Commission nationale de contrôle des interceptions de sécurité

23e rapport d'activité 2014-2015

Commission nationale de contrôle des interceptions de sécurité

35, rue Saint-Dominique
75007 Paris

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

ISBN : 978-2-11-010033-7

Sommaire

Avant-propos

Les institutions n'ont aucune vocation à l'éternité. Nul ne saurait s'en plaindre, surtout lorsqu'il s'agit de renouveler le nom, la composition et la mission d'un organisme pour l'adapter au mieux à des circonstances nouvelles.

La loi sur le renseignement, adoptée au printemps 2015 par le Parlement, a prévu de remplacer la Commission nationale de contrôle des interceptions de sécurité (CNCIS), issue de la loi du 10 juillet 1991, par une Commission nationale de contrôle des techniques de renseignement (CNCTR).

Il revenait donc à la CNCIS d'élaborer, dans des délais abrégés, son vingt-troisième et ultime rapport public (pour 2014) que la loi lui impose, et d'y développer les éléments essentiels de son activité pour les premiers mois connus de l'année 2015. Elle l'a fait selon la structure des récents rapports, en détaillant ses différentes missions et leurs résultats. En particulier, figurent les observations sur les nouveaux dispositifs, mis en œuvre à compter du 1er janvier 2015, de recueil de données de connexion et de « géolocalisation en temps réel ». Elle y a joint, d'une part, une étude de Mme le professeur FAUVARQUE-COSSON sur une de ses préoccupations majeures : la portée de la loi nationale confrontée à la mobilité internationale des données ; d'autre part, une réflexion de Monsieur Jean-Jacques URVOAS, député, président de la commission des lois de l'Assemblée nationale, membre de la Commission, qui a joué un rôle de tout premier plan notamment dans l'élaboration et la discussion du projet de loi sur le renseignement ; enfin, signée de ses trois derniers présidents, une méthodologie du contrôle des services de police et de renseignement, telle qu'elle peut être tirée du (quasi) quart de siècle d'expérience de la Commission.

La CNCIS n'ignore pas que, si détaillées que soient les lois, celles-ci laissent toujours une place à l'interprétation. Elle le sait d'autant plus qu'avec l'accord des Premiers ministres qui se sont succédés depuis 1991, mais aussi pour accroître la sécurité de leurs décisions, son avis, que la loi prévoyait postérieur à chaque décision autorisant une interception, est devenu préalable. En même temps, elle a maintenu une ferme « jurisprudence » : ne peut être l'objet d'une interception qu'une personne personnellement et directement soupçonnée d'implication dans la préparation d'un acte préjudiciant de manière grave à l'ordre ou

à la sécurité. Enfin, elle a pu surveiller l'exécution des interceptions, dont les enregistrements et les transcriptions étaient en temps réel à sa disposition permanente. Ces manières de faire, respectueuses des besoins des services, mais aussi très nécessaires pour la protection des libertés, doivent être regardées comme des acquis sur lesquels il ne convient pas de revenir.

La loi sur le renseignement, que la Commission, avec bien d'autres, a appelé de ses vœux, met en œuvre certains principes utiles. Elle reconnaît que l'emploi d'une technique de renseignement doit être proportionné au risque d'atteinte à l'ordre public identifié. Elle définit des finalités de cet emploi de manière aussi précise que possible. Elle détaille (à l'excès ?) les outils qui peuvent être employés par les services. Elle consacre expressément le principe d'un avis préalable d'une instance de contrôle avant l'usage d'un de ces dispositifs. Elle donne au juge administratif un rôle d'une dimension inédite en la matière, pour contrôler à la fois la décision administrative et le bien-fondé du point de vue adopté par le contrôle.

Elle laisse cependant subsister des déceptions que la pratique ne pourra entièrement effacer, s'agissant du strict domaine du contrôle.

Il n'est pas sûr d'abord que la dimension exacte de ce dernier ait été bien perçue par le législateur. En matière de police ou de renseignement, il ne suffit pas d'aller voir lorsque tout est terminé, au seul vu des pièces de chaque affaire et sur les lieux de l'opération, si leur déroulement a été régulier. C'est avant d'y procéder et pendant que ces opérations ont lieu qu'on doit effectuer les vérifications nécessaires. Autrement dit, ni la CNCIS ni demain la CNCTR n'ont à rythmer leur activité sur le modèle d'un commissaire aux comptes. Elles doivent l'une et l'autre se caler sur les contraintes urgentes et immédiates des nécessités de police, sans rien abandonner de la rigueur de leurs exigences. C'est d'ailleurs ce qu'esquisse la loi, en prescrivant à la CNCTR des délais très réduits pour se prononcer (supérieurs toutefois à la pratique aujourd'hui observée à la CNCIS). Mais le nombre des membres de la commission future, sa composition, les détails de son organisation aux délices desquels la loi s'est abandonnée vont à l'opposé de cette ambition. Faut-il le rappeler à nouveau : la commission allemande comparable se compose de quatre membres ; la commission néerlandaise de trois. Personne n'avait estimé jusqu'alors, que les trois membres de la CNCIS étaient en nombre insuffisant. La conception qui a prévalu dans la loi votée par le Parlement, ajoutée à la possibilité d'une procédure dans l'urgence sans consultation préalable de la CNCTR et dans le dessein de faire instruire une part importante des demandes par l'ensemble du collège des commissaires, est, en l'état, un affaiblissement du contrôle, quoiqu'on ait réellement voulu et quoiqu'on ait pu affirmer sur ce point. Qu'on veuille bien en faire crédit au contrôleur actuel.

Il n'est pas certain non plus que la CNCTR ait à sa disposition les matériaux dont elle a besoin pour l'exercice de ses prérogatives. La loi a fondé ce dernier, en premier lieu, de manière détaillée, sur les déclarations des services : « traçabilité » donc registres, relevés, procès-verbaux… Le papier ne manquera pas. Mais, dans un domaine où le contradictoire n'existe pas, dès lors qu'est en cause une activité réalisée à l'insu des personnes qui en sont l'objet, le seul contrôle efficace est celui de la confrontation du dire et du faire, autrement dit de ce qu'affirment les services et des données qu'ils ont effectivement recueillies.

Mais ces données elles-mêmes ne sont pas un matériau comme un autre. Elles n'ont pas l'épaisseur de véracité d'un indice matériel sur une scène de crime. Le renseignement est de plus en plus affaire de données numériques. Ces données sont fragiles, fongibles, reproductibles ou effaçables. Elles circulent de surcroît très vite et loin. La question de l'efficacité que pose le contrôle réside beaucoup moins dans la question de savoir combien de personnes composeront la commission que de déterminer si, comme la CNCIS l'a demandé, la future commission aura à sa disposition, dans ses locaux ou dans ceux du Groupement interministériel de contrôle, l'intégralité des données recueillies, en temps réel. C'est à cette seule condition que pourra être vérifiée l'adéquation entre l'autorisation donnée et l'usage qui en sera fait.

Enfin, de manière inédite, au contraire de la CNCIS, la future commission aura à maîtriser des dispositifs complexes, dont les résultats dépendront non seulement de leur usage, mais aussi de leur conception. Aujourd'hui, l'organisme de contrôle siège à la commission (dite de l'article R. 226-2 – du Code pénal) qui examine les demandes d'agrément pour ceux qui détiennent ces outils qui servent au renseignement. Demain, il faudra davantage : vérifier que chaque instrument (notamment chaque programme informatique mis en œuvre) recèle bien les possibilités indiquées et non pas d'autres. La CNCIS a donc demandé que la CNCTR ait le contrôle de l'ensemble des dispositifs utilisés pour connaître quelles sont les données qu'ils étaient susceptibles de rassembler. Son succès en la matière a été mitigé.

Réclamer un contrôle effectif n'a pas pour but de donner de l'importance à une institution, qui vivra d'ailleurs dans la confidence ; ni d'alourdir la tâche, dont la CNCIS n'ignore pas – et moins que personne – la difficulté, des services de police et de renseignement ; pas davantage de satisfaire quelque goût malsain pour la personne du père Joseph. Mais si l'on admet, comme les auteurs de la loi, que des mesures qui portent atteinte à des droits des personnes (qu'elles soient consentantes ou non n'y change rien) ne peuvent être accrues que si, et seulement si, elles existent parallèlement à un avis indépendant susceptible d'éclairer la décision publique, alors on doit faire en sorte que cet avis ne soit pas illusoire, et qu'il soit donné, sans complaisance ni faiblesse, en toute

connaissance de cause. Il appartiendra à la CNCTR d'y veiller, quoi qu'il advienne.

Il appartient auparavant à la CNCIS de dresser son dernier bilan d'activité, dans le contexte menaçant et tragique, en matière de sécurité, de l'année 2015. On trouvera donc ci-après les principales données qui ont marqué sa mission depuis le dernier rapport et les premiers éléments tirés de la compétence, mise en œuvre à compter du 1er janvier de cette année, en matière de géolocalisation en temps réel (article L. 246-3 du Code de la sécurité intérieure).

La tradition du rapport est de comporter une étude extérieure. Je dois ma particulière gratitude à Mme Bénédicte FAUVARQUE-COSSON, professeure de droit international privé à l'université Panthéon-Assas, d'avoir accepté de jeter, dans ce rapport, les bases d'une réflexion sur le sujet particulièrement neuf et délicat de l'application de la loi française aux données numériques « circulantes ». Elle a abordé ce thème avec une très grande disponibilité et un complet désintéressement ; elle en a tiré pour ceux qui la liront des éléments d'une très grande clarté.

Il appartient aussi à celui qui a eu la chance de conduire la Commission à son terme de dire combien il est redevable aux présidents qui l'ont précédé (pour une durée bien plus longue que la sienne) dans ce rôle : ils ont tracé les lignes droites d'une action incontestable pour les praticiens, essentielle pour le citoyen et respectée le plus souvent par les pouvoirs publics. Leurs noms figurent dans ce rapport, de même que ceux des sept députés et des dix sénateurs qui ont été, au fil des années, membres de la Commission (aujourd'hui MM. Jean-Jacques URVOAS et François-Noël BUFFET) : tous ces parlementaires, très assidus, ont décidé des choix essentiels avec une conscience remarquable de leur responsabilité en même temps qu'une discrétion exemplaire. Certains d'entre eux ont accepté de retracer leur expérience et leurs idées dans de récents rapports, comme l'a fait M. URVOAS dans celui-ci.

Le quotidien de la Commission existante – c'est-à-dire une disponibilité de sept jours sur sept – a été assuré depuis l'origine par un délégué général et un chargé de mission. Pensant à eux, on se remémore cette formule applicable aux internes des hôpitaux parisiens : *« Depuis le 4 ventôse an X, les internes assurent les gardes des hôpitaux de Paris »* : depuis le 15 juillet 1991, deux magistrats – et, tout récemment trois – ont veillé aux droits en matière d'interceptions de sécurité, illustrant magnifiquement l'idée selon laquelle on peut défendre les libertés autrement qu'en rendant la justice (en dernier lieu, par ordre d'ancienneté à la Commission, M. ABRIAL, Mme MOREL-COUJARD et M. QUÉRÉ). Chacun d'eux l'a fait avec diligence, compétence et intelligence : ils méritent tous ma profonde reconnaissance. Et je ne saurais oublier tous les agents, infatigables et patients, de la Commission dont le travail a contribué à ce qu'elle a pu accomplir (en dernier lieu Mme MASSET, Mme BRUCKER et

M. GERMIN). Leur sérieux, leur sens de l'État, leur conscience des enjeux de la tâche de la Commission, leur préoccupation du bien commun a été une source à la fois d'émerveillement renouvelé et d'une forte motivation pour la mission dévolue à la CNCIS. Pour tous, je souhaite que leur passage, souvent prolongé et décisif à la Commission, soit une source de grande fierté. Elle est, de mon côté, source d'une très vive et durable gratitude.

Jean-Marie Delarue

Le contrôle des techniques de renseignement

Jean-Louis DEWOST
Président de la CNCIS de 2003 à 2009

Hervé PELLETIER
Président de la CNCIS de 2009 à 2014

Jean-Marie DELARUE
Actuel président de la CNCIS

Ce titre constitue évidemment une anticipation ; par conséquent, il a la forme d'une usurpation. Il appartiendra, bien entendu, à l'autorité indépendante créée par la loi sur le renseignement promulguée en 2015, la Commission nationale de contrôle des techniques de renseignement (CNCTR), de définir elle-même, dans le respect des dispositions légales, mais aussi dans les silences de la loi, les modalités et les objectifs du contrôle qu'elle a pour mission d'exercer sur l'emploi par les services des techniques de renseignement autorisées.

La Commission nationale de contrôle des interceptions de sécurité (CNCIS), qui a précédé la CNCTR depuis 1991, dans le seul domaine des « écoutes téléphoniques » et du recueil des données de connexion, puis, depuis 2015, également en matière de « géolocalisation » en temps réel, a, pendant près d'un quart de siècle, effectué sur les opérations des services de police et de renseignement un contrôle de même nature. Sous l'autorité de ses présidents successifs, avec la participation active de ses membres parlementaires et de ses agents, elle peut justifier d'une

certaine expérience. C'est pourquoi, à la veille de la création de la nouvelle commission, il a paru utile de dresser une analyse de ce que doit être un contrôle en la matière.

Dans tous les États, police et renseignement sont contrôlés. Mais ces contrôles peuvent avoir des objectifs tout à fait différents. Dans la plupart des hypothèses, l'efficacité des services peut être approchée, en conjonction avec des interrogations de nature financière. Dans les États autoritaires, la loyauté d'une police indispensable au pouvoir politique est mesurée de près. Mais ce qui sépare les États démocratiques de tous les autres États est (notamment) l'existence d'un contrôle portant sur l'observation de la légalité et le respect des droits des personnes dans les opérations de police, tant judiciaire qu'administrative.

Il s'agit là d'un contrôle délicat qui ne peut résulter que d'un équilibre ciselé entre missions de sécurité et préservation des droits. Que le contrôle soit excessif, et l'on ne manquera pas de dire que l'efficacité des services s'en trouve contrariée ; qu'il soit timoré, et on lui fera grief de céder aux commodités des fonctionnaires. Cet équilibre évolue avec le temps, selon les modalités de fonctionnement admises dans la police, selon les techniques qu'elle emploie, selon, surtout, les objectifs qu'on lui assigne et, par exemple, la place que l'on accorde dans les préoccupations publiques à la sécurité.

Les formes du contrôle

Dans la plupart des États démocratiques dont il est ici question, le contrôle peut revêtir de multiples formes et résulter de l'action de plusieurs organes. Tel est le cas dans le domaine spécifique du renseignement. On peut distinguer de manière schématique :

• Un contrôle de nature parlementaire, largement partagé, qui prend généralement la forme d'un comité spécialisé composé exclusivement de parlementaires ou non ; ainsi, par exemple, « la Commission permanente commune aux deux Assemblées de Roumanie pour l'exercice du contrôle parlementaire de l'activité de la structure » (du renseignement).

En France, ce contrôle est effectué par la Délégation parlementaire au renseignement (article 6 nonies de l'ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires). Cette délégation, qui comprend quatre députés et quatre sénateurs, est de création relativement récente (loi n° 2007-1443 du 9 octobre 2007). Comme le relève son premier rapport public [1], le Congrès

1) Rapport 2008-2009, p. 8.

américain s'était doté d'un tel instrument à la fin des années 1970, le *Bundestag* allemand en 1979 et les Communes en 1994. Les prérogatives de la délégation ont été renforcées par les dispositions relatives au renseignement de la loi n° 2013-1168 de programmation militaire (2014-2019) du 18 décembre 2013 et son rapport pour 2014, nettement plus dense et incisif, s'en est ressenti.

• Un contrôle de nature judiciaire. Il ne fait aucun doute lorsque la police agit dans le cadre d'une enquête ou d'une information judiciaire, dès lors que les techniques de surveillance utilisées par les services, autorisées par le Code de procédure pénale (en particulier par les articles 100 et suivants), le sont sur demande d'un magistrat [1]. Mais, dans certains pays, les moyens de surveillance employés dans le cadre de la police administrative peuvent également être l'objet d'un contrôle par un juge. Il s'agit alors, le plus souvent, notamment dans le monde anglo-saxon, d'une juridiction spécialisée. Au Royaume-Uni, l'*Investigatory Powers Tribunal* connaît des recours individuels dirigés contre l'emploi de moyens de surveillance par les services de renseignement.

