justification.

Les pouvoirs publics semblent être convaincus de la nécessité d'une modification législative. Elle s'impose en effet, pour mieux assurer les tâches nécessaires dans la sécurité juridique. Mais à la condition – chacun doit y veiller – que la loi nouvelle n'altère en rien les acquis de 1991 : « Il conviendra, écrit encore Jean-Louis Dewost[2], d'y regarder à deux fois avant d'entreprendre une révision de la loi de 1991 ».

Regardons-y à deux fois et indiquons ce qui doit figurer dans une loi à venir, sans laquelle elle manquerait à l'équilibre délicat entre sécurité et liberté.

1 - D'abord, elle doit sauvegarder, dans tous les cas de figure, cette architecture voulue en 1991, en quatre piliers : la demande, le contrôle, la décision et l'exécution. En d'autres termes, le service de renseignement formule un besoin, une personne indépendante en contrôle la nécessité, un responsable politique l'autorise, un service distinct en assure, pour le service demandeur, la réalisation. Cette séparation – on ne l'a pas assez relevé – constitue, en elle-même, une garantie d'équilibre. Tout comme la bonne vieille distinction ordonnateurs – comptables préserve, en matière de finances publiques, les agents de la tentation de la corruption. Elle doit être préservée.

2 - Ensuite, et c'est le moins qu'on puisse exiger du nouveau texte, elle doit satisfaire les besoins des services, sous la réserve naturellement que l'atteinte au droit de chacun au respect de sa vie privée soit effectivement rendue nécessaire et demeure proportionnée au risque identifié. La pratique montre que le caractère exceptionnel de l'intrusion, sagement inscrit dans la loi de 1991, se banalise parfois dans la durée et que les

---

1) Entre autres, Jean-Jacques URVOAS et Patrick VERCHERE, Rapport d'information n° 1022 sur l'évaluation du cadre juridique applicable aux services de renseignement, Assemblée nationale, 14 mai 2013, 205 p. ; Bertrand WARUSFEL, *Pour un approfondissement du cadre juridique des interceptions de sécurité,* Commission nationale des interceptions de sécurité, 21e rapport d'activité, Paris, la Documentation française 2013, 171 p., p. 17 *et sq.* ; Sébastien-Yves LAURENT, Pour une véritable politique du renseignement, Paris, Institut Montaigne, 2014, 89 p.
2) *Op. cit.* p. 12.

services peuvent estimer commode, plutôt, que de déférer au juge judiciaire les éléments de l'infraction constatée, de demander le renouvellement de l'intrusion. La loi doit permettre d'éviter ces contournements. Si elle étend la faculté d'user de nouvelles technologies, comme il est normal, cette extension doit en contrepartie mettre fin à toute pratique illégale.

3 - La loi à venir doit s'intéresser à des questions qui ne sont pas aujourd'hui résolues, en ce sens que le contrôle s'exerce mal ou pas du tout dans certains domaines. Tel est le cas pour des investigations dans les flux internationaux de données. Certes, il ne peut être aussi étendu que celui des interceptions. Il ne doit pas pour autant demeurer inexistant. On doit relever avec intérêt que le Conseil d'État, dans sa dernière étude annuelle consacrée au thème de la protection des droits fondamentaux dans le domaine du numérique [1], a émis le vœu que soit défini par la loi « le régime des interceptions des communications à l'étranger ». De manière générale, la loi doit se préoccuper de « combler les vides » et, pour ce faire, conserver un caractère suffisamment général pour anticiper suffisamment le développement technologique.

4 - S'agissant du contrôle de l'utilisation des moyens d'intrusion, sa définition, sa composition et son exercice doivent traduire l'indépendance dont il a déjà été question. Les lois récentes relatives à des autorités administratives indépendantes comportent des garanties plus précises que celles qui figurent dans la loi du 10 juillet 1991 (intégrée au Code de la sécurité intérieure [2]) : elles devraient être reprises. Pour ces raisons, et aussi pour des motifs d'efficacité, on doit aussi s'efforcer d'unifier et de simplifier le contrôle. À cet égard, le rôle de la personnalité qualifiée, imaginée par la loi du 28 janvier 2006, repris et amplifié par l'article 20 de la loi de programmation militaire du 18 décembre 2013, mériterait d'être intégré dans l'activité de la Commission – alors même que la personne qui a exercé ces fonctions n'a nullement démérité.

5 - Pour jouer enfin sa pleine portée, le contrôle doit pouvoir s'exercer à la fois *a priori* et *a posteriori*, c'est-à-dire pouvoir vérifier, dans des conditions de délai et de lecture efficaces, à la fois l'adéquation d'une demande aux motifs définis par le législateur (ce pourquoi celui-ci doit être suffisamment précis) et la manière dont l'exécution de l'autorisation donnée à la demande est cohérente avec les raisons invoquées. On voit bien que si l'un de ces deux éléments vient à manquer, il n'y a plus de contrôle digne de ce nom.

---

1) Conseil d'État, *Le numérique et les droits fondamentaux*, Étude annuelle 2014, Paris, la Documentation française, 2014, 441 p. Voir en particulier la proposition n° 39, p. 320-321.
2) Articles L. 243-1 *et sq.*

C'est à ces conditions que la Commission pourra juger si la loi qui doit modifier la législation de 1991 aura su respecter l'équilibre protecteur alors atteint.

La Commission a perdu à peu de distance en 2014 son président, Hervé Pelletier, et son délégué général, Olivier Guérin, qui ont dû la quitter. Chacun d'eux, à sa manière, inventive et exigeante, a apporté à la Commission des éléments nouveaux et essentiels. À eux, qui permettent au nouveau président d'inscrire sans trop d'appréhension ses pas dans des empreintes solidement dessinées, je voudrais leur exprimer l'hommage que, sans restriction, je leur dois. Comme je dois aussi ma gratitude aux autres membres de la Commission, Jean-Jacques Hyest et Jean-Jacques Urvoas, parlementaires chevronnés tous les deux, et indéfectiblement attachés aux droits et libertés individuels. Le premier d'entre eux a bien voulu témoigner dans le présent rapport de cet attachement. Aux collaborateurs de la CNCIS enfin, Maud Morel-Coujard et Loïc Abrial tout d'abord, Marie-José Masset, Nathalie Brucker et Christophe Germin ensuite, qui démontrent quotidiennement l'intérêt d'une approche collective de la gestion des interceptions de sécurité. Cette équipe expérimentée devra s'enrichir à bref délai de compétences techniques, dont elle est privée encore aujourd'hui.

Enfin je veux exprimer la reconnaissance particulière que je dois aux contributeurs de ce rapport extérieurs à la commission : le professeur Sébastien-Yves Laurent, dont on connaît les compétences en matière de renseignement, a donné au lecteur des réflexions très utiles qu'on lira ci-après ; le service des affaires européennes et internationales (SAEI) du ministère de la Justice, que dirige Valéry Turcey, a recueilli auprès de magistrats de liaison, en fonction dans six pays distincts, une précieuse analyse de droit comparé sur les actes de renseignement et la loi, synthétisée par le bureau du droit comparé, qui n'engage évidemment pas la Chancellerie. Personne n'a ménagé sa peine : que tous en soient vivement remerciés.

Jean-Marie Delarue
Président de la Commission

Contribution de Jean-Jacques HYEST

Sénateur de Seine-et-Marne

Parmi les nombreuses autorités administratives indépendantes (AAI) que la législation a créées ces dernières décennies, la Commission nationale de contrôle des interceptions de sécurité présente quelques singularités qu'il est bon de souligner. Peu connue du grand public, et dont les missions ont fait parfois l'objet de contresens dans les médias et d'attaques de groupes de pression, elle n'en remplit pas moins avec constance et efficacité sa mission de protection de la vie privée, depuis sa création en 1991.

À cet égard, la discussion du projet de loi de programmation militaire (en son article 13) est une bonne illustration de ce qui a été parfois compris comme une restriction des libertés publiques, alors qu'il s'agissait de tenir compte des évolutions technologiques (telle la géolocalisation) afin d'en assurer un contrôle effectif, et plus seulement des communications téléphoniques, sans parler de l'exploitation des données techniques de communication, qui ont suscité des questions, et sur lesquelles la CNCIS a eu toujours une position très ferme, qu'elle a dû rappeler à diverses occasions.

Bien souvent, certains confondent les écoutes administratives et les écoutes judiciaires, et sur ce sujet, je ne puis mieux faire que de renvoyer le lecteur de ce rapport à l'analyse exhaustive qui en a été faite par Jean-Jacques Urvoas, Président de la Commission des Lois de l'Assemblée nationale et membre de la CNCIS (voir rapport 2012-2013 de la Commission p.9 *et sq*). Bien qu'obéissant à des principes stricts, la séparation entre les deux catégories d'écoutes demande une attention particulière, dans la mesure où certains services ont à la fois une mission de renseignement et de police judiciaire.

Dans cette période où la menace terroriste est particulièrement prégnante, on n'aurait cependant garde d'oublier que les interceptions de sécurité concernent aussi la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la Nation, la prévention de la criminalité et de la délinquance organisées et la prévention de la reconstitution ou du maintien de groupements dissous (article L 241-2 du Code de la sécurité intérieure).

L'analyse des statistiques des interceptions révèle que la prévention de la criminalité et de la délinquance organisées (parfois liée au terrorisme) constitue le principal motif des demandes (62 % des demandes en 2011).

La loi du 23 janvier 2006, dans le cadre de la lutte contre le terrorisme, avait institué un dispositif expérimental en son article 6, prévoyant la nomination d'une personnalité qualifiée (auprès du Ministre de l'Intérieur) en ce qui concerne les données techniques de communications, contrôlées par la Commission *a posteriori*, ce qui était peu satisfaisant, et la Commission avait demandé à plusieurs reprises que ce dispositif évolue.

C'est l'objet de l'article 20 de la loi du 18 décembre 2013 dont la mise en œuvre interviendra le 1er janvier 2015, et qui a conservé le principe de la nomination d'une personnalité qualifiée désormais placée auprès du Premier ministre, et désignée par la Commission nationale des interceptions de sécurité. Il eut été sans doute possible de concevoir un système plus simple, donnant à la Commission un rôle identique à celui qu'elle joue pour les interceptions de sécurité ; cela aurait supposé un renforcement de moyens humains et matériels, mais, on peut être néanmoins assuré du contrôle pertinent de la Commission sur les demandes des services.

Après avoir siégé pendant plus de quatre ans à la CNCIS, je puis tirer un bilan très positif du fonctionnement de la Commission, de l'engagement de ses présidents et membres successifs et spécialement de la qualité du délégué général et de son adjoint qui en assurent la permanence quotidienne.

Conçue en 1991 pour « contrôler » les interceptions de sécurité, elle a progressivement acquis le pouvoir de donner son avis « *a priori* », pratique qui a été confirmé par le Premier ministre en 2008.

La Commission a toujours été extrêmement attentive aux nécessités opérationnelles des services et un dialogue constant et constructif avec eux a permis d'assurer une coopération efficace. Le nombre très faible de refus, comme celui des demandes d'interruption des interceptions ; avis qui ont, à une ou deux exceptions près, toujours été suivis par le Premier ministre, sont là pour témoigner du sérieux de son approche.

Parmi les AAI, c'est une des seules qui comprend majoritairement des parlementaires, représentant l'un la majorité, l'autre l'opposition, et présidée par un haut magistrat de l'ordre judiciaire ou administratif. Certains envisagent de faire évoluer sa composition vers une structure plus lourde et couvrant un champ non envisagé par la législation actuelle, mais le modèle original de la CNCIS me paraît néanmoins toujours pertinent.

Au nom de l'efficacité face au développement de la menace terroriste, qui est hélas une réalité, rien ne serait pire que de ne pas respecter l'état de droit et les libertés publiques.

Il faut aussi affirmer la nécessité de la prévention de tous les crimes et délits qui détruisent notre société, et soutenir l'action des services qui en sont chargés, mais aussi veiller à la légalité de leur action. C'est l'équilibre nécessaire d'une véritable démocratie ; et de ce point de vue l'institution et le travail de la CNCIS y ont toujours contribué. Ce n'est pas toujours le cas d'autres grandes démocraties.

Liberté et sécurité dans un monde anomique de données

Sébastien-Yves LAURENT,
Professeur des universités à la Faculté de droit et de science politique de l'université de Bordeaux, enseignant à Sciences-Po

Les rapports annuels successifs de la CNCIS – qui me fait le grand honneur de me donner la plume – attestent en continu et ce depuis plus de vingt ans, que le rapport entre libertés fondamentales et sécurité est un des enjeux les plus délicats à faire respecter dans l'État de droit. L'« ordre public » est un point de jonction classique entre ces deux paradigmes depuis le XIX^e^ siècle. Bien plus récentes, les « données » nées avec l'informatisation de la société dans les années 1970, se trouvent à la croisée de deux libertés, la liberté de correspondre et la protection de la vie privée, qui entrent quotidiennement en conflit avec l'impératif de sécurité dont l'État est le garant et l'ordonnateur. Depuis la loi de 1991, votée par le Parlement français pour éviter de nouvelles condamnations de son système d'écoutes gouvernementales par la CEDH, c'est la CNCIS qui a la charge de trouver le positionnement dans ce qui est souvent désigné comme étant un « équilibre » entre, d'une part, les motifs inscrits dans la loi et pour lesquels des « interceptions de sécurité » mais aussi des « données techniques » peuvent être demandées à la Commission et, d'autre part, la liberté de correspondre, socle fondamental tant de notre droit des libertés que du droit public. On relèvera que le terme d'« équilibre » entre sécurité et liberté, est employé couramment par abus de langage : il postule d'emblée une position où les deux « plateaux de la balance » seraient à la même hauteur. Or, la situation la plus courante est celle d'un non-équilibre… tendant vers un équilibre qu'il est impossible de définir, de jauger ou de mesurer, tout comme l'est le non-équilibre.... Il s'agit donc en fait d'une tension dialectique qui est au cœur de l'État de droit sur un plan juridique et de la démocratie libérale sur un plan politique. Quoi qu'il en soit, on constate que désormais ce sont les interceptions et les captations de données qui sont aujourd'hui – dans le monde entier – un point de cristallisation quotidien de la tension sécurité-libertés.

La CNCIS : des interceptions de correspondance aux méta-données

« Arbitre », « vigie »[1] ... bien des termes peuvent caractériser la Commission qui a la charge de se prononcer – *a priori* – sur les demandes d'écoutes administratives. De 1180 lignes écoutées en permanence en 1991, la CNCIS est passée à 1540 en 1997, 1670 en 2003, puis en 2008 à 1840 « cibles »[2], enfin à 2 190 en 2014 : d'évidence le nombre est modeste et les rapports détaillés de la CNCIS montrent chaque année que la lutte anti-terroriste en pré-judiciaire mobilise une grande partie de ces quotas. Dès sa fondation, la CNCIS avait eu à connaître des « données » car l'article 22 de la loi de 1991 l'autorisait à exercer un contrôle – *a posteriori* – sur les demandes de données techniques faites dans le cadre d'une demande d'interception de sécurité. Le périmètre de la CNCIS s'est élargi depuis : ainsi à compter de 2006, par l'article 6 de la loi n° 2006-64, elle a la charge de se prononcer (toujours *a posteriori*) – dans le cadre de la lutte antiterroriste – sur les demandes de données techniques de connexion ou de communication faites hors du contexte d'une demande d'interception. Ceci peut concerner les numéros de téléphone, les numéros d'abonnement à des services de communications électroniques, la (géo-) localisation des terminaux, enfin les « fadettes ». Le rôle de la CNCIS aurait pu être renforcé de façon considérable à la fin de l'année 2014 si la loi de programmation militaire[3] (LPM) lui avait attribué le contrôle des données techniques de connexion dans le cadre, élargi, de la loi de 1991. Mais l'article 20 de la LPM a confié cette charge à une « personnalité qualifiée » nommée par le Premier ministre (sur proposition de la CNCIS) pour procéder au contrôle des demandes de données techniques de connexion[4] par les autorités exécutives. Parce qu'elles s'appuient sur les principes de légalité (conformité de la demande aux motifs inscrits dans la loi), de proportionnalité (rapport entre le risque encouru supposé et l'atteinte à la vie privée) et de subsidiarité (possibilité éventuelle d'emploi alternatif d'autres moyens), les décisions de la CNCIS démontrent clairement qu'elle œuvre au quotidien en faveur de « l'équilibre », le Conseil d'État ayant déclaré en septembre 2014 qu'il souhaitait d'ailleurs une extension très ample de sa capacité de contrôle[5]. Demain la « personnalité qualifiée » créée par la LPM de 2013

1) Sébastien-Yves Laurent, *Pour une véritable politique publique du renseignement*, Paris, Institut Montaigne, 2014, p. 54.
2) Ce qui a représenté une croissance notable, car un même individu peut avoir plusieurs lignes.
3) Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019.
4) Les données techniques de communication ou de connexion sont en fait ce que l'on appelle aussi des « méta-données », ainsi qu'on le verra plus loin.
5) Conseil d'État, *Le numérique et les droits fondamentaux*, Paris, Documentation française, « Les rapports du Conseil d'État », 2014, p. 30.

aura un rôle tout aussi important que la CNCIS en matière de traitement de la tension sécurité-libertés, mais uniquement en matière de données.

Doutes sur les données

Data / données, ces termes sont partout. Leur ubiquité est totale. Mais ils ne sont jamais définis, nourrissant souvent des contresens. De quoi en effet parle-t-on ? Il est indispensable d'associer l'approche technologique et l'approche juridique. À défaut de sens stabilisé, nous proposons ici une approche toute personnelle : il faut revenir à sa matérialité pour comprendre cette curieuse réalité. La donnée est une information, soit une réalité à l'origine immatérielle, qui est médiatisée et transformée par un traitement informatique/numérique. Ce peut être aussi à l'origine un signal (image, son), porteur d'information et qui est numérisé. Celui-ci le rend matériel en l'inscrivant sur des supports physiques, aujourd'hui de plus en plus variés, aussi bien sédentaires que nomades. Non seulement le support de la donnée est mobile, mais la donnée elle-même est beaucoup plus un flux qu'un stock. La donnée brute (sous sa forme numérique), est donc la transformation de l'information, porteuse de sens, en un langage spécifique (usant de symboles) permettant des calculs, des mises en relation, des instructions. Par ailleurs pour le sens commun, malentendu supplémentaire, la donnée n'est pas la donnée brute de l'informaticien dont nous venons de parler mais la donnée immédiatement signifiante pour l'entendement humain.

On peut distinguer deux grands ensembles de données : les données qui ont un contenu informationnel et les méta-données qui sont en fait des données sur les données, c'est-à-dire pour lesquelles les informations prennent le sens d'informations métriques et statistiques sur des informations. Il s'agit par exemple des données de communication (données sur les communications téléphoniques et sur les échanges utilisant l'Internet), dont nous avons parlé *supra*. Si l'on tente de les définir par leur objet, il existe deux grandes catégories de données, les données personnelles, c'est-à-dire contenant des informations sur un individu et des données relatives aux personnes morales, notamment les entreprises.

En ce qui concerne la première catégorie, la plus médiatisée, celle touchant aux individus, le droit français très innovant qu'était la loi du 6 janvier 1978 (dite « informatique et libertés ») à l'époque de sa réalisation, a consacré les données dans son sens contemporain (articles 5 et 25) et clairement consacré la notion de « données nominatives » (article 31). Celles-ci sont devenues avec la loi du 6 août 2004 les « données à caractère personnel ». Avec cette loi, il s'agissait alors de se conformer au droit européen, en l'occurrence à la directive de l'Union européenne (UE)

de 1995, elle-même fortement inspirée de la convention 108 de 1981[1] qui avait créé l'appellation de « données à caractère personnel ». Malgré ce droit français qui fut à l'origine adapté à la technologie de son temps, le droit paraît aujourd'hui dépassé. En effet, les données de 1978 ne sont pas celles de 2004 qui ne sont pas celles d'aujourd'hui. En outre les données demeurent un angle mort de la réflexion juridique, de la part du législateur autant que de la doctrine. Si la notion de données doit être éclaircie et approfondie, il doit en aller de même des usages non judiciaires de la part des autorités. Ainsi, il demeure des doutes et des imprécisions juridiques fortes sur la captation de données dans un cadre non judiciaire.

On relèvera enfin que la focalisation sur les données personnelles a presque fait des données propres aux personnes morales une catégorie de second ordre. Les accords « Swift » et « Safe Harbour » inconséquemment signés par l'UE avec les États-Unis étaient déjà extrêmement dangereux. Depuis, l'effet Snowden[2] (été 2013) a révélé l'ampleur de l'espionnage économique qui est d'abord un espionnage des données.

Des garanties fondamentales et répétées depuis plus de cinquante ans : l'isolat européen dans le monde (des données)

On connaît bien aujourd'hui les notions fondamentales énoncées très clairement par la Cour de Strasbourg en s'appuyant sur la Convention de sauvegarde des droits de l'homme et dégagées par sa jurisprudence : l'ingérence d'une autorité publique dans la vie privée et dans les correspondances doit se conformer aux principes de légalité et de proportionnalité. Les États signataires se sont lentement adaptés à cet esprit en matière de communication, à commencer par la France qui ne le fit qu'avec la loi de 1991, acte de naissance de la CNCIS. Aux textes internationaux et européens fondateurs sur le secret des correspondances (Déclaration universelle des droits de l'Homme de 1948, Convention précitée de 1950, Pacte international des droits civils et politiques de 1966… etc. jusqu'aux directives de l'UE de 1997 et 2002), se sont ajoutés des textes spécifiques sur les « données », de la convention 108 du Conseil de l'Europe en 1981 à la directive UE de 1995 actuellement en cours de refonte en vue d'élaborer un règlement voté en 2013 et applicable en 2016[3]. L'ensemble de l'édifice, parfois assez composite, a été conforté par l'inscription dans la Charte des droits fondamentaux de l'UE en 2009.

---

1) Celle-ci s'inspirait très largement de la loi française de 1978…
2) *Cf.* Philippe Hayez, « L'effet Snowden. Les politiques du renseignement dans les démocraties », *Le Débat*, n° 181, septembre-octobre 2014, p. 94-102.
3) Un projet a été présenté par la Commission le 25 janvier 2012.

Il faut à ce stade rappeler une évidence : nulle part au monde les données ne sont mieux protégées qu'en Europe. Encore faut-il relever que 46 pays (dont les 28 membres de l'UE) avaient (en 2014) ratifié la convention 108 dont la Russie. C'est un pas important même si la convention ne concerne que le domaine de la cybercriminalité et si les États-Unis ne sont pas soumis à la juridiction de la Cour de Strasbourg…. Il ne faut pas pour autant se laisser emporter par une vue irénique sur la situation européenne : ceci est certes dû à la tradition politique et juridique libérale, mais aussi au fait que c'est une réaction à l'intensité de la surveillance et de la captation de données sur le continent. Il faut rappeler une seconde évidence : ce sont les institutions européennes qui jouent le rôle de vigie et contraignent bien souvent les autorités nationales à respecter des règles d'inspiration libérale. La Cour de Strasbourg, le Conseil de l'Europe, la commission « Libe » du Parlement européen [1], le commissaire européen à la « Justice, aux droits fondamentaux et à la citoyenneté » [2], l'Agence des droits fondamentaux (créée en 2007), enfin le groupe de travail a portée consultative « G29 » rassemblant les autorités de contrôle de chacun des États-membres, exercent un contrôle vigilant à cet égard qui trouve toujours une solide résonance médiatique. Dans le monde réel et dans le monde des données, l'UE est en situation d'exception par son droit très protecteur des données et la multiplicité d'organes juridictionnels et consultatifs qui assurent le contrôle de l'application : ceci ne signifie pas pour autant que les États-Membres assurent un respect strict des textes fondamentaux et des décisions juridictionnelles.

L'intensité des captations de données

Le monde numérique croît, inégalement géographiquement et sociologiquement, mais il croît. Sur plus d'une décennie (2000 à 2014), il a augmenté de plus 670 %. Près de 3 milliards d'individus (et leurs données) seraient aujourd'hui connectés. Peu d'entreprises ne le sont pas. Les marges de progression pour les individus sont importantes : en Asie le taux de pénétration n'est que de plus de 30 %, en Afrique de plus de 20 % et d'à peine 45 % au Moyen-Orient. Cette croissance globale de l'Internet repose sur un océan de données qui s'étend à chaque seconde de connexion.

L'effet Snowden a complètement occulté le travail d'enquête mené par le Parlement européen douze ans plus tôt. Le rapport du député

1) Désignée sous le nom de « commission des libertés civiles, des affaires intérieures et de la justice ».
2) Dans la nouvelle commission (2014-2019), le partage semble être différent avec une commissaire à la « Justice, aux consommateurs et à l'égalité des genres » et un commissaire (par ailleurs vice-président de la commission à la « Meilleure règlementation, aux relations interinstitutionnelles, à l'État de droit et à la Charte des droits fondamentaux »).

Gerhard Schmid[1] avait conclu à l'existence d'un réseau planétaire d'interceptions satellitaires et filaires organisé par les États-Unis en ciblant le continent avec l'aide active d'un État membre de l'Union européenne. À l'époque, le rapport s'alarmait plus des usages de ces interceptions à finalité d'espionnage économique que des enjeux pour les libertés fondamentales. Ce rapport rendu en juillet 2001 avait débouché sur une motion votée par le Parlement le…6 septembre 2001. Néanmoins, il fut le premier rapport public à établir l'existence d'un réseau mondial d'interceptions associant 5 pays, réseau qui était pourtant bien connu des spécialistes[2]. Douze ans après le rapport Schmid, les documents Snowden ont montré la persistance du réseau constitué lors de la Guerre froide, désormais orienté vers la captation de données.

Aujourd'hui comme hier c'est la situation stratégique qui explique, voire justifie ce dispositif d'interception : c'était hier la nécessité de surveiller les capacités nucléaires soviétiques qui était à l'origine du dispositif aérien et satellitaire à vocation électro-magnétique des États-Unis et de l'OTAN. C'est aujourd'hui le terrorisme qui est l'argument principal pour mettre en place un dispositif mondial d'interception des données numériques. Les pratiques de surveillance ont fortement évolué : ponctuelles et ciblées (« targeted surveillance »), elles semblent désormais de plus en plus permanentes et générales (« dragnet surveillance »[3]). L'un des grands dommages collatéraux de la lutte antiterroriste post-2001 est d'avoir brouillé la notion de suspect, cardinale jusque-là dans la totalité des dispositifs pénaux. Les stratégies de contre-surveillance[4] mises en place par les terroristes dans le monde réel et dans le monde cybernétique sont en partie efficaces et amènent les services anti-terroristes à élargir leur surveillance. Ceci a été en quelque sorte théorisé autour de l'idée que le « signal faible » (d'une activité criminelle ou terroriste) peut être débusqué en mettant en place une « surveillance de masse » – pour reprendre les termes employés, dès 1973 (!), par James B. Rule[5] – dans un tout autre contexte, qui s'exerce d'abord et avant tout dans le monde des données. L'idée est que les algorithmes permettent de détecter le « signal faible » dans le « bruit » des données interceptées. Qui plus est l'espionnage économique amène à procéder par la même technique du chalutage pour brasser les données utiles à l'espionnage économique.

---

1) *Cf.* Gerhard Schmid, *Rapport sur l'existence d'un système d'interception mondial des communications privées et économiques, système d'interception ECHELON (2001/2098 (INI),* Rapport A5-0264/2001, Parlement européen, 11 juillet 2001, 210 p.
2) *Cf.* Jeffrey T. Richelson and Desmond Ball*, The Ties That Bind : Intelligence Cooperation Between the UK/USA Countries*, Boston, Unwin Hyman, 1990, 426 p.
3) Jacob Appelbaum, Intervention au Conseil de l'Europe, 28 janvier 2014.
4) Sur cette notion, *cf.* Maurice Cusson, « La surveillance et la contre-surveillance », dans : Maurice Cusson, Frédéric Lemieux et Benoît Dupont, *Traité de sécurité intérieure*, Lausanne, Presses polytechniques et universitaires romandes, 2008, p. 429-436.
5) *Cf.* James B. Rule, *Private Lives and Public Surveillance*, New York, Schocken Books, 1974 [1re éd.: 1973], 382 p.

Un « équilibre » illusoire ?

La poussée sécuritaire post-2001 très dénoncée[1] dans les pays occidentaux est patente. Elle a généré des théories sur l'état d'exception[2] alimentant une critique radicale de l'État de droit et des régimes démocratiques : ce n'est pas là le moindre de ses dangers. Le droit européen et au-delà le droit de *common law* mettent en avant le principe de proportionnalité : dans un État de droit la violence et la coercition doivent être exercées avec mesure, dans un esprit de « proportionnalité ». Il reste que si la notion a envahi le vocabulaire publiciste, elle demeure bien faible en pratique dans le droit français par rapport à d'autres pays. Ce principe est aujourd'hui d'un point de vue normatif, cardinal en dehors de nos frontières mais il est sans aucune portée en matière d'interceptions de masse qui ne sont pas régulées.

Outre le fait que le droit international ne prohibe pas l'espionnage[3], il ne connaît pas les données en dehors de la convention 108 ; de portée géographiquement limitée. Dans cette situation que faire ? La question de la régulation ne se pose pas car il n'existe ni juridiction, ni autorité, ni même volonté. Les interceptions de données ne font d'ailleurs l'objet de communiqués et (vraisemblablement) d'échanges sur ces pratiques concurrentes entre les puissances que depuis que les États-Unis ont été contraints de réagir aux indignations après 2013. À défaut, peut-on espérer une forme d'auto-régulation de la part des « five eyes » et principalement des États-Unis, les seuls à ce jour clairement identifiés ? La commission *ad hoc* nommée par le président Obama a remis en décembre 2013 un rapport subordonnant les interceptions de données à des impératifs de sécurité nationale[4] et indiquant clairement que les pratiques : « must not be directed at illicit or illegitimate ends, such as the theft of trade secrets or obtaining commercial gain for domestic industries »[5]. Cette (mauvaise) plaisanterie n'était qu'un élément de langage destiné aux chancelleries occidentales « alliées » et « partenaires ».

Les données ignorent la géographie[6]. En mouvement permanent ou stockées (provisoirement) dans des pays garantissant une moindre protection juridique, elles cherchent en permanence à échapper à

---

1) Pour ne s'en tenir qu'à des auteurs français, *cf.* Eric Sadin, *Surveillance globale. Enquête sur les nouvelles formes de contrôle*, Paris, Climats, 2009, 234 p. et Michaël Foessel, *État de vigilance. Critique de la banalité sécuritaire*, Paris, éditions les bords de l'eau, 2010, 155 p.
2) Giorgio Amgaben, *État d'exception. Homo sacer II/1*, Paris, Seuil, « L'ordre philosophique », 2003, 151 p.
3) Fabien Lafouasse, *L'espionnage dans le droit international*, Paris, Nouveau monde éditions, « Le Grand jeu », 2012, 491 p.
4) The President's Review group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World*, 12 December 2013, 304 p.
5) *Ibid.*, p. 19.
6) On lira avec profit l'excellent : "Cyberespace : enjeux géopolitiques", *Hérodote*, 1er-2e trimestre 2014, nº 152-153, 312 p.

quelque contrainte que ce soit. Le droit international ignore le monde des données. Les droits internes sont très différents sur les données mais leur profitent, plus qu'aux citoyens et aux entreprises. Il reste que leur mouvement n'est brownien qu'en apparence : elles sont entre les mains de ceux qui les stockent, les font circuler, parce qu'ils les vendent. Les acteurs économiques du numérique, fournisseurs d'accès, hébergeurs, producteurs de contenus sont les auteurs de cette mobilité planétaire. La commercialisation de grande ampleur des données par temps de globalisation et la dé-territorialisation de la surveillance annihilent la dialectique sécurité-libertés. On peut donc parler d'une situation d'anomie entretenue aussi bien par les grands États acteurs de la surveillance que voulue par les sociétés numériques multinationales. Il est assez peu probable que les structures de gouvernance de l'Internet – IGF et Icann notamment – puissent faire en l'état évoluer la situation des données. Il reste que le fonctionnement de ce « système » repose sur la confiance : si les citoyens d'une part, les usagers de l'autre (qui sont les mêmes, mais peuvent réagir pour des raisons différentes) la remettent en cause, alors, mais seulement alors, la situation anomique pourrait être remise en cause.

Le cadre légal du renseignement en droit comparé

(Allemagne, États-Unis, Italie, Pays-Bas, Roumanie, Royaume-Uni)

Étude réalisée par le bureau de droit comparé du Service des affaires européennes et internationales du ministère de la Justice – Octobre 2014

La présente étude a été sollicitée auprès de services du ministère de la Justice par la Commission nationale de contrôle des interceptions de sécurité. Elle a été réalisée grâce au concours des magistrats de liaison en fonction dans les pays concernés. Sa rédaction est l'œuvre du bureau du droit comparé du service des affaires européennes et internationales. Elle est entièrement descriptive. Ni ses termes, ni son contenu n'engagent évidemment la Chancellerie et ne reflètent des choix politiques qui reviennent à la garde des Sceaux.

Étudier le cadre légal du renseignement pose tout d'abord la question du périmètre de l'activité de renseignement. La notion de protection de la sécurité nationale qui dans tous les pays étudiés fonde la raison d'être de l'activité de renseignement, reste une notion fluctuante et non définie juridiquement qui rend complexe la définition d'un cadre légal.

Si l'activité de renseignement reste largement exercée en dehors des règles du droit commun, il est toutefois possible d'identifier l'émergence dans l'ensemble des pays étudiés d'un « droit du renseignement » encadrant les activités des agences du renseignement et instaurant un contrôle de légalité sur leurs actions.

Le cadre légal des services

Les services de renseignement et leurs missions

À l'exception des États-Unis, qui dénombrent un grand nombre d'agences de renseignement, parmi lesquelles la CIA, le FBI et la NSA, les autres pays disposent d'un nombre beaucoup plus réduit d'agences.

Aux États-Unis, il existe 16 agences fédérales de renseignement et une structure de coordination des agences de renseignement. La

coordination entre les agences est effectuée par le *Directeur of National Intelligence,* ou *DNI.*

Dans les autres pays (Allemagne, Italie, Pays-Bas, Roumanie, Royaume-Uni), le nombre d'agences de renseignement est beaucoup plus réduit. En Allemagne, il existe trois grandes agences fédérales : l'Office fédéral pour la protection de la Constitution, le Service de protection militaire et le Service fédéral de renseignement. Il faut toutefois tenir compte de l'existence de services de renseignements régionaux, en raison de la structure fédérale du système juridique institutionnel allemand. En Italie, s'il existe deux grandes agences de renseignement (AISE et AISI), les activités du renseignement sont concentrées autour du « système d'information pour la sécurité de la république » qui regroupe le Comité interministériel pour la sécurité de la République (CISR), la Direction du renseignement pour la sécurité (DIS), l'Agence de renseignements et de la sécurité externe (AISE), l'Agence de renseignements interne (AISI), et une Autorité déléguée. Aux Pays-Bas, il existe deux grands services de renseignement : le Service général de renseignement et de sécurité (GISS) et le Service de renseignement de défense et de sécurité (DISS). En Italie et aux Pays-Bas, à l'instar du système américain, une coordination de l'activité des services est assurée par un coordonnateur. Au Royaume-Uni il n'existe que trois services : le *Secret Intelligence Service* (SIS), également connu sous le nom de MI6, le *Government Communications Headquarters* (GCHQ) et le *British Security Service* (BSS). Le premier service exerce ses missions en dehors du Royaume-Uni.

Selon les pays, les missions confiées aux agences de renseignement peuvent être assez larges ou bien encadrées.

Ce sont les pays de Common Law et l'Italie qui confèrent aux agences de renseignement les missions les plus étendues. Aux États-Unis, le grand nombre d'agences spécialisées dans le renseignement a pour conséquence des missions extrêmement diversifiées, tant sur le territoire national qu'à l'étranger, et portant sur un grand nombre de matières. La CIA fournit des informations sur les gouvernements, les entreprises et les groupes d'individus dans tous les pays du monde pour le compte du gouvernement américain et conduit des opérations non revendiquées (*covert*) à l'étranger ; la NSA protège les informations et systèmes d'information du gouvernement américain ; le FBI a compétence pour répondre au terrorisme, à la criminalité organisée, au contre-espionnage et à la menace cyber ; le NGA fournit du renseignement géo spatial ; la DIA recueille du renseignement militaire étranger, y compris dans des domaines comme l'information politique, économique, industrielle, géographique, économique, et médicale liée à la défense nationale. Au Royaume-Uni, les missions confiées aux agences de renseignement vont bien au-delà de la sécurité nationale et s'étendent même au « bien-être économique » du pays. En Italie, le domaine des missions conférées aux agences de renseignement semble assez étendu, puisqu'il concerne la protection de la République contre les menaces internes ou

étrangères, et porte également sur la protection des « intérêts politiques, militaires, économiques, scientifiques et industriels de l'Italie ».

Dans d'autres pays (Allemagne, Pays-Bas, Roumanie), les missions confiées aux agences de renseignement sont plus traditionnelles et davantage centrées sur la seule sécurité nationale, – entendue toutefois dans un sens large. En Roumanie, les missions confiées concernent très classiquement l'information sur des menaces à la sécurité nationale. Aux Pays-Bas, il s'agit de missions de recueil d'information « sur les situations de danger pour l'existence du régime démocratique ou d'autres intérêts vitaux de la nation » et sur « la sécurité des forces armées ». En Allemagne, les missions d'information concernent la protection de la Constitution (sécurité intérieure) et de l'armée contre des actions perturbatrices relatives à son domaine de compétence, ainsi que le recueil d'informations à l'étranger.

Royaume-Uni

Au Royaume-Uni, les trois services constitutifs de la communauté britannique du renseignement sont :
– Le *Secret Intelligence Service* (SIS), également connu sous le nom de MI6 qui est en charge du renseignement humain hors du Royaume-Uni ;
– Le *Government Communications Headquarters* (GCHQ) qui est en charge du renseignement technique et de la protection des systèmes informatiques nationaux. Il regroupe ainsi des compétences qui en France, sont séparées entre les missions offensives (DGSE) et défensives (ANSSI).
– Le *British Security Service* (BSS), également connu sous le nom de MI5 ; le BSS est le service de sécurité intérieure. Il n'a pas de pouvoirs judiciaires.

Le ministre de tutelle du MI6 et du GCHQ est le Secrétaire d'État aux Affaires Étrangères. Le ministre de tutelle du MI5 est le Home Secretary.

l'ISA (*L'Intelligence Services Act)* de 1994 – qui définit les missions des services extérieurs et techniques – autorise les trois services à recueillir des renseignements :
– dans l'intérêt de la sécurité nationale,
– permettant la prévention d'actes criminels graves,
– pour sauvegarder le bien-être économique du Royaume-Uni.

Les moyens matériels et humains de la communauté britannique du renseignement ont été globalement épargnés par les coupes budgétaires :

Le budget annuel de la communauté britannique du renseignement (SIS, GCHQ, BSS) est d'environ 2 milliards de livres en ressources (soit environ 2,4 milliards d'euros) et 300 millions en capital (soit environ 360 millions d'euros). Les arbitrages entre les trois services sont rendus par le *National Security Adviser*, en concertation avec les chefs des trois

services. Le budget global est rendu public dans le cadre du *Single Intelligence Account* (SIA).

Allemagne

Le renseignement constitue une activité dans le cadre de laquelle la Fédération et les Länder coopèrent, les modalités de cette coopération étant, d'après la Constitution allemande, déterminées par une loi fédérale. Il existe donc des services de renseignement fédéraux et régionaux. Il existe au plan fédéral, trois services de renseignement :
– L'Office fédéral pour la protection de la Constitution (*Bundesamt für Verfassungsschutz ou BfV*), service civil de sécurité intérieure, dépendant du ministère fédéral de l'Intérieur, chargé de lutter contre les tentatives de déstabilisation émanant de groupes terroristes et extrémistes et d'organiser le contre-espionnage ;
– Le Service de protection militaire (*Militärischer Abschirmdienst* ou MAD), dépendant du ministère fédéral de la Défense, équivalent militaire de l'Office fédéral pour la protection de la Constitution dont l´activité concerne les personnels militaires et qui a pour mission de protéger l'armée contre des actions perturbatrices relatives à son domaine de compétence ;
– Le Service fédéral de renseignement (*Bundesnachrichtendienst* ou BND), placé sous l'autorité de la Chancellerie fédérale, chargé de rassembler et exploiter les informations sur l'étranger. En 1955, l'organisation *Gehlen* dite l'Org, héritée des structures de la guerre, devient officiellement un organe fédéral et reçoit en 1956 la désignation de *Bundesnachrichtendienst.* Dans les années 1970, le BND est progressivement démilitarisé et devient civil.

Au plan régional, chaque Land a édicté sa propre loi sur la protection de la Constitution et institué un service de renseignement ad hoc, le *Landesamt für Verfassungsschutz* ou LfV. Indépendants de l'Office fédéral pour la protection de la Constitution, les services de renseignement des Länder sont subordonnés aux ministères régionaux de l'Intérieur.

Pays-Bas

Aux Pays-Bas, aux termes de l'article 1 de la loi du 7 février 2002, les services de renseignement et de sécurité comprennent :
– Le service général de renseignement et de sécurité (GISS) ;
– Le service de renseignement de défense et de sécurité (DISS) ;
– Un coordonnateur.

Dans l'intérêt de la sécurité nationale, le Service Général de renseignement et de sécurité (GISS) qui dépend du ministère de l'Intérieur et des relations extérieures, a notamment pour mission de conduire des enquêtes relatives à des organisations et des personnes qui, en raison des objectifs poursuivis, ou à travers leurs activités, suscitent de sérieuses suspicions de danger pour l'existence du régime démocratique ou d'autres intérêts vitaux de la nation.

Dans l'intérêt de la sécurité nationale, le Service de renseignement de défense et de sécurité (DISS) qui dépend du ministre de la Défense, a notamment pour mission de conduire des enquêtes afin de prendre des mesures pour prévenir des activités susceptibles de causer un dommage à la sécurité ou à la réactivité des forces armées.

Un coordonnateur des services de renseignement et de sécurité, nommé par décret royal, est responsable conformément aux instructions du Premier ministre, du ministre des affaires générales et des autres ministres compétents, de la coordination des missions confiées au GISS et au DISS.

Italie

Le « Système d'information pour la sécurité de la République » regroupe les organes et autorités qui ont la mission d'assurer les activités de Renseignement pour la protection de la République contre les dangers et les menaces internes ou étrangères. Le Système est composé du Président du Conseil des ministres – qui coordonne les politiques en la matière -, d'une Autorité déléguée, du Comité interministériel pour la sécurité de la République (CISR), de la Direction du renseignement pour la sécurité (DIS), de l'Agence de renseignements et de la sécurité externe (AISE) et l'Agence de renseignements interne (AISI).

C'est le Président du Conseil des ministres qui est en charge de la direction et de la responsabilité générale de la politique du renseignement pour la sécurité de la République et de ses institutions. Il est également exclusivement compétent pour la délivrance, la protection et l'opposition du « secret d'État », la nomination et la révocation des directeurs du DIS, des AISE et AISI et la détermination du montant annuel des ressources financières de ces organismes. Il peut par ailleurs demander à l'autorité judiciaire directement ou par l'intermédiaire du DIS copie des pièces pénales et renseignements écrits considérés comme indispensables pour la poursuite des activités de *l'Intelligence* italienne. L'autorité judiciaire peut également transmettre spontanément des informations ou autoriser des agents du DIS à consulter le registre des infractions pénales (Art. 14 loi n°124/2007– Art. 118 bis du CPP).

Le Comité interministériel pour la sécurité de la République (CISR), est un organe consultatif, de proposition et de délibération sur les objectifs généraux de la politique du renseignement. Il est en charge plus particulièrement de la répartition des ressources financières du DIS, des AISE et AISI et de la définition des besoins d'informations des ministres dans leurs activités gouvernementales.

La Direction du renseignement pour la sécurité (DIS) élabore des analyses stratégiques ou relatives à des situations particulières et à des projets d'opérations à soumettre au CISR. Il favorise et assure l'échange des renseignements entre les Agences et les forces de police. Le Bureau

central de l'inspection du DIS est par ailleurs en charge de la surveillance des Agences et du contrôle de la conformité de leurs activités au regard des lois.

Les compétences des deux Agences – l'Agence de renseignement pour la sécurité extérieure (AISE) et l'Agence de renseignement pour la sécurité interne (AISI) – sont réparties selon l'ampleur territoriale de la menace. Elles sont sous l'autorité du Président du Conseil et sont les unités opérationnelles en charge de la protection des intérêts politiques, militaires, économiques, scientifiques et industriels de l'Italie. Elles peuvent être conduites à mener ensemble des actions communes sur le territoire ou à l'extérieur[1].

États-Unis

Aux États-Unis, le renseignement est une activité qui a pris une dimension considérable depuis les attentats du 11 septembre 2001 : près de 200000 personnes travaillent aujourd'hui pour la communauté du renseignement, en incluant les sous-traitants et les militaires, au sein de 16 agences[2] fédérales distinctes et d'une structure de coordination.
On examinera les agences les plus importantes, ainsi que leur structure de coordination.

La CIA : *Central Intelligence Agency* (dont les fonctions se rapprochent au sein de la DGSE de celles des Directions du renseignement et des opérations)

---

1) – L'agence du renseignement et de la sécurité externe (AISE) recherche et élabore les renseignements utiles à la défense de l'indépendance, de l'intégrité et de la sécurité de la République italienne contre des menaces provenant de l'étranger. Elle est en charge de la contre prolifération et du renseignement en dehors du territoire national.
– L'agence du renseignement et de la sécurité interne (AISI) recherche et élabore les renseignements utiles à la protection de la République italienne et des institutions démocratiques prévues par la Constitution sur toute menace, activité subversive et toute forme d'agression criminelle ou terroriste sur le territoire. Elle lutte à l'intérieur du territoire national contre les activités d'espionnage direct ou de nature à porter atteinte aux intérêts nationaux.
2) Les différents services spéciaux en charge du renseignement ont progressivement fait l'objet d'un encadrement juridique à la fois législatif et réglementaire, parfois du fait de certains scandales
La communauté de renseignement des États-Unis est composée de 16 agences :
Service indépendant : *Central Intelligence Agency* (CIA)
Département de l'énergie : *Office of Intelligence and Counterintelligence* (OICI)
Département de la sécurité intérieure : *Office of Intelligence and Analysis* (I&A), *Coast Guard Intelligence* (CGI)
Département d'État : *Bureau of Intelligence and Research* (INR)
Département du Trésor : *Office of Terrorism and Financial Intelligence* (TFI)
Département de la Défense : *Defense Intelligence Agency* (DIA), *National Security Agency* (NSA), *National Geospatial-Intelligence Agency* (NGA), *National Reconnaissance Office* (NRO), *Air Force Intelligence*, *Army Force Intelligence*, *Marine Corps Intelligence*, *Office of Naval Intelligence* (ONI)
Département de la Justice: *Federal Bureau of Investigation, National Security Branch* (FBI/NSB), *Drug Enforcement Administration, Office of National Security Intelligence* (DEA/ONSI).

La CIA[1], agence centrale de renseignement, a été établie en 1947 par le « National Security Act ». Elle a succédé à *l'Office of Strategic Services* (OSS). Elle a le statut juridique d'agence indépendante du gouvernement des États-Unis. Son quartier général est situé en Virginie, à proximité de Washington DC, depuis 1961. Elle dispose de 50 antennes à l'intérieur des États-Unis et de 200 postes à l'étranger.

La CIA s'organise autour de quatre directions principales :

- Le « *National Clandestine Service* » remplaçant depuis 2005 la direction des opérations, qui est responsable de la collecte humaine du renseignement. Elle est responsable du recrutement, de la formation, et du suivi des agents de renseignement en poste à l'étranger. C'est cette entité qui est responsable du renseignement opérationnel (« *actionable intelligence* »).
- La direction du Renseignement qui responsable de l'analyse du renseignement. Elle est organisée en bureaux géographiques et thématiques et se compose d'experts de haut niveau dans leur domaine.
- La direction de la Science et la Technologie ayant pour mission de concevoir de nouvelles technologies pour l'aide à la recherche du renseignement.
- La direction du soutien, responsable de tout le soutien nécessaire au bon fonctionnement de la CIA (communications, sécurité, logistique, services médicaux et financiers).

La CIA a deux rôles majeurs :

- Fournir des renseignements et analyser des informations sur les gouvernements, les entreprises et les individus et groupes d'individus dans tous les pays du monde pour le compte du gouvernement américain.
- Conduire des opérations non revendiquées (*covert*) à l'étranger.

La CIA n'est pas autorisée à mener des actions sur le territoire des États-Unis[2], ou à mener des opérations clandestines sans en informer préalablement les commissions parlementaires.

La NSA : *National Security Agency* (dont les fonctions se rapprochent au sein de la DGSE de la Direction Technique).

La NSA[3] a été créée en 1952 à l'initiative du Président Truman, sous l'égide du ministère de la Défense. Contrairement à la CIA qui a été fondée de manière très officielle, la NSA ne fut officiellement reconnue qu'en 1957, 5 ans après sa création. La NSA rassemble des informations sur le territoire américain et concernant des Américains (à partager avec le FBI principalement), à l'étranger (à partager avec la CIA). Elle emploie près de 35 000 personnes.

Sa mission est :

---

1) https://www.cia.gov/index.html
2) Elle dispose néanmoins d'antennes sur tout le territoire américain, généralement localisées au sein des "field offices" du FBI, et peut, en partenariat avec ce dernier, participer à des opérations sur le sol américain.
3) https://www.nsa.gov/

- De protéger les informations et les systèmes d'information du gouvernement américain.
- De diriger les activités de cryptologie du gouvernement américain.

La NSA est le seul collecteur et « traiteur » du renseignement venant de l'interception de communications.

Le FBI : Federal Bureau of Investigation (dont les fonctions se rapprochent de celles de la DCPJ et de la DGSI)

Créé en 1908, le FBI[1] est le principal service de police judiciaire fédéral américain. Il dispose également d'une compétence en matière de renseignement, notamment dans le domaine du contre-terrorisme et du cyber, devenu la priorité numéro 1.