En France, les opérations de police administrative, celles qui tendent à la préservation de l'ordre public, relèvent de la compétence du juge administratif qui en contrôle à la fois la légalité externe et la légalité interne, notamment la proportionnalité entre la mesure employée et le risque d'atteinte à l'ordre public. Mais la singularité des techniques de surveillance rend le recours devant le juge sur leur emploi très hypothétique : en effet, elles sont prises, par construction, à l'insu des personnes surveillées. Il est certes possible au justiciable de contester une décision qu'il ne connaît pas directement mais dont il subit les effets ; toutefois cette voie n'est guère plus fructueuse, pour des motifs identiques. Par conséquent, le contrôle juridictionnel des services de police et de renseignement reste parfaitement théorique, jusqu'à l'intervention de la loi sur le renseignement.

• Un contrôle, enfin, de nature indépendante, effectué par une autorité de composition variable, mais toujours distincte du pouvoir exécutif [2] : ce procédé est particulièrement développé dans les pays dans lesquels l'accent n'a pas été mis sur le contrôle juridictionnel (quelle que soit son efficacité) : ainsi, pour le domaine du renseignement, la Commission dite G-10 en Allemagne fédérale, la Commission de surveillance néerlandaise ou, dans une matière un peu distincte, le Garant de la protection des données italien.

---

1) Dans la pratique toutefois, compte tenu de leurs charges et des relations qu'ils se doivent d'avoir avec les services enquêteurs, le contrôle des techniques peut être d'effectivité inégale.

2) En cela, de manière décisive, ce contrôle se distingue du contrôle proprement hiérarchique qui peut être le fait d'inspections générales rattachées au ministre compétent. Ces inspections (complétées en France, depuis peu, par l'inspection – interministérielle – du renseignement) ont surtout pour fonction d'intervenir en cas de difficultés survenues.

En France, cette voie a été particulièrement développée, en raison de la place qu'ont prises dans la vie publique, depuis quarante ans, les autorités administratives indépendantes. Trois d'entre elles sont associées de près ou de loin au contrôle des activités de renseignement : la Commission nationale de l'informatique et des libertés (CNIL), pour les bases de données de sécurité qu'elles génèrent, la CNCIS, pour les trois techniques communément employées, et, plus indirectement, la Commission nationale consultative du secret de la défense nationale (CNCSDN), en ce qu'elle autorise ou non la « déclassification » de dossiers protégés par le secret. A titre nettement plus subsidiaire, l'Autorité de régulation des communications électroniques et des postes (ARCEP), qui a notamment pour fonction de réguler le marché des opérateurs téléphoniques, est susceptible de porter un intérêt à la manière dont ces derniers s'acquittent de leurs obligations au titre de l'emploi de techniques de surveillance dans le secteur des communications électroniques. Mais, en réalité, seule la CNCIS intervient en temps utile (c'est-à-dire dans le temps de l'action) dans l'activité des services.

Ces indications générales sur les différentes modalités du contrôle étant rappelées, c'est sur ce contrôle administratif qu'il convient à présent de se concentrer, pour en définir les principales exigences.

À quels caractères doit répondre le contrôleur ?

Il en va du contrôle comme de la norme juridique telle que l'analyse notamment la Cour européenne des droits de l'homme. La perfection abstraite de la loi n'est nullement décisive dans la préservation des droits ; c'est son application aux situations concrètes qui en marque la portée véritable. *« Beaucoup de lois, relève par exemple la Cour, se servent-elles, par la force des choses, de formules plus ou moins vagues dont l'interprétation et l'application dépendent de la pratique »*[1]. Ou encore : *« Afin de préserver la privation de liberté de tout arbitraire, il n'est pas suffisant que cette mesure soit exécutée conformément à la loi ; elle doit être rendue nécessaire par les circonstances »* (CEDH, 5e section, 5 mars 2015, *Kotiy c/ Ukraine*, n° 28718/09, § 42) ; dans le même sens : CEDH, 27 février 2007, *Nešťák c/ Slovaquie*, n° 65559/01, § 74 ou CEDH, 14 octobre 2010, *Khayderinov c/ Ukraine*, n° 38717/04, § 27. En définitive, selon une formule bien connue, *« la Convention*[2] *a pour but de protéger des droits non pas théoriques ou illusoires, mais concrets et effectifs »*

1) CEDH, 22 octobre 2007, Gde Chambre, *Lindon, Otchakovsky-Laurens et July c. / France,* n° 21279/02 et 36448/02, § 41.
2) C'est-à-dire la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.

(CEDH, 9 octobre 1979, *Airey c/ Irlande*, série A n° 32, § 24 – *Grands arrêts*, 5e éd., 2009, n° 2).

Ces affirmations constantes sur l'effectivité du droit s'appliquent aisément au contrôle exercé dans les États démocratiques, spécialement au contrôle des forces de police. Le critère de l'effectivité du contrôle doit en effet les distinguer des autres États.

Or, il n'est rien de plus aisé que de rendre un contrôle ineffectif, c'est-à-dire de faire en sorte que les contrôleurs n'entendent pas ce qu'ils doivent entendre et ne voient pas ce qu'ils ont à voir.

C'est pourquoi le contrôleur doit satisfaire à un certain nombre de caractères, sans doute insuffisants mais assurément nécessaires pour garantir un contrôle effectif.

La première condition est celle d'une entière indépendance vis-à-vis de l'exécutif.

Elle présente deux aspects.

Le contrôleur doit être totalement distinct de l'autorité gouvernementale : il ne peut relever d'aucune tutelle ministérielle, pas plus des autorités ayant en charge les services de police et de renseignement que de toute autre. Sa mission se sépare entièrement de celle des inspections générales rattachées à chaque ministre, dont le rôle est tout à fait utile mais dont la mission s'inscrit nécessairement dans des préoccupations de nature politique.

À cette fin, dépourvu de toute autorité hiérarchique, le contrôleur doit disposer d'un pouvoir symbolique élevé, qu'il tient de la place qui lui est donnée dans l'appareil institutionnel et de la compétence reconnue qui est la sienne et qui doit être assurée par des recrutements de personnes indépendantes et compétentes. Les moyens matériels nécessaires à l'exercice de ses missions (sous la contrepartie d'une gestion rigoureuse) doivent lui être procurés. Il doit enfin disposer d'une expression publique autonome, *a minima* sous la forme d'un rapport annuel.

Cette condition ne fait pas, en l'état de la législation, difficulté en France, dans la mesure où elle s'inscrit dans le cadre mentionné ci-avant des « autorités administratives indépendantes » qui, selon la formule de certaines lois qui leur sont applicables, *« ne reçoivent instruction d'aucune autorité »* et dont les missions ont toujours été séparées de celles des inspections générales. La CNCIS a relevé dès son origine de ce statut, que ses présidents successifs se sont efforcés de rendre constamment respecté et qui n'a pas été sérieusement contesté, au moins dans son principe, par aucun gouvernement.

La deuxième condition consiste à allier, vis-à-vis des services contrôlés, à la fois une très grande ouverture et… une totale fermeture.

Le contrôleur doit impérativement comprendre la nature des missions de ceux qu'il contrôle. Il n'a pas à s'interroger sur le bien-fondé de celles-ci, pour autant qu'elles rentrent dans le cadre de la loi. Mais il doit avoir pleinement conscience de leurs enjeux géopolitiques et de sécurité. Il doit mesurer toutes les servitudes qui s'y attachent, en comprendre les exigences, en assimiler les priorités. Le temps des services de police et de renseignement allie la collecte patiente et multiforme de données et l'analyse de celles-ci le plus souvent dans l'urgence. Ces contraintes, qui nécessitent en particulier des temps de réaction rapides et permanents, doivent être connues du contrôleur, qui doit en assurer le respect dans l'exercice de sa mission. À cette fin, il lui appartient de maintenir, avec tous les professionnels concernés, un dialogue aussi régulier que possible.

Mais, simultanément, sa mission est d'une nature radicalement différente. Le monde du renseignement a ses caractères et ses accommodements qu'il convient d'ignorer. Ce qu'on appellera « l'enjolivement » fait partie du jeu. La connaissance que les services ont la charge de recueillir constitue évidemment un pouvoir qui s'exerce dans l'art de la communiquer. Les demandes que connaît le contrôleur sont remarquables par ce qu'elles disent mais aussi par ce qu'elles peuvent ne pas indiquer. La facilité avec laquelle certaines peuvent passer d'une finalité à l'autre (par exemple de la sauvegarde des intérêts économiques essentiels à la sécurité nationale) est une illustration du caractère parfois imprécis de la réalité présentée.

Le contrôleur n'a pas à épouser cette manière de faire. Il doit être au clair sur les principes qui sont les siens et dégager les lignes d'un contrôle lisible et constant. Dans ces principes, il ne peut y avoir qu'intransigeance, dès lors qu'ils constituent l'armature d'un bon équilibre entre la sécurité et les droits du citoyen. Ceux-ci ne peuvent osciller au gré des nécessités quotidiennes de l'action policière. C'est à celle-ci, au contraire, de s'y faire.

Il s'en déduit, quant à la méthode – c'est là la troisième condition à remplir – que le contrôle ne peut donc reposer sur la seule déclaration des services contrôlés. Chacun peut pressentir qu'un régime entièrement déclaratif est une procédure qui n'a pas sa place en matière de police et de renseignement. C'est une des clés de l'effectivité évoquée d'aller au-delà du déclaratif pour accéder à la réalité du travail effectué. Ceux qui ont institué et mis en œuvre, à compter de 1991, la CNCIS l'ont parfaitement compris, qui ont décidé de mettre à sa disposition, non seulement les motivations des services justifiant les interceptions, mais aussi les enregistrements réalisés et les transcriptions qui en sont faites. Cette mise à disposition n'est pas différée, elle se fait « en temps réel ».

Par conséquent, l'aller et retour permanent du contrôleur entre la demande des services et l'usage qui en est fait (dès lors qu'elle a été autorisée par l'autorité gouvernementale) est la seule manière de vérifier :
– si l'atteinte ainsi portée à la vie privée, au secret des correspondances et à la protection attachée aux données personnelles est nécessaire ;
– dans l'affirmative, si le choix des moyens employés est proportionné au risque contre lequel on entend se prémunir.

Cette vérification doit être constamment possible. Elle est souvent mise en œuvre et s'avère décisive, en particulier lorsqu'il s'agit du renouvellement d'une demande d'interception après quatre mois d'usage. Le contenu des enregistrements est-il en adéquation avec la motivation du service ? Celui qui s'exprime est-il bien la personne surveillée ?Y a-t-il eu des transcriptions de ces interceptions ? Respectent-elles la règle selon laquelle ne doit être transcrit que ce qui regarde le motif pour lequel l'interception a été autorisée ?Y a-t-il même eu communications ? Et s'il n'y en a pas, est-ce la part du comportement d'un délinquant ou celle d'un citoyen sans reproche ? Il convient de se demander, *a contrario*, quelle serait la qualité des réponses apportées à ces questions essentielles dans un régime purement déclaratif : bien médiocre et de nature à rendre le contrôle sans portée.

La quatrième condition découle de la précédente. Le contrôle ne vaut que si aucun secret n'est opposé au contrôleur.

Cette condition ne va pas de soi s'agissant d'un domaine dans lequel le secret est la règle et son partage, l'exception.

Mais si l'on devait admettre que, pour des nécessités de sécurité, tout ou partie des informations détenues par les services échappait au contrôleur, la mission de celui-ci n'aurait aucun caractère de réalisme et, par conséquent, d'effectivité au sens indiqué. Le contrôle porterait sur des dossiers édulcorés, dont la portée ne pourrait être comprise. Les principes de nécessité et de proportionnalité des mesures envisagées ne pourraient donc être appréciés. *« Une ombre de contrôle sur une ombre de dossier »*, dirait Juvénal.

Fort heureusement, il n'en va pas ainsi depuis 1991 et la plupart des services ont livré sans réticences les informations dont ils disposaient, pour faciliter l'expression de l'avis exigé par la loi. On peut penser qu'il y a un lien nécessaire entre la conscience qu'ils avaient de la connaissance par la Commission des enregistrements, et la propension qu'ils ont eue à faire connaître ce qu'ils savaient. Quoi qu'il en soit, on doit cet hommage à beaucoup d'entre eux de ne pas rechigner à éclairer complètement les dossiers, en particulier dans le champ des infractions de droit commun. Certains domaines restent, il est vrai, encore d'accès difficile et certains services moins enthousiastes que d'autres : ce sont des exceptions.

La contrepartie à cet accès au secret est draconienne : les membres de la Commission de contrôle et leurs collaborateurs doivent être soumis

à des règles déontologiques très strictes sur la conservation des informations dont ils sont dépositaires. Rien, même la plus mince information, ne saurait être mentionné par quiconque sur les dossiers examinés. Cette règle ne vaut pas dans l'instant. Elle est perpétuelle, quelle que soit par ailleurs l'habitude prise par des anciens des « services » de distiller leurs confidences auprès de personnes avides de les recueillir. Il se trouve au contraire dans les relations entre la Commission et les services, quant au secret, quelque chose du secret médical entre médecin et patient : *« Il n'y a pas de soins sans confidences, de confidences sans confiance, de confiance sans secret »* [1]. La préservation du secret par le contrôleur est aussi une condition du contrôle. À notre connaissance, depuis 1991, cette obligation n'a jamais été méconnue par la CNCIS. C'est bien le moins.

Ce n'est pas la seule obligation due aux services. La cinquième condition que doit respecter le contrôleur est de remplir un certain nombre de devoirs à leur égard. L'indépendance ne peut signifier l'indifférence à l'égard de leur mission et des servitudes qu'elle implique.

Outre le respect du secret, il leur est dû, comme on l'a déjà évoqué :

– La connaissance des principaux contextes de leur tâche, que ce soit dans les traits de la criminalité ou dans la considération des éléments de sécurité nationale.

– La rapidité avec laquelle le contrôleur est amené à se prononcer sur les dossiers qui lui sont soumis : à cet égard, on ne saurait avoir à l'esprit l'idée d'un contrôle qui, comme il se pratique fréquemment dans l'administration, survenant longtemps après l'action, peut se donner le temps de la composition d'un rapport dont les termes sont pesés au trébuchet ; le contrôle ici évoqué est dans le tempo de l'action ; son effectivité le conduit à ne pas s'en écarter, tout en maintenant les exigences d'un examen approfondi des dossiers.

– La régularité de ses prises de position, en dépit de la variété des situations qui lui sont soumises. Tout en gardant une totale liberté d'appréciation, le contrôleur doit, comme la règle de droit, être aussi prévisible que possible dans son jugement, de manière que les services puissent d'eux-mêmes déterminer les choix qu'ils ont à faire.

Dans ces différents domaines, la CNCIS s'est efforcée à la continuité et à la régularité. S'agissant des délais, elle a jugé utile de se prononcer en moins de 24 heures sur les dossiers qui lui étaient soumis ; pour les demandes présentées en « urgence absolue », en moins d'une heure. Elle l'a fait selon des critères aussi constants que possible, comme on l'indiquera ci-après.

---

1) Selon la formule de l'ouvrage du Dr Bernard Hoerni, *Éthique et déontologie médicale*, 2e éd., Paris, Masson éd., juin 2000.

Cette manière de faire est vraisemblablement incompatible avec les effectifs d'une commission pléthorique. La CNCIS a pu valablement fonctionner à trois membres, comme son équivalent néerlandais ou presque comme son homologue allemand (quatre personnes). Ce nombre peu élevé est le corollaire obligé d'une décision rapide ; sans compter qu'il accroît les chances de la préservation du secret.

La sixième condition est de nature proprement politique et technique à la fois. Elle réside dans la confiance qui doit s'instaurer entre les pouvoirs publics, en l'espèce le Premier ministre ou son directeur de cabinet, le maître d'œuvre technique, c'est-à-dire le directeur du Groupement interministériel de contrôle (GIC), et la Commission, singulièrement son président[1]. Confiance d'abord entre les membres de la Commission dans les décisions prises et l'application qui en est faite. Confiance du Premier ministre dans la Commission, pour lui donner des avis rigoureux, assis sur les réalités et dont le secret est soigneusement préservé. Confiance du Premier ministre et du président de la Commission dans l'exécution stricte des décisions prises par le GIC. Confiance de la Commission dans l'étendue des premiers contrôles opérés par le Groupement sur la réalisation des interceptions. Cette confiance, qui implique une grande compréhension du rôle de chacun et la prise de conscience de l'interdépendance des trois, permet de donner aux procédures leur rigueur, à la prise de décision son rythme et de concentrer l'attention sur les dossiers les plus délicats. Elle suppose des contacts aisés aussi souvent que nécessaire.

La qualité des interceptions de sécurité, c'est-à-dire leur conformité aux libertés établies et l'efficacité qu'en attendent les services, peut être fortement compromise dès lors que l'un de ces liens essentiels disparaît.

La dernière condition qui s'attache au contrôleur tient à ses obligations vis-à-vis des citoyens, pour les libertés desquels il est une garantie voulue par le législateur.

Il en a au moins deux.

La première est de se prononcer, comme on le dit dans les juridictions en matière d'indemnisation, « tous intérêts compris », en prenant donc en considération les préoccupations tenant non seulement à la sécurité et aux besoins des services, mais aussi celles qui s'attachent à la préservation des droits et libertés individuels. Sans quoi, naturellement, le contrôle serait sans portée. Cette évidence dissimule cependant l'étroitesse du chemin qui doit être suivi et l'instabilité du bon équilibre à faire respecter. D'autant que, par expérience, on sait assez vite que la

1) Sur cette condition, voir les considérations de Jean-Louis Dewost dans le chapitre consacré au vingtième anniversaire de la Commission nationale de contrôle dans le *20e rapport d'activité (années 2011-2012)* de la CNCIS, Paris, La Documentation française, décembre 2012, spéc. p. 10 sq.

sécurité parle fort, a une portée immédiate quand, dans le même temps, les libertés sont discrètes et de long terme. La première dit évidemment se garder toujours de quelque atteinte que ce soit aux secondes, mais a une forte propension à faire de nécessité vertu. Les secondes doivent pourtant, simultanément, tenir compte du temps et des mœurs dans lesquels elles s'inscrivent.

La seconde obligation consiste à assurer, malgré l'obligation du secret, la plus grande transparence possible sur ses activités. Les dossiers doivent être tus, mais non pas la réalité du contrôle. Le rapport public a déjà été mentionné. La possibilité pour les citoyens d'introduire des recours devant le contrôleur en est un autre aspect.

La CNCIS a publié chaque année son rapport et elle a enquêté sur toutes les demandes qu'on a bien voulu lui transmettre. Peu en ont eu conscience. Sauf dans des occasions particulières (parfois pénales), elle n'a pas été confrontée aux feux de l'actualité et on ne doit en avoir aucun regret. Mais elle a rempli scrupuleusement, pour qui voulait bien en prendre connaissance, son devoir d'information.

Quels sont les traits auxquels doit satisfaire le contrôle ?

Les traits du contrôleur ne sauraient suffire à définir un contrôle satisfaisant. Ce dernier doit être doté de caractères propres qui en garantissent la portée.

Le contrôle des techniques de renseignement doit être à la fois *a priori* et *a posteriori*.

Il doit être préalable, comme l'affirme la loi de 2015 (article L. 821-1 du Code de la sécurité intérieure). La loi de 1991 ne l'avait pas prévu ainsi en matière d'interceptions de sécurité. Très heureusement, avec l'accord des Premiers ministres successifs, la coutume a voulu que ces derniers ne décident la suite à donner aux demandes qu'une fois l'avis de la Commission nationale de contrôle en main. Cette manière de faire est évidemment plus protectrice du citoyen : elle évite que tout début d'interception ne soit mis en œuvre, alors qu'un avis *a posteriori* du contrôle pourrait certes en arrêter rapidement la réalisation, mais seulement après un début d'exécution. Mais elle garantit aussi à l'exécutif une meilleure protection, en assortissant toute décision de sa part, dans une matière délicate, d'un avis éclairé sur la légalité de la mesure. C'est pourquoi la pratique s'est imposée et maintenue. Il est heureux que la loi l'ait érigée en principe en 2015.

Ce rapport revient plus longuement, dans un chapitre ultérieur, sur les critères qui fondent le contrôle préalable. On se contentera ici d'en faire une énumération succincte.

1) La Commission doit examiner d'abord si la mesure d'interception envisagée est nécessaire.

Cet examen peut surprendre. Il est pourtant dans la logique de la loi, qui précise bien que les interceptions ne peuvent revêtir qu'un caractère « exceptionnel » (article L. 241-2 du Code de la sécurité intérieure). Ce trait d'exception se traduit de deux manières :

Dans la gravité des actes dont les personnes écoutées peuvent être soupçonnées.

Dans le fait qu'il n'est pas possible de recueillir par une autre voie les nécessaires informations dont les services ont besoin. Il existe donc, pour traduire l'exception, un principe de subsidiarité : une interception ne peut être ordonnée, dès lors qu'elle est très intrusive, que si ce qu'elle permet de recueillir comme information ne pouvait être obtenu par les « moyens classiques d'investigation ».

2) La Commission doit ensuite savoir si le moyen sollicité est proportionnel au risque de l'atteinte à l'ordre public. La loi de 2015 a inscrit, on l'a indiqué, dans un texte cette obligation de proportionnalité, pratique constante de la Commission : l'atteinte portée au secret des correspondances ne saurait être justifiée que si le risque d'atteinte à l'ordre public est lui-même d'une gravité certaine.

3) Elle doit également déterminer si les motifs invoqués dans la demande correspondent bien à l'une des finalités définies par la loi qui, seules, peuvent justifier le recours aux interceptions de sécurité.

4) Il appartient aussi à la Commission de vérifier que la personne visée est bien l'auteur potentiel de l'infraction en projet ou de l'acte mettant en cause divers intérêts nationaux. Cette personne doit être identifiée avec précision ou, si l'enquête ne permet pas de l'identifier, elle doit être caractérisée avec suffisamment de détails pour ne pouvoir être confondue avec une autre. La loi de 1991 n'a jamais prévu qu'on puisse écouter les « entourages » (s'ils ne sont pas complices) du seul fait de cette qualité ; elle n'a pas davantage autorisé qu'on intercepte les communications des victimes. La Commission s'en est donc constamment tenue au critère de la présomption d'implication directe et personnelle.

5) Il revient enfin à la Commission de contrôle de vérifier que les renseignements à recueillir relèvent d'une phase administrative et non judiciaire, du moins dans les domaines dans lesquels une infraction est possible (tel n'est pas toujours le cas, par exemple pour des matières que la loi qualifie de sécurité nationale). Autrement dit, que les indices déjà connus et qui doivent être encore rassemblés ne sont pas suffisamment précis et certains pour constituer des éléments justifiant l'ouverture d'une enquête ou d'une information judiciaire. C'est là évidemment une appréciation délicate, dont la justesse dépend du degré de précision de la demande présentée. Mais elle est essentielle : elle engage en effet

la règle de la séparation des pouvoirs, rappelée à plusieurs reprises par le Conseil constitutionnel[1].

Tels sont les critères qu'il incombe au contrôle de vérifier au préalable, c'est-à-dire avant l'examen de la demande des services par l'autorité politique.

Mais le contrôle doit aussi veiller à la manière dont la technique de renseignement est mise en œuvre postérieurement à l'autorisation donnée, afin de savoir si elle lui est bien conforme. On dira également plus loin dans le rapport quels sont les critères pris en considération. On se borne à indiquer ici que le contrôle de l'exécution a quatre principaux objets :

– Il postule que les services peuvent, par la force des choses ou négligence, déborder des limites qui leur ont été imparties ; ces débordements dans le domaine des libertés individuelles affecteraient la nature de la mesure ; les modalités de cette dernière ne seraient plus ni nécessaires ni proportionnées ; elle en deviendrait donc irrégulière ; l'exécution a bien un rapport avec la régularité ou non de l'opération (raisonnement qui est le même que celui tenu par la Cour européenne des droits de l'homme à propos des mesures de privation de liberté, comme il a été mentionné précédemment).

– Il permet de mettre en rapport la motivation des services avec ce qui se déroule dans la suite ; autrement dit, il autorise le contrôle à savoir si les motifs ayant servi de support à la demande sont confirmés par la réalité observée ; cette juxtaposition permet de vérifier si les suspicions des services avaient un fondement ou non ; dans ce dernier cas, à établir s'il a été commis une erreur – bien pardonnable, mais peu fréquente – d'analyse, ou si la demande n'a pas péché par excès, quelles qu'en soient les formes.

– Il contrôle que la ligne est bien active, autrement dit qu'elle est effectivement utilisée ; dans la négative, il n'y a pas de renseignement qui puisse être obtenu et, par conséquent, de motif que la mesure se poursuive ; toutefois, on doit aussi compter avec les téléphones qui ne sont employés qu'à titre exceptionnel par leurs possesseurs, dans le but exclusif de passer des consignes en relation directe avec la Commission d'une infraction.

– Enfin, il vérifie que la personne dont les communications sont interceptées est bien celle qui était définie dans la demande. Un téléphone cellulaire passe aisément de main en main ; un abonnement peut être résilié ; des erreurs de numéro sont possibles. Or, l'autorisation est donnée pour une personne déterminée ; pas une autre.

---

1) En particulier dans sa décision n° 2005-532 DC du 19 janvier 2006 (cons. 5).

Contrôle préalable et contrôle *a posteriori* forment un tout indissociable. Ces deux aspects donnent au contrôle sa vraie dimension et renoncer à l'un d'eux serait dénaturer la portée des vérifications opérées. Renoncer au contrôle préalable est en effet admettre que des interceptions peuvent commencer d'être exécutées sans qu'un tiers indépendant en ait apprécié la validité, par conséquent, que des personnes pourraient en être l'objet alors qu'elles ne devraient pas. Ne pas admettre le contrôle *a posteriori* reviendrait à ignorer que l'exécution comporte des marges de manœuvre et que la coïncidence stricte entre l'autorisation et la réalisation est l'une des vertus qui peut faire admettre le dispositif.

Au demeurant, le contrôle ne se borne pas à émettre des opinions exclusivement favorables ou absolument opposées aux demandes qui lui sont présentées. D'une part, dans la préoccupation constante qui est la sienne de dialogue avec les services, il lui arrive fréquemment de solliciter du demandeur, avant de rendre un avis, des « renseignements complémentaires » destinés à parfaire son information et à se prononcer en connaissance de cause. Tel est le cas lorsqu'une motivation est incomplète ou que les affirmations qu'elle comporte n'apparaissent pas étayées par les circonstances invoquées. Le service n'est donc pas contraint par une démarche effectuée une fois pour toutes. D'autre part, comme le rapport le rappellera ci-après, un avis favorable peut être assorti de conditions tenant à la réalisation de la mesure, spécialement dans sa durée (pour abréger le délai maximum de quatre mois fixé par la loi) ou dans la vérification systématique de ce que donnera l'interception.

C'est à ces conditions que la CNCIS a pu exercer le rôle que lui a confié le législateur.

Quelles questions de fond le contrôle doit-il trancher pour accomplir sa mission ?

Ce sont, au fond, les questions que devaient se poser les auteurs de la loi sur le renseignement avant de définir les missions et la composition de la CNCTR.

On peut en identifier une demi-douzaine.

La première consiste à se demander pour quels motifs, de manière générale, peut-on autoriser des atteintes aux droits des personnes par des interceptions de sécurité ou de manière générale par des techniques mettant en cause le respect dû au droit à une vie privée ou au secret des correspondances ou encore à la protection des données personnelles.

On sait que la France a connu des expériences condamnables, faute d'avoir défini, avant la loi de 1991, de telles finalités. En 1991, cinq ont été inscrites dans la loi. Elles n'ont pas été modifiées jusqu'en 2015.

Une telle durée implique d'ailleurs qu'on ne les change « qu'en tremblant », c'est-à-dire avec de sérieuses raisons.

Trois de ces cinq finalités ont constitué l'essentiel des volumes d'interception (*cf.* la suite de ce rapport). La prévention de la criminalité et de la délinquance organisées a toujours été la plus importante de ces trois.

Ces définitions se ressentent évidemment des évolutions sociales. Il ne serait pas exact de soutenir que la prévention du terrorisme a été insuffisamment prise en considération en 1991. Ce motif se suffit à lui-même et n'a besoin d'aucune précision supplémentaire, d'autant plus que le Code pénal (articles 421-1 et suivants) – dont il est toujours souhaitable de rester proche lorsqu'il s'agit d'éclairer la portée des finalités de la loi – en donne une définition (modifiée il est vrai à plusieurs reprises). En revanche, la forme que prennent certaines formes de violence collective dans la société du XXIe siècle, qui ne se rattachent ni à des manifestations terroristes, ni à aucun but crapuleux, et pas davantage à la sécurité nationale, fait hésiter à ouvrir les interceptions à l'encontre des personnes qui les pratiquent et, même si on devait l'admettre, à la finalité à laquelle les réunir. Il en va ainsi, par exemple, des « *fights* » qu'organisent de manière systématique des « supporters » assistant à des matches de football à l'encontre des soutiens (parfois venus pour « relever le défi ») de l'équipe adverse. Ou encore des personnes qui, parmi d'autres beaucoup plus pacifiques, érigent la contestation de projets d'infrastructure en combats de principe dont la fin justifie tous les moyens, même les plus violents. Faut-il alors faire évoluer les motifs en en élargissant le nombre et en en modifiant les termes ? Les auteurs de la loi de 2015 sur le renseignement s'y sont efforcés, non sans mal, et avec des rédactions contestées lors des débats.

En tout état de cause, un élargissement des motifs se traduit, avec des degrés divers, par un élargissement de la population concernée par les techniques d'investigation qui portent atteinte à la vie privée. On doit, par conséquent, n'en accepter le principe qu'avec beaucoup de précautions, pour des causes précisément identifiées d'insuffisances des finalités existantes ; à la condition d'avoir mesuré au moins approximativement le nombre de mesures induites ; surtout, d'avoir conscience de respecter, dans une nouvelle matière, l'équilibre entre la gravité de l'atteinte à l'ordre public et la gravité de la mesure d'intrusion.

La deuxième question est liée à la précédente : c'est celle de la population susceptible d'être impliquée dans les mesures intrusives, non pas à raison des finalités définies dans la loi, mais de la nature et du volume des techniques employées et des implications requises par les textes en vigueur et la « jurisprudence » de l'organisme de contrôle. Les techniques : suivant qu'un dispositif de demande à un opérateur est relatif aux données de connexion d'un seul appareil téléphonique ou qu'un autre dispositif s'intéresse aux données de connexion de tous les clients

de cet opérateur, la portée est évidemment distincte ; cette distinction a nourri bien des débats de la loi de 2015. Mais la nature des implications paraît encore beaucoup plus décisive : suivant que la possibilité est ouverte de « surveiller » seulement la personne directement et personnellement impliquée ou bien son « entourage », surtout si ce terme n'est pas défini, la population peut passer d'un seul individu à plusieurs centaines ou davantage. La loi doit être très précise sur ceux qu'elle entend soumettre aux mesures qu'elle définit. Le complice du crime envisagé ne fait guère de doute ; mais faut-il y ranger les siens qui n'ont d'autres liens qu'affectifs ou de pure circonstance ? Ceux qui lui rendent service (réparer son véhicule par exemple) ? Il est des pays où l'on surveille, à partir d'une personne, l'entourage de l'entourage de l'entourage ; soit beaucoup d'effectifs, inéluctablement voués à croître. La manière d'englober ou non est encore plus déterminante que les techniques mises en œuvre. Elle n'a guère été questionnée lors du vote de la loi sur le renseignement.

Au surplus, un accroissement du nombre de personnes génère un nombre imposant de possibilités de « croisements », c'est-à-dire d'occurrences dans lesquelles deux personnes vont se trouver associées, sans qu'elles aient nécessairement quelque chose à voir entre elles. Le nombre entretient ainsi le soupçon, qui demande de nouveaux élargissements.