Il emploie près de 35 000 agents, parmi lesquels 2 400 analystes en renseignement. Son quartier général se situe à Washington DC, en face du ministère de la Justice mais devrait déménager dans quelques années à l'extérieur de la ville, et il dispose de 56 bureaux (« *field offices* ») sur le territoire américain ainsi qu'une soixantaine d'antennes à l'étranger, dont les dirigeants sont les « *Legal Attaché* » ou *Legat*. Au sein du FBI, une nouvelle « *National Security Branch* » a été créée en 2006, principalement pour répondre au terrorisme, à la criminalité organisée, au contre-espionnage et à la menace cyber.

La NGA : National Geospatial intelligence Agency

Anciennement appelée *National Imagery and Mapping Agency* (NIMA), la NGA[2], créée en 2003, a pour fonction de collecter, analyser et diffuser le renseignement géo spatial en utilisant l'imagerie aérienne et spatiale.

La DIA : *Defense Intelligence Agency* (dont les fonctions se rapprochent de celles de la Direction du Renseignement Militaire)

L'agence du renseignement de la défense, ou DIA[3], a été créée en 1961. Elle a pour mission de recueillir du renseignement militaire étranger, y compris dans des domaines comme l'information politique, économique, industrielle, géographique, économique, et médicale liée à la défense nationale.

Bien que la DIA soit sous la responsabilité du ministère de la Défense, la majorité de ses 11 000 employés (70 %) sont des civils qui ont pour responsabilité l'acquisition et l'analyse du renseignement partout dans le monde.

La coordination des agences de renseignement :

---

1) http://www.fbi.gov/
2) https://www.nga.mil/Pages/default.aspx
3) http://www.dia.mil/

La coordination est effectuée par le Directeur of National Intelligence, ou DNI (directeur national du renseignement)[1]. Avant 2004, le directeur de la CIA était de facto le directeur de la communauté du renseignement des États-Unis. Depuis l'adoption du « *Intelligence Reform and Terrorism Prevention Act* » de 2004, le directeur de cette communauté est le DNI.

Le bureau du DNI rassemble 1 500 personnes. Il ne contrôle pas les agences dans l'exécution de leurs missions, mais son rôle s'articule en plusieurs axes :
– Il examine les budgets, les nominations et contribue à éviter les doublons entre les agences.
– Il établit les objectifs, les priorités et les directions de la communauté du renseignement.
– Il informe chaque jour le Président des États-Unis sur la situation sécuritaire, du fait de sa fonction de synthèse de tous les avis des agences de renseignement.
– Il publie régulièrement, le « *National Intelligence Estimate* » qui fait le point sur les menaces et les réponses mises en place. Et tous les 4 ans il actualise le papier intitulé « *Global Trends* » qui décrit les tendances lourdes dans un certain nombre de domaines touchant à la sécurité (démographie, géopolitique de l'eau, puissances émergentes…) ;
– Il édicte des circulaires qui s'appliquent à toutes les agences de renseignement sur des sujets transversaux non opérationnels (comme sur la non communication avec les journalistes, les accréditations…).

Le DNI supervise également plusieurs centres qui ont pour objectif d'améliorer la coordination entre les agences :
– Le *National Counter Terrorism Center* (NCTC), qui coordonne les missions de lutte antiterroriste ;
– Le *National Counter Proliferation Center* (NCPC) chargé des questions de prolifération nucléaire ;
– Le *National Counter Intelligence Executive* (NCIX), qui a pour mission de détecter les activités des services de renseignement étrangers et est également impliqué dans la réflexion sur les habilitations de sécurité (« *clearance* ») ;
– Le *National Intelligence Council* (NIC), qui coordonne la production des différentes agences sur certains sujets, en réalisant des notes de prospective sur différents thèmes.

Roumanie

En Roumanie, la loi confère à l'activité de renseignement aux fins de la sécurité nationale le caractère de secret d'État, les informations en cette matière ne pouvant être communiquées que dans les conditions posées par ladite loi.

---

1) http://www.dni.gov/index.php

La structure organise et réalise des activités visant la collecte, l'examen et l'exploitation des informations nécessaires pour connaître, prévenir et contrecarrer toute action constituant, au sens de la loi, une menace à la sécurité nationale de la Roumanie et déroule son activité dans le respect des droits et libertés fondamentales consacrés par la Constitution de la Roumanie.

Les textes relatifs aux services de renseignement

Certains pays comme le Royaume-Uni, les États-Unis ou l'Allemagne disposent de nombreux textes portant sur les activités de renseignement ainsi que sur le contrôle de ces activités.

Au Royaume-Uni, les principaux textes, apparus à partir de 1989, portent sur des domaines variés en relation avec l'activité et le contrôle des services de renseignement. Ils traitent notamment des questions d'identité des agents, de leurs missions, des autorisations (warrants), des accès aux documents, des responsabilités, des contrôles des activités, ainsi que des politiques de prévention du terrorisme.

Les États-Unis comptent également de très nombreuses dispositions en la matière. Ces textes portent sur des questions très diverses en relation avec les activités des agences de renseignement, tels que par exemple, les mesures de surveillance ou bien la coordination des agences entre elles. Il existe aussi des textes régissant l'activité de certaines agences en particulier.

En Allemagne, il existe plusieurs lois définissant les missions et les pouvoirs de chaque service de renseignement, ainsi que des lois précisant les modalités du contrôle parlementaire exercé sur l´activité de ces services. En outre, certains textes régissent la coopération entre la Fédération et les Länder dans le domaine du renseignement. Il existe enfin des dispositions constitutionnelles sur la question.

Les autres pays (Italie, Pays-Bas et Roumanie), disposent d'un nombre plus réduit de textes juridiques sur la question du renseignement. Ces textes sont le plus souvent assez généraux et régissent la question du renseignement dans son ensemble ou sous la forme de grandes thématiques. Aux Pays-Bas, un seul grand texte de portée générale, une loi de 2002, encadre les activités de renseignement. En Italie, c'est essentiellement une loi de 2007 qui régit l'architecture générale de l'intelligence italienne. En Roumanie, il existe une loi très générale de 1992 sur l'activité du renseignement.

Royaume-Uni

Au Royaume-Uni, les textes relatifs à l'activité des services de renseignements britanniques sont de nature législative :
– *L'Official Secrets Act* de 1989, qui protège la confidentialité des identités des membres des services et de leurs opérations.

– *L'Intelligence Services Act (*ISA) de 1994, qui définit les missions des services extérieurs et techniques, les procédures d'autorisation de leurs opérations (warrants), les fonctions des deux commissaires (*commissioners*), magistrats expérimentés nommés par le Premier Ministre pour trois ans, chargés du contrôle de légalité (rapports annuels publiés), ainsi que les attributions de l'organe parlementaire (*Intelligence and Security Committee – ISC*) ;
– Le *Regulation and Investigatory Powers Act* (RIPA) de 2000, qui précise les fonctions des deux commissaires (*Interception of Communications Commissioner et Intelligence Services Commissioner)*, magistrats expérimentés, désignés par le Premier Ministre ayant un pouvoir d'accès à tous les documents personnels des services, au Royaume-Uni et à l'étranger. Les commissaires ont notamment pour mandat de contrôler les autorisations (warrants) signés par le Ministre des Affaires Etrangères (*Foreign Office*) pour les opérations et interceptions sollicitées par le SIS et le GCHQ.
– Le *Security Service Act* de 1989, qui présente la base statutaire (rôle et responsabilités) du MI5.
– Le *Terrorism Act* de 2000, rédigé à la suite des crimes commis par l'IRA, définit les moyens judiciaires de prévention et de lutte contre le terrorisme. Ce texte a été complété avec une approche désormais fondée sur la lutte contre l'extrémisme islamique, par les « *Prevention and Terrorism Act* » de 2001, 2005 et 2006 qui incluent de nouvelles dispositions sur le financement et la propagande des mouvements radicaux[1].
– Le *Justice and Security Act* entré en vigueur au mois de mai 2013 introduit plusieurs modifications importantes dans le contrôle de l'activité des services britanniques de renseignement.

États-Unis

Aux États-Unis, le cadre juridique des actions des agences de renseignement est très développé. Il existe en effet un ensemble de normes et de procédures qui s'appliquent à l'activité des agences de renseignement. Ce cadre normatif comprend à la fois des règles de fond et de procédure. C'est sur ce corpus juridique que se fondent les contrôles qui ont été mis en place à la fois dans chacune des structures, mais aussi et surtout par des autorités extérieures à ces dernières. On peut citer, parmi les nombreux textes, le « *National Security Act* » de 1947 -qui a établi la CIA-, le « *Intelligence Reform and Terrorism Prevention Act* » de 2004 -coordination des agences de renseignement-, le « *Patriot Act* » de 2001 – sur les mesures de surveillance.

1) L'ensemble de ces textes est public et disponible sur internet (www.MI6.gov.uk, www.MI5.gov.uk, www.gchq.gov.uk, www.intelligence.gov.uk). Ces sites présentent également le volet public des rapports annuels des deux commissaires et ceux de l'ISC.

Allemagne

En Allemagne, les missions et les pouvoirs des différents services de renseignement sont définis par des normes propres à chaque service. Ces activités sont encadrées par deux types de textes : des lois définissant les missions et les pouvoirs de chaque service de renseignement, et des lois précisant les modalités du contrôle parlementaire exercé sur l´activité de ces services, étant précisé que l´existence de ce contrôle est ancrée dans la Constitution allemande depuis 2009.

– L'Office fédéral pour la protection de la Constitution *(Bundesamt für Verfassungsschutz ou BfV)* est régi par la loi relative à la coopération entre la Fédération et les Länder en matière de protection de la Constitution. La première partie de la loi est consacrée à la coopération entre la Fédération et les Länder et aux missions des offices pour la protection de la Constitution. L´article 3 de la loi précise que ces offices ont pour mission de rassembler des informations en vue de lutter contre les tentatives de déstabilisation émanant de groupes terroristes et extrémistes et d'organiser le contre-espionnage. La deuxième partie de la loi est consacrée à l´Office fédéral pour la protection de la Constitution en définissant ses pouvoirs et en précisant les conditions dans lesquelles il peut procéder au recueil, au traitement et à l´utilisation des données personnelles. La troisième partie de la loi est consacrée à la communication des données à l´Office fédéral pour la protection de la Constitution par des administrations de la Fédération, des personnes morales de droit public, les ministères publics, les services de douanes et de police, le service d´immigration, de même qu´à la communication de données par l´Office fédéral pour la protection de la Constitution à des autorités allemandes ou étrangères, ainsi qu'aux services de police ou aux ministères publics.

– Le Service fédéral de renseignement (*Bundesnachrichtendienst ou BND*) est régi par la loi relative au Service fédéral de renseignement (*Gesetz über den Bundesnachrichtendienst*) en date du 20 décembre 1990 qui comporte 12 articles : Le premier article de cette loi définit l'organisation et les missions du service fédéral de renseignement qui vise à renseigner la chancellerie fédérale sur des éléments d'information recueillis à l´étranger intéressant la sécurité de l´Allemagne et sa politique extérieure. Les dix articles suivants sont consacrés aux pouvoirs du service de renseignement en vue de rassembler des informations et aux conditions relatives au recueil, au traitement et à l'utilisation des données personnelles.

– Le Service de protection militaire (*Militärischer Abschirmdienst ou MAD*) est régi par la loi relative au service de protection militaire (*Gesetz über den militärischen Abschirmdienst*) en date du 20 décembre 1990.

Pays-Bas

Aux Pays Bas, c'est une loi du 7 février 2002 qui encadre les activités de renseignement. Cette loi relative au renseignement et aux services de sécurité est entrée en application le 29 mai 2002. Elle est toujours en vigueur.

Italie

En Italie, la loi n°124/2007 a créé une nouvelle architecture de *l'Intelligence* italienne qui était régie jusque-là par la loi n°801/1977. La loi n°124/2007 est très précise sur les modalités d'application des textes et est composée de six chapitres (structure du système, organisation, garanties fonctionnelles, contrôle parlementaire, Réglementation du secret et dispositions finales). La loi n°133/2012 est venue compléter le dispositif en modifiant la loi-cadre de 2007 et en accordant des pouvoirs plus importants à l'organe de contrôle parlementaire le COPASIR.

L'organisation, la gestion et les modalités concrètes de fonctionnement sont prévues dans des règlements d'application qui ne sont pas publics. La réforme de 2007 a introduit la responsabilité politique du seul Président du Conseil des Ministres et l'autonomie du Système par rapport aux deux ministères (Défense et l'intérieur), qui étaient jusque-là responsables de la gestion des services du renseignement.

Roumanie

En Roumanie, l'activité de la structure, institution spécialisée en matière de renseignements relatifs à la sécurité nationale de la Roumanie, est régie par la loi 14/1992 sur l'organisation et le fonctionnement de la structure, ainsi que par la loi 51/1991 relative à la sécurité nationale de la Roumanie, republiée. La loi 51/1991 indique les moyens accessibles aux structures chargées de la sécurité nationale, dans des situations constituant des menaces à la sécurité nationale de la Roumanie.

Le cadre légal des activités

Dans les pays anglo-saxons, la légalité de l'intervention des agents est le plus souvent supervisée, en amont, par des équipes de juristes. Contrôlées préventivement, les activités reçoivent en vertu de la loi ou des autorisations délivrées une légitimité et une immunité dans leur action qui sans le supprimer, réduit considérablement l'étendue du contrôle de légalité exercé *a posteriori*. Dans ces pays, les activités des services de renseignement peuvent être « légalisées » *a priori* ou encore « autorisées » en amont par le pouvoir exécutif. Ces autorisations préalables sont largement accordées et constituent de véritables blancs-seings quant à la mise en œuvre des activités des agents.

Dans les autres pays, les activités de renseignement font l'objet d'une « légalisation contrôlée ». Si un certain nombre de pouvoirs d'enquête sont conférés aux agences, il ne leur est en revanche pas permis de commettre des infractions. Par ailleurs, ce sont généralement les mesures les plus attentatoires aux libertés individuelles qui bénéficient d'un cadre légal. En Allemagne, aux Pays-Bas et en Roumanie, la loi impose aux services de renseignement de veiller aux principes de

subsidiarité et de proportionnalité de leur action. Ces règles énoncées par les textes permettent de renforcer le contrôle de légalité qui sera exercé ultérieurement. En Allemagne, de très nombreuses dispositions encadrent le recueil du renseignement, ainsi que l'enregistrement des données. Les atteintes les plus graves aux libertés individuelles doivent ainsi faire l'objet d'autorisations ministérielles et judiciaires préalables. C'est particulièrement le cas pour toutes les méthodes clandestines de recueil d'information.

Le système italien reprend le principe de proportionnalité des actions. Toutefois, les pouvoirs conférés aux agents – en l'occurrence par le Président du conseil – sont très importants, et sur ce plan, la législation italienne se rapproche des pays de Common Law. Une fois le principe de proportionnalité respecté, peu de limites sont fixées aux pouvoirs des agents. Ces derniers peuvent entreprendre tout acte, quelle que soit sa nature, sous réserve de ne pas porter atteinte à la vie humaine et de ne pas mettre en péril la sécurité de l'État.

Cadre légal peu contraignant : immunités largement accordées

Dans les pays de Common Law **(Royaume-Uni, États-Unis),** les pouvoirs conférés par la loi aux services de renseignements sont extrêmement étendus. L'immunité est très largement accordée aux agents de renseignement, qui agissent dans le cadre de leurs missions, quelle que soit la nature de l'acte. Ainsi, les agences de renseignement disposent d'un cadre d'intervention très protecteur et jouissent d'une large immunité dans le cadre de la mise en œuvre de leurs missions. Le système américain est le modèle le plus généreux en ce domaine, dans une logique d'efficacité de l'action des services : on assiste ainsi à un processus de « normalisation » faisant du renseignement une activité intégrée à la vie politique et institutionnelle.

Pour s'assurer de la légalité de leurs actions, les agences de renseignement disposent de nombreux juristes, qui étudient et interprètent les textes : ils sont ainsi consultés en amont des opérations.

Au Royaume-Uni, le système des « warrants » (autorisations) ministériels constitue le cœur de la protection juridique des services pour leurs activités clandestines et leur offre une totale immunité vis-à-vis du système judiciaire britannique. Des « warrants généraux » peuvent être accordés par le ministre (de l'Intérieur ou des Affaires étrangères) et des cibles peuvent être rajoutées sans solliciter de nouveau « warrant ». Les pouvoirs des agences de renseignement britanniques sont toutefois susceptibles d'être plus limités, sur le plan géographique, lorsqu'elles opèrent en dehors du territoire national.

Chaque fois que l'un des trois services (SIS *Secret intelligence service*, GCHQ *Government communications headquarters* et BSS

British security service) prévoit de mener une action dont les auteurs seraient normalement punissables au regard de la loi britannique (qui a compétence extraterritoriale), un dossier d'approbation est soumis, par l'intermédiaire de ses juristes, au Ministre des Affaires étrangères ou de l'Intérieur, ou en son absence et de façon exceptionnelle, à ses subordonnés directs. Ces demandes d'autorisation valent en premier lieu pour les activités sur le territoire britannique car à l'étranger, à l'exception de conventions internationales applicables, les actes illicites restent jugés par les tribunaux locaux et l'immunité de la Couronne n'est pas d'utilité. Les dossiers de demandes de warrants sont construits sur un argumentaire « risques/résultats attendus ». Par ailleurs le ministre signe des warrants génériques (*class autorisation, blanket*) d'une durée de six mois, autorisant à mener à l'étranger des catégories d'actions sans préciser les cibles ni leur localisation.

La signature du document par le ministre accorde l'immunité aux auteurs des actes décrits, quelle que soit leur nature : écoutes téléphoniques, piégeage internet, copie de documents dans une propriété privée, installation de micros dans un véhicule etc. Les membres du MI6 reconnaissent qu'il est exceptionnel qu'un warrant soit refusé, dans la mesure où il a été préalablement discuté entre le chef du service concerné et l'autorité politique. Ces dispositions, prévues par les articles 5 à 7 de *l'Intelligence Services Act de 1994* indiquent par exemple qu'aucune intrusion dans une propriété ou des communications privées n'est illégale si elle est autorisée par un warrant. De surcroit, cette protection juridique ne s'applique pas uniquement aux fonctionnaires du service, mais également aux agents et sources qui pourraient avoir commis les actes illégaux mentionnés dans le warrant (« *for the purpose of the service* »). Les services britanniques insistent régulièrement sur la solidité de leur dispositif de conformité (*compliance*) et soulignent le nombre élevé de juristes internes dédiés à cette mission. Le MI6 compte ainsi une équipe de 18 juristes.

Cadre légal contraignant : principes de proportionnalité et de subsidiarité

Les systèmes allemand, néerlandais et roumain sont assez proches, sur le plan de l'encadrement des pouvoirs conférés aux agences. Contrairement aux pays de Common Law, les agents ne disposent pas de mandats leur conférant une immunité de principe. Si un certain nombre de pouvoirs extraordinaires leurs sont conférés, ils ne peuvent être exercés qu'en respectant les principes de subsidiarité et de proportionnalité.

Ces pouvoirs spéciaux sont détaillés par le législateur, qui en dresse une liste limitative et les agences ne peuvent les utiliser que dans un cadre étroit fixé par les lois qui les réglementent. De façon générale, les pouvoirs sont beaucoup plus réduits, que ceux dont bénéficient les

agences dans les pays de Common Law. En particulier, les services de renseignement allemands ne disposent d'aucun pouvoir de police et n'ont aucune autorisation pour enfreindre les lois. Lorsque les méthodes utilisées portent atteinte aux libertés individuelles, elles sont strictement encadrées par les textes et des organes de contrôle doivent intervenir.

En Roumanie, la matière est régie par l'article 13 de la Loi 51/1991 qui indique les moyens accessibles aux structures chargées de la sécurité nationale, dans des situations constituant des menaces à la sécurité nationale de la Roumanie. Un certain nombre d'opérations peuvent être réalisées, à condition qu'il n'existe pas d'autre possibilité ou des possibilités limitées pour connaitre, prévenir ou contrecarrer les risques ou les menaces à la sécurité nationale, que celles-ci soient nécessaires et proportionnelles compte tenu des circonstances concrètes de la situation et que l'autorisation prévue par la loi ait été obtenue. Les structures peuvent réaliser les démarches suivantes : demander et obtenir des objets, écritures ou informations officielles des autorités, institutions publiques, personnes morales de droit privé ; consulter des spécialistes ou experts ; recevoir des saisines ou des notes d'informations ; réaliser des activités spécifiques à la collecte de l'information qui supposent la restriction de l'exercice de certains droits et libertés fondamentales de l'Homme, effectuées dans le respect des dispositions légales. Aux fins d'assurer la protection des citoyens contre toute immixtion ou atteinte, des règles claires et précises ont été fixées sur la délivrance et la prolongation des autorisations, la période maximale autorisée, la notification des personnes. Sont incriminées l'initiation, la transmission ou la réalisation de telles mesures sans fondement légal ainsi que l'usage abusif des mesures de prévention, découverte ou visant à contrecarrer les menaces à la sécurité nationale.

Aux Pays-Bas, les services de renseignement sont autorisés à traiter les renseignements, en conformité avec une loi de 2002, mais aussi avec une loi relative aux enquêtes de sécurité. Ils sont autorisés à faire appel à des corps administratifs, à des fonctionnaires et, de plus, à toute personne susceptible de détenir des renseignements. L'ensemble des pouvoirs dévolus à ces différents services est autorisé uniquement si la recherche programmée des renseignements ne peut avoir lieu ou ne peut avoir lieu à temps en consultant les sources publiques de renseignement accessibles. Enfin, l'action programmée doit répondre à un principe de proportionnalité et ne pas être exercée si celle-ci cause un préjudice sans comparaison avec l'objectif recherché. Ces services sont ainsi autorisés à :

– mener des surveillances et, dans ce contexte de collecte de renseignements concernant des personnes physiques ou des biens, utiliser des techniques d'observation ou de traçage, de pénétrer dans un lieu sécurisé, introduire des dispositifs techniques pour défaire un codage de données conservées ou traitées dans l'ouvrage automatisé, copier les données conservées ou traitées dans l'ouvrage automatisé ;

– utiliser des personnes physiques, qui sans une identité d'emprunt ou pas, sous la responsabilité et sous les ordres d'un service, sont chargées de collecter, de manière directe, des renseignements relatifs à des personnes et à des organisations qui peuvent être pertinents pour l'accomplissement des missions du service ;
– recevoir et enregistrer des télécommunications non reliées au câble en provenance d'autres pays, défaire le codage des télécommunications, se tourner vers les fournisseurs des réseaux des télécommunications publiques afin de leur demander de fournir des renseignements sur un usager et sur des flux de télécommunications de cet usager.

Il convient enfin de relever que les fonctionnaires des services de renseignement n'ont aucun pouvoir pour enquêter sur des infractions pénales (article 9 de la loi).

En Allemagne, des pouvoirs sont conférés par la loi du 20 décembre 1990 aux services de renseignement, à l'Office fédéral pour la protection de la Constitution (service civil de sécurité intérieure chargé de lutter contre les tentatives de destabilisation émanant de groupes terroristes) et au service fédéral du renseignement. Cette loi précise que le recueil d'information ne doit pas contrevenir à la loi fédérale sur la protection des données, que parmi toutes méthodes de collecte d'information, celle qui sera la moins préjudiciable pour l'intéressé devra être privilégiée et que le principe de proportionnalité doit être observé. Elle contient ensuite un certain nombre de dispositions sur les méthodes clandestines de recherches et de recueil d'informations.

L'Office fédéral pour la protection de la constitution est autorisé à employer des méthodes clandestines de recherche du renseignement telles que le recours à des informateurs, la surveillance, la sonorisation de lieux, la fixation d´images, l'infiltration. Toutefois, ces méthodes doivent figurer dans une note de service qui doit également mentionner l'organe compétent pour autoriser le recours à ces méthodes. Cette note de service est soumise à l'autorisation préalable du ministère de l´Intérieur, lequel doit en informer la Commission parlementaire de contrôle.

S'agissant des pouvoirs relatifs au recueil de certaines données auprès des compagnies aériennes, des établissements bancaires et de crédit, des sociétés de télécommunication, les données personnelles détenues par ces établissements ne peuvent être recueillies par l'Office fédéral pour la protection de la Constitution qu'à l´encontre de personnes à l'égard desquelles il existe des indices concrets permettant d´établir qu'elles encouragent l'accomplissement d'actes de haine ou de violence à l'encontre d'une partie de la population. Le recueil de telles données doit être autorisé par le ministère fédéral de l´Intérieur, sur requête écrite et motivée du responsable de l´Office fédéral pour la protection de la Constitution ou de son représentant ; lorsqu´il s´agit de données futures, la mesure est limitée à une durée de 3 mois renouvelable une fois selon la même procédure. Le contrôle de la légalité de

ces autorisations est par ailleurs effectué de manière permanente par la Commission G-10 (voir partie 3).

Les mesures de sonorisation du domicile et la fixation d'images ne sont autorisées qu´à condition que cela soit indispensable pour empêcher un danger imminent de portée générale ou concernant la vie d´individus et qu'une intervention policière ne puisse être organisée suffisamment rapidement. Dans un tel cas, l´autorisation judiciaire doit être sollicitée sans délai auprès du *Amtsgericht* (Tribunal cantonal) du lieu du siège de l'Office fédéral pour la protection de la Constitution. Ces mesures doivent être ordonnées par le Président de l'Office fédéral pour la protection de la Constitution ou son représentant, dès lors qu'une autorisation judiciaire n'a pas pu être obtenue à temps. L'intéressé qui a fait l´objet de ces mesures attentatoires à ses libertés individuelles doit en être informé après leur réalisation, dès lors que cela ne nuit pas à l'objectif poursuivi par ces mesures. Et la commission parlementaire de contrôle doit en être informée également.

La conservation des données est limitée dans le temps. La création de fichiers est soumise à l´autorisation préalable du ministère fédéral de l´Intérieur et doit être précédée par l'audition du Commissaire fédéral de protection des libertés dans le domaine informatique (*Bundesbeauftragter für den Datenschutz und die Informationsfreiheit*).

Cadre légal accordant des garanties statutaires : immunités fonctionnelles

En Italie, dans le cadre des opérations, les agents peuvent bénéficier, dans les limites strictes prévues par la loi, de certaines « garanties fonctionnelles », telles que des documents d'identité de couverture (Art. 24 loi 124/2007), une activité économique simulée (à titre individuel ou sous forme de société – Art. 25), la possibilité d'opposer un fait justificatif suite à la commission de certaines infractions ou de réaliser des mesures d'interceptions préventives. Ce sont ces deux dernières mesures qui seront développées. Ces larges pouvoirs sont donc attachés à la fonction d'agent du renseignement. Cependant, ces pouvoirs ne peuvent être exercés que lorsque l'agence a respecté le principe de proportionnalité.

• *L'autorisation de commettre des infractions et d'opposer un fait justificatif*

L'opération pouvant constituer une infraction doit être indispensable et proportionnée au regard des intérêts privés lésés, le préjudice causé être le plus faible possible. Cette protection peut être étendue à des personnes externes apportant leur concours. Le bénéfice de la protection

fonctionnelle résulte d'une autorisation préalable dans le cadre d'une opération précise (Art. 17 à 20 loi 124/2007)[1].

L'article 18 réglemente précisément les conditions d'autorisation de ces opérations. Ainsi, de tels agissements, sur requête écrite du directeur d'une Agence, le DIS (Direction du renseignement pour la sécurité) informé, doivent être autorisés par le Président du Conseil ou l'autorité déléguée par décision écrite motivée. Cette autorisation peut être modifiée ou révoquée à tout moment. Tous les actes relatifs à la procédure d'autorisation des garanties fonctionnelles sont conservés près le DIS dans un fichier secret avec les justificatifs des dépenses effectuées. Ces dépenses sont soumises à une vérification spécifique de la part du Bureau de l'inspection du DIS. En cas d'extrême urgence, le Directeur du service intéressé peut autoriser la commission du comportement délictueux sous réserve de prévenir immédiatement et dans tous les cas dans un délai maximal de 24 heures le Président du Conseil ou l'Autorité déléguée qui disposent de 10 jours pour confirmer l'autorisation. Si le comportement ainsi autorisé ou la transmission ne sont pas conformes aux prescriptions légales, le Président du Conseil prend les mesures utiles et en informe sans délai l'autorité judiciaire.

Le DIS, à la demande du directeur de l'Agence intéressée, est chargé d'opposer à l'autorité judiciaire saisie l'existence du fait justificatif. Le Procureur ou le juge saisi informé demande immédiatement au Président du Conseil la confirmation de l'autorisation prévue à l'art. 18. Tous les actes relatifs aux faits incriminés et à la procédure d'opposition sont séparés du reste du dossier et inscrits dans un registre spécial confidentiel. Le Président du Conseil a 10 jours pour confirmer l'existence d'une autorisation et en indiquer les motifs. Cette information est également transmise au COPASIR (Comité parlementaire pour la sécurité de la République). À compter de la confirmation, la procédure judiciaire est suspendue. L'absence de réponse dans le délai précité équivaut à l'absence d'autorisation permettant à l'autorité judiciaire de poursuivre. Lorsque l'autorisation a été confirmée, le juge dit n'y avoir lieu à poursuivre ou relaxe l'intéressé des faits. La décision est alors transmise au ministère public qui la conserve selon des modalités permettant d'en assurer la confidentialité.

Lorsque le fait justificatif est opposé directement par l'agent au moment de l'arrestation en flagrance ou de l'exécution d'une mesure privative de liberté, la poursuite de l'enquête est suspendue et l'agent est conduit par la police judiciaire dans les locaux pour procéder aux premières vérifications pour une durée maximale de 24 heures. Le ministère public est avisé immédiatement et doit solliciter le DIS qui doit confirmer dans les 24 heures à compter de la réception de la demande

1) Cette protection ne peut couvrir des faits de nature à mettre en danger la vie, l'intégrité physique, la liberté personnelle, morale, sexuelle ou encore la santé d'autrui ou encore concernant des agissements mettant en péril la sécurité de l'État.

si une autorisation a été octroyée. Le ministère public peut également demander confirmation directement au Président du Conseil. L'absence de réponse équivaut à une absence d'autorisation.

• *Les interceptions préventives*

La loi autorise les services secrets, après autorisation de l'autorité judiciaire, à violer le secret des communications, constitutionnellement garanti, aux fins de surveillance et de prévention, pour une durée limitée de 40 jours, prorogeables de 20 jours renouvelables. En l'espèce, c'est le Procureur général de Rome qui est compétent pour donner cette autorisation. Selon les chiffres communiqués par le DIS et confirmés dans la presse, ce ne sont que 12 demandes d'interceptions qui ont été faites en 2013 à ce titre, aucune n'ayant été refusée par le Procureur général de Rome. Les informations ainsi recueillies ne peuvent pas être utilisées comme preuve devant le juge et leur destruction doit être ordonnée à l'issue de l'opération des services du renseignement. En revanche, l'accès aux banques de données de l'administration et des organismes de service public ou concessionnaires dans les domaines névralgiques de l'énergie, des transports, de la santé, du crédit bancaire, des télécommunications est possible sans aucune autorisation préalable, sous réserve de la signature d'un accord de coopération. Le COPASIR (Comité parlementaire pour la sécurité publique) doit être toutefois informé de ces conventions et du nombre de connexions par an effectuées, afin de le mettre en mesure d'exercer *a posteriori* ses prérogatives d'inspection.

Le cadre légal du contrôle

On constate dans l'ensemble des pays étudiés un contrôle partagé entre le pouvoir exécutif, le pouvoir législatif et dans une bien moindre mesure, l'autorité judiciaire s'agissant des opérations les plus attentatoires aux libertés individuelles (Allemagne, Roumanie, États-Unis). La Roumanie est le seul pays à avoir confié à l'autorité judiciaire un contrôle permanent de la légalité de l'activité de renseignement.

Dans l'ensemble des pays, le contrôle exercé par l'exécutif s'apparente à une forme de contrôle *a priori*, voire d'autocontrôle dans la mesure où ce dernier veille d'une manière générale à cadrer et délimiter le mandat confié aux services de renseignements. Le contrôle parlementaire s'exerce également différemment selon les pays et majoritairement *a posteriori* sauf en Italie et en Roumanie où la commission parlementaire dédiée dispose d'un pouvoir de contrôle permanent et coercitif vis-à-vis de l'exécutif.

Dans les pays de tradition anglo-saxonne, ce sont les juristes des services de renseignement eux-mêmes qui évaluent à titre préventif la légalité des actes effectués dans le cadre de leur activité, il s'agit donc d'un véritable contrôle interne de la légalité. Aux États-Unis, plusieurs services d'inspection y sont dédiés. Au Royaume-Uni, le contrôle

préventif des services de renseignement repose ainsi essentiellement sur le dialogue avec l'échelon politique. Dans la pratique, l'exécutif peut ainsi refuser des idées inopportunes de manœuvre des services. Un contrôle *a posteriori* de la légalité des actes est en revanche prévu et partagé entre le pouvoir parlementaire et d'autres organes indépendants

Dans les autres pays, le contrôle de la légalité des actes relevant de l'activité de renseignement peut être partagé entre autorités administratives indépendantes[1] et autorité judiciaire. Celles-ci exercent généralement un contrôle sur la légalité des actes les plus attentatoires aux libertés individuelles (interceptions de communications, mesures de sonorisation, recueil de données personnelles). Les processus de contrôle s'exercent alors soit *a priori* (demandes d'autorisation) soit *a posteriori* (notamment par le biais de recours exercés à titre individuel). Des sanctions pénales en cas de manquement des agents des services de renseignement peuvent être également prévues (Roumanie, Royaume-Uni).

Les modes de contrôle

L'efficacité du contrôle de l'activité de renseignement s'appuie sur une répartition équilibrée de ce contrôle entre les différents pouvoirs et institutions de chaque pays. Afin de conserver une vision exhaustive de l'articulation des différents mécanismes de contrôle nationaux, ceux-ci seront analysés pays par pays.

Allemagne

En Allemagne, le contrôle du respect de la légalité par les services de renseignement est dévolu aux trois pouvoirs ainsi qu'à une autorité administrative indépendante (la Commission G-10). Ce contrôle de l'activité des services de renseignement porte sur l'ensemble des outils qu'ils mettent en œuvre. Toutes les atteintes graves aux libertés individuelles font l'objet d'un contrôle *a priori* (le recueil de données auprès des compagnies aériennes, des établissements bancaires et de crédit, des sociétés de télécommunication doit faire l´objet d'une autorisation préalable du ministère fédéral de tutelle ou de la Chancellerie fédérale, les mesures de sonorisation du domicile et de fixation d'images doivent être autorisées par le Tribunal cantonal, les interceptions des télécommunications ordonnées par le ministère fédéral de l'Intérieur à la demande des services de renseignement doivent être autorisées par la commission G-10). Toutes les autres atteintes, y compris celles graves, font l'objet d'un contrôle judiciaire, parlementaire et administratif *a posteriori*.

Contrôle permanent de la légalité par la commission G-10 : cette commission administrative indépendante a été instituée par la loi relative

1) La commission G-10 en Allemagne en 2009, le «Garant pour la protection des données» en Italie, la Commission de surveillance aux Pays-Bas.

à la restriction du secret de la correspondance et des télécommunications (*Gesetz über die Beschränkung des Brief-, Post– und Fernmedegeheimnis*) en date du 26 juin 2001 qui réglemente les conditions dans lesquelles il peut être porté atteinte au droit fondamental consacré à l´article 10 de la Constitution allemande[1]. En application de l´article 10 de cette loi, les interceptions des télécommunications et correspondances réalisées par les services fédéraux de renseignement doivent être ordonnées par le ministère fédéral de l´Intérieur. En application de l´article 14 de cette loi, ce dernier doit informer la commission parlementaire de contrôle tous les semestres des mesures ordonnées et celle-ci devra en informer le parlement dans le cadre de son rapport annuel. En application de l´article 15 de cette même loi, le ministère fédéral de l'Intérieur doit informer la commission G-10 mensuellement des mesures qu'il a ordonnées, avant leur exécution, sauf situation de danger. La commission vérifie la régularité des mesures ainsi ordonnées et si elle estime que ces mesures ne sont pas régulières ou pas indispensables, elles ne doivent pas être exécutées ou doivent être immédiatement levées si elles ont reçu un début d´exécution. La commission décide, à l´issue de l´opération, si l'intéressé peut être informé de la procédure dont il a fait l'objet. En outre, la commission statue sur les plaintes qui lui sont adressées.

Contrôle préventif et *a posteriori* du pouvoir judiciaire : le juge exerce un contrôle *a priori* des mesures de sonorisation du domicile et de fixation d'images qui doivent être autorisées par le Tribunal cantonal et un contrôle *a posteriori* devant les juridictions administratives pour toutes les autres mesures visant au recueil d'information et notamment celles concernant les interceptions téléphoniques.

Contrôle *a posteriori* du pouvoir législatif : ce pouvoir prépondérant est ancré dans la constitution depuis 2009[2] avec la Commission parlementaire de contrôle dont les travaux sont régis par la « *Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes* », soit la loi relative au contrôle parlementaire de l'activité de renseignement de la Fédération, en date du 11 avril 1978 modifiée à plusieurs reprises, et pour la dernière fois le 29 juillet 2009. Cette commission de contrôle est un organe de soutien du Bundestag puisqu'elle n'a pas l'exclusivité du contrôle des services de renseignement. Elle n'exerce pas un contrôle préventif et permanent. Elle est surtout un organe de

1) L´article 10 de la Constitution allemande dispose : « Le secret de la correspondance ainsi que le secret de la poste et des télécommunications sont inviolables. Des restrictions ne peuvent y être apportées qu´en vertu d´une loi. Si la restriction est destinée à défendre l'ordre constitutionnel libéral et démocratique ou l'existence ou la sécurité de la Fédération ou d´un Land, la loi peut disposer que l'intéressé n'en sera pas informé et que le recours juridictionnel est remplacé par le contrôle d'organes et d'organes auxiliaires désignés par la représentation du peuple ».

2) L'article 45 d consacré à cette question dispose que le Parlement désigne un comité chargé du contrôle de l'activité de renseignement de la Fédération et précise que les modalités de ce contrôle sont régies par une loi fédérale.

contrôle de la manière dont l'exécutif exerce son propre contrôle sur l'activité de renseignement. Le gouvernement fédéral est tenu d´informer la commission de manière étendue sur l'activité des services de renseignement et sur des affaires particulièrement importantes. La commission peut exiger du gouvernement fédéral des informations sur d'autres affaires menées par les services de renseignement. Elle soumet un rapport de ses activités au Parlement en milieu et en fin de mandat, en précisant si le gouvernement fédéral a respecté ses obligations d'information à son égard.

Italie

En Italie, le contrôle sur l'activité de renseignement est de nature parlementaire, constitutionnel et administratif. Le contrôle de la légalité de l'activité de recueil, d'utilisation et de conservation des données relève de la compétence exclusive d'une autorité administrative indépendante.

Contrôle renforcé et exclusif de la protection des données : le « Garant de la protection des données » (*Garante della Privacy*). Autorité administrative indépendante, le Garant de la protection des données contrôle les conditions de recueil des informations (Art. 58 du Code de la protection des données). La loi réglemente en effet les conditions de conservation des informations pour l'accomplissement des missions du Système de renseignement pour la sécurité et prévoit une sanction pénale pour toute personne qui ne respecterait pas les règles en la matière. À ce titre, l'article 160 du Code de la protection des données prévoit que cette autorité peut procéder aux vérifications des actes et prendre connaissance y compris de ceux couverts par le secret d'État. Toute demande de la part d'un citoyen contre les informations détenues par le Système de renseignement doit être transmise au *Garant de la Privacy.*

Contrôle parlementaire permanent : le Comité parlementaire pour la sécurité de la République (COPASIR)[1] est en charge du contrôle systématique et continuel du respect de la Constitution et des lois du fonctionnement du Système de l'Intelligence. La loi a doté cet organe de pouvoirs de contrôle et de consultation allant jusqu'à la possibilité d'imposer au Président du Conseil des obligations spécifiques d'informations à son égard. Constitué de 5 députés et 5 sénateurs, soumis au secret y compris à l'issue du mandat, le président est choisi parmi les membres appartenant aux groupes d'opposition. Son rôle est de contrôler le respect de la loi par les différents acteurs du service du renseignement ainsi que par les autres organismes publics dont le gouvernement. Il peut également solliciter l'Autorité judiciaire pour obtenir des copies d'acte ou de documents relatifs à des procédures et enquêtes en cours. Le secret de l'enquête ne lui est pas opposable. La transmission peut par décision motivée de l'autorité judiciaire être retardée de 6 mois renouvelables

1) Art.30 à 38 de la loi n°124/2007 exerce le contrôle parlementaire.

pour des raisons d'instruction du dossier. La clôture des investigations met un terme dans tous les cas à la suspension de la transmission. L'Autorité judiciaire peut également transmettre au COPASIR des documents d'initiative. Il est compétent pour procéder régulièrement à des auditions du Président du Conseil, de l'Autorité déléguée, du Directeur général du DIS, des Directeurs des Agences, des ministres composant le CISR et de manière exceptionnelle, également des agents du Système de renseignement pour la sécurité. Dans ce cas, le Président du conseil peut s'y opposer pour justes motifs. Ce dernier doit également exposer oralement lors d'une séance confidentielle spécialement convoquée, les renseignements utiles de nature à justifier le bien-fondé de l'opposition du secret d'État. Si le COPASIR estime que l'opposition n'est pas fondée, il en réfère au Parlement pour que la responsabilité politique soit discutée. Le Comité peut également entendre toute personne extérieure au Système ou encore demander de réaliser des enquêtes internes aux fins de vérifier le caractère adapté des comportements d'agents ou d'anciens agents des Renseignements. Tous les six mois, le Président du Conseil transmet au Comité un rapport sur l'activité des Agences contenant notamment une analyse sur la situation du Renseignement et les dangers pour la sécurité du pays.

Contrôle constitutionnel *a posteriori* : la Cour constitutionnelle, à qui il ne peut jamais être opposé le secret d'État, est compétente pour régler les conflits entre l'autorité judiciaire et l'exécutif sur l'opposabilité du secret d'État. Par une décision du 11 mars 2009, elle a limité son rôle à un contrôle formel ne portant pas sur les motifs ayant conduit l'autorité politique à apposer le secret d'État, et ce, alors même que celui-ci ne lui est pas opposable et lui permettrait d'examiner les circonstances d'espèce. Pour la Cour, seul le Parlement avec le COPASIR est en droit d'exercer le contrôle au fond des décisions les plus sensibles reposant sur une évaluation discrétionnaire du pouvoir exécutif et de sanctionner politiquement le Gouvernement. Cette décision a été vivement critiquée par de nombreux constitutionnalistes.

Royaume-Uni

Au Royaume-Uni, il n'existe pas d'institution dédiée au contrôle préventif et permanent de la légalité de l'activité de renseignement. Le contrôle s'exerce uniquement *a posteriori*.

Contrôle parlementaire : la Commission « *Intelligence and Security Committee »,* dont le statut est inscrit dans la loi de 1994 sur les services de renseignement, est composée de membres de la Chambre des Communes et de la Chambre des Lords (avec un équilibre politique entre les Conservateurs, les Travaillistes et les Libéraux-Démocrates) sélectionnés par le Premier ministre. Ils ne peuvent être ministres en exercice. Le *Chairman* est choisi par ses pairs. Le comité se réunit à l'extérieur des locaux du Parlement afin que ses membres ne soient pas protégés par leur immunité parlementaire dans le cadre de leurs travaux et les

membres de la Commission sont susceptibles de faire l'objet de poursuites pénales s'il s'avère qu'ils sont à l'origine de fuites. L'*Intelligence Security Committee* contrôle la bonne gestion des ressources des services (la gestion des budgets, des personnels, des propriétés immobilières, etc.) et la politique opérationnelle sous deux conditions : que l'opération en question soit close, qu'elle ait un intérêt national et que le Premier Ministre ait demandé ou approuvé le contrôle par les parlementaires.

Contrôle de légalité : il est exercé par deux commissaires chargés de contrôler l'activité des services (*l'Intelligence Services Commissioner* et *l'Interception of Communications Commissioner)*. Il s'agit de personnalités en fin de carrière, ayant occupé d'éminentes fonctions au sein de la magistrature et dont l'indépendance et la légitimité sont incontestables. L'avis de ces commissaires (également rendu public une fois par an) fait donc autorité. Ils contrôlent la légalité des actions des services lesquels sont contraints de transmettre l'intégralité des documents qu'ils réclament. Le commissaire vérifie notamment l'ensemble des demandes d'aval d'opération rédigées par le SIS ayant été soumises à l'approbation du Secrétaire d'État aux Affaires étrangères, ainsi que toutes les mises en garde (*caveats*) ou *warnings* rédigés pour une opération donnée. Lors de ces contrôles, le commissaire s'attache au-delà de la légalité (celle-ci est généralement respectée, les projets d'opérations étant passés sous les fourches caudines des 14 avocats et juristes du SIS), à contrôler la proportionnalité et la nécessité des actions engagées.

Contrôle suite à un recours individuel : *l'Investigatory Powers Tribunal* est une agence a compétence exclusive pour statuer sur les recours individuels contre l'exercice de pouvoirs intrusifs d'enquête utilisés par les services de renseignements (MI5, MI6 et GCHQ), les agences nationales de lutte contre le crime organisé, la Police de Londres, les services de police d'Irlande du Nord et d'Écosse et certaines administrations (les douanes notamment). Il faut toutefois préciser que *l'Investigatory Powers Tribunal*, est financée par le Home Office. Son impartialité n'est donc pas incontestable. En outre, il n'existe pas d'organe d'appel.

États-Unis

Les agences de renseignement sont toutes sous la responsabilité du Président des États-Unis, qui est le supérieur hiérarchique de l'ensemble des agents travaillant dans le domaine du renseignement. Il n'existe pas d'autorité administrative indépendante chargée d'assurer un contrôle des agences.

Contrôle interne de la licéité des actions : Pour faire respecter le cadre juridique qui leur est applicable, les agences de renseignement ont créé des postes de « *General Counsel* » ayant pour mission d'assurer le contrôle interne de chaque agence. Il s'agit d'un directeur juridique, dont la mission est essentiellement préventive puisqu'il s'agit de donner un avis sur les opérations de l'agence et ainsi de valider la compatibilité de ces dernières avec le cadre juridique.

Contrôle par les inspections générales : dès lors qu'il y a un dysfonctionnement, ce sont les inspections générales de chaque agence qui sont saisies, exerçant ainsi une fonction d'enquête interne non plus préventive, mais en réaction à un dysfonctionnement. L'inspection doit reporter non seulement au chef de l'agence en question, mais aussi à un organe interministériel dépendant de la Maison Blanche : *l'Intelligence Oversight Board (IOB)* À partir de ce stade, il ne s'agit plus seulement de contrôle interne puisqu'une autorité extérieure est saisie. Les inspections générales ont eu un rôle essentiel dans certaines affaires médiatiques : c'est le cas de la question de la torture sur la base militaire de Guantanamo. Elles peuvent être amenées à identifier ou vérifier certains comportements illégaux. Elles peuvent être saisies par des agents qui doutent de la légalité des actions de leur agence, pour qu'une réflexion soit engagée. Elles ont cependant un contrôle limité, car elles ont essentiellement vocation à enquêter sur des dysfonctionnements pour que l'autorité hiérarchique puisse prendre des décisions, et non pour que la justice puisse les sanctionner.

Contrôle par des organismes extérieurs émanant de l'exécutif : *L'Intelligence Oversight Board (IOB)*[1] a été créée par le President Ford suite au scandale du Watergate. Ce service a pour mission de s'assurer de la conformité de l'activité des agences de renseignement avec la Constitution américaine et l'ensemble des normes qui leur sont applicables, qu'elles soient législatives ou réglementaires (*Executive Orders et Presidential Directives*). En 1993, le Président Clinton a imposé à chacune des agences de reporter à l'IOB toutes les informations qui peuvent laisser penser que certains actes ou certaines opérations ont été réalisés en violation du droit applicable. C'est à partir de cette date que l'IOB est devenu un véritable organe de supervision, ou à tout le moins une structure destinée à centraliser les informations relatives aux dysfonctionnements des agences. Le rôle de l'IOB est cependant limité car il n'a pas de capacité d'investigation. En fait, si l'IOB n'est pas un véritable organe de contrôle indépendant, il a surtout pour intérêt d'informer le pouvoir politique et de lui permettre de valider certaines décisions. *L'Oversight Section* dépendant du ministère de la Justice dispose d'une compétence particulière en matière de supervision des agences de renseignement. Il a pour mission d'effectuer une analyse de proportionnalité entre les méthodes mises en place et les atteintes aux libertés individuelles qu'elles représentent. Créée après les attentats du 11 septembre 2001, cette section a été chargée de reporter les incidents dans les programmes, et de travailler avec les agences pour modifier les pratiques pour éviter des incidents similaires par la suite.

Contrôle *a posteriori* par le pouvoir législatif : le Congrès est aujourd'hui le principal organe chargé de contrôler les 16 agences de

1) L'*Intelligence Oversight Board* (IOB) est une subdivision du *President's Intelligence Advisory Board*

renseignement[1]. Ce contrôle prend différentes formes : information sur les opérations menées, contrôle de l'activité, des nominations et du budget.

Les comités du renseignement du Sénat et de la Chambre peuvent également « contrôler » l'activité des agences de renseignement. Pour cela, ils peuvent auditionner les représentants des agences, demander à se faire communiquer des documents ou encore établir une commission d'enquête sur un sujet en particulier. S'agissant de la consultation des documents, les parlementaires doivent les consulter dans une chambre sécurisée. Ils n'ont pas le droit de prendre de notes et ne peuvent pas en parler à leurs collaborateurs lorsqu'il s'agit d'opérations faisant l'objet d'une classification élevée. Les comités du renseignement peuvent également décider de mettre en place une commission d'enquête sur un sujet particulier. Le contrôle des nominations par le Congrès est limité. En effet, seules certaines agences font l'objet d'un vote pour la validation de la nomination de leur directeur. Enfin, le contrôle du budget est un outil très efficace mais pas immédiat. Le contrôle de la légalité des actions n'est donc pas vraiment en temps réel mais *a posteriori*.