La troisième question porte sur le mécanisme de contrôle et ses prérogatives. Quelle est la matérialité de ce qu'il a à contrôler ?

La CNCIS n'avait pas à poser cette question en 1991 de manière aussi élaborée.

Elle a tout de même opéré alors un choix décisif : contrôler non pas l'activité humaine des services faisant réaliser des interceptions de sécurité par le GIC ; mais directement le matériau recueilli par ces services, et la transcription qui en était faite. C'est bien là une différence de nature. Dans le premier cas, le contrôle est dépendant des services qui lui font savoir quelle est leur pratique ; dans le second, il est au cœur de l'action d'investigation et sait précisément, sans opinion intermédiaire, ce qu'il advient. Elle a, d'instinct, compris que le véritable contrôle ne repose pas sur les déclarations des contrôlés, alors même qu'elles seraient insoupçonnables, mais sur la confrontation de la norme à la réalité. Là repose, comme il a été dit précédemment, une grande part de l'effectivité du contrôle.

Mais, en dehors de ce choix, peu d'éléments techniques faisaient obstacle au contrôle, dès lors que le GIC, « neutre » on l'a indiqué, se chargeait des dispositifs techniques dont il rendait d'ailleurs volontiers compte. Contrôler une interception consiste à écouter, s'il en est besoin, les communications qui en sont issues et constater qu'elle a été interrompue à la date prévue ; contrôler les transcriptions, c'est les lire pour vérifier leur adéquation avec l'enregistrement et qu'elles tiennent compte des interdictions de la loi (relatives à ce qui est étranger à l'affaire). En bref, l'œil et l'oreille sont presque suffisants.

Le recueil des données de connexion, qui se distingue dès à présent des interceptions de sécurité (*cf.* ce rapport ci-après) est une opération technique qui passe par l'opérateur après approbation de son principe sur examen d'une demande. Mais cette technique reste cependant relativement simple : sa faisabilité repose sur l'opérateur qui en livre les résultats.

Il en ira autrement avec les techniques autorisées par la nouvelle loi sur le renseignement, par lesquelles les services mettront en œuvre des dispositifs d'une relative complexité technique, dont les résultats dépendront précisément de leurs caractéristiques. Ainsi, s'il est présenté par un service un logiciel permettant de repérer chez un opérateur les communications avec un site du *« darknet »* lié au terrorisme agissant, faut-il que le contrôleur en accepte sans autre forme d'investigation la présentation par le service ? Et si le logiciel est capable aussi d'identifier les communications avec les sites des jeux en ligne pour repérer l'addiction de joueurs, qu'en saura le contrôleur ?

La sophistication des technologies intrusives, dont la fabrication génère un marché où interviennent des acteurs puissants, contraint le contrôleur, demain, à s'adapter. En premier lieu, en se dotant des connaissances techniques qui lui sont nécessaires, par le moyen de recrutements idoines ; en second lieu, en élargissant ses prérogatives à un contrôle non seulement des données obtenues, mais des outils par lesquels elles le sont.

Cette question de la matérialité se distingue à peine d'une autre question relative au contrôle des données recueillies.

L'essentiel de ce qui est recherché par les services – identifier quelqu'un, connaître ses agissements et ses relations – se traduit *in fine* dans la quasi-totalité de ce qui doit être contrôlé par des données numériques (conversations téléphoniques, données de disque d'ordinateur, signaux de balise…).

Les données numériques ont un avantage et deux inconvénients.

L'avantage réside dans la mobilité. Un tour du monde, au mieux des opportunités de coût, est une banalité pour ceux qui ont à transmettre du numérique. *A fortiori* s'il s'agit de transmettre une donnée d'un service déconcentré de police à un organisme de contrôle. La centralisation des données ne pose, dans son principe, aucune difficulté.

Le premier inconvénient est dans la fragilité des réseaux. On le sait bien avec le développement des attaques informatiques de toute nature, par jeu, malveillance, concurrence ou stratégie. Par conséquent, les données sensibles ne doivent pouvoir circuler que sur des réseaux sécurisés par des moyens adéquats. C'est une des garanties que les intrusions autorisées par la loi doivent offrir : que la connaissance des données personnelles par les services de police soit strictement limitée

non seulement selon les finalités définies mais aussi aux personnes auxquelles elles sont destinées. Cette utilisation « étroite » a des contraintes techniques.

Le second inconvénient provient de la vulnérabilité de la donnée. Elle peut disparaître aisément, ou se dissimuler, ou encore être différée. La difficulté du contrôle s'en trouve sensiblement accrue. Comment acquérir la certitude que ce qui lui est présenté correspond trait pour trait à ce qui a été effectivement recueilli. C'est pourquoi des dispositions doivent être prises pour que la véracité des données présentées soit établie ; sans quoi tous les détournements seraient possibles. Elles prennent la forme de diverses solutions techniques : la traçabilité des manipulations apportées aux dispositifs de recueil, la transmission en temps réel des données au contrôle, la duplication pure et simple de certaines d'entre elles si la transmission n'est pas immédiatement envisageable. Ici est en jeu l'exhaustivité du contrôle qui est l'un des aspects de l'effectivité évoquée précédemment.

L'avant-dernière question a trait au contrôle qui peut être fait des activités internationales de renseignement ou de police.

Cette question ne devrait pas se poser dans un contexte classique. Pour un motif très simple. La loi française qui organise un contrôle – celle de 1991 par exemple – ne saurait s'appliquer dans un territoire étranger. Il n'en va autrement que dans des hypothèses particulières, soigneusement délimitées par la règle nationale ou internationale ou bien la jurisprudence ; ainsi pour la loi pénale : le juge français est compétent dans le cas de crimes commis sur ou par des Français à l'étranger. Mais une loi régissant le contrôle d'une administration française n'a d'application que sur le territoire.

Certes, la CNCIS a pu, à l'initiative de ses présidents, et avec l'accord des Premiers ministres du moment, développer non pas un contrôle actif sur les activités à l'étranger, mais un contrôle « passif », en s'assurant que les activités des services à l'étranger ne comportaient aucune trace de téléphones français ni de recueil d'enregistrements en France. Toutefois, il est resté sans lendemain.

La loi de 2015 sur le renseignement aborde heureusement la question (article L. 854-1 du Code de la sécurité intérieure). Elle mérite en effet évolution pour deux raisons :

– La première est de fait. Comme on le sait depuis longtemps[1], la délinquance n'est pas désormais arrêtée par les frontières. C'est le contraire ; elle en joue. Il n'est pas exagéré d'affirmer que plus la délinquance ou le crime sont « organisés » au sens de la loi pénale, plus leur

1) Voir par exemple le fameux « Appel de Genève » de sept magistrats européens spécialisés dans les affaires financières et de corruption, le 1er octobre 1996.

aspect international est développé. Il en va de même du terrorisme : quelques-unes de ses racines sont hexagonales ; mais la part essentielle de la menace a des causes externes. La plupart des affaires de « sécurité nationale » ont également une origine étrangère. C'est pourquoi la distinction qui prévalait autrefois et séparait les services selon leur champ d'intervention s'efface dans la pratique. Identifier un trafiquant introduisant des stupéfiants sur le territoire national implique des moyens de surveillance déployés en France comme à l'étranger. La loi de 2015 en a tiré les conséquences, en envisageant expressément le cas d'utilisateurs de téléphones français ou soumis à des interceptions de sécurité en France qui se trouveraient à l'étranger. Mais cette disposition est loin de couvrir le champ de la réalité.

– La seconde, très délicate, est de droit. Si les données numériques font, comme on l'a indiqué, le tour du monde, quel est donc le régime juridique qui s'y attache ? Faut-il continuer d'espérer leur appliquer une loi nationale mais, dans l'affirmative, sous quelle forme ? Si aucune loi ne prévaut mais seulement les aspects contractuels d'un rapprochement conclu sur un simple « clic », comme on dit, entre un utilisateur et un fournisseur multinational, comment y rentrent des activités régaliennes comme celles du renseignement ?

La loi de 2015 ne s'est pas hasardée sur ce terrain, qui doit être pourtant clarifié. La CNCIS, soucieuse d'avancer en la matière, a demandé à un juriste éminent de tenter une première approche de la question, qu'on n'explorera donc pas davantage ici. On trouvera ci-après la contribution éclairante de Mme le professeur FAUVARQUE-COSSON.

Demain, il faudra bien que le contrôle trouve des éléments de réponse à cette interpénétration, dans le champ de la sécurité, des éléments nationaux et internationaux, si l'on ne veut pas, une fois encore, risquer de laisser des pans importants de l'activité des services hors de vue.

La dernière question, beaucoup plus traditionnelle, est de savoir quelles conséquences doivent être tirées de constats négatifs opérés par le contrôle, singulièrement sous la forme de sanctions éventuelles.

Depuis 1991, la CNCIS est un organisme consultatif. Elle donne un avis au Premier ministre, qui a la liberté de le suivre ou de s'en affranchir.

Cette solution est heureuse. Les autorités administratives indépendantes ne sauraient se substituer à l'exécutif. Leur objet est de faire œuvre d'arbitrage ou de régulation, lorsqu'autrement l'État risquerait d'être juge et partie (ainsi dans le domaine de l'énergie, des banques, des télécommunications ou de l'audiovisuel) ; ou bien de l'éclairer quand une opinion déliée de tout intérêt peut aider l'autorité publique à arbitrer entre deux intérêts majeurs. Telle est cette dernière situation qui se présente quand il faut choisir entre un droit attaché aux personnes et l'atteinte à l'ordre public. Le Gouvernement est responsable de ce dernier.

C'est donc à lui de faire ses choix. Mais ils peuvent être éclairés par les considérations qui ont été rappelées au début de ce propos.

Aucun président de la CNCIS n'a réclamé davantage que de pouvoir ainsi aider les Premiers ministres à se déterminer, le plus souvent par le truchement de leur conseiller chargé des affaires de sécurité.

Mais cette réponse ne règle pas tous les problèmes. Le Premier ministre doit-il tirer, d'une manière ou d'une autre, les conséquences d'une opinion négative du contrôleur ? Plusieurs hypothèses peuvent être envisagées, selon le moment de la mesure concernée.

En amont de la procédure, d'abord, si l'avis porté par le contrôle sur une demande de réalisation d'une mesure est négatif, au motif, par exemple, qu'en l'état du dossier présenté elle n'apparaît pas satisfaire les conditions posées par la loi, l'autorité publique peut-elle se contenter de refuser ou de passer outre ? Ou peut-elle assortir de conditions la mesure pour en atténuer les effets ? Ou engager un dialogue avec le contrôleur pour mieux saisir les motifs ayant conduit à l'avis défavorable ? Toutes ces hypothèses sont en réalité ouvertes. Elles peuvent dépendre de la manière de faire du Premier ministre ou de ses conseillers.

Il importe, au moins, d'éviter une pratique qui n'est pas devenue inhabituelle qui consiste, pour ces derniers, confrontés à une opinion négative du contrôleur, d'aller solliciter de nouvelles informations directement auprès des services et, après les avoir obtenues, de se prononcer ainsi sur une demande qui n'est plus la même, car enrichie de nouveaux éléments, que celle examinée par le contrôleur. Ce n'est pas seulement une manière d'encourager les demandeurs à ne pas tenir à ce dernier un langage de vérité ; c'est, en réalité, priver le Premier ministre de l'avis informé dont la loi l'a doté.

Plus en aval, pendant la réalisation de la mesure après autorisation, s'il est découvert par le contrôle que cette autorisation n'est pas respectée ou qu'existe une illégalité non détectée, que peut-il se passer ? En matière d'interceptions de sécurité, le GIC effectue des contrôles internes efficaces qui peuvent conduire cet organisme à demander l'arrêt de la réalisation (par exemple s'il apparaît dans les enregistrements que la personne visée n'est pas celle qui était demandée). La Commission nationale de contrôle fait de même. Dès lors que l'erreur est constatée, les services obtempèrent toujours. De telles demandes d'interruption sont aussi adressées par la Commission elle-même aux services, en cas de défauts véniels : elles ne font pas davantage difficulté.

En cas d'illégalité incontestable, la Commission a pris l'habitude d'adresser au Premier ministre une « recommandation » tendant à lui demander d'ordonner l'interruption de l'interception. Jusqu'en 2013

inclus[1], cette autorité a toujours réservé une suite immédiate et positive à de telles demandes. On peut souhaiter que cette tradition reprenne c'est-à-dire qu'à l'avenir cette possibilité de « recommandation » soit conservée, ce qu'indique la loi de 2015[2], et que son contenu soit pris avec le sérieux qui convient par ceux auxquels le document est destiné.

À cette possibilité, la loi sur le renseignement ajoute celle de saisir le juge administratif compétent (Conseil d'État), chargé de dire le droit et doté du pouvoir de décider la mesure illégale, c'est-à-dire de rétablir la situation comme si elle n'avait pas existé. On peut faire une lecture positive de cette disposition : c'est dire à coup sûr que la mesure illégale disparaîtra. On a la possibilité aussi d'en avoir une lecture plus nuancée : le temps que le juge se prononce, la mesure aura déjà produit la majorité ou la totalité de ses effets[3] ; le recours au Conseil d'État peut être perçu par le Gouvernement comme une chance supplémentaire de ne pas être désavoué dans un temps rapproché voire d'être suivi par cette juridiction et, par conséquent, de l'encourager à ne pas suivre les recommandations du contrôleur. Si on veut éviter les mesures irrémédiables (pertes d'informations jugées importantes), peut-être aurait-il fallu imaginer des mesures provisoires de suspension, le temps nécessaire à un nouvel éclairage de la légalité de l'opération.

Enfin, postérieurement à la réalisation de l'opération, quelles sont les sanctions possibles dans l'hypothèse d'une mesure irrégulière ? Elles peuvent être matérielles, administratives et indemnitaires.

Matérielles, c'est-à-dire faire disparaître toute trace des données recueillies. Ce que prévoit d'ailleurs la loi de 2015 à l'initiative soit du Premier ministre, soit du juge. Une telle disparition est symboliquement satisfaisante. Elle a toute chance d'être sans véritable effet. On l'a mentionné : les données sont vulnérables et une part de cette vulnérabilité tient à la facilité avec laquelle elles peuvent être dupliquées. Il convient de ne pas pécher par excès de naïveté en ce domaine[4]. Et même si les données sont en effet détruites, ce qu'elles recélaient d'intéressant a pu être analysé, sans que le document d'analyse soit détruit. Le retour en arrière « comme si de rien n'était » n'est pas imaginable sans de sérieuses et détaillées précautions.

Mesures administratives : elles consistent à ordonner les consignes nécessaires pour que, dans les services, soient évitées, d'une

---

1) Il en a donc été autrement depuis cette date.
2) En l'état où elle se présente lorsque ces lignes sont écrites.
3) Voir ce qui a été dit plus haut sur la rapidité d'exécution des mesures comme sur le vieillissement rapide des informations obtenues.
4) Dans le cadre des mesures prises par la firme *Google* après l'arrêt de la Cour de justice de l'Union européenne (Grde Chambre, 13 mai 2014, *Google Spain SL et Google Inc. c/ Agencia española de protección de los datos et Mario Costeja González,* affaire n° C-131/12), le « déréférencement » de certaines données se traduit par la suppression de l'indexation, mais les données, elles, sont toujours conservées.

part, l'exploitation des données recueillies, d'autre part, la répétition des comportements ayant conduit à des demandes irrégulières. De telles mesures sont parfaitement possibles mais elles échappent à la règle, dans la mesure où elles relèvent du pouvoir hiérarchique des ministres. Elles peuvent cependant être suggérées par le contrôleur. Leur application peut être soumise à l'examen de l'inspection des services du renseignement [1], mobilisée le cas échéant à cette fin.

Mesures indemnitaires : la personne objet d'une mesure irrégulière de l'administration a le droit d'être indemnisée du dommage qui en résulte. Cette solution, établie depuis longtemps devant le juge administratif, a été rappelée à propos du contentieux de l'usage des mesures de renseignement tel qu'il figure dans le Code de justice administrative. L'avenir dira ce que fera le juge de cette prescription : le calcul du montant d'un dommage risque en effet d'être particulièrement délicat dans la mesure où la victime ne saura pas quelle part de sa vie privée a été observée ou lesquelles de ses données ont été reproduites [2] ; sans doute des montants forfaitaires pourraient-ils être envisagées.