Contrôle limité du pouvoir judiciaire en matière de collecte du renseignement : il intervient cependant à titre préventif et *a posteriori*. Il autorise certains actes attentatoires aux libertés et il tend à être de plus en plus saisi par les ONG sur le fondement de la violation d'un principe constitutionnel (notamment le quatrième amendement sur la protection de la propriété et de la vie privée). *La Foreign Intelligence Surveillance Court* (FISC) ou tribunal des services du renseignement étranger a été créée en 1978. Il s'agit d'un tribunal spécialisé dont les 7 membres sont nommés par le Président de la Cour Suprême pour examiner les demandes de mandats en matière d'enquêtes relatives à la sécurité nationale, notamment pour réaliser des perquisitions et obtenir des données électroniques de la part des fournisseurs d'accès à internet, gestionnaires d'adresse courriel ou réseaux sociaux. Les juges ont un mandat pour un maximum de 7 ans, non renouvelable, choisis dans des circonscriptions judiciaires différentes. La Cour a pour mission d'examiner les demandes de mandat d'obtention de données électroniques formulées par la NSA, en application de la loi sur la surveillance et le renseignement (« FISA »). Chaque demande de mandat doit contenir la validation par l'Attorney General que la cible de la surveillance proposée doit être une puissance étrangère ou un agent de la puissance étrangère,

1) Le contrôle de la communauté du renseignement par le Congrès a été mise en place à la fin des années 1970, suite à l'affaire du Watergate et aux Commissions d'enquête dites « Church » et « Pike ». Le comité du renseignement de la Chambre comprend aujourd'hui 22 membres, parmi lesquels un membre de la commission des finances, un membre de la commission de la défense, un membre de la commission des affaires judiciaires, et un membre de la commission des affaires étrangères.
Le comité du renseignement du Sénat (*Senate Select Committee on Intelligence* ou SSCI16) comprend aujourd'hui 15 sénateurs.

et, dans le cas où la cible est un citoyen américain ou un étranger résident aux États-Unis, que ce dernier ait été impliqué dans la commission d'un crime. Les juges du tribunal doivent se déplacer à Washington D. C. pour traiter les demandes de mandat à tour de rôle. Afin d'assurer que le tribunal puisse se réunir sous un bref délai, au moins un juge doit être membre du Tribunal de district du District de Columbia. De plus, la loi de 1978 a mis en place une cour d'appel du tribunal des services de renseignement étranger, présidée par trois juges de district ou de cour d'appel, nommés par le Président de la Cour Suprême, qui permet au gouvernement de faire appel d'une décision de refus. Le Patriot Act de 2001 (115 Stat. 272) a étendu la durée pour laquelle le tribunal peut autoriser la surveillance et a augmenté le nombre de juges de 7 à 11. Le contrôle des agences de renseignement par le pouvoir judiciaire peut aussi prendre une forme plus inattendue : celui d'une régulation à la demande des ONG. Il existe en effet une culture du recours au juge très développé de la part des ONG, qui peuvent demander non seulement l'arrêt de certains programmes lancés par le gouvernement, mais aussi la publication de certaines informations.

Pays-Bas

Aux Pays-Bas, le contrôle de la légalité de l'activité de renseignement est essentiellement exercé par la Commission de surveillance. Elle donne des avis (sur demande ou d'office) aux ministres compétents avec possibilité de demander aux ministres d'informer le Parlement. Les ministres compétents, les chefs de service, le coordonnateur et toute personne impliquée dans la mise en œuvre de la loi de 2002 sont tenus, à la demande de la Commission, de fournir tout renseignement à celle-ci et de lui porter assistance lorsqu'elle l'estime nécessaire. Dans la transmission de ces renseignements doivent être précisés ceux touchant la sécurité nationale qui ne peuvent être transmis qu'à la Commission de surveillance. La Commission de surveillance peut requérir toute personne en tant que témoin ou expert aux fins de l'entendre. Elle peut désigner un de ses membres, au besoin accompagné d'un membre du secrétariat, afin de visiter tous lieux nécessaires à l'accomplissement de leurs missions. Dans le cadre de ses missions, la Commission de surveillance est autorisée à conduire une enquête sur la façon dont la loi a été appliquée. Elle peut être aussi missionnée par le Parlement. Le rapport qu'elle rédige contient une partie publique et une partie classifiée qui fait l'objet d'une transmission au ministre compétent qui envoie le rapport public aux deux chambres dans les 6 semaines. La partie classifiée est envoyée confidentiellement à la Commission parlementaire pour le renseignement et les services de sécurité (CIVD). La Commission de surveillance rend un rapport annuel qui est transmis, de même, au Parlement et aux ministres compétents.

Roumanie

En Roumanie, l'activité de la « Structure » du renseignement est pilotée par le Conseil suprême de défense du pays lequel est soumis à la fois à un contrôle de légalité, mais aussi de proportionnalité et de nécessité, avec un examen permanent de la mesure dans laquelle les activités déroulées sont en accord avec la loi, proportionnées au niveau du risque et indispensables pour prévenir et contrecarrer la menace.

L'activité de renseignement est soumise à un mécanisme complexe de contrôle comprenant : un contrôle de légalité (exercé par les organes judiciaires), un contrôle parlementaire (la Commission permanente commune de l'Assemblée nationale et du Sénat pour l'exercice du contrôle parlementaire de l'activité de la structure) et un contrôle financier (la Cour des comptes et le ministère des Finances publiques).

Contrôle *a priori* et permanent de la légalité par l'autorité judiciaire : la loi institue l'obligation de demander une autorisation préalable pour les activités impliquant une restriction temporaire des droits et libertés constitutionnels. Le procureur général du Parquet près la Haute Cour de cassation et de Justice ainsi que les procureurs désignés à cet effet examinent les propositions soumises du point de vue de la légalité et du bien-fondé. Le président de la Haute Cour de cassation et de Justice ainsi que les juges désignés à cet effet sont chargés de délivrer les autorisations et les mandats prévus par la loi pour les situations entraînant une restriction de certains droits ou libertés fondamentales de l'homme. Si les données et renseignements intéressant la sécurité nationale, générés par les activités autorisées, indiquent la préparation ou la commission des faits prévus par la loi pénale, ceux-ci sont consignés par écrit et mis à disposition des organes du parquet accompagnés du mandat ayant été délivré aux fins de leur obtention. Le contrôle de la légalité par le juge est extrêmement approfondi puisque sont examinés à la fois la nécessité et la proportionnalité de la restriction de l'exercice de certains droits ou libertés fondamentales ainsi que le respect des conditions légales relatives aux autorisations.

Contrôle parlementaire permanent : la Commission permanente commune de l'Assemblée nationale et du Sénat contrôle de manière active l'activité de la « structure de renseignement ». Une fois par an ou quand le Parlement le décide, le directeur de la structure présente des rapports relatifs à la réalisation des tâches conférées par loi à la structure. La commission commune peut solliciter « de la structure » des rapports, des notes informatives, des explications écrites, documents, données, informations et peut entendre des personnes afin d'éclaircir les questions analysées. Par ces moyens, la Commission exerce un contrôle effectif et permanent en examinant si, dans l'accomplissement de ses tâches, la structure respecte les dispositions constitutionnelles ainsi que celles comprises dans les autres actes législatifs.

La Commission permanente commune de l'Assemblée nationale et du Sénat pour l'exercice du contrôle parlementaire réalise un contrôle constant de l'activité de la Structure, ses tâches consistant à vérifier le respect des dispositions constitutionnelles et des autres actes législatifs dans l'exercice du rôle de la structure en matière de sécurité nationale, à examiner les cas dans lesquels ont été signalées des violations des dispositions légales et à se prononcer sur les mesures qui s'imposent afin de rétablir la légalité. Elle analyse les saisines formulées par les citoyens se considérant lésés dans leurs droits et libertés par les moyens d'obtention des renseignements relatifs à la sécurité nationale.

Contrôle financier externe et interne : le contrôle externe est effectué par la Cour des Comptes de la Roumanie, la commission parlementaire pour le contrôle de l'activité de la structure et le ministère des Finances publiques. Le contrôle interne est exercé par les services spécialisés de la structure chargés du suivi et de l'évaluation de l'efficience et de l'efficacité de l'activité réalisée, de la régularité des états et du respect des conditions légales et du cadre règlementaire interne.

Sanctions existantes : la réalisation, en dehors des limites de l'autorisation accordée, ou sans autorisation, d'activités spécifiques à la collecte d'informations qui nécessitent une autorisation ; l'obligation de ne pas rendre publiques les informations relatives à la vie privée, l'honneur ou la réputation des personnes, apprises de façon incidente lors de l'obtention des données intéressant la sécurité nationale ; la divulgation ou l'utilisation sans droit par les employés du service de renseignement des données susmentionnées ; le non-respect des dispositions relatives à la protection des informations classifiées entraîne, suivant la loi, une responsabilité disciplinaire, contraventionnelle, civile ou pénale, selon le cas, de l'agent.

Moyens des institutions de contrôle

En Allemagne, les membres de la délégation parlementaire pour le contrôle des services de renseignement qui composent la commission parlementaire de contrôle sont élus à la majorité absolue des députés du Bundestag au début de chaque législature [1]. Le Bundestag détermine souverainement la composition de la délégation, celle-ci établissant son règlement intérieur.

La commission se réunit au moins une fois par trimestre et tout membre peut exiger la tenue d'une réunion. Tout en respectant son obligation de discrétion, la Commission établit deux rapports d'activité à l'intention du Bundestag : l'un à mi-mandat et l'autre en fin de législature. Pour permettre à la commission d'accomplir sa mission, la loi oblige

1) Cette délégation reste en fonction après la fin de la législature, jusqu'à ce que le Bundestag nouvellement élu ait désigné une autre délégation.

le gouvernement fédéral à la tenir informée de l'activité générale des services de renseignement, ainsi que des affaires revêtant une importance particulière. Pour sa part, la commission peut demander à être informée d'autres dossiers. Elle dispose d'un droit de contrôle sur pièces et sur place. Elle a également la possibilité d'auditionner les personnels des services de renseignement et charger des experts indépendants de mener des enquêtes ponctuelles pour son compte. La désignation de ces experts doit se faire à la majorité des deux tiers, après que le ministre compétent a été entendu. En principe, les personnes entendues par la commission sont tenues de faire des déclarations exhaustives et conformes à la vérité. Toutefois, le gouvernement fédéral peut omettre ou refuser d'informer la commission en raison du caractère directement opérationnel de certaines activités, de la nécessité de préserver l'accès à certaines sources d'information ou de protéger les droits de tierces personnes. Un tel refus doit être justifié par le ministre compétent devant la commission. Les membres de la commission peuvent recruter du personnel parmi leur groupe politique, après audition du gouvernement fédéral et avec l'accord de la commission parlementaire de contrôle. Ces collaborateurs peuvent accéder à l'ensemble des pièces et dossiers. Toutefois, ils ne peuvent participer aux délibérations de la commission, sauf autorisation spéciale à la majorité des deux tiers de ses membres (article 11 de la loi). La commission elle-même peut bénéficier de l'aide d'employés des services administratifs du Parlement. Cela doit être prévu dans le budget du parlement (article 12 de la loi). Les délibérations de la commission parlementaire de contrôle sont secrètes et ses membres sont tenus par la confidentialité, y compris après la fin de leur mandat, sauf dans certaines situations.

La Commission G-10 est l'autorité administrative indépendante chargée de se prononcer sur la régularité des mesures prises par les services fédéraux de renseignement concernant le secret des correspondances et des télécommunications. Elle est composée de quatre membres, dont un président qui doit avoir été habilité à exercer les fonctions de magistrat. Les membres de la commission, qui ne sont pas nécessairement des parlementaires, sont nommés par la commission de contrôle parlementaire pour la durée d'une législation. Les membres de la commission sont indépendants et ne reçoivent aucune instruction. Ils se réunissent une fois par mois, au moins. Ils sont autorisés à mener à tout moment des missions de contrôle au sein des locaux des services de renseignement et peuvent consulter tous les documents et données nécessaires à l'accomplissement de leur mission. La commission doit bénéficier des moyens humains et techniques suffisants pour remplir sa mission, notamment de l'aide d'assistants spécialisés. Cela doit être prévu dans le budget du parlement (article 15 de la loi). Les délibérations de la commission G-10 sont secrètes. Les membres de la commission doivent également garder le secret sur l'ensemble des éléments portés à leur connaissance dans le cadre de leurs travaux. Cette obligation perdure après la fin de leur mandat.

Aucune sanction n'est prévue en cas de violation du secret des délibérations par les membres de la commission parlementaire de contrôle ou de la commission G-10.

Aux Pays-Bas, la Commission de surveillance est composée de trois membres nommés par décret royal, sur avis des ministres compétents, pour une période de six ans, renouvelable une fois. C'est la seconde chambre du parlement qui présente une liste de trois candidats pour chaque vacance de poste, liste à partir de laquelle les ministres compétents font leur choix. Dans son avis de proposition, la seconde chambre prend en compte, si elle l'estime nécessaire, une liste de recommandations faites collectivement par le vice-président du Conseil d'État, le président de la Cour de cassation néerlandaise et l'ombudsman.

En dehors des trois membres de l'autorité de contrôle, la commission de surveillance dispose d'un secrétariat qui apporte toute assistance à cette commission. À ce jour, la Commission comprend une secrétaire, cinq fonctionnaires et un conseiller administratif. La Commission dispose de son propre budget adopté dans la même loi que celle qui approuve les budgets du ministre des Affaires générales et celui du Roi.

Contrôle et secret

Dans l'ensemble des pays, et de façon générale, les agences de renseignement ne peuvent opposer, aux autorités de contrôle[1], le caractère de « secret d'État » ou de « secret défense » qui est attribué à leurs documents, afin de leur refuser un droit de consultation. Il existe donc, au bénéfice des autorités de contrôle, un principe de droit de consultation qui leur est réservé. Ce droit peut même, quelques fois, être étendu à la possibilité de réaliser des auditions auprès du personnel des agences ou encore de diligenter des études.

Dans plusieurs pays, ce droit d'accès à l'ensemble des documents classifiés est conféré aux autorités de contrôle, sans restriction particulière et présente un caractère absolu ou quasi-absolu. C'est le cas de la Roumanie et du Royaume-Uni, où les autorités de contrôle disposent d'un droit général d'accès aux documents des services de renseignement.

---

1) S'agissant de l'opposabilité du secret d'État à l'autorité judiciaire, les réponses apportées par les différents pays sont beaucoup plus variables. Par exemple, en Italie, le secret d'État peut être opposé au juge à condition qu'une confirmation du refus de communication des pièces ait été prise par le Président du Conseil. Aux États-Unis, *de facto*, il peut arriver que peu d'informations soient transmises par les services à la juridiction, dans le cadre du contrôle préventif de collecte d'informations (afin d'obtenir par exemple une autorisation de perquisition). Dans ces deux pays, le secret défense peut ainsi, en droit ou en fait, être opposé au juge. Différente est la situation au Royaume-Uni où, à la suite du Justice and Security Act de 2013, la procédure du « closed material procedure » permet au service de renseignement d'invoquer le secret défense, tout en réservant un droit de consultation des pièces au seul bénéfice du juge et du conseiller spécial du plaignant.

C'est encore le cas aux Pays-Bas, où les restrictions d'accès que l'on peut constater, résultent seulement de la pratique, et non des textes. On peut citer enfin le cas de l'Italie où le Comité parlementaire pour la sécurité de la République (COPASIR) dispose d'un droit d'accès à tout document, ainsi que d'un droit de réaliser des auditions toutefois, ce dernier droit est susceptible de restrictions sur décision du Président du Conseil.

Dans d'autres pays, ce droit d'accès, bien que réel et consacré par les textes, est susceptible de subir quelques restrictions. On prendra l'exemple de l'Allemagne et des États-Unis. En Allemagne, la Commission parlementaire de contrôle dispose d'un droit d'accès aux documents des services de renseignement, qui peut toutefois être restreint par le gouvernement fédéral en raison du caractère directement opérationnel de certaines activités, de la nécessité de préserver l'accès à certaines sources d'information ou de protéger les droits de tierces personnes. Aux États-Unis, les comités d'information du Congrès disposent du droit d'accès aux informations, sauf en cas de décision de refus du pouvoir exécutif, qui contrôle la classification de l'information.

Évolution du contrôle de l'activité de renseignement

Face à l'évolution constante des technologies mises en œuvre pour le recueil du renseignement, la plupart des pays cherchent à adapter leur cadre légal. Par ailleurs, l'émoi provoqué par l'affaire *Snowden* a provoqué débats et initiatives.

En Roumanie, le cadre légal en matière de sécurité nationale a subi des changements en février 2014 afin d'être harmonisé avec celui de plusieurs pays de l'UE et complété compte tenu de la jurisprudence de la CEDH en matière de sécurité nationale. Ces interventions législatives et réglementaires ont notamment entraîné l'institution d'une nouvelle procédure relative à la restriction de l'exercice de certains droits ou libertés fondamentales en accord avec les garanties constitutionnelles, une énumération exhaustive des activités spécifiques pouvant être réalisées par les structures de renseignement, le renforcement du contrôle effectif de l'organe judiciaire sur les ingérences dans les droits et libertés de la personne entraînées par les activités des services de renseignements, la possibilité pour le juge examinant la demande d'autorisation de demander des informations complémentaires lorsque les informations initiales ne fournissent pas suffisamment d'arguments de nature à former sa conviction de ce que la mesure est nécessaire et justifiée, la création d'un recours judiciaire pour la personne s'estimant lésée dans ses droits par des actes des organes publics ayant un rôle en matière de sécurité nationale. Aux fins de connaître, prévenir et contrecarrer les menaces à la sécurité nationale, la structure du renseignement roumain met dorénavant l'accent sur l'atténuation de tous les risques potentiels et l'exploitation de tous les leviers permettant l'adaptation aux nouveaux défis lancés à l'environnement de la sécurité.

En Italie, à la suite du scandale *Snowden*, le Garant a pris différentes initiatives afin de renforcer la transparence des services du Renseignement et inciter le Gouvernement italien à assurer une meilleure protection des citoyens quant à la récolte d'information personnelles dans le cadre du Renseignement (demande d'audition par le COPASIR, saisine du Président du Conseil des ministres afin d'avoir des éclaircissements sur les activités de la NSA en Italie et voir adopter des instruments de protection des données compatibles avec les instruments européens de coopération judiciaire et policière). À la suite de ces démarches, un protocole d'accord, dont le contenu n'est pas public, a été signé en novembre 2013 entre le Garant et le DIS afin de réglementer les procédures d'information au regard des attributions de chacun. Un renforcement du contrôle des accès du DIS et des agences aux fichiers des administrations et services publics a été instauré et des modalités de transmission et de conservation par le Garant des renseignements ainsi obtenus a été instauré. Enfin, le DIS peut dorénavant solliciter l'avis du Garant sur les questions de protection des données.

Aux Pays-Bas, en 2012, la Commission de surveillance a demandé à ce que soit procédé à l'examen du dispositif existant par un éminent professeur d'Université. Un rapport a été déposé à ce sujet : *Het toezicht op de inlichtingen -en veiligheidsdiensten : de noodzaak van krachtiger samenspel* (La surveillance des services de renseignements et de sécurité : le besoin d'une action concertée renforcée). Ce rapport et les discussions qui ont suivi ont conduit le gouvernement, pressé par le Parlement, à décider d'une évaluation du cadre législatif et à la constitution d'une commission d'évaluation, la « Commission *Dessens* » (du nom de son président), qui a été nommée le 1er février 2013. À la demande du Parlement il a été demandé à la Commission d'évaluation de porter une attention particulière au système de contrôle et à l'adéquation technique des pouvoirs assignés aux services. Par ailleurs, le ministre de la Défense a émis le souhait d'amender la loi de 2002 en vue de l'adapter aux nouveaux développements technologiques tout en indiquant que cette proposition de réforme n'interviendrait qu'à l'issue des travaux de la commission *Dessens*. En juillet 2013 le Parlement néerlandais a demandé une enquête à la Commission de surveillance au sujet du fonctionnement des services civils et militaires de sécurité. La Commission *Dessens* a rendu son rapport en fin d'année 2013. Le rapport indique que les lois actuelles concernant le Service civil de Renseignements (AIVD) et l'AIVD (pendant militaire) sont inadaptées et a relevé des pratiques concernant les ressources humaines à la limite de la légalité (agents et informateurs). Il se prononce d'une part pour un renforcement des pouvoirs de ces deux services et d'autre part pour que les agences en question puissent être autorisées à enquêter sur le transfert des données personnelles par le câble. Des questions fondamentales ont été soulevées au sujet de l'éthique entourant le recueil de renseignements à grande échelle. Le rapport a été transmis au Parlement au mois de mars 2014. Les ministres de l'Intérieur et de la Défense ont indiqué qu'ils suivraient

les recommandations de la Commission afin notamment d'instaurer une plus grande transparence pour la coopération internationale entre les services. Avant l'été 2014, le ministre de l'Intérieur a indiqué que les services néerlandais du renseignement prenaient part à une initiative pour développer des standards communs sur la coopération internationale entre États de l'Union européenne.

Aux États-Unis, *La Foreign Intelligence Surveillance Court* (FISC) (cour ayant pour mission d'examiner les demandes de mandat d'obtention de données électroniques formulées par la NSA) a fait l'objet de débats quant à son effectivité : les ONG estiment qu'il s'agit d'une chambre d'enregistrement qui n'a pas joué un véritable rôle de contre-pouvoir. Le taux d'approbation des demandes est en effet supérieur à 99,95 %. Beaucoup estiment qu'en l'absence de contradictoire et de débat public, un véritable contrôle est difficilement possible.

Des propositions de réformes ont été avancées, notamment pour assurer un minimum de contradictoire, par exemple en permettant à des ONG d'avoir accès au dossier et de formuler des observations contre les demandes de mandat.

Au Royaume-Uni, à la suite de l'affaire *Snowden* notamment, les Britanniques ont réalisé qu'ils étaient confrontés aux interceptions massives de métadonnées[1] et que la loi RIPA 2000 n'était plus à ce titre adaptée, même si elle prenait déjà en compte, mais à la marge seulement, ces questions de métadonnées. En outre, si la loi offre quelques garde-fous à l'accès aux métadonnées interceptées, elle ne dit rien sur les conditions de leur interception et notamment, des échanges avec des partenaires étrangers. Se pose la question de la nécessité et de la proportionnalité des accès ainsi que leur durée de rétention. Vice premier Ministre et ministre de la Justice sont intervenus publiquement en mars 2014 pour souligner la nécessité de faire évoluer le cadre juridique relatif aux métadonnées. À la suite de l'arrêt de la Cour de Justice de l'Union européenne du 8 avril 2014, qui a jugé contraire aux libertés fondamentales la directive de l'UE imposant aux opérateurs de communication de conserver les données de connexion des internautes, une loi ayant pour objectif de fournir un cadre juridique précis dans ce domaine a été adoptée.

Par ailleurs, le *Deputy Prime Minister*, a d'ores et déjà formulé quelques propositions concrètes : création d'un portail web unique pour les trois agences de renseignement, qui diffuserait davantage d'informations sur leur travail quotidien (statistiques, cadre juridique, etc.), publication d'un rapport annuel de transparence incluant le nombre, la

---

1) Les métadonnées (*Bulk data et Méta Data),* constituent l'ensemble des informations sur le contenant technique à l'opposé du contenu, d'une communication téléphonique ou informatique, par exemple l'adresse mail de l'expéditeur, sa localisation, son heure de connexion.

nature et les motivations des requêtes faites par chaque agence auprès des fournisseurs d'accès et des opérateurs télécoms, étendre le nombre des membres de la commission parlementaire à 11 membres (9 actuellement), choisir son président parmi l'opposition, rendre publiques davantage d'auditions, introduire un droit d'appel pour les jugements de *l'Investigatory Powers Tribunal* (saisi par les citoyens s'estimant victimes d'abus, le seul recours étant actuellement de saisir la Cour européenne de sauvegarde des droits de l'homme, création d'un Inspecteur général des agences de renseignement, qui remplacerait *l'Interception of Communications Commissioner* et *l'Intelligence Services Commissioner*, avec des pouvoirs et des ressources étendus et un profil plus visible dans l'opinion publique.

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

- Président : Jean-Marie Delarue, conseiller d'État honoraire, nommé par le Président de la République par décret du 26 juin 2014, publié au *Journal officiel* le 27 juin 2014.
- Membre parlementaire – Assemblée nationale : Jean-Jacques Urvoas, député (PS) du Finistère, désigné le 23 juillet 2012 par le président de l'Assemblée nationale.
- Membre parlementaire – Sénat : François-Noël Buffet, sénateur (UMP) du Rhône, désigné le 24 novembre 2014 par le président du Sénat.

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

- Maud Morel-Coujard, déléguée générale, depuis sa nomination en date du 1er novembre 2014 ;
- 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.
- Jean-Marie Delarue, conseiller d'État honoraire, 26 juin 2014.

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, à titre personnel.
- Jean-Jacques Hyest, sénateur de Seine-et-Marne, nommé le 2 juin 2010 en remplacement du sénateur Hubert Haenel, nommé membre du Conseil constitutionnel, puis le 6 décembre 2011, à titre personnel.
- François-Noël Buffet, sénateur du Rhône, 24 novembre 2014.

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 no 2012-351 du 12 mars 2012 a abrogé la loi no 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 Code de la sécurité intérieure.

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 lui faire une recommandation d'avertissement pour l'alerter 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 CNCIS 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 prévus par la loi et réalisées par les services habilités. Les investigations 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.

En vertu du même article, la Commission peut procéder à son initiative aux vérifications qu'elle estime nécessaires pour s'assurer que l'interception de sécurité est bien effectuée selon les conditions prévues par la loi et par la décision d'autorisation.

En outre, la CNCIS, ou par délégation de celle-ci, son président peut ordonner les vérifications qui lui paraissent nécessaires à la suite d'informations ou de déclarations publiques de personnes faisant état d'interceptions de leurs communications électroniques ou des données techniques se rattachant à celles-ci.

À l'occasion de ces différents contrôles et dans l'hypothèse où elle constaterait une violation des dispositions légales en matière d'interceptions et de recueil de données techniques, elle doit adresser un avis sans

délai au procureur de la République en application de l'article 40 du Code de procédure pénale.

En revanche, 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. Hors du champ de compétence de la CNCIS, les requêtes des particuliers qui portent sur ces interceptions présumées ou réelles sont déclarées irrecevables.

Elle 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. Ainsi une vingtaine de sites où sont mises en œuvre ces mesures et exploité le renseignement technique sont visités par les agents de la Commission au cours d'une année.

La CNCIS est en outre chargée, en application de l'article 6 de la loi nº 2006-64 du 23 janvier 2006 relative à la lutte 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 de police et de gendarmerie, et qui sont autorisées par une « personnalité qualifiée » placée auprès du ministre de l'Intérieur.

Toutes les autres demandes relatives au recueil des données techniques de communications sont formulées par les services habilités des ministères de l'Intérieur, de la Défense et des Finances et traitées par le Groupement interministériel de contrôle. Elles relèvent de l'article L. 244-2 du Code de la sécurité intérieure (ancien article 22 de la loi du 10 juillet 1991) et sont soumises, au contrôle *a posteriori* de l'autorité administrative indépendante.

La CNCIS est membre de la Commission consultative créée par le décret nº 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 Commission nationale de contrôle des interceptions de sécurité 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 2013 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 garantir son indépendance budgétaire, la Commission est dotée d'un budget opérationnel de programme (BOP), référencé 308AIC.

Les crédits alloués en 2013 se sont élevés à 551 673 euros (607 803 euros en 2012 et 619 897 euros en 2011) dont 474 474 (529 864 euros en 2012 et 523 619 euros en 2011) pour les dépenses du titre II (dépenses de personnel) et 77 199 euros (77 939 euros en 2012 et 96 278 euros en 2011) pour les dépenses de fonctionnement.

Le budget global de la CNCIS a donc connu une diminution de 56 130 euros. Fort heureusement, en raison des missions nouvelles confiées à la CNCIS par le législateur en 2013, cette tendance à la baisse a été provisoirement suspendue pour l'année 2014. Les crédits alloués sont de 567 661 euros dont 475 269 euros pour les dépenses du titre II (dépenses de personnel) et 92 392 euros pour les dépenses de fonctionnement.

L'augmentation des crédits hors titre 2, d'environ 17 % par rapport à la LFI 2013 est justifiée par :
– l'accroissement des attributions de la Commission en matière d'avis et de contrôles des mesures de renseignement concernant les communications électroniques résultant des lois du 9 juillet 2004, du 23 janvier 2006, du 21 décembre 2012 et de la loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale, notamment dans le domaine du recueil des données de connexion et de la géolocalisation ;
– le renforcement de l'effectivité des avis et des contrôles *a posteriori*. Cette orientation fonde la mise en place de contrôles inopinés et l'augmentation de la fréquence des visites programmées. Les développements techniques des outils d'interception des communications électroniques et leur décentralisation entraînent des déplacements plus réguliers sur

l'ensemble du territoire national pour la réalisation des contrôles de la Commission ;
– le développement des actions de communication institutionnelle dans le cadre des débats publics et parlementaires, depuis plus d'un an, portant sur les moyens de surveillance des communications par les services de l'État, sur la protection des données personnelles et de la vie privée notamment en matière de communications électroniques via Internet ainsi que les débats sur le cadre légal et le contrôle des services de renseignement.

Pour autant, le montant alloué pour les dépenses du titre II relatif au personnel a été calculé pour les cinq postes actuellement pourvus, alors que la CNCIS dispose de six ETPT. Cette évolution du plan des effectifs interdit, en l'état, toute possibilité de recrutement, alors même que la Commission envisage de s'adjoindre un sixième agent avant la fin de l'année 2014.

Il faut rappeler que la CNCIS fonctionne à effectifs constants depuis sa création il y a près d'un quart de siècle alors que ses missions se sont considérablement accrues au fil des années. Chargée initialement, en 1991, du seul contrôle de l'exécution des écoutes, elle a très vite été sollicitée pour adresser des avis préalables sur chaque projet d'interception.

En 1997, elle est devenue membre de la Commission consultative placée auprès du Premier ministre pour délivrer 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.

En 2006, elle a reçu pour tâche de contrôler les demandes de données techniques de communications, dont le nombre est au moins dix fois supérieur à celui des demandes d'interceptions de sécurité. Les modalités des vérifications de ces demandes ont été renforcées en 2010 aux fins d'adapter le recueil de ces renseignements aux enjeux de sécurité et de protection des données de communications privées.

Depuis lors, la Commission assure le contrôle systématique et constant des demandes validées, tant par la personnalité qualifiée pour les demandes des services du ministère de l'Intérieur habilités en matière de lutte contre le terrorisme, que par le Groupement interministériel de contrôle pour les demandes des services habilités au titre du Code de la sécurité intérieure et portant sur les différents motifs autorisant l'interception des communications.

En 2013, le législateur a confié à la CNCIS le contrôle du futur dispositif unifié de recueil des données de connexion, ainsi que des mesures de géolocalisation en temps réel administratives. L'ensemble de ces nouveaux outils entrera en vigueur dès le 1er janvier 2015.

Les crédits du BOP CNCIS sont destinés en priorité à permettre le fonctionnement continu de l'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 ». Elle doit accéder aux 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.

Soucieuse de l'utilisation optimale des deniers publics, 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, missions attribuées par le législateur à l'autorité administrative indépendante.

Dans le même souci d'efficacité et de lisibilité de son activité, la Commission a choisi de mettre en œuvre le dispositif de contrôle 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.

Elle s'inscrit pleinement dans la démarche de modernisation de l'action publique définie par la circulaire du Premier ministre du 7 janvier 2013 et visant à l'élaboration d'un plan de modernisation et de simplification de l'action publique destiné à améliorer le service aux citoyens, l'organisation et le fonctionnement des services, ainsi que la mutualisation des fonctions support. Ainsi la Commission a décidé, au-delà des actions internes, de participer au comité de pilotage de ce plan et de s'associer notamment aux programmes « ouverture et partages des données publiques », « accueil et traitement des demandes des requérants » ou encore « projet de mutualisation et immobilier Ségur des AAI et des SPM ».

Enfin, le président, comme les membres de la CNCIS, relèvent du dispositif créé par la loi n° 2013-907 du 11 octobre 2013 relative à la transparence de la vie publique, et se soumettent aux déclarations ainsi qu'aux contrôles définis par le législateur et conduits par la Haute autorité pour la transparence de la vie publique.

La CNCIS prend donc toute sa part dans l'effort collectif de rationalisation des dépenses publiques. Elle poursuit sa recherche d'économies, notamment sur le plan du fonctionnement. Néanmoins, l'extension de ses attributions et des saisines, ainsi que les exigences techniques et matérielles du contrôle dans ces domaines en évolution constante et

rapide, nécessitent de disposer de moyens adaptés aux objectifs de protection des libertés publiques et de sécurité, dévolus par le législateur à la Commission.

Relations extérieures

Dans le prolongement des travaux avec les autorités bulgares, allemandes, belges, roumaines, libanaises, canadiennes et turques 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 ses attributions.

Ces travaux bilatéraux et les projets législatifs exposés par les délégations étrangères montrent une préoccupation commune d'évolution du cadre légal régissant le recueil administratif ou judiciaire du renseignement technique. Ils témoignent de problématiques et de travaux similaires sur les données techniques de communications avec des questions portant sur leur accès (général ou individualisé, aléatoire ou ciblé), sur la détermination de leur régime et sur les modalités du contrôle de ces recueils par les services d'État et les opérateurs privés.

Les agents de la Commission ont 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 continue des magistrats de l'ordre judiciaire sur le traitement judiciaire du renseignement, de la formation initiale des commissaires de police sur le recueil du renseignement technique issu des communications électroniques, ou les conférences auprès d'organismes comme l'institut des hautes études de la défense nationale (IHEDN), ainsi que dans les cycles de formation de l'Académie du renseignement.

Chapitre II

Actualité de la Commission : adoption de règles déontologiques internes

À la suite de sa nomination à la présidence de la CNCIS, M. Jean-Marie Delarue a proposé à l'Assemblée plénière de définir des règles déontologiques applicables tant aux membres de la Commission qu'à ses agents. Adoptées à l'unanimité des membres en septembre 2014, ces règles, entrées en vigueur immédiatement, sont aujourd'hui rendues publiques par le biais du présent rapport.

Règles déontologiques applicables à la Commission nationale de contrôle des interceptions de sécurité

Les présentes dispositions sont applicables aux membres et aux collaborateurs de la Commission nationale de contrôle des interceptions de sécurité, sans préjudice des règles qui leur sont applicables en matière de déontologie au titre de leur appartenance à d'autres corps ou institutions, telles qu'elles figurent notamment dans le Code de déontologie des députés, dans les obligations déontologiques définies par le Conseil supérieur de la magistrature, dans la Charte de déontologie des membres de la juridiction administrative, dans le titre 1er du statut général des fonctionnaires ou dans tout autre texte de portée législative ou réglementaire.

Indépendance

1.1 Tout comportement de nature à faire naître un doute sur l'indépendance des membres et des collaborateurs de la Commission nationale de contrôle des interceptions de sécurité (ci-après la Commission), voire de faire naître un sentiment opposé, doit être écarté.

1.2 À cet effet,
– le président comme les collaborateurs de la Commission ne peuvent exercer d'activité, rémunérée ou non, quelle qu'en soit la nature, en relation avec la mission confiée à la Commission, à l'exception des tâches d'enseignement ou de celles conduisant à des études ou travaux écrits, entrepris après en avoir avisé la Commission ;
– les membres et les collaborateurs de la Commission doivent, de manière générale, éviter de se trouver en situation de conflit d'intérêt : ils ne peuvent en particulier se prononcer sur une question dans laquelle leur indépendance n'est pas assurée ; ils prennent à cet égard toute disposition, en particulier en avisant le président.

1.3 Dans l'hypothèse où, de son propre fait ou du fait d'autrui, un membre ou collaborateur de la Commission se trouverait en conflit d'intérêt, il doit, de sa propre initiative, s'abstenir de participer à la procédure de traitement de toute affaire en cause dans ce conflit, après en avoir avisé.

1.4 Il en va de même lorsque l'existence de liens antérieurs est susceptible de porter atteinte à l'indépendance de jugement des membres et des collaborateurs de la Commission.

1.5 Alors même que les services du Premier ministre contribuent à la gestion matérielle de la Commission, les membres et collaborateurs de la Commission prennent soin de rappeler, chaque fois que nécessaire, le caractère d'indépendance qui s'attache à cette institution et ne sont jamais liés par une décision de caractère politique quelle qu'elle soit.

1.6 Hors du cadre des consultations et expertises requises par le rôle institutionnel de la Commission, le président et les collaborateurs de celle-ci ne participent en aucun cas à la définition des politiques publiques relatives au renseignement et à l'activité de sécurité en général.

1.7 De manière générale, les membres et les collaborateurs veillent à préserver en toutes circonstances leur impartialité et leur neutralité dans les affaires qui leur sont soumises.

1.8 Toute difficulté dans l'application du présent paragraphe est abordée en Commission.

Secret, confidentialité et discrétion

2.1 En vertu de la loi, les membres et les collaborateurs de la Commission sont astreints au secret.

2.2 Non seulement ce secret est absolu et, par conséquent, observé par chacun avec rigueur, mais il appartient à la Commission de prendre les mesures destinées à en faciliter l'observation et à chacun, membre ou collaborateur, d'agir d'initiative pour être à même de respecter les consignes et de garantir pour lui-même la bonne application de l'obligation légale, notamment dans l'usage des moyens de communication.

2.3 L'exigence du secret ne s'étend pas seulement à la vie professionnelle. Elle ne prend pas fin avec l'issue du mandat de membre ou des fonctions de collaborateur à la Commission.

2.4 Le secret n'est pas opposable aux membres et aux collaborateurs de la Commission entre eux. Ils se doivent au contraire mutuellement toute l'information utile en vue d'un bon accomplissement de leur mission.

2.5 Le « secret défense » partagé avec des services tiers ou des responsables publics pour certaines affaires n'induit nullement la levée de ce secret sur d'autres affaires qui ne doivent pas être partagées. En particulier, aucune affaire particulière ou générale protégée ne sera évoquée avec un service ou un agent dont elle ne relève pas.

2.6 La confidentialité est moins rigoureuse dans sa portée. Elle autorise le partage d'informations avec des tiers autorisés. Elle le défend avec ceux qui ne le sont pas.

2.7 Les membres et collaborateurs sont astreints, en tout état de cause, à un devoir de discrétion sur l'ensemble des activités de la Commission qui ne sont couvertes ni par le secret, ni par la confidentialité, ainsi que sur les personnes qui y travaillent.

2.8 Le respect des dispositions du présent paragraphe implique que les tâches incombant à la Commission ne soient accomplies qu'au sein de ses locaux, sauf évidemment celles qui, par nature, ont lieu à l'extérieur, et dans les cas de l'astreinte mentionnée au 4.2 ci-dessous. Les documents mis à la disposition des membres de la Commission lors des assemblées plénières sont donc détruits à l'issue de celles-ci, à l'exception de ceux à usage de procès-verbaux consultables dans les locaux.

2.9 Toute expression ne relevant pas du champ des activités de la Commission reste évidemment libre et celle-ci n'a pas à en connaître. Dans une hypothèse d'expression de cette nature toutefois, membres et collaborateurs doivent se dispenser de faire état de leur qualité à la Commission.

La communication

3.1 Les obligations du §.2 qui précède ne font pas obstacle à l'expression de la Commission pour définir les principes dont elle entend faire application, ou bien de manière générale, ou bien dans un domaine particulier (nouvelle technologie, nouvelle mission demandée aux

services, approche d'une catégorie ou d'une zone déterminée, nouvelle politique publique…).

Le rapport public est le moyen privilégié mais non pas unique, de cette expression.

Lorsque le rôle de la Commission est publiquement mis en cause, elle peut estimer utile de faire connaître son point de vue, à la condition naturellement qu'aucune atteinte ne soit portée aux règles relatives au secret des affaires dont elle a à connaître ou bien de ses travaux.

3.2 L'expression de la Commission est subordonnée à l'accord de l'assemblée plénière, convoquée à cet effet. Elle est normalement du ressort du président. Nul, sans son accord préalable, ne peut se l'approprier dans les cas mentionnés au dernier alinéa du 3.1.

3.3 Les parlementaires membres de la Commission disposent naturellement de la possibilité dans le cadre de leur mandat de commenter l'expression de celle-ci. Ils ne peuvent toutefois y ajouter sur le fond sans préciser qu'en la matière ils ne sauraient l'engager.

3.4 Les collaborateurs de la Commission n'ont pas la possibilité, sauf mandat exprès, d'engager l'institution.

3.5 Si la Commission ou la manière dont elle accomplit sa mission sont publiquement mis en cause, il appartient à l'assemblée plénière de déterminer, éventuellement, le fond et la procédure de réponse, à l'exclusion de toute autre manière de faire.

Les avis de la Commission

4.1 En ce domaine, dans lequel sont confrontées, et doivent être conciliées, les exigences tenant aux libertés individuelles et celles de la sécurité, l'impartialité et la neutralité doivent être constamment observées.

4.2 Les avis rendus sont également tenus par les principes généraux auxquels est tenue la puissance publique, comme le respect du principe de légalité.

4.3 Toutes les affaires soumises à la Commission, dans l'urgence ou non, doivent être examinées avec les informations nécessaires fournies par les services, l'approfondissement et le temps requis et selon le cadre de règles fixées par la Commission en assemblée plénière, indépendamment de l'auteur de la demande et des objectifs visés.

4.4 Les documents fournis doivent être interprétés strictement, sans altération ni omission.

4.5 L'examen des affaires est, chaque fois qu'il est possible, soumis à la collégialité au sein de la Commission, à l'exception de celles dont les délais sont incompatibles avec cette manière de faire.

4.6 Lorsque les informations nécessaires à un examen approprié par la Commission ne lui sont pas parvenues, celle-ci doit décider, selon des règles compréhensibles pour les services et constantes, de surseoir à statuer dans l'attente de renseignements complémentaires. Le sursis à statuer ne saurait valoir avis de la Commission au sens des textes en vigueur : toute décision prise incompétemment par l'autorité publique sur ce seul fondement doit être portée à la connaissance du président de la Commission dans les plus brefs délais.

4.7 De manière concomitante avec ce qui précède, chaque affaire doit être examinée avec le maximum de célérité. Les dossiers présentés selon la procédure dite « d'urgence absolue » doivent être appréhendés et traités dans des délais compatibles avec cette urgence (une heure), selon une procédure identifiable. Ils exigent des temps d'astreinte répartis équitablement. Les collaborateurs qui sont d'astreinte rendent compte immédiatement au président de tout dépassement du délai.

4.8 La rédaction de l'avis est faite par ceux qui ont procédé à l'examen de l'affaire. Ses modalités doivent permettre le respect des règles déterminées aux 4.2 et 4.3 qui précèdent et celles du secret.

Relations avec les auteurs des demandes et les autres agents publics

5.1 Investis d'une mission de contrôle du service public du renseignement, les membres et les collaborateurs de la Commission ne peuvent avoir avec les agents de ce service que des relations conciliables avec l'exercice du contrôle. Elles doivent ainsi se limiter aux relations rendues nécessaires par l'exécution stricte des tâches imparties à la Commission.

5.2 La réalisation de celles-ci ne requiert ni démarches occultes, ni informateurs confidentiels. Toute dérogation jugée nécessaire à cette prohibition doit avoir reçu l'autorisation préalable du président de la Commission et doit être suivie des comptes rendus nécessaires, après vérifications utiles, notamment à l'assemblée plénière.

5.3 Les relations avec l'autorité politique relèvent du président ou de l'assemblée plénière de la Commission.

5.4 Les limites qui précèdent ne s'appliquent pas aux parlementaires membres de la Commission, dès lors qu'ils agissent dans le cadre de leur mandat, en particulier dans le cadre de la délégation parlementaire au renseignement.

Les visites extérieures

6.1 Les membres et collaborateurs de la Commission se soumettent, lors des visites qu'ils effectuent, aux règles de sécurité applicables aux personnes étrangères aux services visités et à toutes celles qui leur seraient réglementairement imposées.

6.2 Ils ne se départissent jamais de la courtoisie requise.

6.3 Ils s'en remettent aux responsables des lieux ainsi qu'aux exploitants du soin de leur permettre l'accès aux données dont ils ont besoin, de leur fournir les documents nécessaires à l'accomplissement du contrôle ou de leur donner les informations qu'ils sollicitent. Ils consignent toutefois avec précision tout refus d'accès aux sources (volontaire ou accidentel) et, plus généralement, tout refus de coopération qui remettrait en cause leur mission.

6.4 Ils se gardent de tout jugement pendant le déroulement de la visite. Ils se bornent à recueillir les informations qui leur sont utiles, à établir leur véracité et à poser les questions requises par leur compréhension. Ils veillent à ce que les questions qu'ils posent sont en lien direct avec les attributions de la Commission. Ils précisent en tant que de besoin en quoi leurs demandes relèvent de ces attributions.

6.5 Dans leur rapport, ils ne font état que de faits établis et présentent comme tels les constats qui ne restent qu'à l'état d'hypothèses.

6.6 Les auteurs du rapport mettent en lumière les considérations qui leur paraissent mériter un examen de la Commission.

Au sein de la Commission

7.1 Membres et collaborateurs de la Commission portent à la connaissance du président, en vertu du devoir de loyauté, les difficultés particulières qu'ils rencontrent dès lors qu'elles sont de nature à compromettre l'exercice de leurs tâches.

7.2 Le président doit prévenir toute anomalie dans l'exécution des missions de la Commission afin d'assurer l'application de la loi. Il doit simultanément assurer aux membres et aux collaborateurs les garanties que celle-ci prévoit.

Chapitre III

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

Le contrôle des autorisations

Il s'agit ici de décrire la nature et la portée du contrôle opéré par la CNCIS sur les demandes d'interceptions dont elle est saisie. La mission confiée par le législateur est celle d'un contrôle de la légalité. La Commission n'a pas de compétence pour juger de l'opportunité pour un service de choisir ce moyen d'investigation à tel ou tel moment de la conduite de son enquête, ni pour porter une appréciation sur la manière dont les enquêteurs exploiteront les renseignements obtenus. La vérification de la légalité ne se limite pas pour autant à un contrôle formel. Elle porte aussi sur les éléments de procédure et de fond des dossiers d'interceptions.

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 des demandes des services habilités validées par le ministre de tutelle. 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 après cette décision, et ce durant toute l'exploitation de l'interception. Il peut entraîner 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 nº 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, l'interception étant 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 considération 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 Groupement interministériel de contrôle (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 quarante-huit 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 autorisées en dépit d'un avis défavorable ou déjà en cours et dont la Commission recommande au Premier ministre de décider de les interrompre, ou préconise directement aux services cette interruption.

Depuis plusieurs années, la Commission sollicite que cette pratique de l'avis *a priori*, 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. Un amendement parlementaire a été déposé en ce sens en novembre 2013 lors des débats relatifs à la loi de programmation militaire 2014-2019.

Le gouvernement, par la voix du ministre de la Défense, s'est opposé à cette consécration législative, indiquant préférer que ce débat ait lieu dans le cadre d'un futur projet de loi sur le renseignement qui serait examiné avant la fin de la législature. Dans un courrier adressé peu après à la CNCIS, le Premier ministre a confirmé cet engagement à inscrire l'avis préalable dans la loi et assuré que, dans cette attente, il continuerait à respecter cette pratique en consultant systématiquement la Commission avant toute décision de mise en œuvre d'une interception de sécurité.

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 nº 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).

L'exigence du respect de ce plafond n'est donc plus la conséquence de contraintes techniques mais un aspect du caractère « exceptionnel » que doit conserver l'atteinte au secret des correspondances de nos concitoyens. Le contingentement participe à l'encadrement de la mise en œuvre des interceptions et demeure un facteur de protection des libertés publiques.

En pratique, il implique que le nombre d'interceptions actives 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, qu'il faut rapprocher de l'augmentation exponentielle du nombre d'utilisateurs des outils de communication.

À titre d'illustration, le nombre d'abonnés à des services mobiles en France est ainsi passé de 280.000 en 1994 à 78,4 millions en juin 2014 soit un taux de pénétration dans la population (hexagone et outre-mer) de 119,2 %. Par ailleurs, 196 milliards de SMS ou MMS ont été échangés en 2013, soit 6 % de plus qu'en 2012 (source ARCEP).

Cette comparaison entre, d'une part, l'évolution des outils de communication et leur emploi, et, d'autre part, l'augmentation limitée des contingents d'interceptions depuis 1991, témoigne du respect constant de la volonté du législateur de conserver aux mesures d'ingérence des pouvoirs publics dans la correspondance privée, leur caractère exceptionnel.

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	2005	2009	2014
Ministère de la Défense	232	330	400	450	285	285
Ministère de l'Intérieur	928	1 190	1 190	1 290	1 455	1 785
Ministère du Budget	20	20	80	100	100	120
Total	1 180	1 540	1 670	1 840	1 840	2 190

(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 2013 a été marquée par le cinquième exercice de traitement des interceptions par référence, non plus aux « lignes téléphoniques » mais à l'objectif visé par la mesure. Il s'agissait pour la Commission de souligner que les garanties et les droits prévues par la loi du 10 juillet 1991 sont attachés à la personne et non à ses moyens de communications. La protection est homogène et unique pour la personne et ce, quel que soit l'outil de communication électronique employé. Elle permet de garantir l'exploitation légale de l'interception à l'égard d'une seule personne et non d'une pluralité d'individus qui emploieraient le même outil de communication.