Ces mesures apparaissent donc comme un effort incontestable, mais dont les effets réels sont relativement limités. C'est la raison pour laquelle l'intervention préalable d'un contrôleur, ou bien au plus tôt de l'exécution de la mesure autorisée, apparaît comme la plus protectrice, dès lors du moins qu'elle repose sur la sincérité des demandes et qu'elle se fonde sur la réalité de cette exécution.

Toutefois, il existe une dimension qui pourrait être, de principe, ajoutée à la mission du contrôleur : celui de vérifier *a posteriori* que des mesures correctrices, qu'elles soient recommandées par lui ou ordonnées par le Premier ministre ou par le juge, ont bien été exécutées.

*
* *

Il a fallu de longues années pour que l'existence d'un contrôle soit admise en matière d'interceptions de sécurité. Il a fallu encore attendre pour que la loi adapte la légalité aux pratiques nées des nouvelles technologies, dont l'évolution n'est évidemment pas terminée. En 2015, toutefois, l'extension du contrôle à ces nouveaux champs n'a pas été discutée. Elle est même apparue, pour les auteurs de la loi, on doit évidemment s'en réjouir, comme la condition nécessaire d'une telle extension. Encore faut-il que ces nouvelles formes permettent un contrôle aussi effectif demain que celui qui a existé dans le domaine des interceptions depuis vingt-cinq ans ou presque. Une analyse précise des dispositions de la loi

1) Mentionnée au I de l'article 6 nonies de l'ordonnance n° 58-1100 de l'ordonnance du 17 novembre 1958, elle a été définie par le décret n° 2014-833 du 24 juillet 2014.
2) Selon la loi de 2015, le juge se bornera en effet à lui faire connaître qu'une illégalité a été commise (article L. 773-7 du Code de justice administrative).

de 2015 devra être faite sur ce point et il appartiendra évidemment au nouveau contrôleur de définir sa propre doctrine et d'en convenir l'emploi avec l'autorité politique. Voilà pourquoi, il a paru utile de rappeler de manière générale quels pouvaient être les éléments essentiels d'un contrôle non pas formel, mais ancré dans les pratiques. C'est évidemment la condition sans laquelle les garanties que le législateur a pris soin de définir ne seraient qu'illusions.

Contribution de Jean-Jacques URVOAS

Député du Finistère
Président de la commission des lois de l'Assemblée nationale

Rapporteur pour l'Assemblée nationale du projet de loi sur le renseignement, j'ai défendu lors des débats nombre de convictions déjà exposées dans mes précédents écrits[1]. Certaines furent partagées par mes collègues et figurent dans le texte voté par le Parlement, d'autres à l'inverse restèrent minoritaires.

Je n'ai ainsi pas été suivi en ce qui concerne la place et le rôle des parlementaires au sein de la nouvelle autorité de contrôle des techniques de renseignement. Avec constance, j'ai milité en faveur de la mise à l'écart de cette structure des députés et sénateurs, sans toutefois parvenir à convaincre, si bien qu'in fine l'assemblée plénière de la CNCTR comporte quatre magistrats, quatre parlementaires et une personnalité qualifiée.

Pour autant, par cohérence avec la position que j'ai toujours soutenue, je ne participerai pas à l'activité de cette nouvelle autorité

1) Voir par exemple Jean-Jacques Urvoas, Floran Vadillo, *Réformer les services de renseignement français : efficacité et impératifs démocratiques*, Paris, Fondation Jean-Jaurès, 2011, p. 35 ; Jean-Jacques Urvoas, « Contrôler les services : ode à la Commission nationale de contrôle des interceptions de sécurité », 21e rapport de la CNCIS, Paris, La Documentation française, 2013, p. 9-16 ; Jean-Jacques Urvoas, « Le contrôle parlementaire des services de renseignement, enfin ! », Note n°7, Fondation Jean-Jaurès/Thémis - Observatoire justice et sécurité - 4 février 2014.

administrative, en dépit des intentions que certains journalistes hostiles au projet de loi n'ont pas manqué de me prêter avec beaucoup d'insistance[1].

Dans cette optique, la présente contribution ambitionne d'être à la fois un témoignage – que j'espère utile – sur mon mandat triennal au sein de la CNCIS, et une réflexion sur les raisons qui m'ont conduit à défendre l'idée d'une commission dont les élus seraient écartés.

Dès l'origine, un choix consensuel

La création d'une instance de contrôle indépendante constituait l'une des dispositions essentielles du rapport sur « les écoutes téléphoniques » commandé par le Premier ministre Pierre Mauroy au Premier président de la Cour de cassation, Robert Schmelck[2]. Mais dix ans s'écoulèrent avant qu'elle ne soit reprise dans le projet de loi déposé le 29 mai 1991 par le Gouvernement d'Édith Cresson.

Ainsi, après la création en 1967 de la Commission des opérations de bourse (COB) et surtout en 1978 de la Commission nationale de l'informatique et des libertés (CNIL), naissait une nouvelle instance collégiale de contrôle. Après de multiples hésitations sur le statut qu'il convenait de donner à celle-ci, le Parlement, à la suite d'un amendement déposé au Sénat, écartant tout à la fois l'instauration d'un établissement public à la tutelle allégée et un rattachement pur et simple aux services du ministère de la Justice, a finalement opté pour l'option la plus radicalement audacieuse.

Le statut de l'autorité ainsi instituée était en effet « l'expression d'un oxymore »[3] : être à la fois une autorité administrative, c'est-à-dire relevant du pouvoir exécutif, mais dans le même temps une autorité indépendante, et donc soustraite au principe rappelé par l'article 20 de la Constitution selon lequel le Gouvernement, responsable devant le Parlement, détermine et conduit la politique de la Nation et dispose à cette fin de l'administration.

Cette initiative fut la première d'une longue série qui aboutit par la suite à la création de la Commission d'accès aux documents administratifs (CADA) (loi du 17 juillet 1978), de la Haute Autorité de l'audiovisuel (loi du 29 juillet 1982) puis de la Commission nationale de la communication et des libertés (loi 30 septembre 1986), du Médiateur de

---

1) Voir par exemple « Loi renseignement : conflit d'intérêts de Jean-Jacques Urvoas », http://www.numerama.com/magazine/32641-loi-renseignement-conflit-d-interets-de-jean-jacques-urvoas.html

2) Il lui fut remis le 25 juin 1982.

3) Jean-Marc Sauvé, audition à l'Assemblée nationale, 11 février 2010.

la République (13 janvier 1989), de la Commission consultative du secret de la défense nationale (CCSDN) (loi du 8 juillet 1998), etc. Le succès de ce modèle est tel qu'il rassemble aujourd'hui près de quarante autorités, sans pour autant constituer une catégorie précisément définie dans notre ordonnancement juridique. Sans doute d'ailleurs est-ce justement la souplesse de la formule qui lui a permis de s'adapter à un nombre aussi conséquent de domaines d'application.

Dans le cas de la CNCIS, sa mission était d'exercer le contrôle externe de légalité et de proportionnalité, consistant à s'assurer que les demandes déposées par les administrations spécialisées respectaient les conditions prévues par la loi et ne portaient pas une atteinte disproportionnée aux droits et libertés des citoyens.

Ces dispositions ne firent pas réellement débat au sein du Parlement, pas plus que la forme juridique retenue[1]. À l'inverse, la composition de la structure cristallisa les controverses.

Le premier point de divergence porta sur la délimitation du collège. Là où le rapport Schmelck préconisait la nomination de neuf membres (quatre parlementaires, trois magistrats, deux personnalités), le Gouvernement fit initialement le choix d'une instance collégiale la plus réduite possible avec trois membres : un président désigné pour une durée de six ans par le Président de la République, 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 son président. La détermination d'un effectif aussi restreint répondait, selon les propos du Garde des sceaux Henri Nallet[2], au souci « d'assurer la confidentialité des travaux de la Commission », présentée comme une condition nécessaire de son efficacité. Pourtant, au cours des débats, le Gouvernement tenta d'y ajouter deux magistrats, membres ou anciens membres du Conseil d'État et de la Cour de cassation, mais le Sénat sut s'y opposer avec succès.

Par la suite d'ailleurs, le législateur persistera dans son choix de doter d'un collège les autorités administratives indépendantes (AAI) chargées de *« protéger les libertés publiques de dimension politique »*[3]. Les seules exceptions en la matière concernent présentement le Défenseur des droits, le Contrôleur général des lieux de privation de liberté, le Médiateur national de l'énergie ainsi que celui du cinéma. En revanche, le périmètre du collège peut varier. Ainsi, alors que la norme se situe entre sept et onze membres[4], d'autres structures, en raison de

1) Seul le député PS de Saône-et-Loire Jean-Pierre Michel s'étonna du fait que la nouvelle mission de contrôle ne soit pas confiée à la CNIL.
2) *Journal officiel*, Assemblée nationale, séance du 13 juin 1991.
3) Roger Fauroux, Bernard Spitz (dir.), Paris, Robert Laffont, 2000.
4) 7 à la CRE et à l'ARCEP, 9 au CSA, à l'ACAM et à l'AFLD, 11 à la CADA.

l'ampleur de leur champ de compétences, sont susceptibles d'accueillir un nombre de membres plus important.

Il y eut ensuite un désaccord touchant au mode de nomination du Président, lequel ne fut tranché qu'à l'occasion de la commission mixte paritaire. L'Assemblée nationale avait marqué sa préférence pour une élection parmi les trois membres n'ayant pas la qualité de parlementaire, système auquel le ministre de la Justice se rallia. Le Sénat privilégia une autre option : le président serait une personnalité désignée conjointement par le vice-président du Conseil d'État et le premier président de la Cour de cassation [1]. Le compromis retenu confia la responsabilité de la désignation du président au chef de l'État à partir d'une liste de quatre noms, établie conjointement par le vice-président du Conseil d'État et le premier président de la Cour de cassation.

Ce rappel vise à souligner que jamais la présence de parlementaires au sein de l'instance ne rencontra pas d'opposition. Certes le député UDC de Seine-et-Marne Jean-Jacques Hyest émit une réserve sur *« l'efficacité d'une structure de trois membres dont deux [seraient] des parlementaires »*, mais les députés considérèrent majoritairement que la « crédibilité » [2] de la Commission était à ce prix.

De surcroît, quelques années auparavant, le 6 septembre 1978, la Cour européenne des droits de l'homme dans son arrêt *Klass contre l'Allemagne*, avait indiqué que la représentation de la diversité parlementaire au sein des autorités de contrôle de l'exécutif, fussent-elles administratives, procédait du renforcement des garanties conventionnelles. Il était dès lors cohérent que les députés français estiment que leur participation relevait de l'exercice d'une forme de contrôle informatif, inhérent au Parlement, tout comme d'ailleurs le fait que nombre de membres de ces autorités soient désignés par les présidents des deux chambres.

Par ailleurs, la participation d'élus à la prise de décision de la CNCIS contribuait probablement à l'acceptation de ses décisions dans ce domaine particulièrement sensible des libertés publiques, et confortait en conséquence la nécessaire confiance dans l'institution. Enfin, pour le Gouvernement, accessoirement, l'implication des parlementaires dans le processus permettait de garantir que les futures décisions soient le produit d'une information fondée sur une connaissance approfondie des réalités et non l'aboutissement d'un raisonnement simplement juridique.

Longtemps d'ailleurs, nulle critique ne vint contester la pertinence d'une telle organisation. Bien au contraire, les présidents successifs de la CNCIS louèrent avec constance, au fil des rapports annuels, l'avantage que représentait à leurs yeux la présence d'élus dans l'assemblée plénière. La seule voix légèrement discordante fut celle du président

---

1) Journal Officiel, Sénat, séance du 25 juin 1991.
2) Rapport n° 2088 de M. François Massot, fait au nom de la Commission des lois, p. 58.

Dieudonné Mandelkern qui estimait nécessaire en 2001 d'élever à cinq le nombre de membres, au prétexte que, trop restreint, celui-ci nuisait au fonctionnement de la CNCIS [1], mais cette réserve ne le conduisit pas pour autant à remettre en cause la présence de parlementaires. Ses prédécesseurs et successeurs, eux, ne formulèrent jamais la moindre critique quant aux modalités du mécanisme en vigueur. À titre d'illustration, il suffit de citer le propos tenu par Jean-Louis Dewost, président de l'instance de 2003 à 2009 et qui, à l'occasion des vingt ans de la loi de 1991, évoque dans le rapport annuel de la CNCIS *« la sagesse du législateur [qui] a prévu que le président soit assisté de deux parlementaires »*, dont l'expérience politique vient *« conforter la vision plus juridique du président »* [2]. Ou encore celui d'Hervé Pelletier qui soulignait dans le 21e rapport la garantie qu'apportait la présence des représentants de la Nation [3].

Et pourtant des questions se posent

Ce n'est que récemment que des interrogations se firent jour. Ainsi en 2010, René Dosière (PS) et Christian Vanneste (UMP) ont estimé dans leur rapport destiné au Comité d'évaluation et de contrôle de l'Assemblée que *« la présence de parlementaires dans les collèges, en particulier pour les AAI traitant des libertés publiques, [fait] débat »* [4].

Après comparaison des avantages – indépendance, légitimité… – et des inconvénients – séparation des pouvoirs, impartialité, voire assiduité insuffisante compte tenu d'un agenda parlementaire toujours plus chargé – leur conclusion se révèle sans appel. Ils considèrent que la présence de parlementaires dans les collèges comporte un *« risque de confusion des pouvoirs et pourrait servir d'alibi cachant l'absence de contrôle »*. Et comme ils reconnaissent qu'il serait improductif de la proscrire de façon générale et absolue, notamment pour les AAI intervenant dans le domaine des libertés publiques, ils préconisent que les élus qui accepteraient d'y siéger démissionnent de leur mandat parlementaire pendant la durée de leurs fonctions au sein du collège.

Puis en 2013, dans un rapport consacré au « cadre juridique des services de renseignement » rédigé en collaboration avec le député UMP du Rhône Patrice Verchère, j'eus l'occasion d'approfondir cette analyse

---

1) CNCIS, *9e rapport d'activité, année 2000*, Paris, La Documentation française, 2001, p. 11.
2) Jean-Louis Dewost, « Le 20e anniversaire de la Commission nationale de contrôle des interceptions de sécurité » 20e rapport d'activité 2011-2012, Paris, La Documentation française, 2012, p. 11.
3) CNCIS, *21e rapport d'activité, années 2012-2013*, Paris, La Documentation française, 2013, p. 6.
4) René Dosière, Christian Vanneste, *Les autorités administratives indépendantes*, rapport d'information, Comité d'évaluation et de contrôle des politiques publiques, n° 2925, Assemblée nationale, 28 octobre 2010.

en développant la conviction que le « contrôle externe de responsabilité » qui relève du pouvoir législatif ne passait pas par la présence de parlementaires au sein de la Commission de contrôle des activités du renseignement dont nous appelions à la création. Et de fait, nous suggérions que cette structure ne soit composée que de magistrats.

Cette position tenait compte des débats qui se déroulaient parallèlement au sein de la section de l'Intérieur du Conseil d'État, saisie pour avis sur le décret qui allait instituer la « plateforme nationale des interceptions judiciaires ». En effet, et même s'il n'existe pas de compte rendu public de ces échanges, il semble qu'évoquant le comité assistant la personnalité qualifiée chargée de la contrôler, la rapporteure du Conseil d'État ait fini par appeler l'attention du Gouvernement sur le risque d'inconstitutionnalité qui découlerait de la présence de parlementaires dans cette structure, laquelle présence, *«* a fortiori *prévue par décret codifié dans le Code de procédure pénale dans un dispositif mettant en œuvre les décisions des magistrats judiciaires dans le cadre de procédures pénales ayant pour objet la constatation des infractions pénales, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs apparaît contraire au principe de la séparation des pouvoirs »*.

En 2014, présidant alors pour l'année la Délégation parlementaire au renseignement (DRP), j'ai souligné dans le rapport d'activité que *« la présence des parlementaires suscitait des interrogations au sein de [la structure] »* [1]. En effet, dans les faits, quelque mois de participation assidue aux réunions plénières de la CNCIS m'avaient conduit à constater que c'est bien son président qui effectue l'essentiel du travail de contrôle, s'appuyant sur les modestes moyens de l'AAI, et que seuls les cas litigieux étaient soumis aux élus de la Nation dans le cadre de la formation plénière. Difficile dès lors de ne pas parvenir à la conclusion que l'activité de contrôle constitue une tâche à plein temps nécessitant un haut degré de technicité. C'est pourquoi la DPR suggéra que les élus soient remplacés par *« des personnalités qualifiées désignées par le président de chaque chambre sur proposition de la Délégation parlementaire au renseignement »*.

Cette préconisation résultait plus globalement d'un constat : la philosophie du contrôle parlementaire a été précisée par la récente loi de programmation militaire, et comme les pouvoirs de la DPR y ont été considérablement étendus, la présence des parlementaires dans une structure externe ne présente plus à mes yeux un intérêt majeur. Le rôle du Parlement pouvait donc consister à nommer des personnalités qualifiées et à recevoir un plus grand nombre d'informations utiles à l'accomplissement de sa mission de contrôle de la responsabilité du Gouvernement en ce domaine (*cf.* ci-après).

---

1) Jean-Jacques Urvoas, *Contrôler les services – an I,* Délégation parlementaire au renseignement, rapport d'activité, Assemblée nationale, n°2482, 18 décembre 2014, p. 74.

En effet, si le contrôle des services est une nécessité parce que les dérapages sont toujours possibles et que les libertés individuelles en pâtiraient, les formes de son exercice sont diverses et cumulatives.

Une philosophie cohérente du contrôle des services

Sur le plan théorique, le contrôle des politiques du renseignement est une compétence partagée. Ainsi le professeur Uri Bar-Joseph de l'université d'Haïfa a établi une architecture de contrôle[1] qui confie cette mission soit à l'exécutif (« participation unilatérale »), soit à la conjugaison d'une multiplicité de regards (« participation multilatérale » où se retrouvent le législatif, le judiciaire et l'informel).

Dans notre pays, cette division des tâches se concrétise en trois dimensions : le contrôle interne, le contrôle externe de légalité et de proportionnalité, le contrôle externe de responsabilité.

Le contrôle interne présente une double déclinaison. La première forme consiste en un contrôle interne exécutif que met en œuvre le Gouvernement afin de s'assurer du bon fonctionnement et de l'efficacité des services placés sous son autorité. C'est maintenant la mission qui incombe à l'Inspection du renseignement, créée par un décret n° 2014-833 du 24 juillet 2014 signé par le Premier ministre Manuel Valls. La seconde forme correspond à un contrôle interne administratif que doit exercer tout chef de service afin de maîtriser le fonctionnement de son administration, d'impulser des réformes, de vérifier la bonne marche de la structure ainsi que la régularité des pratiques mises en œuvre.

Vient en parallèle le contrôle externe de légalité et de proportionnalité, qui ne saurait exister sans la reconnaissance des moyens spéciaux octroyés aux services de renseignement. Il consiste, dans ce cadre, à s'assurer que la mise en œuvre des techniques de recueil de renseignement par les administrations spécialisées respecte les conditions prévues par la loi et ne porte pas une atteinte disproportionnée aux droits et libertés des citoyens. C'est la vocation de la CNCIS pour le seul domaine des écoutes téléphoniques et, demain, de la CNCTR. Pareille structuration correspond de surcroît à la résolution du 17 mai 2010 du Conseil des droits de l'homme de l'Assemblée générale des Nations unies, qui prévoit qu'un *« système efficace de supervision du renseignement [inclue] au moins une institution civile indépendante des services et de l'exécutif »*.

---

1) Uri Bar-Joseph, «The Intelligence Chief Who Went Fishing in the Cold: How Maj Gen. (res.) Eli Zeira Exposed the Identity of Israel's Best Source Ever.» *Intelligence and National Security* 23, n°2, avril 2008, p. 226-248.

Enfin, reste le contrôle externe de responsabilité, qu'il est habituel d'appeler « contrôle parlementaire » et que les Pays-Bas furent le premier pays à formaliser dès 1952. En substance, rien ne saurait justifier que la représentation nationale s'y intéresse dans le détail, au-delà des nécessités de contrôle de la responsabilité gouvernementale, fonction fondamentale du pouvoir législatif dans la théorie de la séparation des pouvoirs. En outre, il convient de prendre en considération le fait que si ces services sont des administrations particulières, ils ne peuvent pour autant s'affranchir du cadre juridique national. Dans cette optique, il revient au pouvoir exécutif de répondre de leurs activités devant la représentation nationale, et il ne paraît pas fondé de leur réserver un traitement parlementaire spécifique. C'est aussi la position exprimée par le Conseil constitutionnel dans sa décision n° 2001-456 DC du 27 décembre 2001. Cette conception suppose néanmoins que les autres formes de contrôle fonctionnent efficacement.

Le rôle du Parlement dans le contrôle des services

C'est donc par la promulgation, le 18 décembre 2013, de la loi de programmation militaire (LPM) que la France s'est enfin dotée des moyens juridiques permettant *« le contrôle parlementaire de l'action du Gouvernement en matière de renseignement et l'évaluation de la politique publique en ce domaine »*. La rupture était ainsi consacrée avec des usages pour le moins fâcheux, qui firent de notre pays l'un de ceux où seule la pression des événements ou le fracas des scandales autorisait le Parlement à se pencher sur le fonctionnement de ces administrations réputées « secrètes ».

Nous venions en effet de fort loin[1] car, comme l'affirma François Fillon lors de l'inauguration de l'Académie du renseignement, le lundi 20 septembre 2010 à l'École militaire à Paris, *« entre démocratie et renseignement, l'histoire nous apprend que les relations n'ont pas toujours été sereines »*.

En dehors du contrôle des fonds secrets opéré par les parlementaires sous la monarchie de Juillet ou la IIe République, ce n'est qu'après la Seconde Guerre mondiale que l'activité des services de renseignement connut un regain de publicité, en commençant à susciter l'intérêt des élus de la Nation. Mais lorsque, au début de l'année 1945, la commission de la justice et de l'épuration de l'assemblée consultative demanda à entendre le directeur général des services (DGER), le général de Gaulle

1) Jean-Jacques Urvoas, « Les enjeux du contrôle et de l'efficacité du renseignement français », *Revue Géoéconomie*, n° 67, novembre-décembre 2013, p. 31-40.

fit part à son président de son refus par une lettre (non publique) du 22 février 1945. D'ailleurs, lors du Conseil des ministres du 28 décembre 1945 au cours duquel fut soumis un projet de décret instituant le Service de documentation extérieure et de contre-espionnage (SDECE) pour succéder à la DGER, le chef de l'État précisa qu'il fallait éviter, entre autres *« écueils »*, qu'un *« contrôle soit établi sur ces services »* [1].

Au demeurant, sa volonté ne pouvait que s'accommoder du désintérêt des parlementaires de la IVe République qui, hormis dans le cadre de la commission d'enquête sur l'affaire des généraux, ne cherchèrent point à s'approprier les thématiques relatives au renseignement. D'une manière générale, *« jusqu'au début des années 1970, il apparaît très clairement que les élus de la Nation n'ont jamais voulu "contrôler" ou "enquêter" sur des administrations aussi singulières »* [2]. Et si entre 1970 et 2005, quelques timides tentatives eurent lieu (notamment à l'initiative de Paul Quilès, alors président de la commission de la défense de l'Assemblée en 1999 [3], puis d'Alain Marsaud, rapporteur de la commission des lois d'un projet de loi relatif à la lutte contre le terrorisme en 2005), il faudra attendre le Gouvernement dirigé par François Fillon pour que soit instituée par le vote de la loi n° 2007-1443 du 9 octobre 2007 une « délégation parlementaire au renseignement ». Au demeurant, ce pas était symboliquement important mais juridiquement d'une portée limitée puisque la structure restait cantonnée au « suivi de l'activité générale » des services.

Cinq années devront encore s'écouler avant que la DPR passe du « suivi » au contrôle. Ainsi, avec la nouvelle écriture découlant de la LPM, la mission est claire et le choix des termes employés pour la qualifier ne doit rien au hasard. La vocation de la DPR est moins de « surveiller » les administrations elles-mêmes que de veiller à l'usage que peut en faire le pouvoir exécutif. En cas d'anomalie avérée, les élus du peuple peuvent alors en imputer la responsabilité au seul Gouvernement et mettre en œuvre les mécanismes prévus par la Constitution en application de la séparation des pouvoirs.

La France ne fait donc pas partie de la poignée de pays (États-Unis, Norvège…) dans lesquels le contrôle parlementaire s'apparente à une forme de surveillance sur les opérations en cours. On pourrait de prime abord le regretter mais il s'agit en réalité d'une heureuse précaution. D'abord parce qu'aux États-Unis, l'expérience a démontré qu'en réponse à ce qu'ils percevaient comme une « entrave » à leur action, les gouvernements multipliaient les procédés pour contourner le Parlement

---

1) Sébastien Laurent, « Les parlementaires face à l'État secret et au renseignement sous les IVe et Ve Républiques : de l'ignorance à la politisation », *Cahiers de la sécurité*, juillet-septembre 2010, n° 13, p. 136.
2) *Ibid.*, p. 137.
3) Proposition de loi de Paul Quilès tendant à la création d'une délégation parlementaire pour les affaires de renseignement, doc. AN n° 1497 (XIe législature), 25 mars 1999.

(extraterritorialisation comme sur la base de Guantanamo, externalisation par le recours à des prestataires privés…). Ensuite parce que la loi se devait de respecter une décision du Conseil constitutionnel interdisant au législateur de s'intéresser aux « opérations en cours »[1]. Enfin parce que cette fonction de contrôle de l'exécutif par le Parlement a trop souvent été *« compromise par la confusion trop fréquente entre le pouvoir de surveiller le gouvernement et la faculté de le renverser »*[2].

Ainsi, dans les limites posées par la Constitution et la préservation de l'activité des services au profit de la Nation, les parlementaires peuvent enfin renouer avec leurs missions fondamentales – qui ont été trop longtemps ignorées en ce domaine. Ce fut le pari du rapport 2014 de la Délégation.

Naturellement, ce premier rapport, même s'il fut jugé *« d'un réel intérêt »*[3], demeure largement perfectible. Les élus de la Nation seront d'ailleurs pour l'essentiel jugés sur leur aptitude à assurer le fonctionnement de la nouvelle délégation parlementaire au renseignement. Car, comme Guy Carcassonne aimait à le répéter, *« ce qui manque à l'Assemblée nationale, ce ne sont pas les pouvoirs, mais les députés pour les exercer »*[4]. Mais dans les faits comme en droit, le contrôle externe de responsabilité des services, qui relève de la seule responsabilité du Parlement, est maintenant possible. Quel intérêt dès lors de maintenir une présence parlementaire dans la future Commission nationale de contrôle des techniques de renseignement ?

1) Décision n° 2001-456 DC du 27 décembre 2001.
2) Francis Hamon, Michel Troper, *Droit constitutionnel*, Paris, LGDJ, 1999, 26e éd, p. 613.
3) Franck Johannès, « Le premier contrôle parlementaire du renseignement ménage les services », *Le Monde*, 18 décembre 2014.
4) Préface au livre de René Dosière, *L'argent caché de l'Élysée*, Paris, Le Seuil, 2007, p. 11.

Les données et la loi française

Contribution de Bénédicte FAUVARQUE-COSSON

Professeur,
Université Panthéon-Assas (Paris II)

Le numérique a révolutionné nos modes de vie et de communication, bouleversé notre économie, supprimé les frontières, démultiplié les horizons et engendré de nouvelles tensions. Protection de la vie privée et de la liberté d'expression d'une part, sécurité nationale et émergence de nouvelles menaces liées à l'utilisation des réseaux informatiques d'autre part : la gouvernance de l'Internet est devenue un enjeu géopolitique mondial. L'évolution des technologies et des mentalités *« a transformé la promesse de liberté, que constituait l'Internet, en un fantastique outil de surveillance »* [1].

Les pratiques de surveillance massive et généralisée de l'ensemble de la population par des acteurs privés pour le compte d'acteurs publics ont montré comment les services de renseignement américains et leurs partenaires dans certains États membres du Conseil de l'Europe portaient atteinte aux droits fondamentaux, notamment au droit au respect de la vie privée (article 8 de la Convention européenne des droits de l'homme).

Dans l'Union européenne, les suites des révélations d'Edward Snowden, le droit au déréférencement consacré par la Cour de justice

1) *Nouveau rôle et nouvelle stratégie pour l'Union européenne dans la gouvernance mondiale de l'Internet.* Rapport d'information du Sénat, au nom de la mission commune d'information, n° 696, 2014, p. 10 ; http://www.senat.fr/rap/r13-696-1/r13-696-11.pdf

de l'Union européenne (CJUE), le projet de règlement européen sur les données personnelles, les mesures visant à une lutte coordonnée contre le terrorisme ont alimenté un large débat public autour de la protection des données personnelles et des libertés numériques.

En France, les attentats de Paris de janvier 2015 ont conduit le gouvernement à vouloir renforcer les moyens de lutte contre le terrorisme. Le projet de loi relatif au renseignement a soulevé un vif émoi. Qualifié de *Big Brother* français, il lui a notamment été reproché de « légaliser le droit pour les services secrets d'accéder à toutes nos données personnelles ». Une pétition, que les « habitants ordinaires de la France qui refusent simplement de vivre dans un "État policier numérique" » ont été invités à signer, soulève cette question : « *Quis custodes custodiet* ? » : *« Qui nous protégera contre ceux qui nous protègent ? »*.

Surveiller ceux qui surveillent : depuis sa création en 1991, la CNCIS assume en partie cette fonction. Cette Commission, originellement créée pour contrôler « les interceptions de sécurité » a vu le périmètre de son action s'accroître lorsqu'elle a été chargée par la loi n° 2006-64 du 20 janvier 2006 du contrôle *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 [1] et désormais (loi n° 2013-1168 du 18 décembre 2013) sur toutes ces demandes – quelles qu'en soient les finalités – et aussi sur les demandes de « géolocalisation » en temps réel. S'agissant de cette dernière technique, la pratique rapidement adoptée lui a permis de donner son avis *a priori.*

La CNCIS est confrontée à maintes difficultés, liées aux nouvelles réalités qui modifient en profondeur l'environnement dans lequel s'effectue le contrôle du recueil de données techniques de communications [2]. Il est prévu qu'elle soit remplacée par une Commission dotée de plus de moyens, la CNCTR. Les réalités à affronter restent les mêmes :

– Des programmes informatiques permettent de savoir ce que la police enregistre. Dans l'absolu, cela devrait faciliter le contrôle des interceptions de sécurité, mais encore faudrait-il que le contrôleur ait la maîtrise de ces programmes. Avec ses moyens limités, la CNCIS ne peut évidemment pas les maîtriser.

– Les données auxquelles s'applique le régime légal des interceptions circulent librement. Or le cadre juridique de la surveillance repose sur une distinction entre les données recueillies dans le pays où siège l'autorité, pour lesquelles un contrôle est organisé, et celles recueillies

1) 22e rapport d'activité, Commission nationale de contrôle des interceptions de sécurité, années 2013-2014, La Documentation française, 2015, CNCIS ; v. not. S.-Y. Laurent, Liberté et sécurité dans un monde anomique de données, p. 11, sp. p. 12.
2) Rappr. J.-M. Delarue, Avant-propos, 22e rapport d'activité de la CNCIS, préc., p. 5.

à l'étranger, non soumises à ce contrôle. Ce critère territorial s'imposait naturellement lorsque la sécurité était principalement assurée par des filatures de personnes ou la saisie de biens matériels : il n'appartenait pas à une autorité administrative française de contrôler ce qui se passait au-delà de nos frontières, alors que la police nationale était elle-même dessaisie de l'affaire. Dans notre monde global et dématérialisé, les investigations ont lieu dans les flux internationaux de données.

– Des « interceptions de sécurité » aux « demandes de données techniques de connexion ou de communication » : le champ du contrôle de l'utilisation des moyens d'intrusion s'est étendu. Aujourd'hui, le rapprochement de multiples données de connexion appliqué à une personne révèle beaucoup plus qu'une écoute téléphonique.