Cette référence, à la « cible » a permis pendant près de neuf ans au Premier ministre de ne pas augmenter le contingent, attitude qui paraît conforme au respect du caractère exceptionnel que doit conserver cette mesure d'investigation particulièrement attentatoire aux libertés. Il convient en outre de souligner l'absence de cas récent de l'emploi de la totalité du contingent général, qui était jusqu'en 2014 de 1 840 objectifs.

Néanmoins, à la lumière des récents travaux consacrés à l'avenir du renseignement, comme le rapport de la mission parlementaire sur l'évaluation du cadre juridique applicable aux services de renseignement déposé le 14 mai 2013 et le rapport de la commission d'enquête sur le fonctionnement des services de renseignement français dans le suivi et la surveillance des mouvements radicaux armés déposé le 24 mai 2013, et des attentes formulées par les services notamment lors des visites de contrôle opérées par la CNCIS, la question d'une augmentation des « quotas » attribués à certains ministères s'est posée à nouveau.

Certains services utilisateurs ont pu exprimer le souhait d'une augmentation de leur contingent pour faire face à des besoins opérationnels nouveaux et des menaces croissantes d'atteintes aux intérêts fondamentaux de la Nation. Deux ministères, l'Intérieur et le Budget, ont en conséquence sollicité une hausse de leurs quotas, respectivement de 330 cibles pour le premier et 20 cibles pour le second.

Saisie pour avis par le Premier ministre, la CNCIS ne s'est pas opposée à l'augmentation sollicitée, mais a subordonné cet avis favorable au strict maintien du niveau d'exigence qu'elle fixe aux services lors de l'exploitation des interceptions de sécurité. En effet, il serait inacceptable que l'augmentation du volume des autorisations données se fasse au détriment de la scrupuleuse observation du cadre légal, qui garantit le caractère exceptionnel que doit conserver l'interception de sécurité, mesure d'investigation particulièrement attentatoire aux libertés.

En application des dispositions de l'article L. 242-2, le Premier ministre a autorisé courant 2014 une hausse des quotas conforme aux demandes des deux ministères concernés. Cette décision a abouti à un nouveau contingent total de 2 190 « cibles ».

Cette augmentation, la plus significative depuis 1997, a eu une conséquence directe sur la méthode d'examen préalable par la Commission des demandes d'interceptions. En effet, l'autorité administrative indépendante n'a bénéficié d'aucun renfort d'effectif pour faire face au surcroît de travail généré par les interceptions supplémentaires. Comme cela sera développé un peu plus loin, elle a dû profondément modifier son fonctionnement pour rendre ses avis non plus une fois par semaine (sauf procédures d'urgence absolue, qui, de façon constante, donnent lieu à un avis dans l'heure) mais au plus tard tous les deux jours et dématérialiser ses échanges avec les services du Premier ministre pour gagner en productivité sans perdre ni en rigueur d'analyse, ni en respect des règles de sécurité.

Le 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 et concrète du fondement des demandes et une meilleure adéquation aux exigences de la Cour européenne des droits de l'homme.

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 l'article L. 212-1 du Code de la sécurité intérieure 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 et du 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. Cet élément 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 par les différents services habilités a été revu en 2006, en 2008, et à nouveau en 2009. Il est appelé à évoluer prochainement, la CNCIS ayant le souci constant d'améliorer la lisibilité comme la compréhension de ses avis. 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 trames normalisées ne constituent pas un cadre restreint. En tant que de besoin, les services peuvent communiquer tout élément qui leur paraît 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 par la CNCIS pour exclure conformément à l'article L. 242-5 du Code de la sécurité intérieure, 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.).

Depuis sa création, la CNCIS porte une attention particulière 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, même indirectement, 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 la 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. À réception de ces renseignements additionnels, elle formulera des observations ou rendra son avis.

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.

Quel que soit l'auteur des questions complémentaires, la réponse du service est systématiquement communiquée à l'autorité de décision comme à celle de contrôle, afin que l'une comme l'autre se prononce sur des dossiers strictement identiques. 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 dans celui 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][1]*. 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 2012-2013*

6 182 interceptions de sécurité ont été sollicitées en 2013 (4 213 interceptions initiales et 1 969 renouvellements). Pour mémoire, 6 145 interceptions de sécurité avaient été sollicitées en 2012 (4 022 interceptions initiales et 2 123 renouvellements). Ces nombres confirment la stabilité observée depuis plusieurs années.

S'agissant des interceptions initiales, 812 de ces 4 213 demandes ont été présentées selon la procédure dite d'urgence absolue (622 en 2012) soit 19,3 % des dossiers, ce qui démontre une forte augmentation, de près de quatre points, par rapport à l'année précédente (15,5 % en 2012).

L'état de la menace, en particulier terroriste, l'ancrage dans le temps et l'accélération des crises au niveau international, comme leur prolongement prévisible sur le territoire national, constituent sans doute une première cause de ce recours plus important à la procédure de l'urgence.

La trop grande rigidité de la procédure « hors urgence », qui conduisait la Commission à ne rendre ses avis qu'une fois par semaine au Premier ministre, représente probablement une autre raison. Elle a pu inciter les services à recourir trop fréquemment à la procédure de l'urgence, y compris lorsqu'elle n'était pas nécessairement « absolue ». La Commission, déterminée à éviter toute utilisation abusive de la procédure d'urgence, a proposé d'introduire plus de fluidité dans le traitement des demandes.

En concertation avec le Premier ministre, elle a désormais demandé à être destinataire chaque jour des demandes qui parviennent au GIC. Ainsi, elle rend quotidiennement ses avis, ou, au plus tard dans les 48 heures. De son côté, le Premier ministre ou son délégué décide, au regard des avis de la CNCIS, deux fois par semaine. Ce nouveau dispositif n'a été possible qu'en modernisant les équipements informatiques et en adaptant les méthodes de travail au sein de la Commission. Cela représente plus de contraintes en termes de délais à respecter pour l'autorité administrative indépendante dont les moyens en personnel

---

1) Article L243-8 du Code de la sécurité intérieure : « *[…]. Alinéa 2 : Si [le Président de la CNCIS] 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. Alinéa 3 : 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. […]* ».

n'ont pas été renforcés pour autant. Mais elle a toujours veillé à remplir ses missions avec la plus grande célérité, condition indispensable au regard de la sensibilité des dossiers dont le traitement ne peut souffrir le moindre retard injustifié.

Cette profonde réorganisation commence à porter ses fruits quant au nombre d'urgences absolues. Les neuf premiers mois d'exercice de l'année 2014 montrent en effet, en dépit de l'augmentation des quotas de certains ministères et d'un état de la menace toujours plus préoccupant, une stabilisation du recours à la procédure de l'urgence absolue.

L'objectif d'un traitement par la Commission de ce type de demande dans un délai inférieur à une heure a, en dépit de l'augmentation des volumes, 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, 365 jours par an.

Au final, si l'on impute à ce chiffre global les 82 avis défavorables donnés par la Commission lors des demandes initiales et des demandes de renouvellement, tous suivis par le Premier ministre, ce sont donc 6 100 interceptions de sécurité qui ont effectivement été pratiquées au cours de l'année 2013 (6 095 en 2012).

Pour ce qui concerne les « motifs légaux » au stade des autorisations initiales, la prévention de la criminalité et délinquance organisées reste le premier motif des demandes initiales avec 60 %, suivie de la prévention du terrorisme avec 24 % et de la sécurité nationale avec 15 %.

Concernant les renouvellements accordés, on note que la sécurité nationale occupe la première place avec 36 %, suivie de la prévention du terrorisme à 31 % et de la criminalité organisée à 30 %. Ces pourcentages de renouvellement rendent compte, de fait, du travail des services en rapport avec certains motifs légaux qui supposent une inscription des investigations dans la durée.

La part légèrement 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 taux de clôture des demandes d'interception pour ouverture d'une procédure judiciaire traduit le respect de ces principes constitutionnels. Il témoigne aussi de l'intérêt de ce dispositif de prévention et de police administrative qui permet d'exclure des hypothèses d'enquête et de stopper les mesures d'investigation avant toute phase judiciaire. Il ouvre aussi la possibilité, en cas de confirmation des soupçons quant à des projets d'infractions de poursuivre par l'ouverture d'une procédure judiciaire avant la commission des faits, ce qui est particulièrement essentiel dans le cadre de la prévention des attentats terroristes.

Le total cumulé des demandes initiales et des renouvellements ayant été autorisés confirme que le motif de la prévention de la criminalité et de la délinquance organisées se détache nettement avec 54 % des requêtes, suivie de celui de la prévention du terrorisme à 28 %, puis celui de la sécurité nationale à 17 %. Ces trois motifs représentent 98 % du total des demandes.

2013 confirme la part toujours plus importante prise par la criminalité organisée année après année (+ 2 points par rapport à 2012). Elle marque surtout une hausse importante du nombre de demandes présentées sous le motif « prévention du terrorisme » (+ 5 points par rapport à 2012), qui est évidemment à mettre en relation avec l'acuité de la menace terroriste. La diminution de la part de la sécurité nationale (- 7 points) est la conséquence mécanique de la hausse des deux autres motifs précités plus qu'une tendance liée à la diminution des risques d'atteintes en la matière. Les deux autres motifs légaux « sauvegarde du potentiel scientifique et économique » et « prévention de la reconstitution de groupements dissous » représentent moins de 2 % 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 3 767 en 2012 dont 172 demandes de renseignements complémentaires et 771 limitations de la durée d'interception sollicitée, à 4 599 en 2013 dont 259 demandes de renseignements complémentaires et 679 limitations de la durée d'interception.

Cette forte augmentation du nombre d'observations confirme que la CNCIS a entendu renforcer son contrôle *a priori* sur chacune des demandes présentées. Les exigences de forme comme de fond se sont accrues, et elles ont permis un gain important dans la qualité de rédaction des motivations. La Commission note que l'ensemble des services concernés a tenu à participer, dans un dialogue constructif, à ce souci d'amélioration des demandes.

Les avis défavorables, comptabilisés dans les observations, se sont élevés à 82 comme il a été dit, parmi lesquels 37 concernent les demandes initiales (dont 2 portant sur des procédures d'urgences absolues) et 45 les demandes de renouvellement. Cela représente 32 avis défavorables de plus qu'en 2012 (+ 64 %), mais sur un total de demandes présentées qui est supérieur à l'année précédente. Il serait précipité de tirer des conséquences de cette augmentation des avis défavorables, dès lors qu'elle porte sur des nombres peu élevés et que, de surcroît, leur nombre était en baisse en 2012 par rapport à 2011. Les tendances peuvent donc fluctuer d'un exercice à l'autre. Néanmoins, ce chiffre confirme, là encore, la vigilance de la CNCIS lors du contrôle de légalité effectué *a priori*, qui est tout sauf un examen purement formel. Ces avis défavorables ont été suivis par le Premier ministre.

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 16 reprises en 2013 (contre 14 en 2012). 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 pour stopper l'exploitation d'interceptions, qui s'éloignent du cadre de l'autorisation délivrée par le Premier ministre ou son délégué. 40 préconisations ont été faites en 2013 contre 38 en 2012, 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 2013 à 138 contre 102 en 2012.

Le contrôle en aval

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 518 interceptions en 2013 ont été examinées plus spécifiquement par la Commission, chiffre légèrement inférieur à celui de 2012 (561). Cette diminution résulte essentiellement du renforcement du contrôle *a priori* exercé par la Commission, laquelle estime qu'il vaut mieux empêcher en amont un service de s'écarter du cadre légal plutôt que de le rappeler à l'ordre une fois que l'atteinte aux libertés a été commise. L'exigence d'une meilleure qualité de la rédaction des demandes permet qu'elles contiennent suffisamment d'éléments précis pour qu'un examen systématique des productions ne s'avère pas indispensable.

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.

Deux recommandations de ce type ont été adressées au Premier ministre au cours de l'année 2013. Elles ont entraîné des rappels de la part du délégué du Premier ministre en direction du service exploitant, qui a tiré les conséquences des difficultés soulevées par la Commission en demandant, à son niveau, la suppression des interceptions concernées.

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, sur des thématiques générales ou dans des dossiers, dans lesquels le recueil d'informations complémentaires et le suivi des productions ne suffisent pas à l'éclairer suffisamment.

Avec 6 100 interceptions accordées en 2013 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.

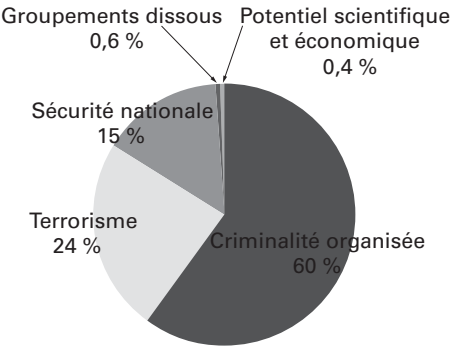
Tableaux annexes

Les demandes initiales d'interceptions

État des demandes initiales d'interceptions (2012 et 2013)

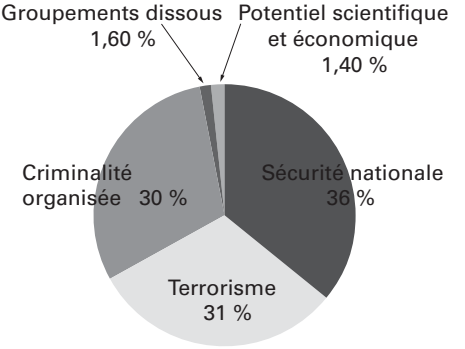
	Demandes initiales		Dont urgences absolues		Accordées	
	2012	2013	2012	2013	2012	2013
TOTAUX	4022	4213	622	812	3994	4176

Répartition des motifs 2013



Les renouvellements d'interceptions

Total des renouvellements demandés : 1924
Répartition des motifs des renouvellements accordés en 2013



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	
2012	2013	2012	2013	2012	2013
3400	3401	622	812	2123	1969

2013

Demandes initiales : 68,15 %. 19,3 % d'entre elles ont été sollicitées selon la procédure de l'urgence absolue.

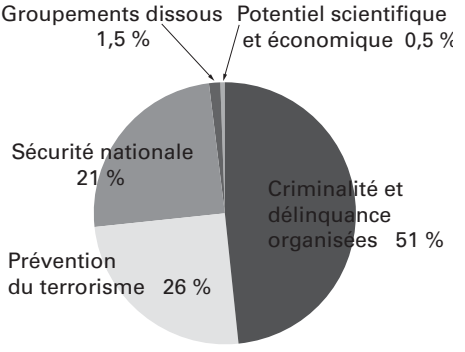
Demandes de renouvellements : 31,85 %.

Demandes d'interceptions : tableau récapitulatif global sur huit ans 2006, 2007, 2008, 2009, 2010, 2011, 2012 et 2013

	2006	2007	2008	2009	2010	2011	2012	2013
Demandes initiales d'interceptions	4203	4 215	4330	3176	3776	4156	4022	4213
Dont « urgences absolues »	714	964	1095	497	522	541	622	812
Demandes de renouvellements	1825	1850	1605	1941	2234	2240	2123	1969
Total	6028	6065	5935	5117	6010	6396	6145	6182

Répartitions des motifs d'interceptions de sécurité accordées en 2013 :

Cumul des demandes initiales et demandes de renouvellements accordées



Répartition entre interceptions et renouvellements accordés

Interceptions accordées en 2013

Interceptions initiales	Renouvellements	Total
4176	1924	6100

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 informatisé et 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, tout en offrant une garantie supplémentaire pour les libertés publiques.

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.

La classification au niveau « secret-défense » des transcriptions des communications interceptées permet une traçabilité parfaite des documents. Ce niveau élevé de protection, que n'offrirait pas une classification « confidentiel-défense », permet une gestion optimale des productions d'interceptions, tant par le GIC que par les services qui en sont destinataires finaux, jusqu'à leur destruction effective et constitue ainsi une garantie en termes de protection des droits des personnes écoutées.

Le contrôle du GIC

Service du Premier ministre, consacré comme tel après 31 années d'existence par le décret no 2002-497 du 12 avril 2002[1], et actuellement dirigé par un officier général, le GIC est un élément clé 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, qui dispose que « *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, puisqu'il n'est pas en charge de l'exploitation du renseignement et des enquêtes, a été considérée par le législateur comme une garantie fondamentale pour la protection des libertés publiques. Elle offre une séparation claire et solide entre « l'autorité qui demande » issue d'un des trois ministères habilités, « l'autorité de contrôle indépendante » qu'est la CNCIS, « l'autorité de décision » qu'est le Premier ministre, et le service qui met en œuvre les moyens d'interception : le GIC.

Au regard de ses attributions, la Commission a toujours réaffirmé l'importance de cette organisation et de ces principes comme une garantie essentielle au bon fonctionnement démocratique des institutions en charge du recueil du renseignement technique.

Le GIC s'adapte en permanence aux avancées technologiques incessantes dans le domaine des communications électroniques qui constituent chaque fois des défis colossaux à relever. Il a ainsi dû intégrer, depuis 1991 la téléphonie mobile, le SMS, le MMS, l'Internet, le dégroupage et la multiplication des opérateurs virtuels.

Conformément à une recommandation prise par la Commission en 1996, le Premier ministre a décidé dès 1997 la mise en place de centres locaux de regroupement des interceptions, sortes de « GIC déconcentrés » répondant aux normes de sûreté 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 administratives. 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.

---

1) CNCIS, 11e rapport - 2002, p. 50.

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, et contrôlé par 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

La CNCIS a poursuivi les visites inopinées ou programmées des services utilisateurs d'interceptions. Lors de ces déplacements, 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, quinze visites de centres d'exploitation et d'échelons centraux 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 problématiques locales et nationales se rapportant aux motifs légaux des interceptions.

Réclamations de particuliers et dénonciations à l'autorité judiciaire

Les saisines de la CNCIS par les particuliers

En 2013, 75 particuliers ont saisi par écrit la CNCIS. Ils n'étaient que 52 en 2012. Cette hausse de près de 50 % semble se poursuivre en 2014 puisque les premières tendances laissent augurer près d'une centaine de saisines. 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 encore en 2013 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 peut sembler insatisfaisante mais il est difficile, notamment au regard des prescriptions de l'article 26 de la loi du 10 juillet 1991 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 no 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 2013, la CNCIS a dû faire usage à deux reprises 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 et de ceux de la « personnalité qualifiée » de l'article 6 de la loi du 23 janvier 2006, exerce un strict contrôle sur ces deux modes de réquisitions administratives, qui doivent fusionner dans un nouveau dispositif le 1er janvier 2015.

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 no 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 aux données techniques de communications.

Ce texte prévoit que les onze services habilités, par le biais du Groupement interministériel de contrôle (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* ». Le GIC, pour satisfaire les demandes, est en relation avec près de soixante-dix opérateurs de réseaux de communications électroniques ou opérateurs virtuels.

Sur ce fondement légal, les demandes d'identification et de données de trafic auprès du GIC sont faites par les services en vue de l'élaboration d'un projet d'interception de sécurité. Ces mesures s'inscrivent dans le cadre de la réalisation visée par la loi, soit l'action de rendre réelle et effective une interception potentielle, 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 de l'article L. 241-2 du Code de la sécurité intérieure (c'est-à-dire 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 ainsi que de la reconstitution ou du maintien de groupements dissous) et par tous les services. Hormis s'agissant de la prévention du terrorisme, ceux du ministère de l'Intérieur 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 Groupement interministériel de contrôle, 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 terrorisme et portant diverses dispositions relatives à 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 proprement dite.

Il encadre très strictement cet accès en le limitant au seul motif de la 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. La Commission nationale de contrôle des interceptions de sécurité même si elle est associée à ces garanties les estime aujourd'hui insuffisantes.

En effet, la loi du 23 janvier 2006 a fait le choix d'un dispositif qui institue une personnalité qualifiée auprès du ministre de l'Intérieur, relevant pour partie de la CNCIS concernant 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 autorisées par la personnalité qualifiée. La loi n° 2012-1432 du 21 décembre 2012 a décidé de proroger « une dernière fois » l'expérimentation, jusqu'au 31 décembre 2015. Le ministre de l'intérieur avait alors souligné devant le Parlement son souhait, de voir regrouper cette procédure particulière dans le droit commun de la procédure de l'article L. 244-2 (débats au Sénat du 16 octobre 2012 et de l'Assemblée nationale du 27 novembre 2012).

L'unification a été décidée par l'article 20 de la loi de programmation militaire du 18 décembre 2013 (amendement déposé au Sénat). Cet article ajoute au titre IV du livre II du Code de la sécurité intérieure un nouveau chapitre 4 comptant cinq articles, entrant en vigueur au 1er janvier 2015. Ces dispositions élargissent aux cinq motifs justifiant des interceptions de sécurité le recueil de données techniques, définissent les conditions de recueil de données techniques « en temps réel » (c'est-à-dire de géolocalisation), enfin décrivent les procédures de demande, de décision et de contrôle.

Section 2 – Statistiques de l'activité pour l'année 2013

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

Au cours de l'année 2013, le Groupement interministériel de contrôle a traité 321 243 demandes. 315 792 d'entre elles portaient sur des mesures d'identification, ainsi que sur des prestations spécifiques comme l'historique d'un identifiant ou l'identification d'une cellule. 5 451 mesures de détails de trafics ont par ailleurs été examinées. L'ensemble des requêtes satisfaites représente une hausse de 61 % par rapport à l'année 2012 [1].

La forte hausse intervenue doit être relativisée puisqu'elle concerne exclusivement les mesures d'identifications (98 % du total des mesures), qui peuvent parfois seulement consister en une consultation d'un annuaire inversé. En revanche, les mesures de détails de trafics (facturations détaillées, trafics géolocalisés, notamment), beaucoup plus intrusives, sont, elles, en baisse de 18 %, et ne représentent désormais que 2 % du total des mesures traitées.

Il convient de rappeler que 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 cinq motifs légaux, y compris en matière de terrorisme, puisqu'ils ne font pas partie des services habilités au titre de l'article 6 de la loi du 23 janvier 2006.

---

1) En 2012, le GIC avait traité 197.097 demandes de prestations annexes, dont 190.431 portaient sur des mesures d'identification, ainsi que sur des prestations spécifiques comme l'historique d'un identifiant ou l'identification d'une cellule, et 6 626 portaient sur des détails de trafics.

Les demandes se répartissent entre les différents motifs légaux de la façon suivante : 71 % d'entre elles portent sur la sécurité nationale, 22 % ont trait à la prévention de la délinquance et de la criminalité organisées, 3 % concernent la prévention du terrorisme, 3 % 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 six années complètes d'expérimentation (de 2008 à 2013), après une augmentation régulière du nombre de demandes présentées par les services, l'année 2011 avait marqué un spectaculaire retournement de tendance, avec 11 635 demandes de moins que l'année précédente. Cette tendance baissière s'était poursuivie en 2012, mais dans une moindre mesure. L'année 2013 montre une hausse des demandes, puisque leur total atteint 36 712 mesures présentées, soit 7 390 de plus qu'en 2012.

	Demandes présentées	**Demandes validées**	**Demandes renvoyées**	**Demandes rejetées**
2008	38 393	34 998	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
2012	29 322	26 563	2 736	23
2013	36 712	34 336	2 372	4
Total sur 6 ans	227 783	205 170	22 357	256

En 2013, et pour la dernière année puisque le mode de calcul a été amélioré dès le 1er janvier 2014, les demandes validées ne correspondent pas au nombre d'objectifs. 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. Depuis le début de l'année 2014, la comptabilisation s'effectue, comme pour les interceptions de sécurité, par « cible », puisque chaque dossier correspond à un « objectif » et peut contenir plusieurs mesures d'identification ou de détail de trafic.

La typologie des mesures sollicitées par les services est identique quelle que soit la période d'exercice, soit près de 65 % de demandes d'identification d'abonnés. Ces mesures sont moins intrusives que les demandes portant sur les détails de trafic qui représentent près de 35 % des dossiers traités.

La diminution du recours au dispositif de l'article 6 par les services en charge de la prévention du terrorisme, évoquée dans les rapports d'activité des années 2010, 2011 et 2012, ne manquait pas de surprendre dans un contexte de forte menace terroriste. Si l'année 2013 marque une hausse du nombre des demandes, elle ne permet pas de retrouver le niveau de 2010, année où 45 716 demandes avaient été présentées.

Dans ses deux précédents rapports, la CNCIS avait tenté de dresser l'inventaire des principaux facteurs susceptibles d'expliquer cette baisse, alors que la France se trouve depuis quelques années dans un contexte de menaces terroristes élevées. Les constatations et analyses faites sur la période 2012-2013 confirment les principales hypothèses évoquées à l'époque, notamment celle d'une utilisation plus ciblée des mesures au regard de leurs conditions d'accès et des résultats qu'elles permettent en matière de renseignement.

Sur ce dernier point, il appert que les mesures dont les résultats confirment les hypothèses d'enquête aboutissent dans la quasi-totalité des cas à des demandes d'interception de sécurité dont une partie de la motivation repose sur les renseignements issus du recueil de données techniques de communications.

Par ailleurs, l'obsolescence de l'ancienne plate-forme de traitement des demandes – définitivement arrêtée début 2014 après plus de six années durant lesquelles elle a correctement rempli son office – et les lenteurs qu'elle pouvait générer avant l'aboutissement des procédures, ont pu également contribuer, d'après les éléments recueillis sur le terrain par la CNCIS lors de ses rencontres avec les enquêteurs, à une certaine désaffection pour le dispositif.

Ces constats confirmaient l'intérêt d'un cadre légal unique et général régissant les interceptions de communications et le recueil de leurs données, qu'appelait de ses vœux la Commission depuis plusieurs années. À ce titre, l'article 20 de la loi no 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 constitue un progrès, mais dont le résultat demeure très imparfait.

Sur les données chiffrées, il faut encore mentionner qu'en 2013, les services de la DCRI et de la DRPP ont été à l'origine de 99 % des 39 712 requêtes présentées dans le cadre du dispositif de l'article 6, ce qui constitue une donnée en légère hausse par rapport à l'année précédente.

Concernant les services à vocation judiciaire, qui emploient ce dispositif au titre du renseignement et de la prévention du terrorisme, 431 demandes ont été formulées, essentiellement par la DGGN (79,5 %) et la DCPJ (20,5 %).

Les mesures sollicitées visent les moyens de communication électronique suivants :

	2008	2009	2010	2011	2012	2013
Téléphonie fixe	13,81 %	17,96 %	21,02 %	19,58 %	19,84 %	20,19 %
Téléphonie mobile	82,10 %	70,03 %	68,11 %	66,38 %	67,23 %	67,08 %
Internet	4,09 %	12,01 %	10,87 %	14,04 %	12,93 %	12,73 %

Ces chiffres permettent un triple constat :
• la téléphonie mobile reste la technologie qui motive le plus grand nombre de demandes ;
• le nombre des requêtes concernant la téléphonie fixe reste stable depuis trois ans autour de 20 % ;
• les prestations Internet sont stables autour de 13 %.

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

Les demandes faites par les services doivent comporter des renseignements précis sur l'objectif et le moyen de communication visé. Elles doivent être motivées. Ces éléments sont indispensables tant dans la phase d'autorisation que du contrôle *a posteriori*.

Les requêtes fondées sur l'article 6 de la loi du 23 janvier 2006 sont autorisées 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 de la sécurité intérieure sont validées par les personnels de permanence et de direction du Groupement interministériel de contrôle.

La loi a conféré à la CNCIS la responsabilité de contrôler *a posteriori* l'activité de ces deux entités et 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 une recommandation au ministre de l'Intérieur en 2013, à laquelle il a été apporté une réponse conformément à la loi.

S'agissant du contrôle de légalité *a priori* et de la validation, la «personnalité qualifiée » a privilégié le recours régulier aux demandes de renseignements complémentaires avant validation ou refus. Le nombre de refus est ainsi resté à un niveau extrêmement bas (0,01 % en 2013).

Les motifs principaux de refus, 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.

La plupart des recommandations adressées au ministre de l'Intérieur depuis l'instauration du régime expérimental de l'article 6 ont eu pour objet de rappeler sa vocation exclusivement préventive et de renseignement. Par décision nº 2005-532 DC du 19 janvier 2006, le Conseil constitutionnel a en effet réaffirmé ce principe à propos de ce dispositif instauré par la loi du 23 janvier 2006, en rappelant la primauté de l'autorité judiciaire dans le domaine de la répression.

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 Groupement interministériel de contrôle afin d'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 aux libertés 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. Elle dispose ainsi d'éléments lui permettant d'apprécier la pertinence des demandes au regard des principes de proportionnalité et de subsidiarité.

Section 4 – Réflexions sur le projet d'unification partielle au 1er janvier 2015 des cadres légaux du recueil de données techniques de communications en matière de police administrative

Rappel d'éléments de droit comparé

Les deux précédents rapports avaient déjà abordé les 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, Canada et Turquie, notamment).

Il ressort de ces analyses comparées que certaines législations prévoient un régime unique pour les demandes d'interceptions et celles portant sur des 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 rencontrées et les organismes étrangers consultés 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 portée au secret des correspondances et à la vie privée.

Éléments de l'évaluation continue faite par la CNCIS

La CNCIS conduit en permanence, en sa qualité d'organe de contrôle de la légalité chargé de la protection du secret des correspondances privées par voie électronique, une évaluation des cadres légaux de recueil de données techniques de communications, et ce depuis la mise en œuvre effective de la dualité de dispositifs en 2007.

En 2012, dans la perspective du renouvellement envisagé du cadre expérimental de l'article 6 de la loi du 23 janvier 2006, la CNCIS avait procédé à un bilan complet et argumenté de ce dispositif, que le président a pu exposer lors d'auditions devant les Commissions des lois du Sénat puis de l'Assemblée nationale en octobre 2012 dans le cadre

des travaux préparatoires de la loi nº 2012-1432 du 21 décembre 2012, qui a prorogé une dernière fois, pour trois ans l'expérience conduite.

Cette évaluation a aussi été menée au regard des évolutions du dispositif du Groupement interministériel de contrôle (GIC) sur les interceptions de sécurité et 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 lorsqu'elle est mise en œuvre par les services habilités des ministères de la Défense et du Budget.

Cette analyse s'est appuyée sur les avis et les recommandations antérieurs de la CNCIS, en particulier son avis issu de sa formation plénière du 14 septembre 2005, qui 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 paraît 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.*»

Dans le cadre des auditions devant les Commissions des lois des deux chambres parlementaires en octobre 2012, la CNCIS a rappelé que la juxtaposition de deux régimes qui offrent les mêmes prestations, mais selon des modalités de fonctionnement juridiques et techniques différentes, était source de confusion pour les services utilisateurs, d'erreurs dans le choix du cadre procédural, voire dans certains cas de tentatives pour utiliser successivement l'un et l'autre des cadres en cas de refus d'une des autorités décisionnaires.

Elle a également souligné 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). Dès lors, la coexistence de deux dispositifs cloisonnés peut entraîner des difficultés dans le travail d'investigation et de renseignement, ainsi que dans la mise en œuvre d'un régime unique et cohérent de protection des correspondances privées par voie des communications électroniques.

Elle a rappelé que 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.

La Commission a noté avec satisfaction que son analyse avait été très largement reprise lors des débats parlementaires ayant conduit à l'adoption de la loi nº 2012-1432 du 21 décembre 2012, tant par le ministre de l'Intérieur que par les principaux orateurs des différents groupes. L'unification des dispositifs semblait devenue un objectif consensuel.

De plus, la convergence «technique» est, de fait, effective depuis le 1er janvier 2014 puisque la plate-forme de l'UCLAT, qui permettait depuis 2007 le recueil des données techniques de communications sollicitées dans le cadre de l'article 6 de la loi du 23 janvier 2006 a été fermée sur décision du gouvernement début 2014. Ces missions sont désormais reprises par le Groupement interministériel de contrôle, qui a conçu pour ce faire une nouvelle plate-forme, permettant un traitement beaucoup plus fluide et sécurisé des demandes.

L'article 20 de la loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire (LPM) pour les années 2014 à 2019

Issu d'un amendement d'origine parlementaire lors des débats au Sénat, ce texte vise à unifier les cadres de recueil de données de connexions dans un dispositif interministériel, sous l'autorité du Premier ministre et le contrôle de la CNCIS. Il prévoit l'instauration d'une procédure administrative de géolocalisation en temps réel, dont le régime juridique est quasi-identique à celui des interceptions de sécurité.

Il ne modifie pas le référentiel des mesures qui peuvent être sollicitées par les services de renseignement et ne comporte aucune disposition d'accès aux contenus de communications électroniques, qui relèvent du régime des interceptions de sécurité.

Ce nouveau dispositif, qui pourrait entrer en vigueur le 1er janvier 2015, doit faire l'objet, s'agissant du futur article L. 246-4 du Code de la sécurité intérieure, d'un décret d'application, pris en Conseil d'État, après avis de la Commission nationale de l'informatique et des libertés (CNIL) et de la CNCIS. La CNCIS a été consultée et a rendu un avis en octobre 2014.

Si le régime prévu par l'article 20 de la LPM constitue un net progrès par rapport au projet initial du gouvernement, puisqu'il tient compte partiellement des préconisations de la CNCIS, il demeure perfectible. En effet, il maintient une pluralité de procédures et de décisionnaires distincts pour les différentes mesures qui peuvent être sollicitées autour du recueil de renseignements liés aux communications électroniques.

Alors que la volonté de la CNCIS lors des débats relatifs à la loi de programmation militaire était d'aboutir à une unification des dispositifs et des procédures et qu'elle avait, en la personne d'un de ses membres parlementaires, déposé un amendement en ce sens, l'article 20 dans sa forme définitive ne permet d'aboutir qu'imparfaitement à ce résultat. Non

seulement la «personnalité qualifiée», qui est maintenue, continuera à prendre des décisions en l'absence d'avis de la CNCIS et sans regard possible du Premier ministre ou de son délégué qui autorise les interceptions de sécurité, mais, au surplus, une nouvelle procédure distincte vient s'ajouter aux deux existantes, s'agissant des autorisations de géolocalisation en temps réel. Le risque d'incohérence entre les différentes autorisations qui seront données concernant un même objectif est donc grand.

La CNCIS rappelle sa préférence, déjà exprimée dans les rapports précédents et lors des auditions devant les assemblées parlementaires, pour la définition d'un régime unique dans le cadre de la loi du 10 juillet 1991, aujourd'hui titre IV du livre II du Code de la sécurité intérieure, basé sur la quadruple distinction entre l'autorité qui demande, celle qui contrôle, celle qui autorise et celle qui met en œuvre.

En effet, ce texte garantirait l'équilibre entre, d'une part, les impératifs de sécurité, 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 se place sous le contrôle de légalité d'une autorité administrative indépendante.

Ce modèle, qui fonctionne depuis plus de vingt ans pour les interceptions de sécurité offre un cadre légal pertinent et fondé juridiquement pour le recueil des données techniques de communications. Il suppose un contrôle préalable systématique de la Commission, quelle que soit la mesure, avant une décision qui relèvera du Premier ministre ou de ses délégués.

Face aux menaces et aux objectifs précités, cette réponse paraît plus appropriée 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 et des mesures d'investigation actuelles comme futures.

Il faut désormais que ce projet soit concrétisé par une modification législative. La CNCIS souhaite vivement que cette réforme, indispensable et urgente, qui idéalement pourrait s'inscrire dans une grande loi sur les actes du renseignement, attentatoires aux libertés individuelles, intervienne le plus rapidement possible.

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 dite « R. 226 » dont la CNCIS est membre permanent.

Depuis le décret n° 97-757 du 10 juillet 1997, la CNCIS a toujours soutenu qu'un contrôle plus efficace des interceptions de sécurité devait porter non seulement sur les demandes d'interception et leur exploitation par les services de l'État, mais également sur les matériels et les équipements acquis, importés, détenus et utilisés par des sociétés privées et les services de l'État, qui comportent des possibilités d'interceptions des communications électroniques attentatoires aux droits des personnes.

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 07 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 aujourd'hui abrogé et remplacé par l'arrêté du 4 juillet 2012 fixant la liste d'appareils et de dispositifs techniques prévue par l'article 226-3 du Code pénal, participe

d'une évolution de l'appréhension de ce secteur d'activité sensible par la puissance publique[1]. 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[2].

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 d'inflexion dans la qualification du caractère « sensible » de ce type de matériel par les pouvoirs publics.

Ainsi, le décret 2005-1739 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 2013. Sa composition est la suivante :
– le directeur général de l'Agence nationale de la 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 2013, la Commission a connu, pour la première fois après plusieurs années de hausse continue, une légère diminution du nombre de ses décisions. Elle a ainsi rendu 840 décisions (contre 558 en 2009, 643 en 2010 et 883 en 2011, 970 en 2012) ventilées comme suit :
. 431 décisions d'autorisation initiale (267 concernant la commercialisation, 164 l'acquisition d'équipements soumis à autorisation) ;
. 89 décisions de renouvellement d'autorisation ;
. 254 décisions d'ajournement ;
. 9 décisions de radiation ou d'annulation ;
. 20 décisions de refus ou de retrait ;
. 37 décisions de mise « hors champ » de l'examen pour autorisation.

1) *Cf.* rapport 2004, p. 34-38 ; rapport 2005, p. 31-33.
2) *Cf.* rapport 2004, p. 38.

La baisse du nombre de décisions, en valeur absolue, n'est absolument pas synonyme d'une diminution de l'activité de la commission consultative. En effet, les dossiers qui lui sont soumis sont de plus en plus complexes, comme le démontre l'augmentation du nombre de décisions d'ajournements (+17 %) rendues nécessaires par le besoin de solliciter des compléments techniques ou administratifs aux auteurs des demandes, dont les dossiers sont trop souvent incomplets. Bon nombre de dossiers que la commission a été contrainte d'ajourner en 2013 ont été traités début 2014. Les premières tendances pour l'exercice en cours laissent d'ailleurs présager une nouvelle et forte hausse du nombre de décisions rendues en 2014.

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[1], à produire leurs registres et à décrire leurs règles internes de gestion des matériels sensibles. Sans préjudice des autres contrôles qui peuvent être opérés sur pièces et sur place par la commission consultative ou par l'autorité administrative indépendante en vertu de ses pouvoirs propres, l'examen de ces demandes permet aux représentants de la CNCIS de s'assurer du respect des règles adoptées en matière d'emploi, ainsi que de l'adéquation des matériels détenus avec les missions confiées à ces services.

Par ailleurs, la loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale (LPM) a élargi le champ de deux incriminations pénales[2] réprimant les cas de fabrication, de détention ou d'utilisation de matériels pouvant servir à enregistrer des conversations privées, à capter des données informatiques ou à intercepter des correspondances.

L'extension consiste à couvrir non plus seulement les seuls matériels conçus pour commettre des atteintes à la vie privée mais également ceux qui sont « de nature à permettre » une utilisation à ces fins. Cette modification de la loi implique un réexamen de l'arrêté du 4 juillet 2012 fixant la liste d'appareils et de dispositifs techniques prévue par l'article 226-3 du Code pénal.

Si le degré de protection attaché aux travaux de cette commission dite « R. 226 » ne permet pas d'en détailler le contenu, la CNCIS rappelle que ses avis au sein de cette structure reposent sur le souci

1) *Cf.* rapport 2001, p. 27.
2) Prévues et réprimées par les articles 226-1 à 226-3 et 226-15 du Code pénal (atteintes à la vie privée et au secret des correspondances).

constant de protéger les citoyens contre tout enregistrement à leur insu de communications ou de données qui y sont rattachées, et ce en raison d'un emploi inadapté ou frauduleux des fonctionnalités d'interception et de captation, offertes par certains matériels.

Les facilités que peuvent avoir certaines personnes privées, y compris appartenant au crime organisé, pour accéder à ce type de matériels particulièrement sensibles et en faire un usage contraire à la loi, démontrent plus que jamais la nécessité d'une vigilance toujours accrue des autorités et la nécessité que le législateur renforce les moyens de contrôle, notamment de la CNCIS, dans ce domaine.

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 des 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 prévention de la reconstitution ou du maintien de groupements dissous, le motif d'interception le plus faible en volume, bien qu'il connaisse quelques développements 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 du Code pénal 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 (article 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 Ve République ou à la sécurité nationale.

Le décret n° 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, page 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*. Néanmoins, les cadres juridiques européens et nationaux contribuent à guider la réflexion de la Commission en ce domaine. Ainsi, certains mouvements sont identifiés comme terroristes par les décisions du Conseil de l'Union européenne en la matière.

Par ailleurs, 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.

En outre, la loi nº 2012-1432 relative à la sécurité et à la lutte contre le terrorisme du 21 décembre 2012 renforce les sanctions contre ceux qui se rendent coupables d'apologie ou de provocation au terrorisme sur internet.

Elle prévoit la poursuite par la justice française des actes de terrorisme commis à l'étranger par des Français ou des personnes résidant habituellement en France, en permettant d'incriminer les personnes ayant participé à des camps d'entraînement terroristes à l'étranger alors même qu'elles n'auront pas commis d'actes répréhensibles sur le territoire français.

Enfin, la dernière loi renforçant les dispositions relatives à la lutte contre le terrorisme qui a été adoptée par le Parlement en octobre 2014 complète notamment la liste définissant les actes de terrorisme afin de rajouter la diffusion de procédés permettant la fabrication d'engins de destruction, la détention de produits incendiaires ou explosifs ou d'éléments entrant dans la composition de produits ou engins explosifs. Elle incrimine également l'entreprise terroriste individuelle.

Ces récentes modifications du cadre pénal national emportent des conséquences sur la définition et la déclinaison du motif « prévention du terrorisme » à partir duquel peut être autorisé et mis en œuvre, dans le cadre de la police administrative, une interception de sécurité ou un recueil de données techniques de communications.

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 la criminalité et à la délinquance organisées », concernant l'ensemble des infractions aggravées par la circonstance de commission en bande organisée (*cf.* article 706-73 du Code de procédure pénale).

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 organisés ». Elle entendait par là se référer à des infractions qui avaient justifié, au plan administratif, la création d'offices spécialisés tels que l'OCRB (Office central pour la répression du banditisme)[1]. La Commission souhaitait 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

1) Remplacé par l'Office central de lutte contre le crime organisé (OCLCO) depuis 2006.

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 en 1994, 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 no 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, au plus, 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 le degré d'organisation, notamment le nombre de personnes sciemment impliquées dans le processus criminel, et la gravité des peines encourues.

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 revêtent pas cette 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.

Il est donc permis de dire que la CNCIS retient, pour l'application du motif prévu à l'article L. 241-2 du Code la sécurité intérieure, une définition de la criminalité organisée qui recouvre totalement le champ couvert aujourd'hui par l'article 706-73 du Code de procédure pénale.

Elle exclut de ce fait l'essentiel des infractions financières commises en bande organisée, lesquelles relèvent en grande majorité de l'article 706-74 du Code de procédure pénale.

La décision du Conseil constitutionnel n° 2014-420/421 QPC du 9 octobre 2014, qui a déclaré inconstitutionnel le 8° bis de l'article 706-73 du Code de procédure pénale relatif à l'escroquerie en bande organisée, ne fait que renforcer la position de la CNCIS.

Le Conseil a relevé dans son considérant n° 13 que, « *même lorsqu'il est commis en bande organisée, le délit d'escroquerie n'est pas susceptible de porter atteinte en lui-même à la sécurité, à la dignité ou à la vie des personnes* ».

Bien que cette observation ait été formulée à propos de la mesure de garde à vue, elle ne peut que faire écho aux restrictions fixées par la CNCIS quant à la liste des infractions pouvant donner lieu à une interception de sécurité, dans le souci constant de se conformer au caractère exceptionnel que doit conserver le recours à cette mesure particulièrement attentatoire aux libertés.

Si la Commission accepte actuellement de prendre en considération, et ce depuis la loi n° 2011-525 du 17 mai 2011, l'escroquerie en bande organisée, la décision du Conseil constitutionnel et les conséquences qui en seront tirées sur le plan législatif, pourrait la conduire à réexaminer sa position.

Toutefois, sur le fondement des définitions de la bande organisée et de l'association de malfaiteurs précitées, constatant le caractère exceptionnel de certains projets criminels, ainsi que la gravité des atteintes présumées, l'Assemblée plénière a pu émettre des avis favorables pour des demandes portant sur des faits de nature à porter atteinte à la vie ou, de manière grave, à la santé publique, alors que ces infractions n'étaient explicitement visées à l'article 706-73 du Code de procédure pénale.

L'ampleur du trafic présumé, les modalités de commission des infractions projetées (notamment leur aspect international), les risques d'atteinte à la santé des victimes, comparables par leurs effets aux intérêts protégés par les incriminations de l'article 706-73, ont fondé ces avis favorables, au cas par cas, dans la mesure où les faits revêtaient le caractère exceptionnel visé par la loi pour autoriser une interception de sécurité.

Prévention de la reconstitution ou du maintien de groupements dissous

Ce motif est directement lié à la mise en œuvre des dispositions de l'ancienne loi du 10 janvier 1936 sur les groupes de combat et les milices privées, désormais abrogée[1] et codifiée à l'article L. 212-1 du Code de la sécurité intérieure.

Ce texte dispose que sont dissous, par décret en Conseil des ministres, toutes les associations ou groupements de fait :
1° Qui provoquent à des manifestations armées dans la rue ;
2° Ou qui présentent, par leur forme et leur organisation militaires, le caractère de groupes de combat ou de milices privées ;
3° Ou qui ont pour but de porter atteinte à l'intégrité du territoire national ou d'attenter par la force à la forme républicaine du Gouvernement ;
4° Ou dont l'activité tend à faire échec aux mesures concernant le rétablissement de la légalité républicaine ;
5° Ou qui ont pour but soit de rassembler des individus ayant fait l'objet de condamnation du chef de collaboration avec l'ennemi, soit d'exalter cette collaboration ;
6° Ou qui, soit provoquent à la discrimination, à la haine ou à la violence envers une personne ou un groupe de personnes à raison de leur origine ou de leur appartenance ou de leur non-appartenance à une ethnie, une nation, une race ou une religion déterminée, soit propagent des idées ou théories tendant à justifier ou encourager cette discrimination, cette haine ou cette violence ;
7° Ou qui se livrent, sur le territoire français ou à partir de ce territoire, à des agissements en vue de provoquer des actes de terrorisme en France ou à l'étranger.

Depuis 1936, près d'une centaine d'organisations ont ainsi fait l'objet d'une dissolution sur la base de ces dispositions légales.

Les interceptions de sécurité fondées sur ce motif suppose que l'objectif soit suspecté d'implication directe et personnelle dans des activités laissant présumer une volonté de reconstituer ou maintenir un groupement dissous, sans pour autant que le service demandeur dispose des éléments suffisants pour caractériser l'un des délits prévus et réprimés par la section 4 du chapitre Ier du titre III du livre IV du Code pénal[2].

---

1) Par l'ordonnance nº 2012-351 du 12 mars 2012.
2) Les articles 431-13 à 431-21 du Code pénal portent sur le maintien ou la reconstitution d'une association ou d'un groupement dissous en application de l'article L 212-1 du Code de la sécurité intérieure, ou l'organisation de ce maintien ou de cette reconstitution, ainsi que l'organisation d'un groupe de combat.

L'éventualité d'une évolution du nombre de motifs légaux

Dans le cadre des réflexions actuelles portant sur l'élaboration d'un projet de loi sur le cadre légal du renseignement, certains, parmi les universitaires[1] ou les praticiens, plaident pour une évolution du nombre ou de la définition des motifs légaux adoptés par le législateur en 1991. La CNCIS n'est pas hostile par principe à améliorer l'adéquation des définitions aux besoins des services de renseignement. Elle restera, dans l'hypothèse d'une révision de ces motifs légaux, extrêmement vigilante quant au maintien de définitions précises et restrictives, afin de respecter le caractère exceptionnel des raisons pouvant autoriser le recours à une interception de sécurité.

1) Parmi lesquels le professeur Bertrand Warusfel, qui avait évoqué sa vision du motif « sécurité nationale » dans le rapport de l'an dernier : *Commission nationale de contrôle des interceptions de sécurité, 21e rapport d'activité*, Paris, la Documentation française, 2013, 172 p., pages 17 *et sq.*

Chapitre 2

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, lesquelles donnent compétence à la CNCIS pour rendre des avis et exercer son contrôle

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. 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 cet article.

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 donc des mesures de surveillance hors de tout contrôle de la CNCIS, seulement lorsque trois conditions cumulatives sont remplies :
– 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 L244-2 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 et 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 évidemment pas, par nature, sauf dans le cas très restrictif prévu à l'article L. 241-3 (aux seules fins de défense des intérêts nationaux), au contrôle de la CNCIS.

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.

Aujourd'hui, force est de constater que la définition de l'article L. 241-3 est obsolète et qu'au regard de l'usage que peuvent légalement en faire les services, pour autant qu'il soit connu, cette disposition semble devenue inutile. Sa suppression doit être envisagée dans le cadre des travaux parlementaires à venir.

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 [1] :
– 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* 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

1) *Cf.* Partie 1 chapitre 4.

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 communications, 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 jour, la Commission est amenée à donner son avis sur plusieurs dizaines de demandes initiales ou de renouvellement d'interceptions de sécurité présentées selon la procédure normale. En outre, et comme cela a déjà été indiqué dans les éléments chiffrés relatant son activité, elle statue à toute heure 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.

Pour l'application de ces critères, 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 des relations avec d'autres individus.

Une motivation pertinente

L'examen de cette pertinence porte sur 3 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 chacun des 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, tout comme les demandes de renseignements complémentaires.

Les avis défavorables sont en légère hausse, mais restent très peu nombreux. 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. En moyenne, depuis 1991, il y est fait recours dix à quinze fois par an. Elles sont en principe 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 pour un réexamen de l'interception et de son exploitation par rapport à l'autorisation et aux dispositions légales. Cela concerne, en moyenne une cinquantaine de mesures par an, qui sont toutes suivies d'une interruption, à l'initiative du service, dans un bref délai.

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.

La présentation délibérément inexacte des faits dans les 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, ainsi 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 nº 91-646 du 10 juillet 1991, devenu l'article L. 241-1 du Code de la sécurité intérieure :

« 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 nº 2002-1138 du 9 septembre 2002 et 2004-204 du 9 mars 2004, modifiée dernièrement par la loi nº 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 nº 91-646 du 10 juillet 1991 (abrogée depuis le 1er mai 2012 conformément à l'article 19, *20°*, de l'ordonnance nº 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. Elle comporte cinq titres, dont le premier sur les interceptions judiciaires et le second sur les interceptions de sécurité.

Les interceptions judiciaires

Titre I (de la loi nº 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 nº 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 nº 2004-204 du 9 mars 2004, art.5. « Aucune interception ne peut avoir lieu sur une ligne dépendant du cabinet d'un magistrat ou de son domicile sans que le premier président ou le procureur général de la juridiction où il réside en soit informé. »

Loi nº 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'extradition (*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 I^er^ : De l'exercice de l'action publique et de l'instruction

Titre III : Des juridictions d'instruction

Chapitre I^er^ : 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 1^er^ du titre III du livre I^er^. 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[1], 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 […]. »

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 no 2007-297 du 5 mars 2007 – article 72 *JORF* 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 « des personnes détenues »[2] peuvent, à l'exception de celles avec leur

1) La loi no2011-267 du 11 mars 2011 a fait passer la durée légale de 15 jours à un mois, renouvelable une fois.
2) Loi n° 2009-1436 du 24 novembre 2009, art 97-II.

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[1].

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. »

Titre II (de la loi nº 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 nº 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 nº 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.

1) Décret nº 2010-1635 du 23 décembre 2010 portant application de la loi pénitentiaire et modifiant le Code de procédure pénale (troisième partie : Décrets).

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 nº 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 quarante-huit 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 nº 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 nº 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 nº 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 nº 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 € 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 « de nature à permettre la réalisation d'opérations »[1] 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

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

1) Nouvelle rédaction issue de l'article 23 de la n° 2013-1168 relative à la programmation militaire.

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 de « 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 nº 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 nº 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 nº 2004-575 du 21 juin 2004 précitée. »

Titre V (de la loi nº 91-646 du 10 juillet 1991 consolidée) :

DISPOSITIONS FINALES

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

Le titre IV « Interceptions de sécurité » du Livre II « Ordre et sécurité publics » du Code de la sécurité intérieure [2]

1) Substitué dans le nouveau Code pénal à l'article 378, mentionné dans la loi du 10 juillet 1991.
2) 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 nº 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 quarante-huit 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, 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-qui concerne les demande 575 du 21 juin 2004 pour la confiance dans l'économie numérique en ce s 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 Ier du titre III du livre Ier 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.

Les textes réglementaires récents visant la loi du 10 juillet 1991

Code de la sécurité intérieure

Partie réglementaire

LIVRE II : ORDRE ET SÉCURITÉ PUBLICS

TITRE IV : INTERCEPTIONS DE SÉCURITÉ

Chapitre II : Conditions des interceptions (ex-décret nº 2002-497 du 12 avril 2002 relatif au groupement interministériel de contrôle)

Section 1 : Groupement interministériel de contrôle (Créée par Décret n°2013-1113 du 4 décembre 2013)

Article R. 242-1

Le groupement interministériel de contrôle est un service du Premier ministre chargé des interceptions de sécurité.

Article R. 242-2

Le groupement interministériel de contrôle a pour missions :
1° de soumettre au Premier ministre les propositions d'interception présentées dans les conditions fixées par l'article L. 242-1 ;
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 L. 242-4, ainsi qu'à la destruction des enregistrements effectués, dans les conditions fixées par l'article L. 242-6.

Article R. 242-3

Le directeur du groupement interministériel de contrôle est nommé par arrêté du Premier ministre.

Décret nº 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 nº 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 nº 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 nº 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 nº 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 nº 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 nº 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 nº 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

Codifié désormais au sein du Code de la sécurité intérieure, Livre II, Titre II, chapitre II (ordonnance n° 2012-351 du 12 mars 2012) :

Article L. 222-2

Les agents dûment habilités des services de la police et de la gendarmerie nationales spécialement chargés de la prévention des actes de terrorisme peuvent accéder aux données conservées par les opérateurs de communications électroniques dans les conditions définies à l'article L. 34-1-1 du Code des postes et des communications électroniques.

Article L. 222-3

Les agents dûment habilités des services de la police et de la gendarmerie nationales spécialement chargés de la prévention des actes de terrorisme peuvent accéder aux données conservées par les prestataires de services de communication au public en ligne dans les conditions définies au II bis de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.
Et, au Livre II, titre IV, chapitre III :

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.

Ces articles appellent 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 ces articles :

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 article 77-1-1 du Code de procédure pénale) et réquisitions administratives (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 qui délimite les interceptions judiciaires (article 100 à 100-7 du Code de procédure pénale) et les 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.

Loi n° 2012-1432 du 21 décembre 2012 relative à la sécurité et à la lutte contre le terrorisme

Article 1er

À la fin du dernier alinéa de l'article L. 222-1 du Code de la sécurité intérieure et du premier alinéa de l'article 32 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, l'année : « 2012 » est remplacée par l'année : « 2015 ».

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 No 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 No 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 « de nature à permettre la réalisation d'opérations »[1] 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.

---

1) Nouvelle rédaction issue de l'article 23 de la loi n°2013-1168 du 18 décembre 2013 relative à la programmation militaire

– 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 secrétariat général de la défense et de la sécurité nationale.

• Le 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.

• 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, abrogé et remplacé par l'arrêté du 4 juillet 2012 :

Arrêté du 4 juillet 2012 fixant la liste d'appareils et de dispositifs techniques prévue par l'article 226-3 du Code pénal

NOR : PRMD1230326A

Le Premier ministre,

Vu la directive 98/34/CE du Parlement européen et du Conseil du 22 juin 1998 modifiée prévoyant une procédure d'information dans le domaine des normes et réglementations techniques et des règles relatives aux services de la société de l'information ;

Vu le Code pénal, notamment les articles 226-3, R. 226-1 et suivants ;

Vu le Code de procédure pénale, notamment les articles 706-102-1 et suivants ;

Vu l'avis de la commission consultative instituée par l'article R. 226-2 du Code pénal en date du 13 septembre 2011 ;

Vu la notification à la Commission européenne no 2012/65/F du 1er février 2012,

Arrête :

Article 1

La liste prévue par l'article 226-3 du Code pénal des appareils et des dispositifs techniques soumis à l'autorisation mentionnée à l'article R. 226-3 de ce Code figure en annexe I au présent arrêté.

Article 2

La liste prévue par l'article 226-3 du Code pénal des appareils et des dispositifs techniques soumis à l'autorisation mentionnée à l'article R. 226-7 de ce Code figure en annexe II au présent arrêté.

Article 3

L'arrêté du 29 juillet 2004 fixant la liste d'appareils prévue par l'article 226-3 du Code pénal est abrogé.

Article 4

Le directeur général de l'Agence nationale de la sécurité des systèmes d'information est chargé de l'exécution du présent arrêté, qui sera publié au *Journal officiel de la République française.*

Annexes

Article Annexe I

APPAREILS ET DISPOSITIFS TECHNIQUES SOUMIS À AUTORISATION EN APPLICATION DE L'ARTICLE R. 226-3 DU CODE PÉNAL

1. Appareils, à savoir tous dispositifs matériels et logiciels, conçus pour réaliser l'interception, l'écoute, l'analyse, la retransmission,

l'enregistrement ou le traitement de correspondances émises, transmises ou reçues sur des réseaux de communications électroniques, opérations pouvant constituer l'infraction prévue par le deuxième alinéa de l'article 226-15 du Code pénal.

Entrent notamment dans cette catégorie :
– les appareils dont les fonctionnalités qui participent à l'interception, l'écoute, l'analyse, la retransmission, l'enregistrement ou le traitement de correspondances ne sont pas activées, quel que soit le moyen d'activation ;
– les appareils permettant, par des techniques non intrusives d'induction électromagnétique ou de couplage optique, d'intercepter ou d'écouter les correspondances transitant sur les câbles filaires ou les câbles optiques des réseaux de communications électroniques.

N'entrent pas dans cette catégorie :
– les appareils de tests et de mesures utilisables exclusivement pour l'établissement, la mise en service, le réglage et la maintenance des réseaux et systèmes de communications électroniques ;
– les appareils conçus pour un usage grand public et permettant uniquement l'exploration manuelle ou automatique du spectre radioélectrique en vue de la réception et de l'écoute de fréquences ;
– les dispositifs permettant de réaliser l'enregistrement des communications reçues ou émises par des équipements terminaux de télécommunications, lorsque cet enregistrement fait partie des fonctionnalités prévues par les caractéristiques publiques de ces équipements.

2. Appareils qui, spécifiquement conçus pour détecter à distance les conversations afin de réaliser à l'insu du locuteur l'interception, l'écoute ou la retransmission de la parole, directement ou indirectement, par des moyens acoustiques, électromagnétiques ou optiques, permettent de réaliser l'infraction prévue par l'article 226-1 du Code pénal.

Entrent dans cette catégorie :
– les dispositifs microémetteurs permettant la retransmission de la voix par moyens hertziens, optiques ou filaires, à l'insu du locuteur ;
– les appareils d'interception du son à distance de type microcanon ou équipés de dispositifs d'amplification acoustique ;
– les systèmes d'écoute à distance par faisceaux laser.

3. Dispositifs techniques, à savoir tous matériels ou logiciels, spécifiquement conçus pour, sans le consentement des intéressés, accéder aux données informatiques, les enregistrer, les conserver et les transmettre, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données ou telles qu'il les y introduit par saisie de caractères, opérations ayant pour objet la captation de données informatiques prévue par l'article 706-102-1 du Code de procédure pénale.

N'entrent pas dans cette catégorie les dispositifs de tests et de mesures des signaux radioélectriques émis par un équipement électronique destinés exclusivement à évaluer la compatibilité ou le champ électromagnétique.

Article Annexe II

APPAREILS ET DISPOSITIFS TECHNIQUES SOUMIS À AUTORISATION EN APPLICATION DE L'ARTICLE R. 226-7 DU CODE PÉNAL

1. Appareils, à savoir tous dispositifs matériels et logiciels, conçus pour réaliser l'interception, l'écoute, l'analyse, la retransmission, l'enregistrement ou le traitement de correspondances émises, transmises ou reçues sur des réseaux de communications électroniques, opérations pouvant constituer l'infraction prévue par le deuxième alinéa de l'article 226-15 du Code pénal.

Entrent notamment dans cette catégorie :
– les appareils dont les fonctionnalités qui participent à l'interception, l'écoute, l'analyse, la retransmission, l'enregistrement ou le traitement de correspondances ne sont pas activées, quel que soit le moyen d'activation ;
– les appareils permettant, par des techniques non intrusives d'induction électromagnétique ou de couplage optique, d'intercepter ou d'écouter les correspondances transitant sur les câbles filaires ou les câbles optiques des réseaux de communications électroniques.

N'entrent pas dans cette catégorie :
– les appareils de tests et de mesures acquis exclusivement pour l'établissement, la mise en service, le réglage et la maintenance des réseaux et systèmes de communications électroniques ;
– les dispositifs permettant de réaliser l'enregistrement des communications reçues ou émises par des équipements terminaux de télécommunications, lorsque cet enregistrement fait partie des fonctionnalités prévues par les caractéristiques publiques de ces équipements.

2. Appareils permettant l'analyse du spectre radioélectrique ou son exploration manuelle ou automatique en vue de la réception et de l'écoute des fréquences n'appartenant pas aux bandes de fréquences attribuées seules ou en partage par le tableau national de répartition des bandes de fréquences au service de radiodiffusion, ou au service radioamateur, ou aux installations radioélectriques pouvant être établies librement en application de l'article L. 33-3 du Code des postes et des communications électroniques, ou aux postes émetteurs et récepteurs fonctionnant sur les canaux banalisés dits CB.

3. Appareils qui, spécifiquement conçus pour détecter à distance les conversations afin de réaliser à l'insu du locuteur l'interception, l'écoute ou la retransmission de la parole, directement ou indirectement, par des moyens acoustiques, électromagnétiques ou optiques, permettent de réaliser l'infraction prévue par l'article 226-1 du Code pénal.

Entrent dans cette catégorie :
– les dispositifs microémetteurs permettant la retransmission de la voix par moyens hertziens, optiques ou filaires, à l'insu du locuteur ;
– les appareils d'interception du son à distance de type microcanon ou équipés de dispositifs d'amplification acoustique ;
– les systèmes d'écoute à distance par faisceaux laser.

4. Dispositifs techniques, à savoir tous matériels ou logiciels, spécifiquement conçus pour, sans le consentement des intéressés, accéder aux données informatiques, les enregistrer, les conserver et les transmettre, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données ou telles qu'il les y introduit par saisie de caractères, opérations ayant pour objet la captation de données informatiques prévue par l'article 706-102-1 du Code de procédure pénale.

N'entrent pas dans cette catégorie les dispositifs de tests et de mesures des signaux radioélectriques émis par un équipement électronique, destinés exclusivement à évaluer la compatibilité ou le champ électromagnétique.

Fait le 4 juillet 2012.

Pour le Premier ministre et par délégation :

Le secrétaire général de la défense

et de la sécurité nationale,

F. Delon

• 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

Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale (extraits)

(…)

Chapitre III : Dispositions relatives au renseignement

Article 20

I. – Le livre II du même Code est ainsi modifié :

1° L'intitulé du titre IV est complété par les mots : « et accès administratif aux données de connexion » ;

2° Il est ajouté un chapitre VI ainsi rédigé :

« Chapitre VI

« Accès administratif aux données de connexion

« Art. L. 246-1. – Pour les finalités énumérées à l'article L. 241-2, peut être autorisé le recueil, auprès des opérateurs de communications électroniques et des personnes mentionnées à l'article L. 34-1 du Code des postes et des communications électroniques ainsi que des personnes mentionnées aux 1 et 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, des informations ou documents traités ou conservés par leurs réseaux ou services de communications électroniques, y compris les 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, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications.

« Art. L. 246-2.-I.- Les informations ou documents mentionnés à l'article L. 246-1 sont sollicités par les agents individuellement désignés et dûment habilités des services relevant des ministres chargés de la sécurité intérieure, de la défense, de l'économie et du budget, chargés des missions prévues à l'article L. 241-2.

« II. – Les demandes des agents sont motivées et soumises à la décision d'une personnalité qualifiée placée auprès du Premier ministre. Cette personnalité est désignée pour une durée de trois ans renouvelable par la Commission nationale de contrôle des interceptions de sécurité, sur proposition du Premier ministre 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. Ces décisions, accompagnées de leur motif, font l'objet d'un enregistrement et sont communiquées à la Commission nationale de contrôle des interceptions de sécurité.

« Art. L. 246-3.- Pour les finalités énumérées à l'article L. 241-2, les informations ou documents mentionnés à l'article L. 246-1 peuvent être recueillis sur sollicitation du réseau et transmis en temps réel par les opérateurs aux agents mentionnés au I de l'article L. 246-2. « L'autorisation de recueil de ces informations ou documents est accordée, sur demande écrite et motivée des ministres de la sécurité intérieure, de la défense, de l'économie et du budget ou des personnes que chacun d'eux a spécialement désignées, par décision écrite du Premier ministre ou des personnes spécialement désignées par lui, pour une durée maximale de trente jours. Elle peut être renouvelée, dans les mêmes conditions de forme et de durée. Elle est communiquée dans un délai de quarante-huit heures au président de la Commission nationale de contrôle des interceptions de sécurité.

« Si celui-ci estime que la légalité de cette autorisation 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 deuxième alinéa. « Au cas où la commission estime que le recueil d'une donnée de connexion a été autorisé en méconnaissance des dispositions du présent titre, elle adresse au Premier ministre une recommandation tendant à ce qu'il y soit mis fin.

« Elle porte également cette recommandation à la connaissance du ministre ayant proposé le recueil de ces données et du ministre chargé des communications électroniques.

« Art. L. 246-4.-La Commission nationale de contrôle des interceptions de sécurité dispose d'un accès permanent au dispositif de recueil

des informations ou documents mis en œuvre en vertu du présent chapitre, afin de procéder à des contrôles visant à s'assurer du respect des conditions fixées aux articles L. 246-1 à L. 246-3. En cas de manquement, elle adresse une recommandation au Premier ministre. Celui-ci fait connaître à la commission, dans un délai de quinze jours, les mesures prises pour remédier au manquement constaté. « Les modalités d'application 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 informations ou documents transmis.

« Art. L. 246-5.-Les surcoûts identifiables et spécifiques éventuellement exposés par les opérateurs et personnes mentionnées à l'article L. 246-1 pour répondre à ces demandes font l'objet d'une compensation financière de la part de l'État. » ;

3° Les articles L. 222-2, L. 222-3 et L. 243-12 sont abrogés ;

4° À la première phrase du premier alinéa de l'article L. 243-7, les mots : « 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 nº 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique » sont remplacés par les références : « des articles L. 243-8, L. 246-3 et L. 246-4 » ;

5° À l'article L. 245-3, après le mot : « violation », sont insérées les références : « des articles L. 246-1 à L. 246-3 et ».

II. – L'article L. 34-1-1 du Code des postes et des communications électroniques est abrogé.

III. – Le II bis de l'article 6 de la loi nº 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique est abrogé.

IV. – Le présent article entre en vigueur le 1er janvier 2015.

(…)

Chapitre IV : Dispositions relatives à la protection des infrastructures vitales contre la cybermenace

Article 23

Le Code pénal est ainsi modifié : 1° Au 1° de l'article 226-3, les mots : « conçus pour réaliser les opérations » sont remplacés par les mots : « de nature à permettre la réalisation d'opérations » ; 2° Au second alinéa de l'article 226-15, les mots : « conçus pour réaliser » sont remplacés par les mots : « de nature à permettre la réalisation ».

Loi nº 2014-372 du 28 mars 2014 relative à la géolocalisation

JORF nº0075 du 29 mars 2014

Texte n°1

NOR : JUSX1329164L

L'Assemblée nationale et le Sénat ont adopté,

Vu la décision du Conseil constitutionnel n° 2014-693 DC du 25 mars 2014,

Le Président de la République promulgue la loi dont la teneur suit :

Article 1

Le titre IV du livre Ier du Code de procédure pénale est complété par un chapitre V ainsi rédigé :

« Chapitre V

« De la géolocalisation

« Art. 230-32. – Il peut être recouru à tout moyen technique destiné à la localisation en temps réel, sur l'ensemble du territoire national, d'une personne, à l'insu de celle-ci, d'un véhicule ou de tout autre objet, sans le consentement de son propriétaire ou de son possesseur, si cette opération est exigée par les nécessités :

« 1° D'une enquête ou d'une instruction relative à un délit prévu au livre II ou aux articles 434-6 et 434-27 du Code pénal, puni d'un emprisonnement d'au moins trois ans ;

« 2° D'une enquête ou d'une instruction relative à un crime ou à un délit, à l'exception de ceux mentionnés au 1° du présent article, puni d'un emprisonnement d'au moins cinq ans ;

« 3° D'une procédure d'enquête ou d'instruction de recherche des causes de la mort ou de la disparition prévue aux articles 74, 74-1 et 80-4 ;

« 4° D'une procédure de recherche d'une personne en fuite prévue à l'article 74-2.

« La géolocalisation est mise en place par l'officier de police judiciaire ou, sous sa responsabilité, par l'agent de police judiciaire, ou prescrite sur réquisitions de l'officier de police judiciaire, dans les conditions et selon les modalités prévues au présent chapitre.

« Art. 230-33. – L'opération mentionnée à l'article 230-32 est autorisée :

« 1° Dans le cadre d'une enquête de flagrance, d'une enquête préliminaire ou d'une procédure prévue aux articles 74 à 74-2, par le procureur de la République, pour une durée maximale de quinze jours consécutifs. À l'issue de ce délai, cette opération est autorisée par le juge des libertés et de la détention à la requête du procureur de la République, pour une durée maximale d'un mois renouvelable dans les mêmes conditions de forme et de durée ;

« 2° Dans le cadre d'une instruction ou d'une information pour recherche des causes de la mort ou des causes de la disparition mentionnées aux articles 74, 74-1 et 80-4, par le juge d'instruction, pour une durée maximale de quatre mois renouvelable dans les mêmes conditions de forme et de durée.

« La décision du procureur de la République, du juge des libertés et de la détention ou du juge d'instruction est écrite. Elle n'a pas de caractère juridictionnel et n'est susceptible d'aucun recours.

« Art. 230-34. – Dans les cas mentionnés aux 1° et 2° de l'article 230-33, lorsque les nécessités de l'enquête ou de l'instruction l'exigent, le procureur de la République ou le juge d'instruction peut, aux seules fins de mettre en place ou de retirer le moyen technique mentionné à l'article 230-32, autoriser par décision écrite l'introduction, y compris en dehors des heures prévues à l'article 59, dans des lieux privés destinés ou utilisés à l'entrepôt de véhicules, fonds, valeurs, marchandises ou matériel, ou dans un véhicule situé sur la voie publique ou dans de tels lieux, à l'insu ou sans le consentement du propriétaire ou de l'occupant des lieux ou du véhicule ou de toute personne titulaire d'un droit sur ceux-ci.

« S'il s'agit d'un lieu privé autre que ceux mentionnés au premier alinéa du présent article, cette opération ne peut intervenir que dans les cas mentionnés aux 3° et 4° de l'article 230-32 ou lorsque l'enquête ou l'instruction est relative à un crime ou à un délit puni d'au moins cinq ans d'emprisonnement. Si ce lieu privé est un lieu d'habitation, l'autorisation est délivrée par décision écrite :

« 1° Dans les cas prévus au 1° de l'article 230-33, du juge des libertés et de la détention, saisi à cette fin par le procureur de la République ;

« 2° Dans les cas prévus au 2° du même article 230-33, du juge d'instruction ou, si l'opération doit intervenir en dehors des heures prévues à l'article 59, du juge des libertés et de la détention, saisi à cette fin par le juge d'instruction.

« La mise en place du moyen technique mentionné à l'article 230-32 ne peut concerner ni les lieux mentionnés aux articles 56-1 à 56-4, ni le bureau ou le domicile des personnes mentionnées à l'article 100-7.

« Art. 230-35. – En cas d'urgence résultant d'un risque imminent de dépérissement des preuves ou d'atteinte grave aux personnes ou aux biens, les opérations mentionnées à l'article 230-32 peuvent être mises en place ou prescrites par un officier de police judiciaire. Celui-ci en informe immédiatement, par tout moyen, le procureur de la République ou le juge d'instruction dans les cas mentionnés aux articles 230-33 et 230-34. Ce magistrat peut alors ordonner la mainlevée de la géolocalisation.

«Toutefois, si l'introduction dans un lieu d'habitation est nécessaire, l'officier de police judiciaire doit recueillir l'accord préalable, donné par tout moyen :

« 1° Dans les cas prévus au 1° de l'article 230-33, du juge des libertés et de la détention, saisi à cette fin par le procureur de la République ;

« 2° Dans les cas prévus au 2° du même article 230-33, du juge d'instruction ou, si l'introduction doit avoir lieu en dehors des heures prévues à l'article 59, du juge des libertés et de la détention, saisi à cette fin par le juge d'instruction.

« Ces magistrats disposent d'un délai de vingt-quatre heures pour prescrire, par décision écrite, la poursuite des opérations. À défaut d'une telle autorisation dans ce délai, il est mis fin à la géolocalisation. Dans les cas prévus au premier alinéa du présent article, l'autorisation comporte l'énoncé des circonstances de fait établissant l'existence du risque imminent mentionné à ce même alinéa.

« Art. 230-36. – Le juge d'instruction ou l'officier de police judiciaire commis par lui ou autorisé par le procureur de la République peut requérir tout agent qualifié d'un service, d'une unité ou d'un organisme placé sous l'autorité du ministre de l'intérieur et dont la liste est fixée par décret, en vue de procéder à l'installation et au retrait du moyen technique mentionné à l'article 230-32.

« Art. 230-37. – Les opérations prévues au présent chapitre sont conduites sous le contrôle du magistrat qui les a autorisées ou qui a autorisé leur poursuite.

« Le fait que ces opérations révèlent des infractions autres que celles visées dans la décision de ce magistrat ne constitue pas une cause de nullité des procédures incidentes.

« Art. 230-38. – L'officier de police judiciaire ou l'agent de police judiciaire agissant sous sa responsabilité dresse procès-verbal de chacune des opérations de mise en place du moyen technique mentionné à l'article 230-32 et des opérations d'enregistrement des données de localisation. 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.

« Art. 230-39. – L'officier de police judiciaire ou l'agent de police judiciaire agissant sous sa responsabilité décrit ou transcrit, dans un procès-verbal qui est versé au dossier, les données enregistrées qui sont utiles à la manifestation de la vérité.

« Art. 230-40. – Lorsque, dans une instruction concernant l'un des crimes ou délits entrant dans le champ d'application de l'article 706-73, la connaissance de ces informations est susceptible de mettre gravement en danger la vie ou l'intégrité physique d'une personne, des membres

de sa famille ou de ses proches et qu'elle n'est ni utile à la manifestation de la vérité, ni indispensable à l'exercice des droits de la défense, le juge des libertés et de la détention, saisi à tout moment par requête motivée du juge d'instruction, peut, par décision motivée, autoriser que n'apparaissent pas dans le dossier de la procédure :

« 1° La date, l'heure et le lieu où le moyen technique mentionné à l'article 230-32 a été installé ou retiré ;

« 2° L'enregistrement des données de localisation et les éléments permettant d'identifier une personne ayant concouru à l'installation ou au retrait du moyen technique mentionné à ce même article.

« La décision du juge des libertés et de la détention mentionnée au premier alinéa du présent article est jointe au dossier de la procédure. Les informations mentionnées aux 1° et 2° sont inscrites dans un autre procès-verbal, qui est versé dans un dossier distinct du dossier de la procédure, dans lequel figure également la requête du juge d'instruction prévue au premier alinéa. Ces informations sont inscrites sur un registre coté et paraphé, qui est ouvert à cet effet au tribunal de grande instance.

« Art. 230-41. – La personne mise en examen ou le témoin assisté peut, dans les dix jours à compter de la date à laquelle il lui a été donné connaissance du contenu des opérations de géolocalisation réalisées dans le cadre prévu à l'article 230-40, contester, devant le président de la chambre de l'instruction, le recours à la procédure prévue à ce même article. S'il estime que les opérations de géolocalisation n'ont pas été réalisées de façon régulière, que les conditions prévues audit article ne sont pas remplies ou que les informations mentionnées à ce même article sont indispensables à l'exercice des droits de la défense, le président de la chambre de l'instruction ordonne l'annulation de la géolocalisation. Toutefois, s'il estime que la connaissance de ces informations n'est pas ou n'est plus susceptible de mettre gravement en danger la vie ou l'intégrité physique d'une personne, des membres de sa famille ou de ses proches, il peut également ordonner le versement au dossier de la requête et du procès-verbal mentionnés au dernier alinéa du même article. Le président de la chambre de l'instruction statue par décision motivée, qui n'est pas susceptible de recours, au vu des pièces de la procédure et de celles figurant dans le dossier mentionné au même alinéa.

« Art. 230-42. – Aucune condamnation ne peut être prononcée sur le [Disposition déclarée non conforme à la Constitution par la décision du Conseil constitutionnel n° 2014-693 DC du 25 mars 2014.] fondement des éléments recueillis dans les conditions prévues à l'article 230-40, sauf si la requête et le procès-verbal mentionnés au dernier alinéa de ce même article ont été versés au dossier en application de l'article 230-41.

« Art. 230-43. – Les enregistrements de données de localisation 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.

« Art. 230-44. – Le présent chapitre n'est pas applicable lorsque les opérations de géolocalisation en temps réel ont pour objet la localisation d'un équipement terminal de communication électronique, d'un véhicule ou de tout autre objet dont le propriétaire ou le possesseur légitime est la victime de l'infraction sur laquelle porte l'enquête ou l'instruction ou la personne disparue au sens des articles 74-1 ou 80-4, dès lors que ces opérations ont pour objet de retrouver la victime, l'objet qui lui a été dérobé ou la personne disparue.

« Dans les cas prévus au présent article, les opérations de géolocalisation en temps réel font l'objet de réquisitions conformément aux articles 60-1, 60-2, 77-1-1, 77-1-2, 99-3 ou 99-4. »

Article 2

La section 7 du chapitre IV du titre II du Code des douanes est complétée par un article 67 bis-2 ainsi rédigé :

« Art. 67 bis-2.-Si les nécessités de l'enquête douanière relative à la recherche et à la constatation d'un délit douanier puni d'une peine d'emprisonnement d'une durée égale ou supérieure à cinq ans l'exigent, tout moyen technique destiné à la localisation en temps réel, sur l'ensemble du territoire national, d'une personne, à l'insu de celle-ci, d'un véhicule ou de tout autre objet, sans le consentement de son propriétaire ou de son possesseur, peut être mis en place ou prescrit par les agents des douanes habilités par le ministre chargé des douanes dans des conditions fixées par décret, sur autorisation, dans les conditions et selon les modalités prévues au chapitre V du titre IV du livre Ier du Code de procédure pénale, du procureur de la République près le tribunal de grande instance dans le ressort duquel la mise en place du moyen technique est envisagée ou du juge des libertés et de la détention de ce tribunal. »

Article 3

[Dispositions déclarées non conformes à la Constitution par la décision du Conseil constitutionnel no 2014-693 DC du 25 mars 2014.]

Article 4

La présente loi est applicable dans les îles Wallis et Futuna, en Nouvelle-Calédonie et en Polynésie française.

La présente loi sera exécutée comme loi de l'État.

Fait à Paris, le 28 mars 2014.

François Hollande

Par le Président de la République :

Le Premier ministre,

Jean-Marc Ayrault

La garde des Sceaux,

ministre de la Justice,

Christiane Taubira

(1) Loi nº 2014-372. – Travaux préparatoires : Sénat : Projet de loi nº 257 (2013-2014) ; Rapport de M. Jean-Pierre Sueur, au nom de la commission des lois, nº 284 (2013-2014) ; Texte de la commission nº 285 (2013-2014) ; Discussion et adoption, après engagement de la procédure accélérée, le 20 janvier 2014 (TA nº 64, 2013-2014). Assemblée nationale : Projet de loi, adopté par le Sénat, nº 1717 ; Rapport de M. Sébastien Pietrasanta, au nom de la commission des lois, nº 1732 ; Discussion et adoption le 11 février 2014 (TA nº 290). Assemblée nationale : Rapport de M. Sébastien Pietrasanta, au nom de la commission mixte paritaire, nº 1798 ; Discussion et adoption le 24 février 2014 (TA nº 308). Sénat : Projet de loi, modifié par l'Assemblée nationale, nº 364 (2013-2014) ; Rapport de M. Jean-Pierre Sueur, au nom de la commission mixte paritaire, nº 374 (2013-2014) ; Texte de la commission nº 375 (2013-2014) ; Discussion et adoption le 24 février 2014 (TA nº 88, 2013-2014). – Conseil constitutionnel : Décision nº 2014-693 DC en date du 25 mars 2014, publiée au Journal officiel de ce jour.

Décret nº 2014-1162 du 9 octobre 2014 portant création d'un traitement automatisé de données à caractère personnel dénommé « Plate-forme nationale des interceptions judiciaires »

JORF nº 0236 du 11 octobre 2014

Texte nº 3

DÉCRET

NOR : JUST1406439D

Publics concernés : magistrats, greffiers, officiers et agents de police judiciaire, agents des douanes et des services fiscaux habilités à effectuer des enquêtes judiciaires, particuliers.

Objet : mise en œuvre de la plate-forme nationale des interceptions judiciaires.

Entrée en vigueur : le texte entre en vigueur le lendemain de sa publication.

Notice : le décret met en place la plate-forme nationale des interceptions judiciaires, constituant un traitement automatisé de données à caractère personnel. Il s'agit d'un outil centralisé ayant pour finalité l'enregistrement et la mise à disposition des magistrats, des officiers et agents de police judiciaire de la gendarmerie et de la police nationales ainsi que des agents des douanes et des services fiscaux habilités à effectuer des enquêtes judiciaires, du contenu des communications électroniques interceptées et des données et informations communiquées

par les opérateurs de communications électroniques et les prestataires techniques en réponse aux réquisitions. Le décret fixe les catégories de données à caractère personnel dont l'enregistrement est autorisé, établit la liste des personnes pouvant y accéder, définit les modalités de contrôle de la plate-forme par une personnalité qualifiée assistée d'un comité, et prévoit les modalités d'établissement et de conservation des scellés. Aucune interconnexion n'est prévue avec d'autres traitements de données à caractère personnel.

Références : le présent décret peut être consulté sur le site Légifrance (http ://www.legifrance.gouv.fr).

Le Premier ministre,

Sur le rapport de la garde des Sceaux, ministre de la Justice,

Vu le Code pénal, notamment son article 226-13 ;

Vu le Code de procédure pénale, notamment ses articles 74-2,80-4,100 à 100-7,230-32 et 706-95 ;

Vu le Code des postes et des communications électroniques, notamment son article L. 34-1 ;

Vu la loi nº 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article 26 ;

Vu la loi nº 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications, notamment ses articles 1er et 22 ;

Vu la loi nº 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, notamment son article 6 ;

Vu le décret nº 2006-1405 du 17 novembre 2006 modifiant le décret nº 64-754 du 25 juillet 1964 relatif à l'organisation du ministère de la justice et instituant une délégation aux interceptions judiciaires ;

Vu le décret nº 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 ;

Vu l'avis de la Commission nationale de l'informatique et des libertés en date du 16 janvier 2014 ;

Le Conseil d'État (section de l'intérieur) entendu,

Décrète :

Article 1

Le titre IV du livre Ier du Code de procédure pénale (partie réglementaire) est complété par un chapitre III bis ainsi rédigé :

« Chapitre III bis

« De la plate-forme nationale des interceptions judiciaires

« Art. R. 40-42. – Le ministre de la justice est autorisé à mettre en œuvre un traitement automatisé de données à caractère personnel dénommé : "plate-forme nationale des interceptions judiciaires (PNIJ)", placé sous la responsabilité du secrétaire général du ministère de la justice.

« Art. R. 40-43. – Afin de faciliter la constatation des infractions à la loi pénale, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs, ce traitement enregistre et met à la disposition des magistrats, des officiers et agents de police judiciaire de la gendarmerie et la police nationales chargés de les seconder ainsi que des agents des douanes et des services fiscaux habilités à effectuer des enquêtes judiciaires :

« a) Le contenu des communications électroniques interceptées sur le fondement des articles 74-2, 80-4, 100 à 100-7 et 706-95 ;

« b) Les données et les informations communiquées en application des articles 60-1, 60-2, 77-1-1, 77-1-2, 99-3, 99-4, 230-32, des articles R. 10-13 et R. 10-14 du Code des postes et des communications électroniques et du décret nº 2011-219 du 25 février 2011.

« Art. R. 40-44. – Le traitement peut enregistrer des données à caractère personnel de la nature de celles mentionnées au I de l'article 8 de la loi nº 78-17 du 6 janvier 1978 dans la seule mesure où elles sont évoquées au cours des communications électroniques ou apparaissent dans les informations communiquées visées à l'article précédent.

« Art. R. 40-45. – Conformément aux dispositions de l'article R. 15-33-72 du présent Code la plate-forme transmet les réquisitions établies par les magistrats, les officiers de police judiciaire de la gendarmerie et la police nationales ainsi que les agents des douanes et des services fiscaux habilités à effectuer des enquêtes judiciaires, préalablement authentifiés par leur administration d'origine, à la catégorie d'organismes visée par le 1° de l'article R. 15-33-68, reçoit leurs réponses et les met à la disposition des magistrats, officiers et agents précités.

« Art. R. 40-46. – Dans la mesure où elles sont nécessaires à la poursuite des finalités définies à l'article R. 40-43, peuvent être conservées dans le traitement automatisé les données à caractère personnel et informations suivantes :

« 1° Pour les communications électroniques faisant l'objet d'une interception judiciaire :
« a) Identité (nom, nom marital, nom d'usage, prénoms) de la personne physique émettrice ou destinataire de la communication électronique, surnom, alias, date et lieu de naissance, sexe, filiation, situation familiale, nationalité ;
« b) Dénominations, enseigne commerciale, représentants légaux et dirigeants de la personne morale émettrice ou destinataire de la

communication électronique ainsi que les numéros d'inscription au registre du commerce et des sociétés ;
« c) Adresse ou toute autre information permettant d'identifier le domicile, le lieu ou l'établissement ;
« d) Éléments d'identification de la liaison et données relatives aux outils de communications utilisés ;
« e) Numéro de téléphone (fixe et mobile, personnel et professionnel) ;
« f) Adresse de courrier électronique ou données relatives aux services demandés ou utilisés ;
« g) Données à caractère technique relatives à la localisation de la communication et de l'équipement terminal ;
« h) Données relatives au trafic des communications de la liaison interceptée ;
« i) Contenu des communications électroniques interceptées ainsi que les informations qui leurs sont liées ;
« j) Données permettant d'établir la facturation et le paiement ;

« 2° Pour les communications électroniques faisant l'objet d'une mesure de géolocalisation en temps réel :
« a) Données de signalisation du réseau générées par l'usage du terminal de communication, transmises en temps réel ;
« b) Mise à jour des données de signalisation du terminal de communication, sur sollicitation du réseau, à la demande, transmise en temps réel ;

« 3° Pour les données et les informations communiquées en application des articles 60-2, 77-1-2 et 99-4, des articles R. 10-13 et R. 10-14 du Code des postes et des communications électroniques et du décret nº 2011-219 du 25 février 2011 :
« a) Identité (nom, nom marital, nom d'usage, prénoms) de la personne physique émettrice ou destinataire de la communication électronique, surnom, alias, date et lieu de naissance, sexe, filiation, situation familiale, nationalité ;
« b) Dénominations, enseigne commerciale, représentants légaux et dirigeants de la personne morale émettrice ou destinataire de la communication électronique, ainsi que les numéros d'inscription au registre du commerce et des sociétés ;
« c) Adresse ou toute autre information permettant d'identifier le domicile, le lieu ou l'établissement ;
« d) Éléments d'identification de la liaison et données relatives aux outils de communications utilisés ;
« e) Numéro de téléphone (fixe et mobile, personnel et professionnel) ;
« f) Adresse de courrier électronique ou données relatives aux services demandés ou utilisés ;
« g) Données relatives au trafic de communications ;
« h) Données à caractère technique relatives à la localisation de la communication et de l'équipement terminal ;
« i) Données permettant d'établir la facturation et le paiement.

« Sont également enregistrées, le cas échéant, les informations relatives aux faits, lieux, dates et qualification pénale des infractions objets de l'enquête. Enfin peuvent être enregistrées, le cas échéant, les informations relatives à la reconnaissance vocale du locuteur.

« Art. R. 40-47. – I. – Les magistrats accèdent à l'ensemble des données à caractère personnel et informations enregistrées dans le traitement, pour les besoins des procédures dont ils sont saisis.

« II. – Pour les besoins des procédures dont ils sont saisis, les officiers et agents de police judiciaire de la gendarmerie et la police nationales, respectivement visés aux 2° à 4° de l'article 16 et à l'article 20 ainsi que les agents des douanes et des services fiscaux habilités à effectuer des enquêtes judiciaires, respectivement visés par les articles 28-1 et 28-2, spécialement habilités et individuellement désignés par leur supérieur hiérarchique, accèdent aux données et informations enregistrées dans le traitement, à l'exception de celles qui sont placées sous scellés.

« III. – Pour l'exercice de leurs attributions, les greffiers, individuellement désignés par le directeur de greffe, ont accès aux données à caractère personnel et aux informations placées sous scellés enregistrées dans le traitement.

« IV. – Pour l'exercice des missions qui leur sont confiées, les interprètes-traducteurs accèdent, sur autorisation de l'officier de police judiciaire ou de l'agent habilité des douanes ou des services fiscaux et pour une durée limitée aux communications électroniques désignées par ce dernier.

« V. – Pour la mise au clair des données chiffrées, sur autorisation du magistrat saisi de la procédure, le service visé à l'article 230-2 accède aux données et informations relatives au contenu des interceptions chiffrées et, le cas échéant, aux données et informations utiles au déchiffrement que lui désigne l'officier de police judiciaire, l'agent des douanes ou des services fiscaux habilité à procéder à des enquêtes judiciaires.

« VI. – Pour l'exercice de leurs attributions, dont la résolution des difficultés techniques rencontrées par les personnes mentionnées aux I et II, les magistrats, fonctionnaires et agents du ministère de la justice chargés du fonctionnement, de la maintenance et de l'entretien de la plate-forme nationale des interceptions judiciaires, individuellement désignés par le secrétaire général du ministère de la justice, accèdent pour une durée limitée aux données et informations enregistrées dans le traitement, sur autorisation expresse du magistrat saisi de la procédure.

« VII. – Les personnes auxquelles peuvent être confiées par contrat les prestations détachables des finalités judiciaires du traitement ne peuvent avoir accès aux données à caractère personnel et informations enregistrées par le traitement, sauf en cas de difficultés techniques exceptionnelles. Dans cette hypothèse, un accès ponctuel, limité à la durée nécessaire à la résolution de ces difficultés, leur est délivré, sur

autorisation expresse du délégué aux interceptions judiciaires et du magistrat saisi de la procédure.

« Art. R. 40-48. – Dans le cadre de l'exercice des missions qui leur sont confiées, les données et informations relatives à l'identité et à la qualité des interprètes-traducteurs sont conservées par le traitement.

« Art. R. 40-49. – Les données et informations mentionnées aux 1° et 2° de l'article R. 40-46 sont placées sous scellés au sein du traitement jusqu'à expiration du délai de prescription de l'action publique.

« Les données mentionnées au 3° du même article ainsi que les informations relatives à la reconnaissance vocale du locuteur sont conservées jusqu'à la date de clôture des investigations en matière de communications électroniques par l'officier de police judiciaire ou l'agent des douanes ou des services fiscaux habilité à procéder à des enquêtes judiciaires, et de transmission de la procédure à l'autorité judiciaire compétente.

« Art. R. 40-50. – Toute opération relative au traitement fait l'objet d'un enregistrement comprenant l'identification de l'utilisateur, la date, l'heure et la nature de l'action. Ces informations sont conservées pendant une durée de cinq ans.

« Art. R. 40-51. – La plate-forme nationale des interceptions judiciaires est mise en œuvre par la délégation aux interceptions judiciaires, service du secrétariat général, dirigée par un magistrat de l'administration centrale du ministère de la justice.

« La constitution et la conservation des données et informations placées sous scellés au sein du traitement relèvent de la délégation aux interceptions judiciaires. Les demandes tendant à l'établissement et la délivrance des reproductions de ces scellés sont transmises par le greffier au responsable de la délégation.

« Art. R. 40-52. – Les magistrats, fonctionnaires et agents de ce ministère chargés du fonctionnement, de la maintenance et de l'entretien de la plate-forme nationale des interceptions judiciaires ainsi que les personnes auxquelles peuvent être confiées par contrat les prestations détachables des finalités judiciaires du traitement sont habilités au niveau confidentiel défense. Ils sont soumis au secret professionnel dans les conditions et sous les peines prévues à l'article 226-13 du Code pénal.

« Art. R. 40-53. – La plate-forme nationale des interceptions judiciaires est placée sous le contrôle d'une personnalité qualifiée, désignée pour une durée de cinq ans non renouvelable par arrêté du garde des sceaux, ministre de la justice, et assistée par un comité composé de cinq membres.

« La délégation aux interceptions judiciaires, lui adresse, sur sa demande, toutes informations relatives au traitement.

« Cette personnalité peut ordonner toutes mesures nécessaires à l'exercice de son contrôle. Cette personnalité et les membres du comité de contrôle disposent d'un accès permanent aux lieux où se trouve la plate-forme nationale des interceptions judiciaires.

« Elle établit un rapport annuel qu'elle adresse au garde des sceaux, ministre de la justice.

« Les pouvoirs qui lui sont confiés s'exercent sans préjudice du contrôle exercé par la Commission nationale de l'informatique et des libertés en application des dispositions et selon les modalités prévues par les articles 41 et 44 de la loi n° 78-17 du 6 janvier 1978.

« Art. R. 40-54. – Le comité mentionné à l'article précédent comprend :
« a) Un sénateur et un député respectivement choisis par le président du Sénat, après chaque renouvellement partiel du Sénat, et par le président de l'Assemblée nationale, pour la durée de la législature, sur proposition de la commission compétente de chaque assemblée ;
« b) Un magistrat du siège honoraire de la Cour de cassation, désigné pour une durée de cinq ans non renouvelable par arrêté du garde des sceaux, ministre de la justice ;
« c) Une personnalité qualifiée, désignée pour une durée de cinq ans non renouvelable par arrêté du garde des sceaux, ministre de la justice, sur proposition du ministre chargé des communications électroniques ;
« d) Une personnalité qualifiée, désignée pour une durée de cinq ans non renouvelable par arrêté du garde des sceaux, ministre de la justice, sur proposition du ministre de l'intérieur.

« Art. R. 40-55. – Les droits d'accès et de rectification des données mentionnés à l'article R. 40-46 s'exercent de manière indirecte dans les conditions prévues aux articles 41 et 42 de la loi n° 78-17 du 6 janvier 1978.

« Art. R. 40-56. – En application du VI de l'article 32 et du dernier alinéa de l'article 38 de la loi n° 78-17 du 6 janvier 1978, les droits d'information et d'opposition ne s'appliquent pas au présent traitement. »

Article 2

À l'article R. 223 du même Code, après le mot : « compétente », sont insérés les mots : « ou, s'il est dressé au titre du 9° de l'article R. 92, au secrétaire général du ministère de la Justice si la réquisition a été transmise par la plate-forme nationale des interceptions judiciaires à l'opérateur ».

Article 3

L'article R. 225 du même Code est ainsi modifié :

1° Le premier alinéa est remplacé par les dispositions suivantes :

« Lorsque l'état ou mémoire porte sur des frais mentionnés au 1° et au 3° de l'article R. 224-1 et à l'article R. 224-2, le greffier ou tout autre

fonctionnaire de catégorie B des services judiciaires, après avoir procédé s'il y a lieu aux redressements nécessaires, certifie avoir vérifié la réalité de la dette et son montant. Lorsque l'état porte sur des frais mentionnés au 2° de l'article R. 224-1, ce certificat est établi par le fonctionnaire de catégorie A ou B, délégué à cette fin par le secrétaire général du ministère de la justice si la réquisition a été transmise par la plate-forme nationale des interceptions judiciaires à l'opérateur. » ;

2° Au troisième alinéa après les mots : « ou tout autre fonctionnaire de catégorie B des services judiciaires », sont ajoutés les mots : « ou le fonctionnaire de catégorie A ou B, délégué à cette fin par le secrétaire général du ministère de la Justice ».

Article 4

Le décret nº 2007-1145 du 30 juillet 2007 portant création d'un traitement automatisé de données à caractère personnel dénommé « Système de transmission d'interceptions judiciaires » est abrogé six mois après la mise en œuvre de la plate-forme nationale des interceptions judiciaires, constatée par arrêté du garde des sceaux, ministre de la justice, et au plus tard le 31 décembre 2015.

Article 5

La garde des Sceaux, ministre de la Justice, le ministre des Finances et des Comptes publics, le ministre de l'Intérieur et le ministre de l'Économie, de l'Industrie et du Numérique sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret, qui sera publié au *Journal officiel de la République française*.

Fait le 9 octobre 2014.