Le contrôle des moyens d'intrusion doit s'adapter à ce monde nouveau tout à la fois déterritorialisé et cloisonné du fait d'ignorances réciproques :
– les données ignorent les frontières et circulent librement partout ;
– le législateur interne définit un régime légal de surveillance des communications qui ne s'applique pas à l'ensemble des communications ;
– les raisonnements traditionnels, fondés sur des règles de conflit de lois qui servent à répartir les compétences législatives, ignorent les nouvelles technologies et le monde international des données. Le rattachement territorial n'a plus la même valeur qu'autrefois ;
– la distinction entre données personnelles et non personnelles est brouillée du fait des nouveaux moyens d'intrusion ;
– les utilisateurs ignorent leurs droits et adoptent des comportements ambivalents. Ils défendent la liberté d'expression et veulent utiliser librement les données (ce qui est un obstacle à la réglementation). Ils souhaitent protéger leur vie privée, mais pas nécessairement leurs données personnelles[1]. Ils demandent à l'État d'assurer leur sécurité, mais s'inquiètent d'un État qui aurait trop de pouvoirs de surveillance[2] ;
– les juristes ignorent l'informatique ; ils estiment que les questions fondamentales ne sont pas d'ordre technique mais social. Les informaticiens

1) En 2014 la CNIL a enregistré environ 5825 plaintes, ce qui correspond à une légère hausse des demandes (+ 3 %). 39 % de ces plaintes concernent des problématiques d'e-réputation : suppression de textes, photographies, vidéos, coordonnées, commentaires, faux profils en ligne, la réutilisation de données publiquement accessibles sur Internet, etc. Depuis la décision de la Cour de justice de l'Union européenne en mai 2014, la CNIL a reçu 200 plaintes consécutives à des refus de déréférencement par les moteurs de recherche. Bilan 2014 : les données personnelles au cœur du débat public et des préoccupations des Français, *16 avril 2015, http ://www. cnil. fr*

2) Le 13 avril 2015, l'Observatoire des libertés du numérique, groupement d'associations incluant la Quadrature du Net, a appelé à manifester devant le Palais Bourbon. La police a compté « plusieurs dizaines de manifestants », ce qui est peu au regard de l'émoi politique et médiatique suscité par le projet de loi sur le renseignement. La pétition « STOP Loi Renseignement » a reçu, en quelques jours, plus de 100 000 signatures. https://www.change.org

ignorent quant à eux les juristes. En janvier 2000, Lawrence Lessig publiait son fameux article *Code Is Law* – (Le code informatique fait loi) dans lequel il expliquait que sur Internet, la régulation des comportements passait moins par les normes juridiques que par l'architecture technique des plateformes que nous utilisons et qui crée de facto une forme de régulation supra-nationale[1]. Il s'inquiétait déjà du respect de la vie privée : *« S'il n'existe aucune incitation à protéger la vie privée – si la demande n'existe pas sur le marché, et que la loi est muette – alors le code ne le fera pas »*.

Dans un monde idéal, les principes applicables aux données – qu'il s'agisse d'assurer la sécurité des États (surveillance des communications) ou de protéger la sphère privée (protection des données personnelles) – seraient identiques dans tous les pays. Ce monde n'existe pas. Dans notre monde divisé en États souverains, les questions de sécurité et de souveraineté relèvent de la loi nationale. La surveillance des communications par les pouvoirs publics est un élément essentiel de la stratégie de défense et de sécurité de la France. C'est *« l'un des instruments d'une responsabilité éminente de l'État, celle d'assurer la protection de la sécurité de la population et la défense des intérêts fondamentaux de la Nation »*[2]. De son côté, la protection de la vie privée est un droit fondamental consacré par des sources d'origines diverses, notamment européennes (Conseil de l'Europe avec la Convention européenne des droits de l'homme, Union européenne avec la Charte des droits fondamentaux). Un cadre européen se forme[3]. Le législateur français, ne peut

---

1) L. Lessig, Code is law", http://harvardmagazine.com/2000/01/code-is-law-html. "Our choice is not between 'regulation' and 'no regulation'. The code regulates. It implements values, or not. It enables freedoms, or disables them. It protects privacy, or promotes monitoring. People choose how the code does these things. People write the code. Thus the choice is not whether people will decide how cyberspace regulates. People—coders—will. The only choice is whether we collectively will have a role in their choice—and thus in determining how these values regulate—or whether collectively we will allow the coders to select our values for us".
L'architecte de systèmes d'information conçoit l'architecture du système d'information. Il travaille généralement en équipe, en relation avec un ingénieur système et un ingénieur réseau, et en interface avec les différentes directions métier de l'entreprise.

2) *Le numérique et les droits fondamentaux,* Étude annuelle du Conseil d'État, 2014, La Documentation française, 2014, p. 195. L'étude de droit comparé sur le cadre légal du renseignement, élaborée par le Service des affaires européennes et internationales du ministère de la Justice et publiée dans le 22e rapport annuel (2013-2014, préc., p 19 et s.) de la Commission nationale de contrôle des interceptions de sécurité a tout de même permis *« 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 »*, (p. 19), ce qui est un premier pas. L'argument comparatiste est utilisé par les défenseurs de la loi sur le renseignement, qui relèvent le retard de la France en la matière.

3) Dans l'Union européenne ce cadre européen a progressivement été façonné par des directives et règlements relatifs aux données, par la CJUE (qui veille à ce que les droits fondamentaux soient préservés tant par le législateur européen que par les États membres), par la Charte de l'Union européenne.

l'ignorer au motif qu'il est question de sécurité. Le cadre juridique de la surveillance des communications doit donc tenir compte, d'une part, du rôle de l'État en matière de protection de la sécurité nationale et, d'autre part, de l'ensemble des atteintes aux droits fondamentaux que la surveillance peut faire courir, notamment à la vie privée. La France ne peut progresser seule sous peine d'affecter l'efficacité de la prévention du crime organisé, du terrorisme et des autres atteintes à la sécurité nationale. Pour le renseignement, l'objectif d'unification des droits apparaît encore hors de portée tant les questions de souveraineté nationale sont en jeu. Imagine-t-on un droit global du renseignement ?

Dans cet article sur la loi nationale et les données, on s'interrogera sur ce que peut faire la loi nationale en matière de sécurité, dans le contexte européen et international qu'il lui appartient de respecter. Ces quelques réflexions visent à tendre un fil entre deux approches qui ont le même objet – les données – et qui néanmoins s'opposent : vocation quasi-exclusive de la loi nationale pour la sphère de sécurité ; développement du droit européen pour la sphère privée, porté par les droits fondamentaux et les aspirations contemporaines à l'extraterritorialité du droit.

La sécurité de la nation : quelles limites à la loi nationale ?

Le Code de la sécurité intérieure ne définit pas le champ d'application des dispositions de la loi française. Par suite d'un raisonnement caractéristique de la méthode des lois de police[1], on considère que les dispositions de ce code qui sont relatives aux mesures d'interceptions ou d'accès aux métadonnées ne s'appliquent que si l'opérateur est soumis à la loi française pour les communications concernées, notamment pour ce qui concerne la conservation des données et le droit d'accès des autorités[2]. En dehors du champ de la loi française, le cadre juridique français des interceptions effectuées sur le territoire ne s'applique pas. Seul intervient l'article L. 241-3 de ce code, anciennement article 20 de la loi du 10 juillet 1991, qui permet aux pouvoirs publics de prendre des mesures *« pour assurer, aux seules fins de défense des intérêts nationaux, la surveillance et le contrôle des transmissions empruntant la voie hertzienne [qui] 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 »*. Ce texte ne fixe aucune autre condition à ces interceptions que celle de leur finalité exclusive à la défense des intérêts nationaux. En pratique, cela signifie que, contrairement à la Direction générale de la sécurité intérieure (DGSI) qui opère sur

1) Sur cette méthode, v. la deuxième partie de cette étude.
2) Sur ce point, v. *Le numérique et les droits fondamentaux,* préc. sp. p. 206 et p.214.

le territoire, la Direction générale de la sécurité extérieure (DGSE) peut s'affranchir des contrôles prévus par la réglementation nationale.

Pour expliquer que les garanties dont bénéficient les personnes qui sont à l'étranger soient moindres, l'étude du Conseil d'État relève que l'interception de leurs communications *« n'est pas susceptible de porter atteinte à leurs droits dans la même mesure que si elles se situaient sur le territoire ; elles ne peuvent en particulier faire l'objet de mesures juridiques contraignantes qui se fonderaient sur des éléments collectés »* [1]. Cette même étude observe encore que *« la CEDH n'a pas remis en cause le principe de cette différenciation »* et que *« le droit international public ne condamne pas non plus les activités conduites par un État de collecte de renseignements à l'étranger »* [2]. L'étude n'en considère pas moins nécessaire, notamment pour satisfaire à *« l'exigence de prévisibilité de la loi issue de la jurisprudence de la CEDH »* [3], de définir les garanties qui entourent les interceptions des communications à l'étranger. Ainsi, la proposition n° 39 recommande de *« Définir par la loi le régime des interceptions des communications à l'étranger. La loi déterminerait les finalités de ces interceptions et habiliterait l'Autorité de contrôle des services de renseignement à exercer son contrôle sur ces activités »*. La proposition n° 40 appelle à *« Définir le régime juridique de l'utilisation par les services de renseignement, sur autorisation administrative, de certains moyens d'investigation spéciaux prenant appui sur des techniques numériques (déchiffrement, captation de données informatiques…) »* [4]. La proposition n° 41 forme le souhait que l'autorité chargée du contrôle des opérations techniques de collecte de renseignement soit *« dotée de moyens et de prérogatives renforcés »*. Dans quelle mesure la réforme projetée du renseignement tient-elle compte de ces propositions ?

La première version du projet de loi relatif au renseignement, publiée officiellement le 19 mars 2015, a été adoptée en première lecture à l'Assemblée nationale le 5 mai 2015 [5]. Le texte, amendé suite à diverses réactions [6], modernise les moyens des services de renseignement. Il prévoit notamment que ce qu'on a appelé « boîtes noires » pourront être installées chez les opérateurs de télécommunications, visant à détecter les comportements suspects à partir des métadonnées, sur la base d'un algorithme propriétaire. Il autorise également la mise en place d'autres outils : logiciels espions ou encore IMSI-catcher (une fausse antenne qui

1) Le numérique et les droits fondamentaux, préc, p. 214.
2) *Ibid.*
3) Étude préc., p. 30, 214 (et les références), 319-320.
4) Étude préc., p.322.
5) http://www.assemblee-nationale.fr/14/projets/pl2669.asp
6) Voir en particulier l'avis rendu le 5 mars 2015, par la Commission nationale de l'informatique et des libertés (CNIL) qui a exprimé de fortes réserves sur le nouveau cadre juridique des techniques de recueil du renseignement (interceptions de sécurité, accès administratifs aux données de connexion).

permet d'intercepter les appels téléphoniques d'un téléphone mobile qui se trouve à proximité). L'utilisation de ces dispositifs de surveillance sera contrôlée par la Commission nationale de contrôle des techniques de renseignement (CNCTR)[1].

Le chapitre IV du projet de loi, intitulé « Les mesures de surveillance internationale », contient le futur article L. 854-1 Code de la sécurité intérieure.

L'article L. 854-1. – I.[2] prévoit que : *« Le Premier ministre ou les personnes spécialement déléguées par lui peuvent autoriser, aux seules fins de protection des intérêts publics mentionnés à l'article L. 811-3, la surveillance et le contrôle des communications qui sont émises ou reçues à l'étranger. Ces mesures sont exclusivement régies par le présent article.*

« L'interception des communications concernées et l'exploitation ultérieure des correspondances sont soumises à autorisation du Premier ministre ou des personnes spécialement déléguées par lui. Pour l'application du premier alinéa du présent I, un décret en Conseil d'État, pris après avis de la Commission nationale de contrôle des techniques de renseignement, définit les conditions d'exploitation, de conservation et de destruction des renseignements collectés et précise la procédure de délivrance des autorisations d'exploitation des correspondances.

« Un décret en Conseil d'État non publié, pris après avis de la Commission nationale de contrôle des techniques de renseignement et porté à la connaissance de la délégation parlementaire au renseignement, précise, en tant que de besoin, les modalités de mise en œuvre de la surveillance et du contrôle des communications prévus au présent I. »

---

1) Voir dans le sens d'un encadrement plus strict, les amendements de la commission des lois du Sénat ; pour une synthèse, *cf.*, rapport n° 460, préc. p. 8.
Une note de l'Inria, institut de recherche dédié au numérique, a aussi soulevé certains points techniques, en particulier ceci : la loi prévoit que cette analyse se fera sur des données anonymes, l'identification intervenant uniquement si une menace est détectée, mais *« Il n'existe pas aujourd'hui de technique d'anonymisation sûre. Un texte de loi ne devrait pas se fonder sur la notion de donnée anonyme ou anonymisée »*. La note alerte aussi sur les dérives possibles d'une détection algorithmique des personnes soupçonnées de terrorisme. Note du 30 mars 2015, *Le Monde*, 13 mai 2015, http://www.lemonde.fr/pixels/article/2015/05/13/la-note-interne-de-l-inria-qui-etrille-la-loi-sur-le-renseignement

2) Il s'agit ici de la version remaniée et adoptée en première lecture par l'Assemblée nationale, le 5 mai 2015 : http://www.assemblee-nationale.fr/14/ta/ta0511.asp

Ce dispositif législatif qui introduit des dispositions propres aux mesures de surveillance internationale devrait, par contrecoup, mettre fin à certaines pratiques, récemment révélées au public[1].

Le droit américain accorde aussi une plus grande liberté aux services de renseignements lorsque sont en cause des interceptions de communications à l'étranger. Il existe toutefois une différence avec le droit français : le critère ne tient pas à la localisation des données (le nouvel article L. 854-1 vise les « communications qui sont émises ou reçues à l'étranger »), mais à la personne visée : la protection garantie par le 4e amendement, qui fournit la base constitutionnelle de la protection de la vie privée, ne s'étend pas aux non-Américains. À la suite des attentats du 11 septembre 2001, les pouvoirs d'interception des communications ont été étendus par la section 215 du *Foreign Intelligence Surveillance Act*. C'est dans ce cadre législatif que le *Foreign Intelligence Surveillance Court* (FISC) a autorisé, à partir de 2006, la collecte systématique des métadonnées des opérateurs téléphoniques et leur stockage par la NSA. En 2008, le *FISA Amendment Act* (FAA), a introduit la distinction suivante : lorsque la personne visée est une personne américaine ou résidant aux États-Unis *(US Person)* l'administration doit obtenir l'accord de la FISC ; dans le cas contraire, la section 702 du FISA lui permet d'agir sans autorisation préalable. C'est sur le fondement de ce texte qu'ont eu lieu les collectes les plus massives (l'étude du Conseil d'État note que *« l'un des juges de la FISC a relevé que 250 millions de communications sur Internet étaient interceptées chaque année »*[2]).

En Europe, l'indignation provoquée par ces pratiques a conduit à des prises de position favorables à une plus grande protection non

1) Le 11 avril 2015, *Le Monde* dévoilait l'existence d'un « Big Brother dissimulé au cœur du renseignement » : la *Plateforme nationale de cryptage et de décryptement*, laquelle se livre déjà aux pratiques que la loi a pour but de légaliser. Un an plus tôt, *Le Monde* avait révélé que la DGSE disposait d'un libre accès intégral aux réseaux et aux flux de données qui transitent par la société française de télécommunications Orange, y compris les informations relatives aux ressortissants étrangers et français article publié le 20 mars 2014, « Espionnage : comment Orange et les services secrets coopèrent ». L'information n'a pas échappé au rapporteur de la Commission des questions juridiques et des droits de l'homme de l'Assemblée parlementaire du Conseil de l'Europe, Pieter Omtzigt, qui souligne que cette coopération entre la DGSE et FranceTelecom-Orange passe par des connexions informelles effectuées par des ingénieurs qui « naviguent » entre les deux institutions « depuis au moins les 30 dernières années » (Les opérations de surveillance massive, rapport de la Commission des questions juridiques et des droits de l'homme, Assemblée parlementaire, Conseil de l'Europe, Doc. 13734 18 mars 2015, paragraphe 26, p. 12).
2) Le numérique et les droits fondamentaux, préc., p. 204.

seulement des « citoyens européens »[1] mais aussi des « personnes en Europe », critère certes plus flou mais qui présente l'avantage de ne pas discriminer entre ceux qui ont la nationalité d'un État membre et ceux qui y résident.