Manuel Valls

Par le Premier ministre :

La garde des Sceaux, ministre de la Justice,

Christiane Taubira

Le ministre des Finances et des Comptes publics,

Michel Sapin

Le ministre de l'Intérieur,

Bernard Cazeneuve

Le ministre de l'Économie, de l'Industrie et du Numérique,

Emmanuel Macron

Chapitre III

Jurisprudence et actualités parlementaires

Arrêt du Conseil d'État nº 361118 (2e et 7e sous-sections réunies du 25 novembre 2013)

Vu le pourvoi, enregistré le 16 juillet 2012 au secrétariat du contentieux du Conseil d'État, présenté par le ministre de l'économie et des finances ; le ministre demande au Conseil d'État d'annuler l'arrêt nº 10PA04326 du 9 mai 2012 de la cour administrative d'appel de Paris en tant qu'il a condamné l'État à verser aux sociétés France Télécom et Orange France respectivement les sommes de 1 093 828,04 euros et 243 410,58 euros assorties des intérêts au taux légal à compter du 1er avril 2008, capitalisés à compter du 2 avril 2009 ;

Vu les autres pièces du dossier ;

Vu la Constitution, notamment son Préambule et son article 61-1 ;

Vu l'ordonnance nº 58-1067 du 7 novembre 1958 ;

Vu le Code des postes et des communications électroniques ;

Vu le livre des procédures fiscales, notamment son article L. 83 ;

Vu la loi nº 2001-1276 du 28 décembre 2001 ;

Vu la loi nº 2004-669 du 9 juillet 2004 ;

Vu la loi nº 2005-1720 du 30 décembre 2005 ;

Vu la décision nº 2000-441 DC du Conseil constitutionnel du 28 décembre 2000 ;

Vu la décision nº 2001-457 DC du Conseil constitutionnel du 27 décembre 2001 ;

Vu le Code de justice administrative ;

Après avoir entendu en séance publique :
– le rapport de Mme Airelle Niepce, Maître des requêtes en service extraordinaire,
– les conclusions de Mme Béatrice Bourgeois-Machureau, Rapporteur public,

La parole ayant été donnée, avant et après les conclusions, à la SCP Rocheteau, Uzan-Sarano, avocat de France Télécom et de la société Orange France ;

1. Considérant qu'en vertu de l'article L. 83 du livre des procédures fiscales, les administrations de l'État, des départements et des communes, les entreprises concédées ou contrôlées par l'État, les départements et les communes, ainsi que les établissements ou organismes de toute nature soumis au contrôle de l'autorité administrative, doivent communiquer à l'administration, sur sa demande, les documents de service qu'ils détiennent sans pouvoir opposer le secret professionnel, y compris, ainsi qu'il a été précisé par l'article 62 de la loi du 28 décembre 2001 de finances rectificative pour 2001, les données conservées et traitées par les opérateurs de télécommunications dans le cadre de l'article L. 32-3-1 du Code des postes et télécommunications, devenu l'article L. 34-1 du Code des postes et communications électroniques ;

2. Considérant que, selon l'article L. 32-3-1 du Code des postes et télécommunications, devenu l'article L. 34-1 du Code des postes et communications électroniques à compter de l'entrée en vigueur de la loi du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle, les "opérateurs de télécommunications (…) sont tenus d'effacer ou de rendre anonyme toute donnée relative à une communication dès que celle-ci est achevée, sous réserve des dispositions des II, III et IV. / II. – Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales, et dans le seul but de permettre, en tant que de besoin, la mise à disposition de l'autorité judiciaire d'informations, il peut être différé pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques. Un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés, détermine, dans les limites fixées par le IV, ces catégories de données et la durée de leur conservation, selon l'activité des opérateurs et la nature des communications ainsi que les modalités de compensation, le cas échéant, des surcoûts identifiables et spécifiques des prestations assurées à ce titre, à la demande de l'État, par les opérateurs. / (…) / IV. – Les données conservées et traitées dans les conditions définies aux II et III

portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs et sur les caractéristiques techniques des communications assurées par ces derniers. / Elles ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications. / (…) " ;

3. Considérant qu'il ressort des énonciations de l'arrêt attaqué que la société France Télécom et l'État ont signé, le 9 février 2000, une convention relative aux prestations rendues par France Télécom à la direction générale des impôts dans le cadre du droit de communication prévu aux articles L. 81, L. 83 et L. 85 du livre des procédures fiscales ; que cette convention a été conclue pour une durée d'un an à compter du 1er janvier 2000 tout en prévoyant qu'elle était tacitement renouvelable deux fois ; qu'un avenant, signé le 10 janvier 2001, a transféré à la société France Télécom Mobile, devenue par la suite la société Orange France, les droits et obligations résultant de la convention du 9 février 2000 et liées aux activités de téléphonie mobile de France Télécom ; qu'après l'expiration de cette convention, le 31 décembre 2002, l'administration fiscale, tout en continuant de solliciter les sociétés France Télécom et Orange France dans le cadre de l'exercice de son droit de communication, a refusé de verser une compensation financière en contrepartie ; que, le 26 mars 2008, les sociétés France Télécom et Orange France ont demandé à l'État d'être indemnisées au titre des prestations accomplies à la demande de l'administration fiscale pour les années 2002 à 2007 ; qu'après avoir envisagé un règlement transactionnel du litige, le ministre du budget, des comptes publics et de la réforme de l'État a décidé, le 5 novembre 2008, de rejeter cette demande ;

4. Considérant que les sociétés France Télécom et Orange France ont saisi le tribunal administratif de Paris de conclusions tendant à la condamnation de l'État à leur verser les sommes auxquelles elles prétendent au titre des années 2002 à 2007, lesquelles ont été complétées en cours d'instance par de nouvelles demandes concernant les années 2008 et 2009 ; que, par un jugement du 1er juillet 2010, le tribunal administratif de Paris a, d'une part, rejeté les demandes indemnitaires des deux sociétés au titre des années 2002 et 2003, au motif que les créances correspondantes étaient prescrites, et celles présentées au titre des années 2008 et 2009, au motif qu'elles étaient irrecevables ; qu'il a, d'autre part, condamné l'État à verser aux sociétés France Télécom et Orange France respectivement les sommes de 1 093 828,04 euros et 243 410,58 euros correspondant aux années 2004 à 2007, assorties des intérêts au taux légal à compter du 7 décembre 2008 et de la capitalisation des intérêts à compter du 8 novembre 2009, sur le fondement de la responsabilité sans faute de l'État pour rupture d'égalité devant les charges publiques ; que, par un arrêt du 9 mai 2012, la cour administrative d'appel de Paris a annulé le jugement du 1er juillet 2010 pour irrégularité mais a mis à la charge de l'État les mêmes indemnités sur le

fondement de la responsabilité extracontractuelle de l'État pour faute ; que le ministre de l'économie et des finances se pourvoit en cassation contre cet arrêt en tant qu'il a condamné l'État à verser ces indemnités, majorées des intérêts et de la capitalisation des intérêts, aux sociétés France Télécom et Orange France ;

Sur la question prioritaire de constitutionnalité :

5. Considérant qu'aux termes du premier alinéa de l'article 23-5 de l'ordonnance du 7 novembre 1958 portant loi organique sur le Conseil constitutionnel : "Le moyen tiré de ce qu'une disposition législative porte atteinte aux droits et libertés garantis par la Constitution peut être soulevé, y compris pour la première fois en cassation, à l'occasion d'une instance devant le Conseil d'État (...) " ; qu'il résulte des dispositions de ce même article que le Conseil constitutionnel est saisi de la question prioritaire de constitutionnalité à la triple condition que la disposition contestée soit applicable au litige ou à la procédure, qu'elle n'ait pas déjà été déclarée conforme à la Constitution dans les motifs et le dispositif d'une décision du Conseil constitutionnel, sauf changement de circonstances, et que la question soit nouvelle ou présente un caractère sérieux ;

6. Considérant que les sociétés France Télécom et Orange France soutiennent, en réponse au pourvoi formé par le ministre de l'économie et des finances, que les dispositions de l'article L. 83 du livre des procédures fiscales, en ce qu'elles ne prévoient aucune compensation financière à la mise en œuvre du droit de communication exercé par l'administration fiscale, méconnaissent le droit de propriété et le principe d'égalité devant les charges publiques tels que garantis respectivement par les articles 2 et 17 et par l'article 13 de la Déclaration des droits de l'homme et du citoyen ;

7. Considérant que le droit de communication général conféré par l'article L. 81 du livre des procédures fiscales permet aux agents de l'administration, pour l'établissement de l'assiette et le contrôle des impôts, d'avoir connaissance, dans les conditions précisées par les dispositions du chapitre II du titre II du livre des procédures fiscales, de documents et de renseignements détenus par un très grand nombre de personnes physiques ou morales, afin de pouvoir vérifier la véracité des déclarations des contribuables ; que, dans ce cadre, ainsi qu'il a été dit au point 1, les dispositions de l'article L. 83 mettent en œuvre le droit de communication auprès des administrations de l'État, des départements et des communes, des entreprises concédées ou contrôlées par l'État ainsi que des établissements ou organismes de toute nature soumis au contrôle de l'autorité administrative, y compris, à l'égard des données conservées et traitées par les opérateurs de communications électroniques ; que ce droit de communication ne s'exerce que sur des documents de service que les personnes destinataires des demandes de l'administration fiscale détiennent du fait de leur activité ;

8. Considérant, d'une part, que l'article 13 de la Déclaration des droits de l'homme et du citoyen n'interdit pas de faire supporter des charges particulières à certaines catégories de personnes pour un motif d'intérêt général, dès lors qu'il n'en résulte pas de rupture caractérisée de l'égalité devant les charges publiques ; que les sujétions résultant, pour les personnes visées par la loi, de l'exercice du droit de communication ne portent que sur l'accès à des documents ou informations déterminés, détenus par ces personnes dans le cadre de leur activité, et ne se traduisent que par des charges d'une portée limitée ; qu'elles répondent à l'objectif à valeur constitutionnelle de lutte contre la fraude fiscale ; qu'alors même que le législateur ne l'a pas assorti d'une contrepartie financière, il ne résulte pas de rupture caractérisée de l'égalité devant les charges publiques de l'exercice d'un tel droit de communication par l'administration fiscale ;

9. Considérant, d'autre part, que l'exercice du droit de communication n'emporte aucune privation de propriété au sens de l'article 17 de la Déclaration des droits de l'homme et du citoyen ; que si, en vertu de l'article 2 de cette Déclaration, les atteintes portées au droit de propriété doivent être justifiées par un motif d'intérêt général et proportionnées à l'objectif poursuivi, l'exercice du droit de communication, qui se borne à prévoir l'accès de l'administration fiscale à certains documents, ne traduit aucune atteinte au droit de propriété ;

10. Considérant qu'il résulte de ce qui précède que la question de la conformité aux droits et libertés garantis par la Constitution de l'article L. 83 du livre des procédures fiscales, modifié notamment par l'article 62 de la loi du 28 décembre 2001, à l'encontre duquel le grief d'inconstitutionnalité a été spécialement rejeté dans les motifs de la décision du Conseil constitutionnel n° 2001-457 DC du 27 décembre 2001, n'est pas nouvelle et ne présente pas un caractère sérieux ; qu'ainsi, sans qu'il soit besoin de renvoyer au Conseil constitutionnel la question prioritaire de constitutionnalité invoquée, le moyen tiré de ce que la disposition contestée porte atteinte aux droits et libertés garantis par la Constitution doit être écarté ;

Sur le pourvoi du ministre de l'Économie et des Finances :

11. Considérant que, pour juger que l'administration fiscale avait, en s'abstenant, au terme, le 31 décembre 2002, de la convention conclue le 9 février 2000, d'assurer une compensation financière des surcoûts identifiables et spécifiques des prestations assurées au titre de l'exercice du droit de communication par les sociétés France Télécom et Orange France, commis une faute de nature à engager la responsabilité extracontractuelle de l'État, la cour administrative d'appel de Paris s'est fondée sur ce que le Conseil constitutionnel aurait, dans sa décision n° 2000-441 DC du 28 décembre 2000, posé un principe de juste rémunération du concours apporté par les opérateurs de réseaux de télécommunications aux activités menées par l'État, dans l'intérêt général de la population, dans le cadre de

ses missions tendant à la sauvegarde de l'ordre public, que le régime défini à l'article L. 34-1 du Code des postes et des communications électroniques aurait institué, en application de ce principe, un mécanisme de compensation financière concernant les prestations accomplies sur réquisition des autorités judiciaires et que le législateur, s'il n'a pas étendu ce mécanisme de compensation financière aux prestations effectuées par les opérateurs pour répondre aux demandes de l'administration fiscale au titre de l'article L. 83 du livre des procédures fiscales, n'aurait pas pour autant entendu exclure ces prestations du champ de ce supposé principe de juste rémunération ;

12. Mais considérant, d'une part, que, par sa décision n° 2000-441 DC du 28 décembre 2000, le Conseil constitutionnel a déclaré contraires à la Constitution des dispositions législatives qui prévoyaient de mettre à la charge des opérateurs de réseaux de télécommunications le coût des investissements et une partie des charges d'exploitation permettant de réaliser des interceptions de communications justifiées par les nécessités de la sécurité publique, au motif que "le concours ainsi apporté à la sauvegarde de l'ordre public, dans l'intérêt général de la population, est étranger à l'exploitation des réseaux de télécommunications [et] que les dépenses en résultant ne sauraient dès lors, en raison de leur nature, incomber directement aux opérateurs " ; que le Conseil constitutionnel a, en conséquence, précisé que demeuraient applicables les dispositions de l'article L. 35-6 du Code des postes et télécommunications, alors en vigueur, selon lesquelles "les prescriptions exigées par la défense et la sécurité publique et les garanties d'une juste rémunération des prestations assurées à ce titre, à la demande de l'État, par les opérateurs (…) sont déterminées par leur cahier des charges " ; qu'en statuant ainsi sur la conformité à la Constitution de dispositions relatives à la pratique des interceptions justifiées par les nécessités de la sécurité publique, le Conseil constitutionnel n'a pas, contrairement à ce qu'a jugé la cour administrative d'appel, posé, de façon générale, le principe d'une juste rémunération du concours qui peut être apporté par les opérateurs de réseaux de télécommunications à toutes les activités, quelles qu'elles soient, menées par l'État dans l'intérêt général ;

13. Considérant, d'autre part, que l'article L. 83 du livre des procédures fiscales, non plus qu'aucune disposition des articles L. 81 et suivants du même livre, ne prévoit de compensation financière pour l'exercice du droit de communication, qui n'implique pas la réalisation de prestations particulières mais se borne à imposer aux personnes visées de communiquer à l'administration fiscale, sur sa demande, des informations qu'elles détiennent dans le cadre de leur activité sans pouvoir opposer le secret professionnel ; que, s'agissant des opérateurs de télécommunications, si l'article L. 83 du livre des procédures fiscales précise que les documents que ces derniers doivent communiquer à l'administration fiscale sur demande comprennent les données conservées et traitées par ces opérateurs dans le cadre de l'article L. 32-3-1 du Code des postes et télécommunications, devenu l'article L. 34-1 du Code des postes et communications

électroniques, cette référence n'a ni pour objet ni pour effet d'étendre à l'exercice du droit de communication de l'article L. 83 du livre des procédures fiscales les dispositions du II de l'article L. 32-3-1, devenu le III de l'article L. 34-1, qui renvoient à un décret en Conseil d'État le soin de déterminer des modalités de compensation des surcoûts identifiables et spécifiques pour les prestations assurées au titre de la recherche, de la constatation et de la poursuite des infractions pénales ou d'un manquement à l'obligation définie à l'article L. 3363 du Code de la propriété intellectuelle ;

14. Considérant qu'il résulte de ce qui précède qu'en jugeant que le refus de l'administration fiscale d'assurer une compensation financière aux opérateurs de télécommunications, pour les surcoûts identifiables et spécifiques des prestations assurées par ces derniers au titre de l'exercice du droit de communication prévu à l'article L. 83 du livre des procédures fiscales, était constitutif d'une faute de nature à engager la responsabilité extracontractuelle de l'État, la cour administrative d'appel de Paris a commis une erreur de droit ; que, par suite, sans qu'il soit besoin d'examiner les autres moyens du pourvoi, le ministre de l'économie et des finances est fondé à demander l'annulation de l'arrêt qu'il attaque en tant qu'après avoir annulé le jugement du tribunal administratif de Paris du 1er juillet 2010, il a mis à la charge de l'État les mêmes indemnités que celles prévues par ce jugement, sur le fondement de la responsabilité extracontractuelle de l'État pour faute ;

15. Considérant qu'il y a lieu, dans les circonstances de l'espèce, de régler, dans cette mesure, l'affaire au fond en application des dispositions de l'article L. 821-2 du Code de justice administrative ;

Sur le règlement du litige :

16. Considérant, d'une part, qu'ainsi qu'il vient d'être dit, aucune disposition législative ne prévoit que l'exercice du droit de communication prévu par l'article L. 83 du livre des procédures fiscales implique le versement d'une compensation financière aux personnes qui communiquent à l'administration fiscale, sur sa demande, les documents de service qu'elles détiennent ;

17. Considérant qu'eu égard à la portée limitée des sujétions résultant, pour les personnes visées par la loi, de l'exercice du droit de communication qui ne porte que sur l'accès de l'administration fiscale à des documents ou informations déterminés, détenus par ces personnes dans le cadre de leur activité, et au motif d'intérêt général de lutte contre la fraude fiscale qui les justifient, les sociétés requérantes ne sont pas fondées à soutenir que les dispositions de l'article L. 83 seraient incompatibles avec les exigences résultant de l'article 1er du premier protocole additionnel à la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales ;

18. Considérant que la circonstance que, par l'effet de la convention signée le 9 février 2000, laquelle a pris fin le 31 décembre 2002, l'État ait versé aux sociétés requérantes une compensation financière en contrepartie de l'exercice du droit de communication, n'était pas de nature à faire naître une espérance légitime de continuer de bénéficier d'une contrepartie financière non prévue par la loi, qui serait constitutive d'un bien au sens du premier protocole additionnel à la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales ;

19. Considérant, par suite, qu'en refusant d'accorder une compensation aux sociétés France Télécom et Orange France après l'expiration de la convention du 9 février 2000, l'administration n'a pas commis de faute de nature à engager la responsabilité de l'État ;

20. Considérant, d'autre part, qu'il résulte des principes qui gouvernent l'engagement de la responsabilité sans faute de l'État que le silence d'une loi sur les conséquences que peut comporter sa mise en œuvre ne saurait être interprété comme excluant, par principe, tout droit à réparation des préjudices que son application est susceptible de provoquer ; que le préjudice résultant de l'application de la loi doit faire l'objet d'une indemnisation par l'État lorsque, excédant les aléas inhérents à l'activité de ceux qui en demandent réparation, il revêt un caractère grave et spécial interdisant de le regarder comme une charge devant incomber normalement à ceux qui le subissent ;

21. Considérant que le préjudice résultant, le cas échéant, de la mise en œuvre du droit de communication reconnu à l'administration fiscale par les articles L. 81 et suivants du livre de procédures fiscales, eu égard au nombre d'entités, organismes, établissements ou entreprises qui y sont astreints, sans que la situation des opérateurs de télécommunication puisse à cet égard être distinguée de celle des autres destinataires de ce droit, ne présente pas un caractère spécial ; qu'il ne résulte au demeurant pas de l'instruction que la mise en œuvre du droit de communication se traduirait, pour les sociétés requérantes, par un préjudice financier d'une gravité telle qu'il excèderait la charge normale susceptible de leur être imposée dans l'intérêt général ; qu'il s'ensuit, en tout état de cause, que les conditions mises à l'engagement de la responsabilité de l'État sur le fondement de la rupture d'égalité devant les charges publiques ne sont pas réunies ;

22. Considérant qu'il résulte de ce qui précède, sans qu'il soit besoin de statuer sur les fins de non-recevoir opposées par le ministre, que les sociétés France Télécom et Orange France ne sont pas fondées à demander la condamnation de l'État à les indemniser, à raison de l'exercice du droit de communication prévu à l'article L. 83 du livre des procédures fiscales au titre des années 2004 à 2007 ;

23. Considérant que les dispositions de l'article L. 761-1 du Code de justice administrative font obstacle à ce qu'une somme soit mise à ce titre à la charge de l'État qui n'est pas, dans la présente instance, la partie perdante, au titre des frais exposés par les sociétés France Télécom et Orange France et non compris dans les dépens ;

DÉCIDE :

Article 1er : Il n'y a pas lieu de renvoyer au Conseil constitutionnel la question prioritaire de constitutionnalité soulevé par les sociétés France Télécom et Orange France.

Article 2 : Les articles 2 à 5 de l'arrêt de la Cour administrative d'appel de Paris du 9 mai 2012 sont annulés.

Article 3 : Les conclusions présentées par la société France Télécom et par la société Orange France devant le tribunal administratif de Paris tendant à la condamnation de l'État à leur verser une indemnité, majorée des intérêts au taux légal, à raison de l'exercice du droit de communication prévu à l'article L. 83 du livre des procédures fiscales au titre des années 2004 à 2007 sont rejetées.

Article 4 : Les conclusions des sociétés France Télécom et Orange France présentées au titre des dispositions de l'article L. 761-1 du Code de justice administrative sont rejetées.

Article 5 : La présente décision sera notifiée au ministre de l'Économie et des Finances et aux sociétés France Télécom et Orange France. Copie en sera adressée au Conseil constitutionnel et au Premier ministre.

Arrêt du 7 janvier 2014 de la Chambre criminelle de la Cour de cassation nº 13-85246.

LA COUR DE CASSATION, CHAMBRE CRIMINELLE, a rendu l'arrêt suivant :

Statuant sur le pourvoi formé par :
– M. Meshal X…,

contre l'arrêt de la chambre de l'instruction de la cour d'appel de VERSAILLES, en date du 4 juillet 2013, qui, dans l'information suivie contre lui notamment des chefs de vol avec arme en bande organisée, en récidive, et association de malfaiteurs, a prononcé sur sa demande d'annulation de pièces de la procédure ;

La COUR, statuant après débats en l'audience publique du 26 novembre 2013 où étaient présents : M. Louvel, président, M. Pers, conseiller rapporteur, MM. Arnould, Le Corroller, Mmes Mirguet, Vannier, Duval-Arnould, conseillers de la chambre, Mme Harel-Dutirou, M. Roth, conseillers référendaires ;

Avocat général : M. Cordier ;

Greffier de chambre : Mme Randouin ;

Sur le rapport de M. le conseiller Pers, les observations de Me Spinosi, avocat en la Cour, et les conclusions de M. l'avocat général Cordier ;

Vu l'ordonnance du président de la chambre criminelle, en date du 10 octobre 2013, prescrivant l'examen immédiat du pourvoi ;

Vu le mémoire produit ;

Sur le moyen unique de cassation, pris de la violation des articles 6 et 8 de la Convention européenne des droits de l'homme, préliminaire, 62-2, 63-1, 706-96, 591 et 593 du Code de procédure pénale ;

« en ce que la chambre de l'instruction a dit n'y avoir lieu à annulation d'actes de la procédure ;

« aux motifs que, sur la nullité alléguée de l'ordonnance de soit communiqué du 25 avril 2012 et du réquisitoire supplétif du 26 avril 2012 : qu'en application des articles 51 et 80, alinéa 1, du Code de procédure pénale, le juge d'instruction est saisi de plein droit de toutes les circonstances, y compris aggravantes se rattachant au fait principal visé dans le réquisitoire introductif ; qu'en l'espèce, le magistrat instructeur saisi par réquisitoire introductif du 29 février 2012 du vol commis au préjudice de la bijouterie D... sous la qualification de vol avec arme, pouvait retenir la circonstance de bande organisée, que résultait des éléments de l'enquête sans avoir besoin de solliciter du ministère public des réquisitions supplétives ; que d'ailleurs, dans l'ordonnance de soit communiqué contestée, le magistrat instructeur ne demande que l'avis du procureur de la République sur la retenue de cette circonstance aggravante, avis qui n'était pas nécessaire ; qu'en revanche, il ne pouvait informer sur le délit d'association de malfaiteurs, non visé au réquisitoire introductif, sans réquisitions supplétives ; que la demande du juge d'instruction concernant cette nouvelle infraction trouvait sa justification dans "le rapport d'information sur des faits nouveaux "qui lui avait été transmis par la brigade de répression du banditisme le 25 avril 2012, et qui faisait état de ce que M. Y..., au travers des interceptions téléphoniques et des surveillances, préparait de nouveaux faits délictueux, prenant de nombreux rendez-vous avec des individus méfiants, ne parlant qu'à demi-mots afin de mettre au point un plan lucratif ; que ces préparatifs étaient corroborés par les propos tenus par Mme Y... à sa mère, selon lesquels son mari souhaitait se livrer à des activités rentables qui lui semblaient douteuses ; que l'ordonnance de soit communiqué du 25 avril 2013 était donc motivée par l'apparition, dans le cadre de l'exécution de la commission rogatoire, de faits nouveaux, non visés par le réquisitoire introductif et postérieurs à celui-ci ; que cette ordonnance est donc justifiée et régulière ; que le réquisitoire supplétif du 26 avril 2012 saisissant le magistrat instructeur de faits d'association de malfaiteurs commis courant 2012 et faisant expressément référence "aux éléments nouveaux apparus au cours de l'enquête diligentée par la BR6 de la DRPJ" et qui satisfait en la forme aux conditions essentielles de son existence légale est régulier

et justifié ; qu'il ne saurait donc être annulé ; qu'il ne peut être reproché aux magistrats d'avoir établi ces actes dans le but de pouvoir recourir aux règles procédurales applicables à la criminalité et à la délinquance organisées, en particulier aux articles 706-96 à 706-102 du Code de procédure pénale, dont l'utilisation ne sera sollicitée par les enquêteurs que le 6 septembre 2012, soit plusieurs mois plus tard ; qu'en conséquence, il n'y a pas lieu d'annuler l'ordonnance de soit communiqué et le réquisitoire supplétif contestés ;

que sur le placement en garde à vue de M. X..., contrairement à ce qui est allégué, le requérant n'a pas été placé en garde à vue dans le but d'enregistrer ses éventuelles conversations avec M. Y... dans les geôles ; qu'en effet, il résultait de l'enquête que M. X... avait été vu sur la vidéo surveillance à Villetaneuse, une heure avant le vol de la bijouterie D... en compagnie de trois autres individus a proximité de deux Renault Clio, et de la BMW volée, faussement immatriculée qui allait être utilisée pour commettre ledit vol ; qu'au moment de la commission des faits, il n'émettait ni ne recevait d'appel téléphonique ; qu'après les faits il était fréquemment en relation avec M. Y... dont l'ADN avait été relevé dans la bijouterie ; que, pour communiquer, M. X... utilisait des taxiphones ou des mobiles aux noms de tiers ; qu'il employait un langage codé et donnait ses rendez-vous en des lieux difficiles à surveiller ou non identifiables ; que ces éléments constituaient des raisons plausibles de soupçonner qu'il avait pu participer au crime et aux délits visés dans les réquisitoires introductif et supplétif ; qu'en conséquence, son placement en garde à vue qui répond aux exigences de l'article 62-2, alinéa 1, du Code de procédure pénale n'est pas constitutif d'un détournement de procédure ;

– que sur la sonorisation des cellules de garde à vue, pour permettre le recours à ce dispositif, l'article 706-96 du Code de procédure pénale exige :

– que l'information concerne un crime ou un délit entrant dans le champ d'application de l'article 706-73,

– l'avis du procureur de la République,

– une ordonnance motivée et une commission rogatoire spéciale du juge d'instruction, fixant la durée d'utilisation de ce dispositif, qui ne peut excéder quatre mois renouvelables,

– que l'opération soit effectuée sous l'autorité et le contrôle du juge d'instruction ;

– qu'au cas présent, dans un rapport du 6 septembre 2012, la BRB a sollicité du magistrat instructeur l'autorisation de mettre en place un dispositif d'enregistrement sonore dans les cellules de garde à vue qui seraient occupées par M. Y... et M. X... à compter du 24 septembre 2012 au matin pour une durée maximale de 96 heures au commissariat de police de Fontenay-le-Fleury ; que le 6 septembre 2012, le juge d'instruction a pris une ordonnance de soit communiqué au ministère public aux fins de réquisitions ou d'avis sur l'autorisation de sonorisation d'un local de garde à vue, faisant référence au rapport joint de la BRB de la DRPJ

du même jour ; que le 11 septembre 2012, le procureur de la République a émis un avis favorable à l'utilisation de ce dispositif sous réserve que les deux gardés à vue soient placés dans deux cellules distinctes ; que le 17 septembre 2012, le juge d'instruction a rendu une ordonnance motivée d'autorisation de captation et d'enregistrement de paroles en application de l'article 706-96 du Code de procédure pénale, du 24 septembre 2012 au matin au 28 septembre 2012 au matin au plus tard ; qu'à la même date, il a délivré aux enquêteurs une commission rogatoire spéciale à cette fin ; que l'autorisation de sonorisation des cellules de garde à vue de M. Y... et M. X... qui répond aux exigences des articles 706-96 et suivants du Code de procédure pénale est donc régulière ; qu'en outre, les opérations se sont déroulées sous l'autorité et le contrôle du magistrat instructeur ; que la délivrance anticipée, le 17 septembre 2012, de l'ordonnance autorisant la sonorisation et de la commission rogatoire spéciale pour une garde à vue le 24 septembre 2012, soit cinq jours ouvrables à l'avance était nécessaire pour permettre la préparation du dispositif ; qu'elle ne fait grief à personne ;
– que sur la violation alléguée de l'article 62-2 du Code de procédure pénale par cette sonorisation, l'article 62-2 du Code de procédure pénale énumère six critères dont l'un au moins doit être retenu pour justifier d'une mesure de garde à vue ; qu'en l'espèce, pour fonder la mesure de garde à vue prise à l'encontre de M. X..., les enquêteurs ont retenu les objectifs suivants :
– permettre l'exécution des investigations impliquant la présence ou la participation de la personne,
– garantir sa présentation devant le magistrat afin que ce dernier puisse apprécier la suite à donner à l'enquête,
– empêcher que la personne ne se concerte avec d'autres personnes susceptibles d'être ses coauteurs ou complices ;
– que, comme cela a déjà été mentionné, la garde à vue de M. X... n'avait pas pour objet la réalisation de la sonorisation, mais était juridiquement fondée, au regard des éléments déjà réunis à son encontre ; que la sonorisation, qui ne constitue pas un motif de placement en garde à vue, n'a pas à figurer dans l'énumération des critères de l'article 62-2 du Code de procédure pénale ; que la sonorisation n'est pas en contradiction avec le 5° dudit article ; qu'en effet, la concertation à éviter concerne toutes les personnes qui pourraient être impliquées dans la commission de l'infraction et pas seulement celles qui se trouvent en garde à vue en même temps ; qu'en l'espèce, l'enquête avait déjà établi que quatre personnes s'étaient réunies à Villetaneuse avant le vol de la bijouterie et que trois l'avaient commis ; que lors de la garde à vue de M. Y... et M. X..., il restait encore à identifier et à interpeller au moins deux personnes, à savoir le troisième auteur du vol, et la personne qui a pris en charge ces trois auteurs à Argenteuil après l'incendie de la BMW ;
– qu'en conséquence, la garde à vue de M. X... avait notamment pour objectif d'empêcher des concertations frauduleuses avec ces deux personnes ; que la sonorisation n'est donc ni un détournement des

dispositions encadrant la garde à vue, ni une violation de l'article 62-2 du Code de procédure pénale ;
– que sur la violation invoquée de l'article 63-1 du Code de procédure pénale par la sonorisation, l'article 63-1 du Code de procédure pénale en son 3° dispose que la personne gardée à vue est informée de son droit lors des auditions, de se taire ; que comme le spécifie cette disposition, et contrairement à ce qui est soutenu, le droit au silence ne s'applique qu'aux auditions, et non aux périodes de repos qui séparent les auditions, qu'il n'est ni démontré ni même allégué que M. X… aurait été incité à converser avec M. Y… qui occupait une cellule distincte de la sienne pendant les temps de repos ; que la sonorisation des geôles n'est donc pas constitutive d'une violation du droit de se taire ; que le dispositif critiqué et le droit au silence s'appliquaient a des phases différentes de la garde à vue ;
– que sur la violation alléguée du droit au respect de la vie privée par la sonorisation, la notion même de garde à vue, mesure privative de liberté, très encadrée par la loi quant à sa justification, sa durée et aux modalités de son déroulement est exclusive de celle de vie privée ; que même pendant les périodes de repos passées en geôles, les personnes gardées à vue doivent faire l'objet d'une surveillance constante pour assurer leur sécurité, celle des autres et la protection des locaux qu'ils occupent, que la captation, la fixation, la transmission et l'enregistrement de paroles prononcées par des personnes depuis leurs cellules de garde à vue ne constituent pas non plus une violation de l'article 8-1 de la Convention européenne des droits de l'homme puisqu'ils s'inscrivent dans le cadre des prérogatives autorisées par l'article 8-2 de ladite convention qui permet l'ingérence d'une autorité publique dans l'exercice du droit au respect de la vie privée lorsque cette ingérence est prévue par la loi et qu'elle constitue une mesure nécessaire à la défense de l'ordre, telle que la manifestation de la vérité dans une procédure criminelle prévue par l'article 81, alinéa 1, du Code de procédure pénale ;
– que sur l'association de la garde à vue et de la sonorisation des geôles qui constituerait un procédé déloyal de recueil de la preuve, ce mode de recueil de la preuve ne doit pas être considéré comme déloyal ou susceptible de porter atteinte aux droits de la défense, dès lors que les règles relatives à la garde à vue et les droits inhérents à cette mesure ont été respectés, et que la sonorisation a été menée conformément aux restrictions et aux règles procédurales protectrices des droits fondamentaux posées expressément par la commission rogatoire du juge d'instruction, et qu'il peut être discuté tout au long de la procédure ; qu'il résulte de tout ce qui précède que l'ordonnance de soit communiqué du 25 avril 2012 et le réquisitoire supplétif du 26 avril 2012 étaient justifiés en fait et en droit et n'avaient pas pour objectif le recours à la sonorisation des geôles de garde à vue qui sera autorisée près de cinq mois plus tard, que l'autorisation de sonorisation a été délivrée dans le respect des articles 706-96 et suivants du Code de procédure pénale ; que ce dispositif a été utilisé conformément aux exigences légales, selon les modalités fixées par le magistrat instructeur et sous son autorité et son contrôle ; que la

garde à vue de M. X... a été décidée en application de l'article 62-2 du Code de procédure pénale et non pour permettre l'enregistrement des propos qu'il serait susceptible de tenir depuis sa cellule ; que tout au long de cette mesure, il a bénéficié des droits garantis par la loi ; que la sonorisation des geôles n'a violé ni l'article 62-2, ni le droit de se taire prévu par l'article 63-1, 3°, du Code de procédure pénale ; que la sonorisation ne constitue pas une violation du droit au respect de la vie privée, et est autorisée par l'article 8-2 de la Convention européenne de sauvegarde et de protection des droits de l'homme ; que l'association de la garde à vue et de la sonorisation n'est pas constitutive d'un mode déloyal de recueil de la preuve ; qu'en conséquence, la procédure est régulière et qu'il n'y a pas lieu de procéder aux annulations sollicitées ;

« 1°) alors que la procédure pénale doit être équitable et contradictoire et préserver l'équilibre des droits des parties ; que si la sonorisation de lieux privés ou publics est légalement prévue par l'article 706-96 du Code de procédure pénale en matière de criminalité organisée, elle ne saurait être mise en œuvre durant le repos d'un gardé à vue dans sa cellule ; qu'en effet, la combinaison de ces deux mesures coercitives destinées à la manifestation de la vérité porte une atteinte intolérable aux droits de la défense ; qu'en conséquence, il appartenait à la chambre de l'instruction de prononcer leur annulation ;

« 2°) alors qu'en tout état de cause, une sonorisation mise en œuvre durant une mesure de garde à vue constitue un stratagème actif de la part des autorités policières et judiciaires ; qu'en l'espèce, la sonorisation de la cellule de M. X..., placé dans une cellule contiguë à celle de son complice présumé durant leur temps de repos, assurait aux enquêteurs le recueil de propos qu'ils n'auraient pu intercepter dans d'autres circonstances ; qu'il résulte de cette violation évidente du principe de loyauté de la preuve que les éléments ainsi recueillis devaient être écartés des débats ;

« 3°) alors que, par ailleurs, la garde à vue est une mesure de contrainte judiciaire qui ne peut se dérouler que lorsqu'elle constitue l'unique moyen de parvenir à l'un des objectifs précisément fixés par l'article 62-2 du Code de procédure pénale ; qu'en l'espèce, tant la garde à vue que la mesure de sonorisation ont été planifiées à l'avance en vue d'une sonorisation de la cellule du demandeur ainsi que de celle d'une autre personne impliquée dans l'affaire ; que la chambre de l'instruction ne pouvait se retrancher derrière les autres objectifs mentionnés sur le procès-verbal par les enquêteurs pour refuser d'annuler cette mesure dont le but a été illégalement détourné ;

« 4°) alors que l'article 63-1 du Code de procédure pénale impose la notification au gardé à vue, dès le début de la mesure, de son droit de faire des déclarations, de répondre aux questions qui lui sont posées, ou de se taire ; que tel qu'il est garanti par l'article 6 de la Convention européenne, le droit de ne pas s'incriminer soi-même concerne le respect

de la détermination d'un accusé à garder le silence et présuppose que, dans une affaire pénale, l'accusation cherche à fonder son argumentation sans recourir à des éléments de preuve obtenus par la contrainte ou des pressions, au mépris de la volonté de l'accusé ; que la sonorisation des cellules de garde à vue visant à surprendre les propos de la personne durant son temps de repos est manifestement contraire aux textes précités ;

« 5°) alors qu'il résulte de la jurisprudence européenne que l'enregistrement des voix des requérants lors de leur inculpation et à l'intérieur de leur cellule au commissariat constitue une ingérence dans leur droit au respect de leur vie privée au sens de l'article 8 § 1 de la Convention européenne et doit donc être prévue par la loi ; qu'en l'espèce, si l'article 706-96 du Code pénal prévoit les modalités de la sonorisation en tous lieux privés ou publics, en matière de criminalité organisée, aucune disposition légale ni aucune jurisprudence ne permettait au demandeur de prévoir qu'il était susceptible d'être mis sur écoute durant le déroulé même de sa mesure de garde à vue ; qu'il en résulte que la condition selon laquelle l'ingérence dans le droit à la vie privée doit être prévue par la loi n'est pas remplie, de sorte qu'il y a eu violation de l'article 8 de la Convention européenne ;

« 6°) alors que, subsidiairement, l'ingérence n'est autorisée par l'article 8 § 2 de la Convention européenne que si elle constitue une mesure nécessaire dans une société démocratique et proportionnelle à l'objectif visé ; qu'en l'espèce, la mise en œuvre de la sonorisation des geôles de garde à vue ne répond pas à ce critère de nécessité dès lors qu'elle est motivée, de façon abstraite et générale, par la « difficulté des enquêteurs à rassembler des éléments de preuve » sans qu'il soit justifié de l'existence d'autres obstacles spécifiques liés au déroulement des investigations " ;

Vu l'article 6 de la Convention européenne des droits de l'homme et l'article préliminaire du Code de procédure pénale, ensemble le principe de loyauté des preuves ;

Attendu que porte atteinte au droit à un procès équitable et au principe de loyauté des preuves le stratagème qui en vicie la recherche par un agent de l'autorité publique ;

Attendu qu'il résulte de l'arrêt attaqué et des pièces de la procédure que, dans le cadre d'une information ouverte à la suite d'un vol à main armée, le juge d'instruction a, par ordonnance, prise sur le fondement des articles 706-92 à 706-102 du Code de procédure pénale, autorisé la mise en place d'un dispositif de sonorisation dans les cellules de garde à vue d'un commissariat de police ; que MM. Y... et X..., identifiés comme ayant pu participer aux faits objet de la poursuite, ont été placés en garde à vue dans deux cellules contiguës et ont pu, ainsi, communiquer pendant leurs périodes de repos ; qu'au cours de ces périodes, ont été enregistrés des propos de M. X... par lesquels il s'incriminait lui-même ;

que celui-ci, mis en examen et placé en détention provisoire, a déposé une requête en annulation de pièces de la procédure ;

Attendu que, pour écarter les moyens de nullité des procès-verbaux de placement et d'auditions en garde à vue, des pièces d'exécution de la commission rogatoire technique relative à la sonorisation des cellules de garde à vue et de la mise en examen, pris de la violation du droit de se taire, du droit au respect de la vie privée et de la déloyauté dans la recherche de la preuve, la chambre de l'instruction énonce que le mode de recueil de la preuve associant la garde à vue et la sonorisation des cellules de la garde à vue ne doit pas être considéré comme déloyal ou susceptible de porter atteinte aux droits de la défense, dès lors que les règles relatives à la garde à vue et les droits inhérents à cette mesure ont été respectés et que la sonorisation a été menée conformément aux restrictions et aux règles procédurales protectrices des droits fondamentaux posées expressément par la commission rogatoire du juge d'instruction et qu'il peut être discuté tout au long de la procédure ;

Mais attendu qu'en statuant ainsi, alors que la conjugaison des mesures de garde à vue, du placement de MM. Y... et X... dans des cellules contiguës et de la sonorisation des locaux participait d'un stratagème constituant un procédé déloyal de recherche des preuves, lequel a amené M. X... à s'incriminer lui-même au cours de sa garde à vue, la chambre de l'instruction a méconnu les textes susvisés et le principe ci-dessus énoncé ;

D'où il suit que la cassation est encourue ;

Par ces motifs :

CASSE et ANNULE, en toutes ses dispositions, l'arrêt susvisé de la chambre de l'instruction de la cour d'appel de Versailles, en date du 4 juillet 2013, et pour qu'il soit à nouveau jugé, conformément à la loi,

RENVOIE la cause et les parties devant la chambre de l'instruction de la cour d'appel de Paris, à ce désignée par délibération spéciale prise en chambre du conseil ;

ORDONNE l'impression du présent arrêt, sa transcription sur les registres du greffe de la chambre de l'instruction de la cour d'appel de Versailles et sa mention en marge ou à la suite de l'arrêt annulé ;

Ainsi fait et jugé par la Cour de cassation, chambre criminelle, et prononcé par le président le sept janvier deux mille quatorze ;

En foi de quoi le présent arrêt a été signé par le président, le rapporteur et le greffier de chambre ;

Décision attaquée : Chambre de l'instruction de la cour d'appel de Versailles, du 4 juillet 2013

Décision du Conseil constitutionnel nº 2014-693 DC du 25 mars 2014 – Loi relative à la géolocalisation

Le Conseil constitutionnel a été saisi, dans les conditions prévues à l'article 61, deuxième alinéa, de la Constitution, de la loi relative à la géolocalisation, le 27 février 2014, par MM. Bruno Le Roux, Avi Assouly, Alexis Bachelay, Jean-Paul Bacquet, Dominique Baert, Gérard Bapt, Serge Bardy, Christian Bataille, Mme Kheria Bouziane, MM. Jean-Louis Bricout, Jean-Jacques Bridey, Alain Calmette, Mme Colette Capdevielle, M. Christophe Caresche, Mme Fanélie Carrey-Conte, M. Christophe Castaner, Mme Marie-Anne Chapdelaine, M. Alain Claeys, Mmes Marie-Françoise Clergeau, Carole Delga, Françoise Descamps-Crosnier, MM. Jean-Pierre Dufau, William Dumas, Mme Laurence Dumont, MM. Olivier Dussopt, Christian Eckert, Matthias Fekl, Jean Pierre Fougerat, Mme Michèle Fournier-Armand, MM. Christian Franqueville, Jean-Marc Germain, Jean-Patrick Gille, Marc Goua, Mme Chantal Guittet, M. Régis Juanico, Mme Chaynesse Khirouni, M. Jean-Marie Le Guen, Mme Annie Le Houerou, M. Michel Lefait, Mme Martine Lignières-Cassou, MM. François Loncle, Jean Philippe Mallé, Mme Jacqueline Maquet, M. Jean-René Marsac, Mme Sandrine Mazetier, MM. Michel Ménard, Kléber MESQUIDA, Pierre-Alain Muet, Philippe Nauche, Mme Ségolène Neuville, M. Philippe Plisson, Mme Émilienne Poumirol, MM. Michel Pouzol, Denys Robiliard, Mme Odile Saugues, MM. Gilbert Sauvan, Christophe Sirugue, Mme Julie Sommaruga, M. Gérard Terrier, Mme Sylvie Tolmont, MM. Jean-Louis Touraine et Jean-Jacques Urvoas, députés.

LE CONSEIL CONSTITUTIONNEL,

Vu la Constitution ;

Vu l'ordonnance nº 58-1067 du 7 novembre 1958 modifiée portant loi organique sur le Conseil constitutionnel ;

Vu le Code de procédure pénale ;

Vu les observations du Gouvernement, enregistrées le 18 mars 2014 ;

Le rapporteur ayant été entendu ;

1. Considérant que les députés requérants défèrent au Conseil constitutionnel la loi relative à la géolocalisation ; qu'ils demandent au Conseil constitutionnel de se prononcer sur la conformité aux droits de la défense de l'article 230-40 du Code de procédure pénale tel qu'il résulte de l'article 1er ;

– SUR L'ARTICLE 1er :

2. Considérant que l'article 1er de la loi complète le titre IV du livre Ier du Code de procédure pénale par un chapitre V intitulé « De la géolocalisation » et comprenant les articles 230-32 à 230-44 ;

3. Considérant que l'article 230-32 définit la géolocalisation comme « tout moyen technique destiné à la localisation en temps réel, sur l'ensemble du territoire national, d'une personne, à l'insu de celle-ci, d'un véhicule ou de tout autre objet, sans le consentement de son propriétaire ou de son possesseur » ; que les articles 230-32 et 230-33 définissent les cas dans lesquels le recours à cette technique de surveillance peut être autorisé ainsi que les modalités et la durée de cette autorisation ;

4. Considérant que l'article 230-34 définit les conditions dans lesquelles le procureur de la République, le juge d'instruction ou le juge des libertés et de la détention, selon le type d'enquête ou d'instruction et l'incrimination des faits, peuvent, lorsque les nécessités de l'enquête ou de l'instruction l'exigent, autoriser l'introduction dans certains lieux privés ou dans un véhicule aux fins de mettre en place ou de retirer le moyen technique permettant la géolocalisation ;

5. Considérant que l'article 230-35 prévoit qu'en cas d'urgence résultant d'un risque imminent de dépérissement des preuves ou d'atteinte grave aux personnes ou aux biens, les opérations de géolocalisation peuvent être mises en place ou prescrites par un officier de police judiciaire qui en informe immédiatement le procureur de la République ou le juge d'instruction, lequel peut en ordonner la mainlevée ;

6. Considérant que les articles 230-38 et 230-39 prévoient que l'officier de police judiciaire dresse procès-verbal des opérations de mise en place du moyen technique de géolocalisation, des opérations d'enregistrement des données de localisation et des données enregistrées qui sont utiles à la manifestation de la vérité ; que l'article 230-43 prévoit la destruction des enregistrements des données de localisation à l'expiration du délai de prescription de l'action publique ;

7. Considérant que les articles 230-40 à 230-42 fixent les conditions dans lesquelles le juge des libertés et de la détention peut autoriser que certaines informations relatives à l'installation ou au retrait du moyen technique de géolocalisation ou l'enregistrement des données de localisation et les éléments permettant d'identifier une personne ayant concouru à l'installation ou au retrait du moyen technique n'apparaissent pas dans le dossier de la procédure d'instruction ;

8. Considérant que l'article 230-44 prévoit que les dispositions du chapitre V précité ne sont pas applicables lorsque les opérations de géolocalisation ont pour objet la localisation d'un équipement terminal de communication électronique, d'un véhicule ou de tout autre objet dont le propriétaire ou le possesseur légitime est la victime de l'infraction sur laquelle porte l'enquête ou l'instruction ou la personne disparue, dès lors que ces opérations ont pour objet de retrouver la victime, l'objet qui lui a été dérobé ou la personne disparue ;

En ce qui concerne la mise en œuvre de la géolocalisation :

9. Considérant que le législateur tient de l'article 34 de la Constitution l'obligation de fixer lui-même le champ d'application de la loi pénale ; que, s'agissant de la procédure pénale, cette exigence s'impose notamment pour éviter une rigueur non nécessaire lors de la recherche des auteurs d'infractions ;

10. Considérant qu'il incombe au législateur d'assurer la conciliation entre, d'une part, la prévention des atteintes à l'ordre public et la recherche des auteurs d'infractions, toutes deux nécessaires à la sauvegarde de droits et de principes de valeur constitutionnelle, et, d'autre part, l'exercice des droits et des libertés constitutionnellement garantis ; qu'au nombre de celles-ci figurent la liberté d'aller et venir, qui découle de l'article 4 de la Déclaration des droits de l'homme et du citoyen de 1789, et le droit au respect de la vie privée, l'inviolabilité du domicile et le secret des correspondances, protégés par son article 2 ;

11. Considérant qu'il résulte de l'article 66 de la Constitution que la police judiciaire doit être placée sous la direction et le contrôle de l'autorité judiciaire ;

12. Considérant que si le législateur peut prévoir des mesures d'investigation spéciales en vue de constater des crimes et délits d'une gravité et d'une complexité particulières, d'en rassembler les preuves et d'en rechercher les auteurs, c'est sous réserve, d'une part, que les restrictions qu'elles apportent aux droits constitutionnellement garantis soient proportionnées à la gravité et à la complexité des infractions commises et n'introduisent pas de discriminations injustifiées et, d'autre part, que ces mesures soient conduites dans le respect des prérogatives de l'autorité judiciaire à qui il incombe en particulier de garantir que leur mise en œuvre soit nécessaire à la manifestation de la vérité ;

Quant au droit au respect de la vie privée :

13. Considérant que la géolocalisation est une mesure de police judiciaire consistant à surveiller une personne au moyen de procédés techniques en suivant, en temps réel, la position géographique d'un véhicule que cette personne est supposée utiliser ou de tout autre objet, notamment un téléphone, qu'elle est supposée détenir ; que la mise en œuvre de ce procédé n'implique pas d'acte de contrainte sur la personne visée ni d'atteinte à son intégrité corporelle, de saisie, d'interception de correspondance ou d'enregistrement d'image ou de son ; que l'atteinte à la vie privée qui résulte de la mise en œuvre de ce dispositif consiste dans la surveillance par localisation continue et en temps réel d'une personne, le suivi de ses déplacements dans tous lieux publics ou privés ainsi que dans l'enregistrement et le traitement des données ainsi obtenues ;

14. Considérant que le recours à la géolocalisation ne peut avoir lieu que lorsque l'exigent les nécessités de l'enquête ou de l'instruction concernant un crime ou un délit puni d'une peine d'emprisonnement

d'au moins trois ans, s'agissant d'atteinte aux personnes, d'aide à l'auteur ou au complice d'un acte de terrorisme ou d'évasion, ou d'au moins cinq ans d'emprisonnement, s'agissant de toute autre infraction, ainsi qu'à des enquêtes ou instructions portant sur la recherche des causes de la mort, des causes de la disparition d'une personne ou des procédures de recherche d'une personne en fuite ;

15. Considérant que le recours à la géolocalisation est placé sous la direction et le contrôle de l'autorité judiciaire ; que, dans les cas prévus par le 1° de l'article 230-33, le procureur de la République ne peut l'autoriser que pour une durée maximale de 15 jours consécutifs ; qu'à l'issue de ce délai, elle est autorisée par le juge des libertés et de la détention pour une durée maximale d'un mois renouvelable ; que, dans les cas prévus au 2° du même article, le juge d'instruction peut l'autoriser pour une durée maximale de quatre mois renouvelable ; que, lorsqu'en cas d'urgence elle est mise en place ou prescrite par un officier de police judiciaire, le procureur de la République ou le juge d'instruction, immédiatement informé, peut en prescrire la mainlevée ;

Quant à l'inviolabilité du domicile :

16. Considérant que, lorsque la mise en place ou le retrait du moyen technique permettant la géolocalisation rend nécessaire l'introduction, y compris de nuit, dans un lieu privé, celle-ci doit être autorisée par décision écrite, selon le cas, du procureur de la République, du juge d'instruction ou du juge de la liberté et de la détention, au regard de la gravité et de la complexité des faits et des nécessités de l'enquête ou de l'instruction ; qu'en cas d'urgence défini à l'article 230-35, l'opération peut être mise en place par l'officier de police judiciaire qui en informe immédiatement le magistrat qui dispose de vingt-quatre heures pour prescrire par décision écrite la poursuite des opérations ; que, si l'introduction dans un lieu d'habitation est nécessaire, l'opération ne peut, en tout état de cause, être mise en place sans l'autorisation préalable du juge compétent donnée par tout moyen ; que l'introduction dans des lieux privés à usage d'entrepôt ou dans un véhicule sur la voie publique ou dans de tels lieux n'est possible que si l'opération est exigée pour les nécessités d'une enquête ou d'une instruction relative à un crime ou un délit contre les personnes ou pour des délits particuliers, punis d'un emprisonnement d'au moins trois ans ; que, s'il s'agit d'un autre lieu privé, l'introduction n'est possible que lorsque l'enquête ou l'instruction est relative à un crime ou un délit puni d'au moins cinq ans d'emprisonnement ou dans le cas d'une procédure ou d'une instruction pour recherche des causes de la mort ou de la disparition, ou d'une procédure de recherche d'une personne en fuite ; que le cinquième alinéa de l'article 230-34 interdit la mise en place d'un moyen technique de géolocalisation dans l'un des lieux mentionnés aux articles 56-1 à 56-4 du Code de procédure pénale et dans le bureau ou le domicile des personnes mentionnées à son article 100-7 ;

17. Considérant qu'il résulte de tout ce qui précède que le législateur a entouré la mise en œuvre de la géolocalisation de mesures de nature à garantir que, placées sous l'autorisation et le contrôle de l'autorité judiciaire, les restrictions apportées aux droits constitutionnellement garantis soient nécessaires à la manifestation de la vérité et ne revêtent pas un caractère disproportionné au regard de la gravité et de la complexité des infractions commises ; que, par ces dispositions, le législateur n'a pas opéré entre les droits et libertés en cause une conciliation déséquilibrée ;

En ce qui concerne le dossier de la procédure :

18. Considérant 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 » ; que sont garantis par cette disposition le droit des personnes intéressées à exercer un recours juridictionnel effectif ainsi que le respect des droits de la défense qui implique en particulier l'existence d'une procédure juste et équitable garantissant l'équilibre des droits des parties ;

19. Considérant que l'officier de police judiciaire ou l'agent de police judiciaire agissant sous sa responsabilité dresse procès-verbal de chacune des opérations de mise en place du moyen de géolocalisation et des opérations d'enregistrement des données de localisation, qui mentionne la date et l'heure auxquelles l'opération a commencé et celles auxquelles elle s'est terminée ; qu'il décrit ou transcrit, dans un procès-verbal versé au dossier, les données enregistrées utiles à la manifestation de la vérité ; que, toutefois, les dispositions de l'article 230-40 permettent que les informations relatives à la date, l'heure et le lieu où le moyen technique de géolocalisation a été installé ou retiré, ainsi que l'enregistrement des données de localisation et les éléments permettant d'identifier une personne ayant concouru à l'installation ou au retrait de ce moyen, n'apparaissent pas dans le dossier de la procédure mais soient inscrits dans un procès-verbal versé dans un dossier distinct de la procédure auquel les parties n'ont pas accès et dans lequel figure également la requête du juge d'instruction aux fins de mise en œuvre de cette procédure ; que ces informations sont inscrites sur un registre coté et paraphé ouvert à cet effet au tribunal de grande instance ;

Quant aux articles 230-40 et 230-41 :

20. Considérant, en premier lieu, qu'en vertu de l'article 230-40, cette possibilité n'est ouverte que dans le cadre d'une information judiciaire portant sur des crimes et délits relevant de la criminalité ou la délinquance organisées entrant dans le champ d'application de l'article 706-73 du Code de procédure pénale ; qu'elle n'est permise que lorsque, d'une part, « la connaissance de ces informations est susceptible de mettre gravement en danger la vie ou l'intégrité physique d'une personne, des membres de sa famille ou de ses proches » et, d'autre part, lorsque cette connaissance « n'est ni utile à la manifestation de la vérité

ni indispensable à l'exercice des droits de la défense » ; que l'autorisation d'y recourir est prise par décision motivée du juge des libertés et de la détention saisi par requête motivée du juge d'instruction ;

21. Considérant, en deuxième lieu, que, si la procédure prévue à l'article 230-40 est mise en œuvre, sont néanmoins versées à la procédure la décision écrite du magistrat autorisant la géolocalisation en application de l'article 230-33, la décision du magistrat autorisant, le cas échéant, l'introduction dans un lieu privé en application de l'article 230-34, la décision du juge des libertés et de la détention autorisant le recours à la procédure prévue à l'article 230-40 ainsi que les opérations d'enregistrement des données de localisation qui ne permettent pas d'identifier une personne ayant concouru à l'installation ou au retrait du moyen technique de géolocalisation ;

22. Considérant, en troisième lieu, que l'article 230-41 dispose que la personne mise en examen ou le témoin assisté peut contester devant le président de la chambre de l'instruction le recours à la procédure prévue par l'article 230-40 ; que ce magistrat peut annuler la géolocalisation s'il estime que les opérations de géolocalisation n'ont pas été réalisées de façon régulière, que les conditions prévues par l'article 230-40 ne sont pas réunies ou que les informations qui n'ont pas été versées à la procédure sont indispensables à l'exercice des droits de la défense ; qu'il peut également ordonner le versement de ces informations au dossier de la procédure s'il estime que leur connaissance n'est pas ou n'est plus susceptible de mettre gravement en danger la vie ou l'intégrité physique d'une personne, des membres de sa famille ou de ses proches ;

23. Considérant que, toutefois, le délai de dix jours dans lequel la personne mise en examen ou le témoin assisté peut contester le recours à la procédure prévue par l'article 230-40 court « à compter de la date à laquelle il lui a été donné connaissance du contenu des opérations de géolocalisation réalisées dans le cadre prévu » à cet article ; qu'eu égard à la complexité des investigations en matière de criminalité et de délinquance organisées, ces dispositions ne sauraient, sans méconnaître les droits de la défense, être interprétées comme permettant que le délai de dix jours commence à courir avant que la décision du juge des libertés et de la détention rendue en application de l'article 230-40 ne soit formellement portée à la connaissance de la personne mise en examen ou du témoin assisté ; qu'en outre, les droits de la défense seraient également méconnus si la chambre de l'instruction, saisie dans les conditions prévues par les articles 170 et suivants du Code de procédure pénale, aux fins d'annulation des actes relatifs aux autorisations d'installation du dispositif technique de géolocalisation et à leur enregistrement, ne pouvait également exercer le contrôle et prendre les décisions prévus par l'article 230-41 dudit Code ;

24. Considérant que, sous les réserves énoncées au considérant précédent, les dispositions des articles 230-40 et 230-41 ne sont pas contraires à l'article 16 de la Déclaration de 1789 ;

Quant à l'article 230-42 :

25. Considérant que le principe du contradictoire et le respect des droits de la défense impliquent en particulier qu'une personne mise en cause devant une juridiction répressive ait été mise en mesure, par elle-même ou par son avocat, de contester les conditions dans lesquelles ont été recueillis les éléments de preuve qui fondent sa mise en cause ;

26. Considérant que l'article 230-42 prévoit qu'aucune condamnation ne peut être prononcée « sur le seul fondement » des éléments recueillis dans les conditions prévues à l'article 230 40, sauf si la requête et le procès-verbal mentionnés au dernier alinéa de ce même article ont été versés au dossier en application de l'article 230-41 ; qu'en permettant ainsi qu'une condamnation puisse être prononcée sur le fondement d'éléments de preuve alors que la personne mise en cause n'a pas été mise à même de contester les conditions dans lesquelles ils ont été recueillis, ces dispositions méconnaissent les exigences constitutionnelles qui résultent de l'article 16 de la Déclaration de 1789 ; que, par suite, à l'article 230-42, le mot « seul » doit être déclaré contraire à la Constitution ; que, par voie de conséquence, sauf si la requête et le procès-verbal mentionnés au dernier alinéa de l'article 230-40 ont été versés au dossier en application de l'article 230-41, il appartiendra à la juridiction d'instruction d'ordonner que les éléments recueillis dans les conditions prévues à l'article 230-40 soient retirés du dossier de l'information avant la saisine de la juridiction de jugement ; que, pour le surplus et sous cette réserve, l'article 230-42 ne méconnaît pas l'article 16 de la Déclaration de 1789 ;

27. Considérant qu'il résulte de tout ce qui précède que, sous les réserves énoncées aux considérants 23 et 26, le surplus de l'article 1er de la loi, qui ne méconnaît aucune autre exigence constitutionnelle, doit être déclaré conforme à la Constitution ;

– SUR L'ARTICLE 3 :

28. Considérant qu'aux termes de la seconde phrase du premier alinéa de l'article 45 de la Constitution : « Sans préjudice de l'application des articles 40 et 41, tout amendement est recevable en première lecture dès lors qu'il présente un lien, même indirect, avec le texte déposé ou transmis » ;

29. Considérant que l'article 3 modifie l'article 706-161 du Code de procédure pénale pour modifier les compétences de l'Agence de gestion et de recouvrement des avoirs saisis et confisqués ; que cet article, introduit par voie d'amendement au Sénat en première lecture, ne présente pas de lien avec les dispositions qui figuraient dans le projet de loi ; que, par suite, il a été adopté selon une procédure contraire à la Constitution ;

30. Considérant qu'il n'y a lieu, pour le Conseil constitutionnel, de soulever d'office aucune autre question de constitutionnalité,

DÉCIDE : Article 1er. – Sont contraires à la Constitution les dispositions suivantes de la loi relative à la géolocalisation : – à l'article 1er, le mot « seul » figurant à l'article 230-42 du Code de procédure pénale ; – l'article 3. Article 2. – Sous les réserves énoncées aux considérants 23 et 26, le surplus de l'article 1er de la même loi est conforme à la Constitution. Article 3. – La présente décision sera publiée au *Journal officiel de la République française*. Délibéré par le Conseil constitutionnel dans sa séance du 25 mars 2014 où siégeaient : M. Jean-Louis Debré, Président, Mmes Claire Bazy Malaurie, Nicole Belloubet, MM. Guy Canivet, Michel Charasse, Renaud Denoix de Saint Marc et Mme Nicole Maestracci.

JORF du 29 mars 2014 page 6125, texte no 2 (@ 2)

ECLI : FR : CC : 2014 : 2014.693. DC

Arrêt de la Cour de justice de l'Union européenne – grande chambre – 8 avril 2014

ARRÊT DE LA COUR (grande chambre)

8 avril 2014

«Communications électroniques – Directive 2006/24/CE – Services de communications électroniques accessibles au public ou de réseaux publics de communications – Conservation de données générées ou traitées dans le cadre de la fourniture de tels services – Validité – Articles 7, 8 et 11 de la charte des droits fondamentaux de l'Union européenne »

Dans les affaires jointes C-293/12 et C-594/12,

ayant pour objet des demandes de décision préjudicielle au titre de l'article 267 TFUE, introduites par la High Court (Irlande) et le Verfassungsgerichtshof (Autriche), par décisions, respectivement, des 27 janvier et 28 novembre 2012, parvenues à la Cour les 11 juin et 19 décembre 2012, dans les procédures

Digital Rights Ireland Ltd (C-293/12)

contre

Minister for Communications, Marine and Natural Resources,

Minister for Justice, Equality and Law Reform,

Commissioner of the Garda Síochána,

Irlande,

The Attorney General,

en présence de :

Irish Human Rights Commission,

et

Kärntner Landesregierung (C-594/12),

Michael Seitlinger,

Christof Tschohl e.a.,

LA COUR (grande chambre),

composée de M. V. Skouris, président, M. K. Lenaerts, vice-président, M. A. Tizzano, Mme R. Silva de Lapuerta, MM. T. von Danwitz (rapporteur), E. Juhász, A. Borg Barthet, C. G. Fernlund et J. L. da Cruz Vilaça, présidents de chambre, MM. A. Rosas, G. Arestis, J. -C. Bonichot, A. Arabadjiev, Mme C. Toader et M. C. Vajda juges,

avocat général : M. P. Cruz Villalón,

greffier : M. K. Malacek, administrateur,

vu la procédure écrite et à la suite de l'audience du 9 juillet 2013,

considérant les observations présentées :
– pour Digital Rights Ireland Ltd, par MM. F. Callanan, SC, et F. Crehan, BL, mandatés par M. S. McGarr, solicitor,
– pour M. Seitlinger, par Me G. Otto, Rechtsanwalt,
– pour M. Tschohl e. a., par Me E. Scheucher, Rechtsanwalt,
– pour l'Irish Human Rights Commission, par M. P. Dillon Malone, BL, mandaté par Mme S. Lucey, solicitor,
– pour l'Irlande, par Mme E. Creedon et M. D. McGuinness, en qualité d'agents, assistés de MM. E. Regan, SC, et D. Fennelly, JC,
– pour le gouvernement autrichien, par MM. G. Hesse et G. Kunnert, en qualité d'agents,
– pour le gouvernement espagnol, par Mme N. Díaz Abad, en qualité d'agent,
– pour le gouvernement français, par MM. G. de Bergues et D. Colas ainsi que par Mme B. Beaupère-Manokha, en qualité d'agents,
– pour le gouvernement italien, par Mme G. Palmieri, en qualité d'agent, assistée de M. A. De Stefano, avvocato dello Stato,
– pour le gouvernement polonais, par MM. B. Majczyna et M. Szpunar, en qualité d'agents,
– pour le gouvernement portugais, par M. L. Inez Fernandes et Mme C. Vieira Guerra, en qualité d'agents,
– pour le gouvernement du Royaume-Uni, par M. L. Christie, en qualité d'agent, assisté de Mme S. Lee, barrister,
– pour le Parlement européen, par MM. U. Rösslein et A. Caiola ainsi que par Mme K. Zejdová, en qualité d'agents,
– pour le Conseil de l'Union européenne, par MM. J. Monteiro et E. Sitbon ainsi que par Mme I. Šulce, en qualité d'agents,

– pour la Commission européenne, par Mme D. Maidani ainsi que par MM. B. Martenczuk et M. Wilderspin, en qualité d'agents,

ayant entendu l'avocat général en ses conclusions à l'audience du 12 décembre 2013,

rend le présent

Arrêt

1 Les demandes de décision préjudicielle portent sur la validité de la directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE (JO L 105, p. 54).

2 La demande présentée par la High Court (affaire C-293/12) concerne un litige opposant Digital Rights Ireland Ltd (ci-après «Digital Rights») au Minister for Communications, Marine and Natural Resources, au Minister for Justice, Equality and Law Reform, au Commissioner of the Garda Síochána, à l'Irlande ainsi qu'à l'Attorney General au sujet de la légalité de mesures législatives et administratives nationales concernant la conservation de données relatives à des communications électroniques.

3 La demande présentée par le Verfassungsgerichtshof (affaire C-594/12) est relative à des recours en matière constitutionnelle introduits devant cette juridiction respectivement par la Kärntner Landesregierung (gouvernement du Land de Carinthie) ainsi que par MM. Seitlinger, Tschohl et 11 128 autres requérants au sujet de la compatibilité de la loi transposant la directive 2006/24 dans le droit interne autrichien avec la loi constitutionnelle fédérale (Bundes-Verfassungsgesetz).

Le cadre juridique

La directive 95/46/CE

4 La directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO L 281, p. 31), a, conformément à son article 1er, paragraphe 1, pour objet d'assurer la protection des libertés et des droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel.

5 Quant à la sécurité des traitements de telles données, l'article 17, paragraphe 1, de ladite directive dispose :

«Les États membres prévoient que le responsable du traitement doit mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion

ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite.

Ces mesures doivent assurer, compte tenu de l'état de l'art et des coûts liés à leur mise en œuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger. »

La directive 2002/58/CE

6 La directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO L 201, p. 37), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009 (JO L 337, p. 11, ci-après la «directive 2002/58»), a pour objectif, conformément à son article 1er, paragraphe 1, d'harmoniser les dispositions des États membres nécessaires pour assurer un niveau équivalent de protection des droits et des libertés fondamentaux, et en particulier du droit à la vie privée et à la confidentialité, en ce qui concerne le traitement des données à caractère personnel dans le secteur des communications électroniques, ainsi que la libre circulation de ces données et des équipements et des services de communications électroniques dans l'Union européenne. En vertu du paragraphe 2 du même article, les dispositions de cette directive précisent et complètent la directive 95/46 aux fins énoncées au paragraphe 1 susmentionné.

7 En ce qui concerne la sécurité du traitement des données, l'article 4 de la directive 2002/58 prévoit :

«1. Le fournisseur d'un service de communications électroniques accessible au public prend les mesures d'ordre technique et organisationnel appropriées afin de garantir la sécurité de ses services, le cas échéant conjointement avec le fournisseur du réseau public de communications en ce qui concerne la sécurité du réseau. Compte tenu des possibilités techniques les plus récentes et du coût de leur mise en œuvre, ces mesures garantissent un degré de sécurité adapté au risque existant.

1 *bis*. Sans préjudice des dispositions de la directive 95/46/CE, les mesures visées au paragraphe 1, pour le moins :
– garantissent que seules des personnes autorisées peuvent avoir accès aux données à caractère personnel à des fins légalement autorisées,
– protègent les données à caractère personnel stockées ou transmises contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelles et le stockage, le traitement, l'accès et la divulgation non autorisés ou illicites, et
– assurent la mise en œuvre d'une politique de sécurité relative au traitement des données à caractère personnel.

Les autorités nationales compétentes en la matière sont habilitées à vérifier les mesures prises par les fournisseurs de services de communications électroniques accessibles au public, ainsi qu'à émettre des recommandations sur les meilleures pratiques concernant le degré de sécurité que ces mesures devraient atteindre.

2. Lorsqu'il existe un risque particulier de violation de la sécurité du réseau, le fournisseur d'un service de communications électroniques accessible au public informe les abonnés de ce risque et, si les mesures que peut prendre le fournisseur du service ne permettent pas de l'écarter, de tout moyen éventuel d'y remédier, y compris en en indiquant le coût probable. »

8 Quant à la confidentialité des communications et des données relatives au trafic, l'article 5, paragraphes 1 et 3, de ladite directive dispose :

«1. Les États membres garantissent, par la législation nationale, la confidentialité des communications effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles au public, ainsi que la confidentialité des données relatives au trafic y afférentes. En particulier, ils interdisent à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés sauf lorsque cette personne y est légalement autorisée, conformément à l'article 15, paragraphe 1. Le présent paragraphe n'empêche pas le stockage technique nécessaire à l'acheminement d'une communication, sans préjudice du principe de confidentialité.

[…]

3. Les États membres garantissent que le stockage d'informations, ou l'obtention de l'accès à des informations déjà stockées, dans l'équipement terminal d'un abonné ou d'un utilisateur n'est permis qu'à condition que l'abonné ou l'utilisateur ait donné son accord, après avoir reçu, dans le respect de la directive 95/46/CE, une information claire et complète, entre autres sur les finalités du traitement. Cette disposition ne fait pas obstacle à un stockage ou à un accès techniques visant exclusivement à effectuer la transmission d'une communication par la voie d'un réseau de communications électroniques, ou strictement nécessaires au fournisseur pour la fourniture d'un service de la société de l'information expressément demandé par l'abonné ou l'utilisateur. »

9 Aux termes de l'article 6, paragraphe 1, de la directive 2002/58 :

«Les données relatives au trafic concernant les abonnés et les utilisateurs traitées et stockées par le fournisseur d'un réseau public de communications ou d'un service de communications électroniques accessibles au public doivent être effacées ou rendues anonymes lorsqu'elles ne sont plus nécessaires à la transmission d'une communication sans préjudice des paragraphes 2, 3 et 5 du présent article ainsi que de l'article 15, paragraphe 1. »

10 L'article 15 de la directive 2002/58 dispose à son paragraphe 1 :

«Les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale – c'est-à-dire la sûreté de l'État – la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe. Toutes les mesures visées dans le présent paragraphe sont prises dans le respect des principes généraux du droit communautaire, y compris ceux visés à l'article 6, paragraphes 1 et 2, du traité sur l'Union européenne.»

La directive 2006/24

11 Après avoir lancé une consultation auprès des représentants des services répressifs, du secteur des communications électroniques et des experts en matière de protection des données, la Commission a présenté, le 21 septembre 2005, une analyse d'impact des options politiques relatives à des règles concernant la conservation des données relatives au trafic (ci-après l' «analyse d'impact»). Cette analyse a servi de base à l'élaboration de la proposition de directive du Parlement européen et du Conseil sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public, et modifiant la directive 2002/58/CE [COM(2005) 438 final, ci-après la «proposition de directive»], présentée le même jour, qui a abouti à l'adoption de la directive 2006/24 sur le fondement de l'article 95 CE.

12 Le considérant 4 de la directive 2006/24 énonce :

«L'article 15, paragraphe 1, de la directive 2002/58/CE énumère les conditions dans lesquelles les États membres peuvent limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de ladite directive. Toute limitation de ce type doit constituer une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour des raisons spécifiques d'ordre public, à savoir pour sauvegarder la sécurité nationale (c'est-à-dire la sûreté de l'État), la défense et la sécurité publique, ou pour assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées de systèmes de communications électroniques.»

13 Selon la première phrase du considérant 5 de la directive 2006/24, «[p] lusieurs États membres ont légiféré sur la conservation de données par les fournisseurs de services en vue de la prévention, de la recherche, de la détection et de la poursuite d'infractions pénales ».

14 Les considérants 7 à 11 de la directive 2006/24 sont libellés comme suit :

«(7) Dans ses conclusions, le Conseil 'Justice et affaires intérieures' du 19 décembre 2002 souligne qu'en raison de l'accroissement important des possibilités qu'offrent les communications électroniques, les données relatives à l'utilisation de celles-ci sont particulièrement importantes et constituent donc un instrument utile pour la prévention, la recherche, la détection et la poursuite d'infractions pénales, notamment de la criminalité organisée.

(8) Dans sa déclaration du 25 mars 2004 sur la lutte contre le terrorisme, le Conseil européen a chargé le Conseil d'envisager des propositions en vue de l'établissement de règles relatives à la conservation, par les fournisseurs de services, des données relatives au trafic des communications.

(9) En vertu de l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH) [signée à Rome le 4 novembre 1950], toute personne a droit au respect de sa vie privée et de sa correspondance. 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, entre autres, à la sécurité nationale, à la sûreté publique, à la défense de l'ordre et à la prévention des infractions pénales, ou à la protection des droits et des libertés d'autrui. Étant donné que la conservation des données s'est révélée être un outil d'investigation nécessaire et efficace pour les enquêtes menées par les services répressifs dans plusieurs États membres et, en particulier, relativement aux affaires graves telles que celles liées à la criminalité organisée et au terrorisme, il convient de veiller à ce que les données conservées soient accessibles aux services répressifs pendant un certain délai, dans les conditions prévues par la présente directive. […]

(10) Le 13 juillet 2005, le Conseil a réaffirmé, dans sa déclaration condamnant les attentats terroristes de Londres, la nécessité d'adopter dans les meilleurs délais des mesures communes relatives à la conservation de données concernant les télécommunications.

(11) Eu égard à l'importance des données relatives au trafic et des données de localisation pour la recherche, la détection et la poursuite d'infractions pénales, il est nécessaire, comme les travaux de recherche et l'expérience pratique de plusieurs États membres le démontrent, de garantir au niveau européen la conservation pendant un certain délai, dans les conditions prévues par la présente directive, des données

traitées par les fournisseurs de communications électroniques dans le cadre de la fourniture de services de communications électroniques accessibles au public ou d'un réseau public de communications. »

15 Les considérants 16, 21 et 22 de ladite directive précisent :

« (16) Les obligations incombant aux prestataires de services concernant les mesures visant à garantir la qualité des données, qui résultent de l'article 6 de la directive 95/46/CE, tout comme leurs obligations concernant les mesures visant à garantir la confidentialité et la sécurité du traitement des données, qui résultent des articles 16 et 17 de ladite directive, sont pleinement applicables aux données qui sont conservées au sens de la présente directive.

(21) Étant donné que les objectifs de la présente directive, à savoir l'harmonisation des obligations incombant aux fournisseurs de conserver certaines données et de faire en sorte que ces données soient disponibles aux fins de la recherche, de la détection et de la poursuite d'infractions graves telles que définies par chaque État membre dans son droit interne, ne peuvent pas être réalisés de manière suffisante par les États membres et peuvent donc, en raison des dimensions ou des effets de la présente directive, être mieux réalisés au niveau communautaire, la Communauté peut prendre des mesures conformément au principe de subsidiarité consacré à l'article 5 du traité. Conformément au principe de proportionnalité, tel qu'énoncé audit article, la présente directive n'excède pas ce qui est nécessaire pour atteindre ces objectifs.

(22) La présente directive respecte les droits fondamentaux et observe les principes reconnus, notamment, par la charte des droits fondamentaux de l'Union européenne. La présente directive ainsi que la directive 2002/58/CE visent notamment à veiller à ce que les droits fondamentaux liés au respect de la vie privée et des communications des citoyens et à la protection des données à caractère personnel, tels que consacrés aux articles 7 et 8 de la charte, soient pleinement respectés. »

16 La directive 2006/24 prévoit l'obligation des fournisseurs de services de communications électroniques accessibles au public ou des réseaux publics de communications de conserver certaines données qui sont générées ou traitées par ces fournisseurs. À cet égard, les articles 1er à 9, 11 et 13 de cette directive disposent :

Article premier

Objet et champ d'application

1. La présente directive a pour objectif d'harmoniser les dispositions des États membres relatives aux obligations des fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications en matière de conservation de certaines données qui sont générées ou traitées par ces fournisseurs, en vue de garantir la disponibilité de ces données à des fins de recherche,

de détection et de poursuite d'infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne.

2. La présente directive s'applique aux données relatives au trafic et aux données de localisation concernant tant les entités juridiques que les personnes physiques, ainsi qu'aux données connexes nécessaires pour identifier l'abonné ou l'utilisateur enregistré. Elle ne s'applique pas au contenu des communications électroniques, notamment aux informations consultées en utilisant un réseau de communications électroniques.

Article 2

Définitions

1. Aux fins de la présente directive, les définitions contenues dans la directive 95/46/CE, dans 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') [...], ainsi que dans la directive 2002/58/CE s'appliquent.

2. Aux fins de la présente directive, on entend par :

a) 'données', les données relatives au trafic et les données de localisation, ainsi que les données connexes nécessaires pour identifier l'abonné ou l'utilisateur ;

b) 'utilisateur', toute entité juridique ou personne physique qui utilise un service de communications électroniques accessible au public à des fins privées ou professionnelles sans être nécessairement abonnée à ce service ;

c) 'service téléphonique', les appels téléphoniques (notamment les appels vocaux, la messagerie vocale, la téléconférence et la communication de données), les services supplémentaires (notamment le renvoi et le transfert d'appels), les services de messagerie et multimédias (notamment les services de messages brefs, les services de médias améliorés et les services multimédias) ;

d) 'numéro d'identifiant', le numéro d'identification exclusif attribué aux personnes qui s'abonnent ou s'inscrivent à un service d'accès à l'internet ou à un service de communication par l'internet ;

e) 'identifiant cellulaire', le numéro d'identification de la cellule où un appel de téléphonie mobile a commencé ou a pris fin ;

f) 'appel téléphonique infructueux', toute communication au cours de laquelle un appel téléphonique a été transmis mais est resté sans réponse ou a fait l'objet d'une intervention de la part du gestionnaire du réseau.

Article 3

Obligation de conservation de données

1. Par dérogation aux articles 5, 6 et 9 de la directive 2002/58/CE, les États membres prennent les mesures nécessaires pour que les données visées à l'article 5 de la présente directive soient conservées, conformément aux dispositions de cette dernière, dans la mesure où elles sont générées ou traitées dans le cadre de la fourniture des services de communication concernés par des fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications, lorsque ces fournisseurs sont dans leur ressort.

2. L'obligation de conserver les données visées au paragraphe 1 inclut la conservation des données visées à l'article 5 relatives aux appels téléphoniques infructueux, lorsque ces données sont générées ou traitées, et stockées (en ce qui concerne les données de la téléphonie) ou journalisées (en ce qui concerne les données de l'internet), dans le cadre de la fourniture des services de communication concernés, par des fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications, lorsque ces fournisseurs sont dans le ressort de l'État membre concerné. La présente directive n'impose pas la conservation des données relatives aux appels non connectés.

Article 4

Accès aux données

Les États membres prennent les mesures nécessaires pour veiller à ce que les données conservées conformément à la présente directive ne soient transmises qu'aux autorités nationales compétentes, dans des cas précis et conformément au droit interne. La procédure à suivre et les conditions à remplir pour avoir accès aux données conservées dans le respect des exigences de nécessité et de proportionnalité sont arrêtées par chaque État membre dans son droit interne, sous réserve des dispositions du droit de l'Union européenne ou du droit international public applicables en la matière, en particulier la CEDH telle qu'interprétée par la Cour européenne des droits de l'homme.

Article 5

Catégories de données à conserver

1. Les États membres veillent à ce que soient conservées en application de la présente directive les catégories de données suivantes :

a) les données nécessaires pour retrouver et identifier la source d'une communication :

1) en ce qui concerne la téléphonie fixe en réseau et la téléphonie mobile :

i) le numéro de téléphone de l'appelant ;

ii) les nom et adresse de l'abonné ou de l'utilisateur inscrit ;

2) en ce qui concerne l'accès à l'internet, le courrier électronique par l'internet et la téléphonie par l'internet :

i) le(s) numéro(s) d'identifiant attribué(s) ;

ii) le numéro d'identifiant et le numéro de téléphone attribués à toute communication entrant dans le réseau téléphonique public ;

iii) les nom et adresse de l'abonné ou de l'utilisateur inscrit à qui une adresse IP (protocole internet), un numéro d'identifiant ou un numéro de téléphone a été attribué au moment de la communication ;

b) les données nécessaires pour identifier la destination d'une communication :

1) en ce qui concerne la téléphonie fixe en réseau et la téléphonie mobile :

i) le(s) numéro(s) composé(s) [le(s) numéro(s) de téléphone appelé(s)] et, dans les cas faisant intervenir des services complémentaires tels que le renvoi ou le transfert d'appels, le(s) numéro(s) vers le(s) quel(s) l'appel est réacheminé ;

ii) les nom et adresse de l'abonné (des abonnés) ou de l'utilisateur (des utilisateurs) inscrit(s) ;

2) en ce qui concerne le courrier électronique par l'internet et la téléphonie par l'internet :

i) le numéro d'identifiant ou le numéro de téléphone du (des) destinataire(s) prévu(s) d'un appel téléphonique par l'internet ;

ii) les nom et adresse de l'abonné (des abonnés) ou de l'utilisateur (des utilisateurs) inscrit(s) et le numéro d'identifiant du destinataire prévu de la communication ;

c) les données nécessaires pour déterminer la date, l'heure et la durée d'une communication :

1) en ce qui concerne la téléphonie fixe en réseau et la téléphonie mobile, la date et l'heure de début et de fin de la communication ;

2) en ce qui concerne l'accès à l'internet, le courrier électronique par l'internet et la téléphonie par l'internet :

i) la date et l'heure de l'ouverture et de la fermeture de la session du service d'accès à l'internet dans un fuseau horaire déterminé, ainsi que l'adresse IP (protocole internet), qu'elle soit dynamique ou statique, attribuée à une communication par le fournisseur d'accès à l'internet, ainsi que le numéro d'identifiant de l'abonné ou de l'utilisateur inscrit ;

ii) la date et l'heure de l'ouverture et de la fermeture de la session du service de courrier électronique par l'internet ou de téléphonie par l'internet dans un fuseau horaire déterminé ;

d) les données nécessaires pour déterminer le type de communication :

1) en ce qui concerne la téléphonie fixe en réseau et la téléphonie mobile, le service téléphonique utilisé ;

2) en ce qui concerne le courrier électronique par l'internet et la téléphonie par l'internet, le service internet utilisé ;

e) les données nécessaires pour identifier le matériel de communication des utilisateurs ou ce qui est censé être leur matériel :

1) en ce qui concerne la téléphonie fixe en réseau, le numéro de téléphone de l'appelant et le numéro appelé ;

2) en ce qui concerne la téléphonie mobile :

i) le numéro de téléphone de l'appelant et le numéro appelé ;

ii) l'identité internationale d'abonné mobile (IMSI) de l'appelant ;

iii) l'identité internationale d'équipement mobile (IMEI) de l'appelant ;

iv) l'IMSI de l'appelé ;

v) l'IMEI de l'appelé ;

vi) dans le cas des services anonymes à prépaiement, la date et l'heure de la première activation du service ainsi que l'identité de localisation (identifiant cellulaire) d'où le service a été activé ;

3) en ce qui concerne l'accès à l'internet, le courrier électronique par l'internet et la téléphonie par l'internet :

i) le numéro de téléphone de l'appelant pour l'accès commuté ;

ii) la ligne d'abonné numérique (DSL) ou tout autre point terminal de l'auteur de la communication ;

f) les données nécessaires pour localiser le matériel de communication mobile :

1) l'identité de localisation (identifiant cellulaire) au début de la communication ;

2) les données permettant d'établir la localisation géographique des cellules, en se référant à leur identité de localisation (identifiant cellulaire), pendant la période au cours de laquelle les données de communication sont conservées.

2. Aucune donnée révélant le contenu de la communication ne peut être conservée au titre de la présente directive.

Article 6

Durées de conservation

Les États membres veillent à ce que les catégories de données visées à l'article 5 soient conservées pour une durée minimale de six mois et maximale de deux ans à compter de la date de la communication.

Article 7

Protection et sécurité des données

Sans préjudice des dispositions adoptées en application des directives 95/46/CE et 2002/58/CE, chaque État membre veille à ce que les fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications respectent, au minimum, les principes suivants en matière de sécurité des données, pour ce qui concerne les données conservées conformément à la présente directive :
a) les données conservées doivent être de la même qualité et soumises aux mêmes exigences de sécurité et de protection que les données sur le réseau ;
b) les données font l'objet de mesures techniques et organisationnelles appropriées afin de les protéger contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelle, ou le stockage, le traitement, l'accès ou la divulgation non autorisés ou illicites ;
c) les données font l'objet de mesures techniques et organisationnelles appropriées afin de garantir que l'accès aux données n'est effectué que par un personnel spécifiquement autorisé ;

et
d) les données sont détruites lorsque leur durée de conservation prend fin, à l'exception des données auxquelles on a pu accéder et qui ont été préservées.

Article 8

Conditions à observer pour le stockage des données conservées

Les États membres veillent à ce que les données visées à l'article 5 soient conservées conformément à la présente directive de manière à ce que les données conservées et toute autre information nécessaire concernant ces données puissent, à leur demande, être transmises sans délai aux autorités compétentes.

Article 9

Autorité de contrôle

1. Chaque État membre désigne une ou plusieurs autorités publiques qui sont chargées de surveiller l'application, sur son territoire, des dispositions adoptées par les États membres en application de l'article 7 pour ce qui concerne la sécurité des données conservées. Ces autorités peuvent être les mêmes que celles visées à l'article 28 de la directive 95/46/CE.

2. Les autorités visées au paragraphe 1 exercent en toute indépendance la surveillance visée audit paragraphe.

[…]

Article 11

Modification de la directive 2002/58/CE

À l'article 15 de la directive 2002/58/CE, le paragraphe suivant est inséré :

« *1 bis*. Le paragraphe 1 n'est pas applicable aux données dont la conservation est spécifiquement exigée par la [directive 2006/24] aux fins visées à l'article 1er, paragraphe 1, de ladite directive. »

[…]'

Article 13

Recours, responsabilité et sanctions

1. Chaque État membre prend les mesures nécessaires pour veiller à ce que les mesures nationales mettant en œuvre le chapitre III de la directive 95/46/CE, relatif aux recours juridictionnels, à la responsabilité et aux sanctions, soient intégralement appliquées au traitement des données effectué au titre de la présente directive.

2 Chaque État membre prend, en particulier, les mesures nécessaires pour faire en sorte que l'accès intentionnel aux données conservées conformément à la présente directive ou le transfert de ces données qui ne sont pas autorisés par le droit interne adopté en application de la présente directive soient passibles de sanctions, y compris de sanctions administratives ou pénales, qui sont efficaces, proportionnées et dissuasives. **»**

Les litiges au principal et les questions préjudicielles

L'affaire C-293/12

17. Digital Rights a introduit le 11 août 2006 un recours devant la High Court dans le cadre duquel elle soutient qu'elle est propriétaire d'un téléphone portable qui a été enregistré le 3 juin 2006 et qu'elle utilise celui-ci depuis cette date. Elle met en cause la légalité de mesures législatives et administratives nationales concernant la conservation de données relatives à des communications électroniques et demande, notamment, à la juridiction de renvoi de constater la nullité de la directive 2006/24 et de la septième partie de la loi de 2005 sur la justice pénale (infractions terroristes) [Criminal Justice (Terrorist Offences) Act 2005] prévoyant que les fournisseurs de services de communications téléphoniques doivent conserver les données afférentes à ces dernières relatives au trafic et à la localisation pour une période déterminée par la loi, afin de prévenir et de détecter les infractions, d'enquêter sur celles-ci et de les poursuivre ainsi que de garantir la sécurité de l'État.

18. La High Court, considérant qu'elle n'est pas en mesure de trancher les questions relatives au droit national dont elle est saisie sans que la validité de la directive 2006/24 ait été examinée a décidé de surseoir à statuer et de poser à la Cour les questions préjudicielles suivantes :

«1) La restriction faite aux droits de la partie requérante en matière d'utilisation de téléphonie mobile qui découle des exigences des articles 3, 4 et 6 de la directive 2006/24 est-elle incompatible avec l'article 5, paragraphe 4, TUE, en ce qu'elle est disproportionnée et qu'elle n'est pas nécessaire ou qu'elle est inappropriée pour atteindre les objectifs légitimes tels que :
a) permettre que certaines données soient disponibles aux fins des enquêtes sur les infractions graves et aux fins de la détection et de la poursuite de ces dernières,

et/ou
b) garantir le bon fonctionnement du marché intérieur de l'Union européenne ?

2) En particulier,
a) La directive 2006/24 est-elle compatible avec le droit des citoyens à circuler et à résider librement sur le territoire des États membres, consacré à l'article 21 TFUE ?
b) La directive 2006/24 est-elle compatible avec le droit au respect de la vie privée consacré par l'article 7 de la [charte des droits fondamentaux de l'Union européenne (ci-après la «Charte»)] et par l'article 8 de la [CEDH] ?
c) La directive 2006/24 est-elle compatible avec le droit à la protection des données à caractère personnel qui figure à l'article 8 de la Charte ?
d) La directive 2006/24 est-elle compatible avec le droit à la liberté d'expression consacré par l'article 11 de la Charte et par l'article 10 de la [CEDH] ?
e) La directive 2006/24 est-elle compatible avec le droit à une bonne administration consacré par l'article 41 de la Charte ?

3) Dans quelle mesure les traités, et en particulier le principe de coopération loyale consacré à l'article 4, paragraphe 3, TUE, exigent-ils qu'une juridiction nationale examine et évalue la compatibilité des mesures nationales transposant la directive 2006/24 avec les garanties prévues par la [Charte], y compris son article 7 (tel que repris de l'article 8 de la [CEDH]) ?»

L'affaire C-594/12

19. À l'origine de la demande de décision préjudicielle dans l'affaire C-594/12 se trouvent plusieurs recours introduits devant le Verfassungsgerichtshof, formés respectivement par la Kärntner Landesregierung ainsi que par MM. Seitlinger, Tschohl et 11 128 autres requérants demandant l'annulation de l'article 102 bis de la loi de 2003 sur les télécommunications (Telekommunikationsgesetz 2003), qui a été

introduit dans cette loi par la loi fédérale modifiant celle-ci (Bundesgesetz, mit dem das Telekommunikationsgesetz 2003 – TKG 2003 geändert wird, BGBl. I, 27/2011) aux fins de la transposition de la directive 2006/24 dans le droit interne autrichien. Ces parties considèrent, notamment, que cet article 102 bis viole le droit fondamental des particuliers à la protection de leurs données.

20. Le Verfassungsgerichtshof se demande, notamment, si la directive 2006/24 est compatible avec la Charte en ce qu'elle permet le stockage d'une masse de types de données à l'égard d'un nombre illimité de personnes pour une longue durée. La conservation des données toucherait presque exclusivement des personnes dont le comportement ne justifie aucunement la conservation des données les concernant. Ces personnes seraient exposées à un risque accru de voir les autorités rechercher leurs données, prendre connaissance de leur contenu, s'informer de leur vie privée et utiliser ces données à de multiples fins, compte tenu, notamment, du nombre incommensurable de personnes ayant accès aux données pendant une période de six mois au minimum. Selon la juridiction de renvoi, il existe des doutes, d'une part, quant au fait que cette directive serait en mesure d'atteindre les objectifs qu'elle poursuit et, d'autre part, quant au caractère proportionné de l'ingérence dans les droits fondamentaux concernés.

21. C'est dans ces conditions que le Verfassungsgerichtshof a décidé de surseoir à statuer et de poser à la Cour les questions préjudicielles suivantes :

1) Sur la validité d'actes d'institutions de l'Union :

Les articles 3 à 9 de la directive 2006/24 sont-ils compatibles avec les articles 7, 8 et 11 de la [Charte] ?

2) Sur l'interprétation des traités :

a) Au vu des explications sur l'article 8 de la Charte, lesquelles ont été élaborées, aux termes de l'article 52, paragraphe 7, de la Charte, en vue de guider l'interprétation de [celle-ci] et sont dûment prises en considération par le Verfassungsgerichtshof, la directive 95/46 et le règlement (CE) nº 45/2001 du Parlement européen et du Conseil, du 18 décembre 2000, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données [(JO 2001, L 8, p. 1),] doivent-ils être considérés au même titre que les conditions fixées à l'article 8, paragraphe 2, et à l'article 52, paragraphe 1, de la Charte pour apprécier la licéité d'empiètements ?

b) Dans quel rapport se trouvent le 'droit de l'Union' visé à l'article 52, paragraphe 3, dernière phrase, de la Charte et les directives en matière de droit à la protection des données ?

c) Au vu des conditions et restrictions apportées par la directive 95/46 et le règlement [...] nº 45/2001 à la sauvegarde du droit fondamental à la protection des données inscrit dans la Charte, faut-il prendre en

considération, dans l'interprétation de l'article 8 de [celle-ci], des changements découlant du droit dérivé ultérieur ?
d) Compte tenu de l'article 52, paragraphe 4, de la Charte, le principe de la prévalence du niveau supérieur de protection inscrit à l'article 53 de la Charte a-t-il pour conséquence que les limites assignées par [cette dernière] aux restrictions que peut valablement apporter le droit dérivé doivent être tracées plus étroitement ?
e) Au regard de l'article 52, paragraphe 3, de la Charte, du cinquième alinéa du préambule et des explications sur l'article 7 de [celle-ci], indiquant que les droits garantis à l'article 7 correspondent à ceux qui sont garantis par l'article 8 de la CEDH, la jurisprudence que la Cour européenne des droits de l'homme a consacrée à l'article 8 de la CEDH peut-elle donner des indications dans l'interprétation de l'article 8 de la Charte qui rejaillissent sur l'interprétation de ce dernier article ? »

22. Par décision du président de la Cour du 11 juin 2013, les affaires C-293/12 et C-594/12 ont été jointes aux fins de la procédure orale et de l'arrêt.

Sur les questions préjudicielles

Sur la deuxième question, sous b) à d), dans l'affaire C-293/12 et la première question dans l'affaire C-594/12

23. Par la deuxième question, sous b) à d), dans l'affaire C-293/12 et la première question dans l'affaire C-594/12, qu'il convient d'examiner ensemble, les juridictions de renvoi demandent en substance à la Cour d'examiner la validité de la directive 2006/24 à la lumière des articles 7, 8 et 11 de la Charte.

Sur la pertinence des articles 7, 8 et 11 de la Charte au regard de la question de la validité de la directive 2006/24

24. Il résulte de l'article 1er ainsi que des considérants 4, 5, 7 à 11, 21 et 22 de la directive 2006/24 que celle-ci a pour objectif principal d'harmoniser les dispositions des États membres relatives à la conservation, par les fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communication, de certaines données générées ou traitées par ces fournisseurs en vue de garantir la disponibilité de ces données à des fins de prévention, de recherche, de détection et de poursuite des infractions graves, telles que celles liées à la criminalité organisée et au terrorisme, dans le respect des droits consacrés aux articles 7 et 8 de la Charte.

25. L'obligation des fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications, prévue à l'article 3 de la directive 2006/24, de conserver les données énumérées à l'article 5 de celle-ci aux fins de les rendre, le cas échéant, accessibles aux autorités nationales compétentes soulève des questions relatives à la protection tant de la vie privée que des communications consacrée à l'article 7 de la Charte à la protection des données à

caractère personnel prévue à l'article 8 de celle-ci ainsi qu'au respect de la liberté d'expression garantie par l'article 11 de la Charte.

26. À cet égard, il convient de relever que les données que doivent conserver les fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications, au titre des articles 3 et 5 de la directive 2006/24, sont, notamment, les données nécessaires pour retrouver et identifier la source d'une communication et la destination de celle-ci, pour déterminer la date, l'heure, la durée et le type d'une communication, le matériel de communication des utilisateurs, ainsi que pour localiser le matériel de communication mobile, données au nombre desquelles figurent, notamment, le nom et l'adresse de l'abonné ou de l'utilisateur inscrit, le numéro de téléphone de l'appelant et le numéro appelé ainsi qu'une adresse IP pour les services Internet. Ces données permettent, notamment, de savoir quelle est la personne avec laquelle un abonné ou un utilisateur inscrit a communiqué et par quel moyen, tout comme de déterminer le temps de la communication ainsi que l'endroit à partir duquel celle-ci a eu lieu. En outre, elles permettent de connaître la fréquence des communications de l'abonné ou de l'utilisateur inscrit avec certaines personnes pendant une période donnée.

27. Ces données, prises dans leur ensemble, sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci.

28. Dans de telles circonstances, même si la directive 2006/24 n'autorise pas, ainsi qu'il découle de ses articles 1er, paragraphe 2, et 5, paragraphe 2, la conservation du contenu de la communication et des informations consultées en utilisant un réseau de communications électroniques, il n'est pas exclu que la conservation des données en cause puisse avoir une incidence sur l'utilisation, par les abonnés ou les utilisateurs inscrits, des moyens de communication visés par cette directive et, en conséquence, sur l'exercice par ces derniers de leur liberté d'expression, garantie par l'article 11 de la Charte.

29. La conservation des données aux fins de leur accès éventuel par les autorités nationales compétentes, telle que prévue par la directive 2006/24, concerne de manière directe et spécifique la vie privée et, ainsi, les droits garantis par l'article 7 de la Charte. En outre, une telle conservation des données relève également de l'article 8 de celle-ci en raison du fait qu'elle constitue un traitement des données à caractère personnel au sens de cet article et doit, ainsi, nécessairement satisfaire aux exigences de protection des données découlant de cet article (arrêt Volker und Markus Schecke et Eifert, C-92/09 et C-93/09, EU : C : 2010 : 662, point 47).

30. Si les renvois préjudiciels dans les présentes affaires soulèvent notamment la question de principe de savoir si les données des abonnés et des utilisateurs inscrits peuvent ou non, au regard de l'article 7 de la Charte, être conservées, ils concernent également celle de savoir si la directive 2006/24 répond aux exigences de protection des données à caractère personnel découlant de l'article 8 de la Charte.

31. Eu égard aux considérations qui précèdent, il convient, aux fins de répondre à la deuxième question, sous b) à d), dans l'affaire C-293/12 et à la première question dans l'affaire C-594/12, d'examiner la validité de la directive au regard des articles 7 et 8 de la Charte.

Sur l'existence d'une ingérence dans les droits consacrés par les articles 7 et 8 de la Charte

32. En imposant la conservation des données énumérées à l'article 5, paragraphe 1, de la directive 2006/24 et en permettant l'accès des autorités nationales compétentes à celles-ci, cette directive déroge, ainsi que l'a relevé M. l'avocat général notamment aux points 39 et 40 de ses conclusions, au régime de protection du droit au respect de la vie privée, instauré par les directives 95/46 et 2002/58, à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques, ces dernières directives ayant prévu la confidentialité des communications et des données relatives au trafic ainsi que l'obligation d'effacer ou de rendre anonymes ces données lorsqu'elles ne sont plus nécessaires à la transmission d'une communication, hormis si elles sont nécessaires à la facturation et uniquement tant que cette nécessité perdure.

33. Pour établir l'existence d'une ingérence dans le droit fondamental au respect de la vie privée, il importe peu que les informations relatives à la vie privée concernées présentent ou non un caractère sensible ou que les intéressés aient ou non subi d'éventuels inconvénients en raison de cette ingérence (voir, en ce sens, arrêt Österreichischer Rundfunk e. a., C-465/00, C-138/01 et C-139/01, EU : C : 2003 : 294, point 75).

34. Il en résulte que l'obligation imposée par les articles 3 et 6 de la directive 2006/24 aux fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communication de conserver pendant une certaine durée des données relatives à la vie privée d'une personne et à ses communications, telles que celles visées à l'article 5 de cette directive, constitue en soi une ingérence dans les droits garantis par l'article 7 de la Charte.

35 En outre, l'accès des autorités nationales compétentes aux données constitue une ingérence supplémentaire dans ce droit fondamental (voir, en ce qui concerne l'article 8 de la CEDH, arrêts Cour EDH, Leander c. Suède, 26 mars 1987, série A n°116, § 48 ; Rotaru c. Roumanie [GC], n° 28341/95, § 46, CEDH 2000-V, ainsi que Weber et Saravia c. Allemagne (déc.), n° 54934/00, § 79, CEDH 2006-XI). Ainsi, les articles

4 et 8 de la directive 2006/24 prévoyant des règles relatives à l'accès des autorités nationales compétentes aux données sont également constitutifs d'une ingérence dans les droits garantis par l'article 7 de la Charte.

36. De même, la directive 2006/24 est constitutive d'une ingérence dans le droit fondamental à la protection des données à caractère personnel garanti par l'article 8 de la Charte puisqu'elle prévoit un traitement des données à caractère personnel.

37 Force est de constater que l'ingérence que comporte la directive 2006/24 dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte s'avère, ainsi que l'a également relevé M. l'avocat général notamment aux points 77 et 80 de ses conclusions, d'une vaste ampleur et qu'elle doit être considérée comme particulièrement grave. En outre, la circonstance que la conservation des données et l'utilisation ultérieure de celles-ci sont effectuées sans que l'abonné ou l'utilisateur inscrit en soient informés est susceptible de générer dans l'esprit des personnes concernées, ainsi que l'a relevé M. l'avocat général aux points 52 et 72 de ses conclusions, le sentiment que leur vie privée fait l'objet d'une surveillance constante.

Sur la justification de l'ingérence dans les droits garantis par les articles 7 et 8 de la Charte

38. Conformément à l'article 52, paragraphe 1, de la Charte, toute limitation de l'exercice des droits et des libertés consacrés par celle-ci doit être prévue par la loi, respecter leur contenu essentiel et, dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées à ces droits et libertés que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui.

39. En ce qui concerne le contenu essentiel du droit fondamental au respect de la vie privée et des autres droits consacrés à l'article 7 de la Charte, il convient de constater que, même si la conservation des données imposée par la directive 2006/24 constitue une ingérence particulièrement grave dans ces droits, elle n'est pas de nature à porter atteinte audit contenu étant donné que, ainsi qu'il découle de son article 1er, paragraphe 2, cette directive ne permet pas de prendre connaissance du contenu des communications électroniques en tant que tel.

40. Cette conservation des données n'est pas non plus de nature à porter atteinte au contenu essentiel du droit fondamental à la protection des données à caractère personnel, consacré à l'article 8 de la Charte, en raison du fait que la directive 2006/24 prévoit, à son article 7, une règle relative à la protection et à la sécurité des données selon laquelle, sans préjudice des dispositions adoptées en application des directives 95/46 et 2002/58, certains principes de protection et de sécurité des données doivent être respectés par les fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de

communications, principes selon lesquels les États membres veillent à l'adoption de mesures techniques et organisationnelles appropriées contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelle des données.

41. Quant à la question de savoir si ladite ingérence répond à un objectif d'intérêt général, il convient de relever que, si la directive 2006/24 est destinée à harmoniser les dispositions des États membres relatives aux obligations desdits fournisseurs en matière de conservation de certaines données qui sont générées ou traitées par ces derniers, l'objectif matériel de cette directive vise, ainsi qu'il découle de son article 1er, paragraphe 1, à garantir la disponibilité de ces données à des fins de recherche, de détection et de poursuite d'infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne. L'objectif matériel de cette directive est, dès lors, de contribuer à la lutte contre la criminalité grave et ainsi, en fin de compte, à la sécurité publique.

42. Il ressort de la jurisprudence de la Cour que constitue un objectif d'intérêt général de l'Union la lutte contre le terrorisme international en vue du maintien de la paix et de la sécurité internationales (voir, en ce sens, arrêts Kadi et Al Barakaat International Foundation/Conseil et Commission, C-402/05 P et C-415/05 P, EU : C : 2008 : 461, point 363, ainsi que Al-Aqsa/Conseil, C-539/10 P et C-550/10 P, EU : C : 2012 : 711, point 130). Il en va de même de la lutte contre la criminalité grave afin de garantir la sécurité publique (voir, en ce sens, arrêt Tsakouridis, C-145/09, EU : C : 2010 : 708, points 46 et 47). Par ailleurs, il convient de relever, à cet égard, que l'article 6 de la Charte énonce le droit de toute personne non seulement à la liberté, mais également à la sûreté.

43. À cet égard, il ressort du considérant 7 de la directive 2006/24 que, en raison de l'accroissement important des possibilités offertes par les communications électroniques, le Conseil «Justice et affaires intérieures» du 19 décembre 2002 a considéré que les données relatives à l'utilisation de celles-ci sont particulièrement importantes et constituent donc un instrument utile dans la prévention des infractions et la lutte contre la criminalité, notamment la criminalité organisée.

44. Force est donc de constater que la conservation des données aux fins de permettre aux autorités nationales compétentes de disposer d'un accès éventuel à celles-ci, telle qu'imposée par la directive 2006/24, répond effectivement à un objectif d'intérêt général.

45. Dans ces conditions, il y a lieu de vérifier la proportionnalité de l'ingérence constatée.

46. À cet égard, il convient de rappeler que le principe de proportionnalité exige, selon une jurisprudence constante de la Cour, que les actes des institutions de l'Union soient aptes à réaliser les objectifs légitimes poursuivis par la réglementation en cause et ne dépassent pas les limites de ce qui est approprié et nécessaire à la réalisation de ces

objectifs (voir, en ce sens, arrêts Afton Chemical, C-343/09, EU : C : 2010 : 419, point 45 ; Volker und Markus Schecke et Eifert, EU : C : 2010 : 662, point 74 ; Nelson e. a., C-581/10 et C-629/10, EU : C : 2012 : 657, point 71 ; Sky Österreich, C-283/11, EU : C : 2013 : 28, point 50, ainsi que Schaible, C-101/12, EU : C : 2013 : 661, point 29).

47. En ce qui concerne le contrôle juridictionnel du respect de ces conditions, dès lors que des ingérences dans des droits fondamentaux sont en cause, l'étendue du pouvoir d'appréciation du législateur de l'Union peut s'avérer limitée en fonction d'un certain nombre d'éléments, parmi lesquels figurent, notamment, le domaine concerné, la nature du droit en cause garanti par la Charte, la nature et la gravité de l'ingérence ainsi que la finalité de celle-ci (voir, par analogie, en ce qui concerne l'article 8 de la CEDH, arrêt Cour EDH, S et Marper c. Royaume-Uni [GC], n^{os} 30562/04 et 30566/04, § 102, CEDH 2008-V).

48. En l'espèce, compte tenu, d'une part, du rôle important que joue la protection des données a` caractère personnel au regard du droit fondamental au respect de la vie privée et, d'autre part, de l'ampleur et de la gravité de l'ingérence dans ce droit que comporte la directive 2006/24, le pouvoir d'appréciation du législateur de l'Union s'avère réduit de sorte qu'il convient de procéder à un contrôle strict.

49. En ce qui concerne la question de savoir si la conservation des données est apte à réaliser l'objectif poursuivi par la directive 2006/24, il convient de constater que, eu égard à l'importance croissante des moyens de communication électronique, les données qui doivent être conservées en application de cette directive permettent aux autorités nationales compétentes en matière de poursuites pénales de disposer de possibilités supplémentaires d'élucidation des infractions graves et, à cet égard, elles constituent donc un instrument utile pour les enquêtes pénales. Ainsi, la conservation de telles données peut être considérée comme apte à réaliser l'objectif poursuivi par ladite directive.

50. Cette appréciation ne saurait être remise en cause par la circonstance, invoquée notamment par MM. Tschohl et Seitlinger ainsi que par le gouvernement portugais dans leurs observations écrites soumises à la Cour, qu'il existe plusieurs modalités de communications électroniques qui ne relèvent pas du champ d'application de la directive 2006/24 ou qui permettent une communication anonyme. Si, certes, cette circonstance est de nature à limiter l'aptitude de la mesure de conservation des données à atteindre l'objectif poursuivi, elle n'est toutefois pas de nature à rendre cette mesure inapte, ainsi que l'a relevé M. l'avocat général au point 137 de ses conclusions.

51. En ce qui concerne le caractère nécessaire de la conservation des données imposée par la directive 2006/24, il convient de constater que, certes, la lutte contre la criminalité grave, notamment contre la criminalité organisée et le terrorisme, est d'une importance primordiale pour garantir la sécurité publique et son efficacité peut dépendre dans

une large mesure de l'utilisation des techniques modernes d'enquête. Toutefois, un tel objectif d'intérêt général, pour fondamental qu'il soit, ne saurait à lui seul justifier qu'une mesure de conservation telle que celle instaurée par la directive 2006/24 soit considérée comme nécessaire aux fins de ladite lutte.

52. S'agissant du droit au respect de la vie privée, la protection de ce droit fondamental exige, selon la jurisprudence constante de la Cour, en tout état de cause, que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci doivent s'opérer dans les limites du strict nécessaire (arrêt IPI, C-473/12, EU : C : 2013 : 715, point 39 et jurisprudence citée).

53. À cet égard, il convient de rappeler que la protection des données à caractère personnel, résultant de l'obligation explicite prévue à l'article 8, paragraphe 1, de la Charte, revêt une importance particulière pour le droit au respect de la vie privée consacré à l'article 7 de celle-ci.

54. Ainsi, la réglementation de l'Union en cause doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant un minimum d'exigences de sorte que les personnes dont les données ont été conservées disposent de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données (voir, par analogie, en ce qui concerne l'article 8 de la CEDH, arrêts Cour EDH, Liberty et autres c. Royaume-Uni, no 58243/00, § 62 et 63, du 1er juillet 2008 ; Rotaru c. Roumanie, précité, § 57 à 59, ainsi que S et Marper c. Royaume-Uni, précité, § 99).

55. La nécessité de disposer de telles garanties est d'autant plus importante lorsque, comme le prévoit la directive 2006/24, les données à caractère personnel sont soumises à un traitement automatique et qu'il existe un risque important d'accès illicite à ces données (voir, par analogie, en ce qui concerne l'article 8 de la CEDH, arrêts Cour EDH, S et Marper c. Royaume-Uni, précité, § 103, ainsi que M. K. c. France, no 19522/09, § 35, du 18 avril 2013).

56. Quant à la question de savoir si l'ingérence que comporte la directive 2006/24 est limitée au strict nécessaire, il convient de relever que cette directive impose, conformément à son article 3 lu en combinaison avec son article 5, paragraphe 1, la conservation de toutes les données relatives au trafic concernant la téléphonie fixe, la téléphonie mobile, l'accès à l'internet, le courrier électronique par Internet ainsi que la téléphonie par l'internet. Ainsi, elle vise tous les moyens de communication électronique dont l'utilisation est très répandue et d'une importance croissante dans la vie quotidienne de chacun. En outre, conformément à son article 3, ladite directive couvre tous les abonnés et utilisateurs inscrits. Elle comporte donc une ingérence dans les droits fondamentaux de la quasi-totalité de la population européenne.

57. À cet égard, il importe de constater, en premier lieu, que la directive 2006/24 couvre de manière généralisée toute personne et tous les moyens de communication électronique ainsi que l'ensemble des données relatives au trafic sans qu'aucune différenciation, limitation ni exception soient opérées en fonction de l'objectif de lutte contre les infractions graves.

58. En effet, d'une part, la directive 2006/24 concerne de manière globale l'ensemble des personnes faisant usage de services de communications électroniques, sans toutefois que les personnes dont les données sont conservées se trouvent, même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales. Elle s'applique donc même à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec des infractions graves. En outre, elle ne prévoit aucune exception, de sorte qu'elle s'applique même à des personnes dont les communications sont soumises, selon les règles du droit national, au secret professionnel.

59. D'autre part, tout en visant à contribuer à la lutte contre la criminalité grave, ladite directive ne requiert aucune relation entre les données dont la conservation est prévue et une menace pour la sécurité publique et, notamment, elle n'est pas limitée à une conservation portant soit sur des données afférentes à une période temporelle et/ou une zone géographique déterminée et/ou sur un cercle de personnes données susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave, soit sur des personnes qui pourraient, pour d'autres motifs, contribuer, par la conservation de leurs données, à la prévention, à la détection ou à la poursuite d'infractions graves.

60. En deuxième lieu, à cette absence générale de limites s'ajoute le fait que la directive 2006/24 ne prévoit aucun critère objectif permettant de délimiter l'accès des autorités nationales compétentes aux données et leur utilisation ultérieure à des fins de prévention, de détection ou de poursuites pénales concernant des infractions pouvant, au regard de l'ampleur et de la gravité de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, être considérées comme suffisamment graves pour justifier une telle ingérence. Au contraire, la directive 2006/24 se borne à renvoyer, à son article 1er, paragraphe 1, de manière générale aux infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne.

61. En outre, quant à l'accès des autorités nationales compétentes aux données et à leur utilisation ultérieure, la directive 2006/24 ne contient pas les conditions matérielles et procédurales y afférentes. L'article 4 de cette directive, qui régit l'accès de ces autorités aux données conservées, ne dispose pas expressément que cet accès et l'utilisation ultérieure des données en cause doivent être strictement restreints à des fins de prévention et de détection d'infractions graves précisément délimitées

ou de poursuites pénales afférentes à celles-ci, mais il se borne à prévoir que chaque État membre arrête la procédure à suivre et les conditions à remplir pour avoir accès aux données conservées dans le respect des exigences de nécessité et de proportionnalité.

62. En particulier, la directive 2006/24 ne prévoit aucun critère objectif permettant de limiter le nombre de personnes disposant de l'autorisation d'accès et d'utilisation ultérieure des données conservées au strict nécessaire au regard de l'objectif poursuivi. Surtout, l'accès aux données conservées par les autorités nationales compétentes n'est pas subordonné à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante dont la décision vise à limiter l'accès aux données et leur utilisation à ce qui est strictement nécessaire aux fins d'atteindre l'objectif poursuivi et intervient à la suite d'une demande motivée de ces autorités présentée dans le cadre de procédures de prévention, de détection ou de poursuites pénales. Il n'a pas non plus été prévu une obligation précise des États membres visant à établir de telles limitations.

63. En troisième lieu, s'agissant de la durée de conservation des données, la directive 2006/24 impose, à son article 6, la conservation de celles-ci pendant une période d'au moins six mois sans que soit opérée une quelconque distinction entre les catégories de données prévues à l'article 5 de cette directive en fonction de leur utilité éventuelle aux fins de l'objectif poursuivi ou selon les personnes concernées.

64. Cette durée se situe, en outre, entre six mois au minimum et vingt-quatre mois au maximum, sans qu'il soit précisé que la détermination de la durée de conservation doit être fondée sur des critères objectifs afin de garantir que celle-ci est limitée au strict nécessaire.

65. Il résulte de ce qui précède que la directive 2006/24 ne prévoit pas de règles claires et précises régissant la portée de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte. Force est donc de constater que cette directive comporte une ingérence dans ces droits fondamentaux d'une vaste ampleur et d'une gravité particulière dans l'ordre juridique de l'Union sans qu'une telle ingérence soit précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au strict nécessaire.

66. De surcroît, en ce qui concerne les règles visant la sécurité et la protection des données conservées par les fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications, il convient de constater que la directive 2006/24 ne prévoit pas des garanties suffisantes, telles que requises par l'article 8 de la Charte, permettant d'assurer une protection efficace des données conservées contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données. En effet, en premier lieu, l'article 7 de la directive 2006/24 ne prévoit pas de règles spécifiques et adaptées à la vaste quantité des données dont la conservation

est imposée par cette directive, au caractère sensible de ces données ainsi qu'au risque d'accès illicite à celles-ci, règles qui seraient destinées notamment à régir de manière claire et stricte la protection et la sécurité des données en cause, afin de garantir leur pleine intégrité et confidentialité. En outre, il n'a pas non plus été prévu une obligation précise des États membres visant à établir de telles règles.

67. L'article 7 de la directive 2006/24, lu en combinaison avec les articles 4, paragraphe 1, de la directive 2002/58 et 17, paragraphe 1, second alinéa, de la directive 95/46, ne garantit pas que soit appliqué par lesdits fournisseurs un niveau particulièrement élevé de protection et de sécurité par des mesures techniques et organisationnelles, mais autorise notamment ces fournisseurs à tenir compte de considérations économiques lors de la détermination du niveau de sécurité qu'ils appliquent, en ce qui concerne les coûts de mise en œuvre des mesures de sécurité. En particulier, la directive 2006/24 ne garantit pas la destruction irrémédiable des données au terme de la durée de conservation de celles-ci.

68. En second lieu, il convient d'ajouter que ladite directive n'impose pas que les données en cause soient conservées sur le territoire de l'Union, de sorte qu'il ne saurait être considéré qu'est pleinement garanti le contrôle par une autorité indépendante, explicitement exigé par l'article 8, paragraphe 3, de la Charte, du respect des exigences de protection et de sécurité, telles que visées aux deux points précédents. Or, un tel contrôle, effectué sur la base du droit de l'Union, constitue un élément essentiel du respect de la protection des personnes à l'égard du traitement des données à caractère personnel (voir, en ce sens, arrêt Commission/Autriche, C-614/10, EU : C : 2012 : 631, point 37).

69. Eu égard à l'ensemble des considérations qui précèdent, il convient de considérer que, en adoptant la directive 2006/24, le législateur de l'Union a excédé les limites qu'impose le respect du principe de proportionnalité au regard des articles 7, 8 et 52, paragraphe 1, de la Charte.

70. Dans ces conditions, il n'y a pas lieu d'examiner la validité de la directive 2006/24 au regard de l'article 11 de la Charte.

71 En conséquence, il y a lieu de répondre à la deuxième question, sous b) à d), dans l'affaire C-293/12 et à la première question dans l'affaire C-594/12 que la directive 2006/24 est invalide.

Sur la première question et la deuxième question, sous a) et e), ainsi que sur la troisième question dans l'affaire C-293/12 et sur la seconde question dans l'affaire C-594/12

72. Il résulte de ce qui a été jugé au point précédent qu'il n'y a pas lieu de répondre à la première question, à la deuxième question, sous a) et e), et à la troisième question dans l'affaire C-293/12 non plus qu'à la deuxième question dans l'affaire C-594/12.

Sur les dépens

73. La procédure revêtant, à l'égard des parties au principal, le caractère d'un incident soulevé devant les juridictions de renvoi, il appartient à celles-ci de statuer sur les dépens. Les frais exposés pour soumettre des observations à la Cour, autres que ceux desdites parties, ne peuvent faire l'objet d'un remboursement.

Par ces motifs, la Cour (grande chambre) dit pour droit :

La directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE, est invalide.

Décision du Conseil constitutionnel n° 2014-420/421 QPC du 09 octobre 2014

M. Maurice L. et autre [Prolongation exceptionnelle de la garde à vue pour des faits d'escroquerie en bande organisée]

Le Conseil constitutionnel a été saisi le 16 juillet 2014 par la Cour de cassation (chambre criminelle, arrêt n° 4428 du 16 juillet 2014), dans les conditions prévues à l'article 61-1 de la Constitution, d'une question prioritaire de constitutionnalité posée par M. Maurice L., relative à la conformité aux droits et libertés que la Constitution garantit du 8° bis de l'article 706-73 du Code de procédure pénale.

Il a été saisi le même jour dans les mêmes conditions par la Cour de cassation (chambre criminelle, arrêt n° 4429 du même jour) d'une question prioritaire de constitutionnalité posée par M. Bernard T., relative à la conformité aux droits et libertés que la Constitution garantit de l'article 706-88 du Code de procédure pénale

LE CONSEIL CONSTITUTIONNEL :

Vu la Constitution ; Vu l'ordonnance n° 58-1067 du 7 novembre 1958 modifiée portant loi organique sur le Conseil constitutionnel ; Vu le Code pénal ; Vu le Code de procédure pénale ; Vu la loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité, ensemble la décision du Conseil constitutionnel n° 2004-492 DC du 2 mars 2004 ; Vu la décision du Conseil constitutionnel n° 2010-31 QPC du 22 septembre 2010 ; Vu la loi n° 2011-392 du 14 avril 2011 relative à la garde à vue, notamment son article 16 ; Vu la loi n° 2011-525 du 17 mai 2011 de simplification et d'amélioration de la qualité du droit, notamment son article 157 ; Vu la loi n° 2014-535 du 27 mai 2014 portant transposition de la directive 2012/13/UE du Parlement européen et du Conseil, du 22 mai 2012, relative au droit à l'information dans le cadre des procédures

pénales, notamment son article 4 ; Vu le règlement du 4 février 2010 sur la procédure suivie devant le Conseil constitutionnel pour les questions prioritaires de constitutionnalité ; Vu les observations produites pour la SAS Consortium de réalisation et la SAS CDR Créances, parties en défense, par Me Benoît Chabert, avocat au barreau de Paris, enregistrées le 7 août 2014 ; Vu les observations produites pour M. Maurice L. par Me Paul-Albert Iweins, avocat au barreau de Paris, enregistrées les 8 et 28 août 2014 ; Vu les observations produites pour M. Bernard T. par la SCP Lyon-Caen et Thiriez, avocat au Conseil d'État et à la Cour de cassation, enregistrées les 8 et 28 août 2014 ; Vu les observations produites par le Premier ministre, enregistrées le 8 août 2014 ; Vu les pièces produites et jointes au dossier ; Me Iweins et Me Frédéric Thiriez, pour les requérants, Me Chabert, pour les parties en défense et M. Xavier Pottier, désigné par le Premier ministre, ayant été entendus à l'audience publique du 23 septembre 2014 ; Le rapporteur ayant été entendu ;

1. Considérant qu'il y a lieu de joindre ces questions prioritaires de constitutionnalité pour statuer par une seule décision

2. Considérant que les questions prioritaires de constitutionnalité doivent être regardées comme portant sur les dispositions applicables au litige à l'occasion duquel elles ont été posées ; qu'ainsi le Conseil constitutionnel est saisi du 8° bis de l'article 706-73 du Code de procédure pénale, dans sa rédaction actuellement en vigueur, et de l'article 706-88 du même Code, dans sa rédaction postérieure à la loi du 14 avril 2011 susvisée et antérieure à la loi 27 mai 2014 susvisée ;

3. Considérant que le titre XXV du livre IV du Code de procédure pénale, qui, dans sa rédaction antérieure à la loi du 27 mai 2014 susvisée, comprend les articles 706-73 à 706-106, est consacré à la procédure applicable à la criminalité et à la délinquance organisée ; que l'article 706-73 fixe la liste des crimes et délits pour lesquels la procédure applicable à l'enquête, la poursuite, l'instruction et le jugement est soumise aux dispositions particulières de ce titre XXV ; que le 8° bis de cet article 706-73, dans sa rédaction résultant de la loi du 17 mai 2011 susvisée, désigne le « délit d'escroquerie en bande organisée prévu par le dernier alinéa de l'article 313-2 du Code pénal » ;

4. Considérant qu'aux termes de l'article 706-88 du Code de procédure pénale, dans sa rédaction postérieure à la loi du 14 avril 2011 : « Pour l'application des articles 63, 77 et 154, si les nécessités de l'enquête ou de l'instruction relatives à l'une des infractions entrant dans le champ d'application de l'article 706-73 l'exigent, la garde à vue d'une personne peut, à titre exceptionnel, faire l'objet de deux prolongations supplémentaires de vingt-quatre heures chacune.

« Ces prolongations sont autorisées, par décision écrite et motivée, soit, à la requête du procureur de la République, par le juge des libertés et de la détention, soit par le juge d'instruction. « La personne gardée à vue doit être présentée au magistrat qui statue sur la prolongation

préalablement à cette décision. La seconde prolongation peut toutefois, à titre exceptionnel, être autorisée sans présentation préalable de la personne en raison des nécessités des investigations en cours ou à effectuer.

« Lorsque la première prolongation est décidée, la personne gardée à vue est examinée par un médecin désigné par le procureur de la République, le juge d'instruction ou l'officier de police judiciaire. Le médecin délivre un certificat médical par lequel il doit notamment se prononcer sur l'aptitude au maintien en garde à vue, qui est versé au dossier. La personne est avisée par l'officier de police judiciaire du droit de demander un nouvel examen médical. Ces examens médicaux sont de droit. Mention de cet avis est portée au procès-verbal et émargée par la personne intéressée ; en cas de refus d'émargement, il en est fait mention.

« Par dérogation aux dispositions du premier alinéa, si la durée prévisible des investigations restant à réaliser à l'issue des premières quarante-huit heures de garde à vue le justifie, le juge des libertés et de la détention ou le juge d'instruction peuvent décider, selon les modalités prévues au deuxième alinéa, que la garde à vue fera l'objet d'une seule prolongation supplémentaire de quarante-huit heures.

« Par dérogation aux dispositions des articles 63-4 à 63-4-2, lorsque la personne est gardée à vue pour une infraction entrant dans le champ d'application de l'article 706-73, l'intervention de l'avocat peut être différée, en considération de raisons impérieuses tenant aux circonstances particulières de l'enquête ou de l'instruction, soit pour permettre le recueil ou la conservation des preuves, soit pour prévenir une atteinte aux personnes, pendant une durée maximale de quarante-huit heures ou, s'il s'agit d'une infraction mentionnée aux 3° ou 11° du même article 706-73, pendant une durée maximale de soixante-douze heures.

« Le report de l'intervention de l'avocat jusqu'à la fin de la vingt-quatrième heure est décidé par le procureur de la République, d'office ou à la demande de l'officier de police judiciaire. Le report de l'intervention de l'avocat au-delà de la vingt-quatrième heure est décidé, dans les limites fixées au sixième alinéa, par le juge des libertés et de la détention statuant à la requête du procureur de la République. Lorsque la garde à vue intervient au cours d'une commission rogatoire, le report est décidé par le juge d'instruction. Dans tous les cas, la décision du magistrat, écrite et motivée, précise la durée pour laquelle l'intervention de l'avocat est différée.

« Lorsqu'il est fait application des sixième et septième alinéas du présent article, l'avocat dispose, à partir du moment où il est autorisé à intervenir en garde à vue, des droits prévus aux articles 63-4 et 63-4-1, au premier alinéa de l'article 63-4-2 et à l'article 63-4-3 » ;

5. Considérant que, selon les requérants, en ce qu'elles permettent le recours à une mesure de garde à vue de quatre-vingt-seize heures dans le cadre d'une enquête ou d'une instruction portant sur des faits qualifiés d'escroquerie en bande organisée, les dispositions combinées du 8° bis de l'article 706-73 du Code de procédure pénale et de son article 706-88 méconnaissent le principe de rigueur nécessaire des mesures de contrainte dans la procédure pénale, la protection de la liberté individuelle et les droits de la défense ;

6. Considérant que, s'agissant de l'article 706-88 du Code de procédure pénale, la question prioritaire de constitutionnalité ne porte que sur ses cinq premiers alinéas relatifs à la durée de la garde à vue ;

SUR LES NORMES DE CONSTITUTIONNALITÉ APPLICABLES :

7. Considérant qu'aux termes de l'article 7 de la Déclaration des droits de l'homme et du citoyen de 1789 : « Nul homme ne peut être accusé, arrêté ni détenu que dans les cas déterminés par la loi, et selon les formes qu'elle a prescrites. Ceux qui sollicitent, expédient, exécutent ou font exécuter des ordres arbitraires, doivent être punis ; mais tout citoyen appelé ou saisi en vertu de la loi doit obéir à l'instant : il se rend coupable par la résistance » ; qu'aux termes de son article 9 : « Tout homme étant présumé innocent jusqu'à ce qu'il ait été déclaré coupable, s'il est jugé indispensable de l'arrêter, toute rigueur qui ne serait pas nécessaire pour s'assurer de sa personne doit être sévèrement réprimée par la loi » ; que son article 16 dispose : « Toute société dans laquelle la garantie des droits n'est pas assurée, ni la séparation des pouvoirs déterminée, n'a point de Constitution » ;

8. Considérant que le législateur tient de l'article 34 de la Constitution l'obligation de fixer lui-même le champ d'application de la loi pénale ; que, s'agissant de la procédure pénale, cette exigence s'impose notamment pour éviter une rigueur non nécessaire lors de la recherche des auteurs d'infractions ;

9. Considérant qu'il incombe au législateur d'assurer la conciliation entre, d'une part, la prévention des atteintes à l'ordre public et la recherche des auteurs d'infractions, toutes deux nécessaires à la sauvegarde de droits et de principes de valeur constitutionnelle, et, d'autre part, l'exercice des libertés constitutionnellement garanties ; qu'au nombre de celles-ci figurent la liberté d'aller et venir, l'inviolabilité du domicile, le secret des correspondances et le respect de la vie privée, protégés par les articles 2 et 4 de la Déclaration de 1789, ainsi que la liberté individuelle, que l'article 66 de la Constitution place sous la protection de l'autorité judiciaire ;

SUR LES CINQ PREMIERS ALINÉAS DE L'ARTICLE 706-88 DU CODE DE PROCÉDURE PÉNALE :

10. Considérant que les cinq premiers alinéas de l'article 706-88 du Code de procédure pénale sont renvoyés au Conseil constitutionnel dans

leur rédaction résultant de la loi du 9 mars 2004 susvisée ; que, dans les considérants 21 à 27 de sa décision du 2 mars 2004 susvisée, le Conseil constitutionnel a spécialement examiné l'article 706-88 inséré dans le Code de procédure pénale par l'article 1er de la loi du 9 mars 2004 ; qu'il a jugé que ces dispositions ne portaient pas une atteinte excessive à la liberté individuelle ; que, dans l'article 2 du dispositif de cette décision, il a déclaré ces dispositions conformes à la Constitution ; que, par suite, les cinq premiers alinéas de l'article 706-88 ont déjà été déclarés conformes à la Constitution dans les motifs et le dispositif d'une décision du Conseil constitutionnel ; que, comme le Conseil constitutionnel l'a jugé dans sa décision du 22 septembre 2010 susvisée, en l'absence de changement des circonstances, depuis la décision du 2 mars 2004 susvisée, en matière de lutte contre la délinquance et la criminalité organisées, il n'y a pas lieu, pour le Conseil constitutionnel, de procéder à un nouvel examen de ces dispositions ; qu'au surplus, le grief tiré de ce que les dispositions contestées permettent le recours à une mesure de garde à vue de quatre-vingt-seize heures pour des faits d'escroquerie en bande organisée met en cause non l'article 706-88 du Code de procédure pénale en lui-même, mais l'inscription de cette infraction dans la liste prévue par son article 706-73 ;

SUR LE 8° BIS DE L'ARTICLE 706-73 DU CODE DE PROCÉDURE PÉNALE :

11. Considérant que l'inscription d'un crime ou d'un délit dans la liste des infractions visées par l'article 706-73 du Code de procédure pénale a pour effet de permettre, lors des enquêtes ou des instructions portant sur ce crime ou ce délit, la mise en œuvre d'une mesure de garde à vue dans les conditions prévues à l'article 706-88 du Code de procédure pénale et le recours à ceux des pouvoirs spéciaux d'enquête ou d'instruction prévus par le titre XXV du livre IV du Code de procédure pénale qui sont applicables à toutes les infractions visées par l'article 706-73 ;

12. Considérant que l'article 706-88 du Code de procédure pénale prévoit que, si les nécessités d'une enquête l'exigent, la garde à vue d'une personne peut, à titre exceptionnel, faire l'objet de deux prolongations supplémentaires de vingt-quatre heures chacune décidées par le juge des libertés et de la détention ou par le juge d'instruction ; que, dans ce cas, ces prolongations, qui s'ajoutent à la durée de droit commun définie par l'article 63 du même Code, portent à quatre-vingt-seize heures la durée maximale de la garde à vue ; que cet article permet également que l'intervention de l'avocat soit différée pendant une durée maximale de quarante-huit heures, en considération de raisons impérieuses tenant aux circonstances particulières de l'enquête ou de l'instruction, soit pour permettre le recueil ou la conservation des preuves, soit pour prévenir une atteinte aux personnes ; que ce report est décidé par le juge d'instruction lorsque la garde à vue est mise en œuvre au cours d'une information judiciaire ; que, dans les autres cas, il est décidé par le procureur

de la République pour la première prolongation et par le juge des libertés et de la détention pour la seconde ;

13. Considérant que l'escroquerie est un délit contre les biens défini par l'article 313-1 du Code pénal comme « le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge » ; que, même lorsqu'il est commis en bande organisée, le délit d'escroquerie n'est pas susceptible de porter atteinte en lui-même à la sécurité, à la dignité ou à la vie des personnes ; qu'en permettant de recourir à la garde à vue selon les modalités fixées par l'article 706-88 du Code de procédure pénale au cours des enquêtes ou des instructions portant sur ce délit, le législateur a permis qu'il soit porté à la liberté individuelle et aux droits de la défense une atteinte qui ne peut être regardée comme proportionnée au but poursuivi ; que, par suite, le 8° bis de l'article 706-73 du Code de procédure pénale méconnaît ces exigences constitutionnelles et doit être déclaré contraire à la Constitution ;

SUR LES CONSÉQUENCES DE L'ADOPTION DE LA LOI DU 27 MAI 2014 SUSVISÉE :

14. Considérant que, selon le Premier ministre, la modification apportée à l'article 706-88 du Code de procédure pénale par la loi du 27 mai 2014 susvisée a mis fin à l'inconstitutionnalité dénoncée par les requérants de sorte qu'il n'y aurait en tout état de cause pas lieu d'abroger les dispositions déclarées contraires à la Constitution ;

15. Considérant que l'article 4 de la loi du 27 mai 2014 susvisée a complété l'article 706-88 du Code de procédure pénale par un alinéa aux termes duquel : « Le présent article n'est pas applicable au délit prévu au 8° bis de l'article 706-73 ou, lorsqu'elles concernent ce délit, aux infractions mentionnées aux 14° à 16° du même article. Toutefois, à titre exceptionnel, il peut être appliqué si les faits ont été commis dans des conditions portant atteinte à la sécurité, à la dignité ou à la vie des personnes ou aux intérêts fondamentaux de la nation définis à l'article 410-1 du Code pénal ou si l'un des faits constitutifs de l'infraction a été commis hors du territoire national, dès lors que la poursuite ou la réalisation des investigations nécessaires à la manifestation de la vérité rend indispensable, en raison de leur complexité, la prolongation de la garde à vue. Les ordonnances prolongeant la garde à vue sont prises par le juge des libertés et de la détention, sur requête du procureur de la République ou du juge d'instruction. Elles sont spécialement motivées et font référence aux éléments de fait justifiant que les conditions prévues au présent alinéa sont réunies. Les sixième et septième alinéas du présent article ne sont pas applicables » ;

16. Considérant que ni les éléments constitutifs du délit d'escroquerie ni les circonstances aggravantes de ce délit ne font référence à des faits d'atteinte à la sécurité, à la dignité ou à la vie des personnes ; que le fait d'obtenir la remise de fonds, de valeur ou d'un bien quelconque par violence ou menace est qualifié par ailleurs d'extorsion ; qu'en permettant le recours à la garde à vue dans les conditions prévues par l'article 706-88 du Code de procédure pénale pour des faits d'escroquerie en bande organisée lorsque les faits ont été commis dans des conditions portant atteinte à la sécurité, à la dignité ou à la vie des personnes ou « aux intérêts fondamentaux de la nation définis à l'article 410-1 du Code pénal » ou si l'un des faits constitutifs de l'infraction a été commis hors du territoire national, les dispositions ajoutées à l'article 706-88 du Code de procédure pénale par la loi du 27 mai 2014 n'ont pas mis fin à l'inconstitutionnalité du 8° bis de l'article 706-73 du Code de procédure pénale ;

SUR LES EFFETS DANS LE TEMPS DE LA DÉCLARATION D'INCONSTITUTIONNALITÉ DU 8° BIS DE L'ARTICLE 706-73 DU CODE DE PROCÉDURE PÉNALE :

17. 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 ;

18. Considérant que l'inscription d'un crime ou d'un délit dans la liste des infractions visées par l'article 706-73 du Code de procédure pénale a également pour effet de permettre le recours à ceux des pouvoirs spéciaux d'enquête ou d'instruction prévus par le titre XXV du livre IV du Code de procédure pénale qui sont applicables à toutes les infractions visées par l'article 706-73 ; que, par suite, l'appréciation des effets dans le temps de la déclaration d'inconstitutionnalité du 8° bis de l'article 706-73 requiert d'apprécier également la conformité à la Constitution du recours à ces pouvoirs spéciaux d'enquête ou d'instruction ;

19. Considérant que l'article 706-80 du Code de procédure pénale permet que, sauf opposition du procureur de la République préalablement informé, la compétence des officiers de police judiciaire et des agents de police judiciaire soit étendue à l'ensemble du territoire national

pour la surveillance des personnes suspectées d'avoir commis certaines infractions ; que les articles 706-81 à 706-87 permettent au procureur de la République ou au juge d'instruction, lorsque les nécessités de l'enquête ou de l'instruction le justifient, d'autoriser l'organisation d'une opération d'infiltration d'un officier ou d'un agent de police judiciaire consistant « à surveiller des personnes suspectées de commettre un crime ou un délit en se faisant passer, auprès de ces personnes, comme un de leurs coauteurs, complices ou receleurs » ;

20. Considérant que les articles 706-89 à 706-94 fixent les conditions dans lesquelles, au cours d'une enquête préliminaire, d'une enquête de flagrance ou d'une instruction préparatoire, le juge des libertés et de la détention ou le juge d'instruction peut autoriser les perquisitions, visites domiciliaires et saisies de pièces à conviction en dehors des heures prévues par l'article 59 ;

21. Considérant que l'article 706-95 prévoit que, si les nécessités de l'enquête de flagrance ou de l'enquête préliminaire le justifient, le juge des libertés et de la détention peut autoriser l'interception, l'enregistrement et la transcription de correspondances émises par la voie des télécommunications ;

22. Considérant que les articles 706-96 à 706-102-9 prévoient que, lorsque les nécessités de l'information l'exigent, le juge d'instruction peut autoriser par ordonnance motivée la mise en place, sous son autorité et son contrôle, d'une part, d'un « dispositif technique ayant pour objet, sans le consentement des intéressés, la captation, la fixation, la transmission et l'enregistrement de paroles prononcées par une ou plusieurs personnes à titre privé ou confidentiel, dans des lieux ou véhicules privés ou publics, ou de l'image d'une ou plusieurs personnes se trouvant dans un lieu privé » et, d'autre part, d'un « dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, les conserver et les transmettre, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données ou telles qu'il les y introduit par saisie de caractères » ;

23. Considérant que l'article 706-103 prévoit qu'au cours de l'information, le juge des libertés et de la détention peut, afin de garantir le paiement des amendes encourues ainsi que, le cas échéant, l'indemnisation des victimes, ordonner des mesures conservatoires sur les biens, meubles ou immeubles, divis ou indivis, de la personne mise en examen ;

24. Considérant qu'en permettant le recours à ces pouvoirs spéciaux d'enquête et d'instruction pour les délits d'escroquerie commis en bande organisée, le législateur a estimé que la difficulté d'appréhender les auteurs de ces infractions tient à l'existence d'un groupement ou d'un réseau dont l'identification, la connaissance et le démantèlement posent des problèmes complexes ; qu'eu égard à la gravité du délit d'escroquerie en bande organisée, le législateur a pu, à cette fin, fixer

des règles spéciales de surveillance et d'investigation dans les enquêtes et les instructions portant sur une telle infraction ; que, compte tenu des garanties encadrant la mise en œuvre de ces mesures spéciales d'enquête et d'instruction, les atteintes au respect de la vie privée et au droit de propriété résultant de leur mise en œuvre ne revêtent pas un caractère disproportionné au regard du but poursuivi ;

25. Considérant, en premier lieu, que l'abrogation immédiate du 8° bis de l'article 706-73 du Code de procédure pénale aurait pour effet non seulement d'empêcher le recours à une garde à vue de quatre-vingt-seize heures pour des faits d'escroquerie en bande organisée, mais aussi de faire obstacle à l'usage des autres pouvoirs spéciaux de surveillance et d'investigation prévus par le titre XXV du livre IV du même Code et aurait dès lors des conséquences manifestement excessives ; qu'afin de permettre au législateur de remédier à l'inconstitutionnalité du 8° bis de l'article 706-73 du Code de procédure pénale, il y a lieu de reporter au 1er septembre 2015 la date de cette abrogation ;

26. Considérant, en deuxième lieu, qu'afin de faire cesser l'inconstitutionnalité constatée à compter de la publication de la présente décision, il y a lieu de juger que les dispositions du 8° bis de l'article 706-73 du Code de procédure pénale ne sauraient être interprétées comme permettant, à compter de cette publication, pour des faits d'escroquerie en bande organisée, le recours à la garde à vue prévue par l'article 706-88 du Code de procédure pénale ;

27. Considérant, en troisième lieu, que la remise en cause des actes de procédure pénale pris sur le fondement des dispositions déclarées inconstitutionnelles méconnaîtrait l'objectif de valeur constitutionnelle de recherche des auteurs d'infractions et aurait des conséquences manifestement excessives ; que, par suite, les mesures de garde à vue prises avant la publication de la présente décision et les autres mesures prises avant le 1er septembre 2015 en application des dispositions déclarées contraires à la Constitution ne peuvent être contestées sur le fondement de cette inconstitutionnalité,

DÉCIDE :

Article 1er. – Le 8° bis de l'article 706-73 du Code de procédure pénale est contraire à la Constitution.

Article 2. – La déclaration d'inconstitutionnalité de l'article 1er prend effet sous la réserve énoncée au considérant 26 et dans les conditions prévues aux considérants 25 et 27.

Article 3. – Il n'y a pas lieu, pour le Conseil constitutionnel de statuer sur la question prioritaire de constitutionnalité portant sur les cinq premiers alinéas de l'article 706-88 du Code de procédure pénale.

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.

Délibéré par le Conseil constitutionnel dans sa séance du 9 octobre 2014, où siégeaient : M. Jean-Louis Debré, Président, M. Jacques Barrot, Mme Nicole Belloubet, MM. Guy Canivet, Renaud Denoix de Saint Marc, Hubert Haenel et Mme Nicole Maestracci.

Actualités parlementaires : loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme

Le projet de loi a pour objet d'adapter la législation relative à la lutte contre le terrorisme afin de prendre en compte des évolutions inquiétantes, qui concernent la nature des actes et le comportement des auteurs. Il « vise à renforcer les moyens de lutte contre la propagande terroriste, tant sur le plan de la procédure pénale qu'en matière de police administrative ». Il se compose de cinq chapitres.

Le chapitre Ier (article 1er) a pour objet de créer un dispositif d'interdiction de sortie du territoire afin d'empêcher le départ de ressortissants français dès lors qu' « il existe des raisons sérieuses de croire qu'il projette des déplacements à l'étranger ayant pour objet la participation à des activités terroristes, des crimes de guerre ou des crimes contre l'humanité [ou] sur un théâtre d'opérations de groupements terroristes et dans des conditions susceptibles de le conduire à porter atteinte à la sécurité publique lors de son retour sur le territoire français ».

Le chapitre II (article 2) renforce les dispositions applicables aux étrangers assignés à résidence.

Le chapitre III (articles 3 à 6) renforce la répression des actes de terrorisme et tire les conséquences de l'intégration de l'apologie et de la propagande dans la stratégie médiatique des organisations terroristes. Ainsi, l'article 3 complète la liste définissant les actes de terrorisme afin de rajouter la diffusion de procédés permettant la fabrication d'engins de destruction, la détention de produits incendiaires ou explosifs ou d'éléments entrant dans la composition de produits ou engins explosifs ; l'article 5 incrimine l'entreprise terroriste individuelle ; l'article 6 permet au juge des référés d'ordonner l'arrêt d'un service de communication au public en ligne en cas de provocation à la commission d'actes terroristes et d'apologie du terrorisme.

Le chapitre IV (articles 7 à 15) renforce les moyens de prévention et d'investigation. L'article 9 permet ainsi à l'autorité administrative de demander aux fournisseurs d'accès à internet de bloquer l'accès aux sites provoquant aux actes de terrorisme ou en faisant l'apologie ; l'article 10 adapte le Code de procédure pénale pour que les perquisitions des systèmes informatiques puissent s'appliquer aux données stockées dans le nuage notamment ; l'article 15 porte à trente jours (au

lieu de 10) la durée de conservation des enregistrements des interceptions de sécurité.

Le chapitre V (articles 16 à 18) traite des dispositions relatives à l'outre-mer.

Le Gouvernement ayant engagé une procédure accélérée sur ce texte le 9 juillet 2014, il n'a fait l'objet que d'une seule lecture par chacune des chambres du Parlement, puis d'une réunion de la Commission mixte paritaire le 21 octobre 2014.

S'agissant des dispositions relatives aux interceptions de sécurité, l'article 15 du projet de loi proposait de modifier l'article L242-6 du Code de la sécurité intérieure pour porter de dix à trente jours le délai maximal au terme duquel les enregistrements des interceptions de sécurité doivent être détruits sous l'autorité du Premier ministre.

Il convient d'observer que cette disposition avait une portée bien plus large que la lutte contre le terrorisme puisqu'elle aurait concerné les cinq motifs visés à l'article L241-2 du Code de la sécurité intérieure, dont quatre sont sans rapport avec l'objet du projet de loi. Ce texte n'était donc pas le vecteur législatif adéquat pour envisager de modifier une modification du régime actuel.

Ce triplement du délai de conservation des enregistrements aurait en outre un impact considérable en termes d'atteintes portées au secret des correspondances, sans pour autant permettre de réels gains au plan opérationnel.

Aucun des arguments techniques en faveur de cet allongement à trente jours figurant dans l'étude d'impact n'est en effet recevable. Le trop faible nombre d'interprètes en langues rares au sein des services de renseignement ne pourra trouver de solution que par le recrutement de traducteurs ; l'augmentation du stock d'enregistrements à traduire ne ferait qu'aggraver la situation. Les contraintes liées à la circulation de documents classifiés contenant les données recueillies dans le cadre des interceptions de sécurité n'ont rien à voir avec la conservation des enregistrements, puisqu'elles ne portent que sur les transcriptions de communications déjà rédigées. Les informations selon lesquelles les services ne seraient destinataires des facturations détaillées liées aux interceptions de sécurité qu'une dizaine de jours après la date de la conversation sont manifestement obsolètes : ces données techniques sont fournies au plus tard tous les quatre jours au service titulaire de l'écoute autorisée et contiennent les éléments permettant ensuite identifications ou recoupements. S'agissant de l'augmentation du contingent d'interceptions autorisé par le Premier ministre, aucun service n'a l'obligation d'utiliser la totalité de son quota disponible, à plus forte raison s'il n'a pas les capacités d'exploiter ensuite les communications interceptées.

Par ailleurs, l'allongement de la durée de conservation n'apportera strictement aucun avantage sur le plan de la « judiciarisation » des

procédures. Aucune donnée issue des interceptions de sécurité ne peut, en raison de son caractère classifié, être versée directement à une enquête pénale. Les informations recueillies dans le cadre des écoutes administratives ne peuvent être obtenues par l'autorité judiciaire qu'à l'issue de la procédure de déclassification prévue par les articles L. 2312-1 à L. 2312-8 du Code de la défense. Dans cette hypothèse, ce sont les transcriptions et leur analyse qui peuvent donner lieu à une éventuelle levée du secret-défense au profit de l'autorité judiciaire, qui interviendrait, en tout état de cause, au-delà du délai de trente jours. L'allongement du délai à trente jours risque donc plutôt de différer de plusieurs semaines une nécessaire décision de « passage en judiciaire », faisant perdre un temps précieux et des informations parfois décisives aux magistrats et services saisis ensuite de l'enquête pénale.

Surtout, ce triplement de la durée de conservation des enregistrements pourrait conduire les services, qui bénéficieront plus longtemps de l'accès aux communications, à différer leur retranscription, voire à s'affranchir de cette obligation légale. Or la transcription est l'outil qui permet l'exercice du contrôle démocratique par la Commission nationale de contrôle des interceptions de sécurité qui vérifie que les écoutes sont réalisées conformément au cadre légal. Imaginer que des individus seront écoutés durant une durée de trente jours sans garantir les moyens d'un contrôle effectif sur les informations obtenues par les services de renseignement constituerait un recul important pour la protection des libertés.

Conformément aux préconisations de la CNCIS lorsqu'elle a été entendue par les rapporteurs de l'Assemblée nationale puis du Sénat, cet article 15 a été supprimé du texte par la Commission mixte paritaire. Cette décision permet de préserver les garanties apportées par l'effacement à dix jours des enregistrements et de rappeler que les interceptions de sécurité constituent des atteintes plus exceptionnelles que celles ordonnées par le juge judiciaire. Elles visent des personnes dont l'implication dans des projets d'atteintes aux intérêts fondamentaux de la Nation est exclusivement présumée et qui, pour la majorité d'entre elles, ne feront jamais l'objet d'une procédure judiciaire. La durée de conservation des correspondances privées de ces personnes strictement limitée à dix jours est une garantie essentielle de leur protection et du caractère exceptionnel de ces mesures intrusives.

Table des matières

Le vingt-deuxième rapport d'activité de la Commission nationale de contrôle des interceptions de sécurité comporte trois axes de présentation :

- les perspectives et enjeux pour la CNCIS dans un contexte d'évolution du cadre légal des interceptions et du renseignement ;

- le compte-rendu des missions confiées à la Commission par le Code de la sécurité intérieure (ex-loi du 10 juillet 1991) et la loi du 23 janvier 2006 ;

- l'information, à destination des services utilisateurs autorités publiques et citoyens, relative aux avis généraux, recommandations et préconisations de la Commission, en matière d'exploitation des communications électroniques.

Le présent rapport consacre en conséquence sa première partie à la présentation de la CNCIS, de son actualité, puis de ses activités d'expertise et de contrôle.

La deuxième partie est constituée par l'exposé général de ses avis et préconisations.

Enfin, la troisième partie est destinée à offrir au lecteur une documentation actualisée sur les textes relatifs aux missions de la Commission, ainsi que des éléments d'information sur le contexte juridique dans lequel elle inscrit son action.

CNIS
COMMISSION NATIONALE DE CONTRÔLE DES INTERCEPTIONS DE SÉCURITÉ

Liberté • Égalité • Fraternité
RÉPUBLIOUE FRANCAISE

Diffusion
Direction de l'information légale et administrative
La **documentation** Française
Tél. : 01 40 15 70 10
www.ladocumentationfrancaise.fr

Imprimé en France

ISBN : 978-2-11-009866-5
DF : 5HC38540
Prix 18€