Le 8 décembre 2014, dans une « Déclaration commune des autorités européennes de protection des données réunies au sein du "Groupe de l'article 29" »[2], les CNIL européennes ont réaffirmé les valeurs communes de l'Europe et proposé des actions concrètes pour élaborer un cadre éthique européen pour le monde numérique.

La première partie de cette déclaration *(*articles 1-5) est consacrée aux *Valeurs européennes.* L'article 1er rappelle que *« La protection des données à caractère personnel est un droit fondamental »*, ce que consacre déjà la Charte de l'Union (article 8). Il précise encore que *« les données à caractère personnel (y compris les métadonnées de communication) ne peuvent être traitées comme un seul objet de commerce, un actif économique ou un bien de consommation »*.

La deuxième partie de cette déclaration, intitulée « Surveillance à des fins de sécurité » pose des principes communs, applicables aux « personnes en Europe » (articles 6-11). *« La surveillance secrète, massive et indiscriminée de personnes en Europe, que ce soit par des acteurs publics ou privés, qu'ils agissent au sein des États membres de l'Union ou ailleurs, n'est pas conforme aux traités et législation européens. Elle est inacceptable sur le plan éthique. »* (Article 6).

Cette déclaration commune établit un lien entre sphère de sécurité et sphère privée, droit national et droit de l'Union. Elle rappelle que s'il n'existe pas de directive ou règlement sur le renseignement car il s'agit d'une prérogative nationale, les législateurs nationaux ne peuvent s'affranchir des limites posées par le droit de l'Union. Les États membres, lorsque leur action entre dans le champ d'action du droit de l'Union, doivent respecter les droits fondamentaux garantis par la Charte de

---

1) Rapport de la Commission des libertés civiles, de la justice et des affaires intérieures, rapporteur Claude Moraes, adopté le 12 mars 2014 par le Parlement européen, v. sp. les considérants J et K. Parmi les principales recommandations, il est proposé au Parlement européen d'enjoindre aux États-Unis « – *d'interdire les activités de surveillance de masse aveugle, – de placer les droits des citoyens de l'Union européenne sur un pied d'égalité avec ceux des ressortissants des États-Unis, – d'adhérer à la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (convention n° 108) du Conseil de l'Europe, comme ils ont adhéré à la convention de 2001 sur la cybercriminalité, renforçant ainsi le fondement juridique commun entre les alliés transatlantiques* ».

2) L'article 29 de la directive du 24 octobre 1995 sur la protection des données et la libre circulation de celles-ci a institué un groupe de travail de ces vingt-sept « CNIL européennes ». Par référence à ce texte, c'est le « groupe de l'article 29 » (G29), dont la mission est notamment de contribuer à l'élaboration du droit européen, par voie de recommandations, d'avis ou de déclarations (actuellement présidé par la présidente de la CNIL, Isabelle Falque-Pierrotin).

l'Union européenne qui consacre la protection des données à caractère personnel (articles 7 et 8). Des limitations de l'exercice d'un droit fondamental peuvent certes être admises par le droit de l'Union mais uniquement *« dans le respect du principe de proportionnalité »* et *« si elles sont nécessaires et répondent objectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui »* (article 52.1)[1]. De plus, pour collecter ces renseignements, les autorités françaises peuvent s'adresser à des opérateurs privés, soumis au droit de l'Union en matière de conservation de données.

Dans l'arrêt *Digital Rights Ireland*[2], la CJUE a remis en cause le cadre européen de la conservation des données de communication électronique à la suite de l'invalidation de la directive n° 2006/24/C relative à la conservation des données qui prévoit que les durées de conservation fixées par les États pour la conservation des données sur lesquelles elle porte (métadonnées) doivent être comprises entre six mois et deux ans. La Cour a ainsi montré la sensibilité des métadonnées et l'ampleur de l'ingérence dans les droits à la vie privée et à la protection des données personnelles que représente leur conservation systématique. L'arrêt a aussi soulevé la question de la conformité des législations nationales sur les données à la Charte des droits fondamentaux – plus précisément, de tout système national de conservation générale des métadonnées[3]. La CJUE a reconnu que la lutte contre le terrorisme et contre la criminalité organisée sont des buts d'intérêt général qui justifient des limitations de l'exercice d'un droit fondamental, mais elle a estimé qu'il fallait exercer un contrôle strict de proportionnalité et qu'en l'espèce, les articles 7 et 8 de la Charte avaient été méconnus car la directive ne prévoyait pas de garanties suffisantes quant à la sécurité des données conservées et n'imposait pas la conservation sur le territoire de l'Union, ce qui ne permettait pas de garantir le contrôle par une autorité indépendante de protection des données personnelles, prévu par l'article 8.3 de la Charte.

Déjà, certains États membres ont réformé leurs lois. Un régime européen de protection des données personnelles se forme, que le

---

1) Sur cette question v. Le numérique et les droits fondamentaux, préc., p. 199 s.
2) C-293/12 et C-594/12 Digital Rights Ireland et Seitlinger e. a.
3) Voir sur cette discussion, *Le numérique et les droits fondamentaux,* préc., p. 199 s., sp. p. 210.
Cf. l'art. L 34-1-1 du Code des postes et des communications électroniques qui prévoit que l'ensemble des métadonnées sont conservées pendant une durée d'un an par les opérateurs de communications électroniques, en vue de répondre aux besoins de l'autorité judiciaire, de la HADOPI, de l'ANSSI ou de la lutte contre le terrorisme ; ou encore l'article 6 de la loi pour la confiance dans l'économie numérique qui impose la même obligation aux hébergeurs.

législateur français doit respecter lorsqu'il définit le cadre de la surveillance des communications[1].

Dans le monde global des données, les valeurs européennes fondamentales entrent en concurrence avec d'autres valeurs, constitutionnellement protégées dans d'autres régions du monde (par exemple, le droit à la liberté d'expression aux États-Unis).

La protection des données personnelles : universalisme et extraterritorialité de la loi européenne ?

Pour les données, phénomène déterritorialisé, le cadre juridique ne devrait idéalement être ni étatique ni régional, mais global. Cependant, les obstacles à la mise en place d'un dispositif mondial sont nombreux. L'un d'eux – non le moindre – tient au fait que les philosophies sous-jacentes aux grands systèmes divergent profondément.

L'approche américaine consiste, on l'a vu, à protéger les ressortissants américains (article 4 de la Constitution), ou ceux domiciliés aux États-Unis. Dans le monde, les États qui se reconnaissent dans la façon de voir américaine opposeront la prétention européenne à raisonner en termes de droits fondamentaux et à imposer leur hiérarchie en cas de conflits entre ces droits. En effet, l'approche européenne, qui met en avant les droits fondamentaux, se veut universelle (du moins lorsque les questions de sécurité ne sont pas directement en cause). Comme l'ont relevé les CNIL européennes, *« Les droits des personnes au regard de la protection de leurs données doivent être combinés avec les autres droits fondamentaux, notamment la prohibition de toute discrimination et la liberté d'expression, qui sont de valeur égale dans toute société démocratique. Ils doivent également être articulés avec l'impératif de sécurité »*[2]. Cette combinaison implique toutefois de procéder à une hiérarchisation. Dans l'arrêt *Google Spain* du 13 mai 2014 la CJUE a énoncé que les droits fondamentaux d'une personne au titre des articles 7 et 8 de la Charte prévalaient non seulement sur l'intérêt économique de l'exploitant du moteur de recherche, mais également sur l'intérêt du public à accéder à ladite information lors d'une recherche portant sur le nom de

1) L'étude du Conseil d'État suggère un renforcement des garanties sur trois types de surveillance : la conservation et l'accès aux métadonnées en France, les interceptions judiciaires du contenu des communications, la surveillance des communications à l'étranger (préc., p. 208).
2) Avis G 29, 10 avril 2014, art. 2.

cette personne[1]. Ce droit à l'oubli est perçu, aux États-Unis, comme une menace pour la liberté d'expression[2].

Dans un univers dématérialisé et internationalisé, quelle place reste-t-il pour les raisonnements habituels des juristes privatistes, centrés sur le droit des États qui utilisent la méthode des « règles de conflits de lois », elle-même fondée sur la localisation du siège du rapport de droit, le principe de proximité, le postulat de l'égalité entre loi française et étrangère, l'application de la loi étrangère par le juge français, le recours exceptionnel à l'exception d'ordre public international français ou aux lois de police ? On s'attachera ici à dégager les grandes lignes de ces raisonnements pour en discerner les limites et ouvrir d'autres pistes de réflexions.

Pour résoudre les conflits potentiels de lois en présence, il faut définir le champ d'application de la loi française (ou européenne) et celui des autres lois. Depuis le XIXe siècle, cela se fait grâce à la méthode des conflits de lois qui constitue, avec les conflits de juridictions, le cœur du droit international privé. C'est l'approche du droit international privé, mise en œuvre qu'il s'agisse de déterminer la loi applicable aux personnes, aux relations de familles, aux obligations contractuelles ou non contractuelles, etc. Elle repose sur un postulat d'égalité entre loi française et loi étrangère, lui-même fondé sur l'idée du juriste allemand F. Carl von Savigny de « communauté de droit entre nations civilisées ».

Ces raisonnements sont-ils adaptés dans un monde dématérialisé ? Les données se jouent non seulement des frontières territoriales, mais aussi des branches du droit et des catégories juridiques. Qualifier, comme on le fait souvent, les données de « personnelles », devrait conduire à rattacher les données à une personne et donc à la loi nationale ou à celle de sa résidence habituelle, mais l'on raisonne surtout en termes de droits fondamentaux. Par ailleurs, sait-on seulement ce qu'englobe cette catégorie « données personnelles » ? Qu'en est-il par exemple des données supposées anonymes ou de celles qui sont « personnalisables », telle une adresse IP ? Ou de l'immense majorité des données qui ne sont pas « personnelles ? » Le traitement juridique des données repose sur une tension dialectique entre droit public et droit privé, entre sphère de sécurité, sphère privée et sphère commerciale.

---

1) Arrêt de la Cour (Grde Chambre) du 13 mai 2014 (demande de décision préjudicielle de l'Audiencia Nacional – Espagne) – Google Spain SL, Google Inc. / Agencia de Protección de Datos (AEPD), Mario Costeja González ; Affaire C-131/12. La Cour précise : *« Cependant, tel ne serait pas le cas s'il apparaissait, pour des raisons particulières, telles que le rôle joué par ladite personne dans la vie publique, que l'ingérence dans ses droits fondamentaux est justifiée par l'intérêt prépondérant dudit public à avoir, du fait de cette inclusion, accès à l'information en question. »*

2) W. Maxwell, La jurisprudence américaine en matière de liberté d'expression sur Internet, in *Le numérique et les droits fondamentaux,* préc., p. 393.

L'Internet déstabilise les catégories juridiques traditionnelles. Les données transcendent la dichotomie public/privé.

Contre la toute-puissance du marché, un garde-fou est indispensable, y compris en droit privé, branche du droit qui s'est constitutionnalisée : c'est la méthode des lois de police, qui permet d'écarter la règle de conflit de lois et de déterminer unilatéralement le champ d'application d'une loi. L'unilatéralisme est surtout utilisé là où les intérêts publics sont concernés[1]. Ainsi par exemple, en droit fiscal, douanier, pénal, l'État se préoccupe uniquement de l'application des lois qu'il édicte pour ses objectifs propres : réduire le déficit budgétaire, réprimer les crimes ou délits, assurer la sécurité sur son territoire[2]. On dénombre beaucoup de lois de police en droit de la concurrence, du travail, de la sécurité sociale, mais aussi en droit des contrats et des sociétés. L'évolution libérale des rapports juridiques dans une économie mondialisée explique l'essor des lois de police, comme un contrepoids. Les États reviennent sur la scène à travers les lois de police qu'ils édictent pour protéger leur intérêt étatique ou ceux d'une catégorie de personnes (par exemple, les consommateurs)[3].

Le plus souvent, la règle elle-même ne précise rien. Il revient alors au juge de dire si la disposition législative est une loi de police et s'applique donc en fonction de ce qu'il estime être le but et la volonté d'application de la règle, sans passer par le détour de la règle de conflit de lois. Pour identifier ces lois, le juge est guidé par la définition de Phocion Francescakis : *« Lois dont l'observation est nécessaire pour la sauvegarde de l'organisation politique, sociale, ou économique du pays »*, qui a inspiré le législateur européen dans l'article 9 du règlement Rome I sur la loi applicable aux obligations contractuelles : *« Une loi de police est une disposition impérative dont le respect est jugé crucial par un pays pour la sauvegarde de ses intérêts publics, tels que son organisation politique, sociale ou économique, au point d'en exiger l'application à*

---

1) On qualifie d'unilatéraliste toute méthode qui raisonne en termes de détermination du champ d'application des lois. L'expression a été forgée à la fin du XIXe siècle, contre la méthode des règles de conflit bilatérales, à une époque où le conflit de lois était envisagé comme un conflit de souverainetés.

2) B Audit et L. d'Avout, *Droit international privé*, Economica, 2014, p. 159. En droit fiscal, un État ne fixe les critères d'exigibilité que de ses propres impôts (sous réserve de l'existence d'accords par lesquels les États organisent une certaine coopération entre eux, tels des conventions d'entraide fiscale). Si la situation se localise hors du champ d'application de la loi donnée, il ne s'en préoccupe pas : la méthode des conflits de lois n'est pas mise en œuvre et les lois étrangères ne sont pas appliquées par les organes nationaux. Dans le Code pénal de 1992, les dispositions sur « l' *application de la loi pénale dans l'espace* » (art. L. 113-2 s.) posent uniquement les critères d'application de la loi française. Ces critères sont la commission de l'infraction sur le territoire ou en un lieu assimilé, ou par un national à l'étranger ou au détriment du national, ou les infractions qui portent atteinte à des intérêts nationaux fondamentaux.

3) Ces règles sont aussi connues sous le nom de lois d'application immédiate ou lois d'application nécessaire, ou encore, de lois « internationalement impératives ».

toute situation entrant dans son champ d'application, quelle que soit par ailleurs la loi applicable au contrat d'après le présent règlement ».

La CJUE admet que les juges nationaux donnent un caractère d'application nécessaire aux règles issues des règlements et directives (transposition d'une directive d'harmonisation minimale), au détriment de la loi choisie par les parties. Par ailleurs, elle contrôle l'application des dispositions nationales, à titre de lois de police ou d'application nécessaire, chaque fois qu'il est allégué que celles-ci pourraient constituer une gêne à l'exercice des libertés fondamentales instituées par le traité [1].

Qu'en est-il en matière de données personnelles, domaine marqué d'un côté par les droits fondamentaux protégés par le droit constitutionnel national et européen, et de l'autre par la globalisation et les intérêts commerciaux qui tendent à faire de l'individu son propre législateur dans un monde où s'efface la souveraineté nationale ?

La directive n° 95/46/CE de 2005 contient ses propres règles visant à déterminer le champ d'application dans l'espace de leurs dispositions [2]. Pour que le droit national issu de sa transposition s'applique, il faut soit un établissement dans le pays en question, soit, en l'absence d'établissement dans un pays de l'Union, des moyens de collecte (dès lors qu'il existe un dispositif qui envoie des informations depuis un ordinateur ou un smartphone, comme par exemple des cookies, il y a moyen de collecte).

Le champ d'application territorial est ainsi défini, non pas par rapport à la personne dont les données sont protégées, mais en fonction de l'entreprise qui les traite (or la protection des données personnelles est un droit fondamental de la personne). L'application de cette législation n'est pas nécessairement limitée au territoire européen : les transferts

---

1) Elle l'a fait pour assurer la liberté de prestation de services (CJCE 23 novembre 1999, *Arblade*) ou la liberté d'établissement des sociétés (CJCE, 9 mars 1999, *Centros ;* 5 novembre 2002, *Überseering, C-208/00 ;* 30 septembre 2003, Inspire Art, **aff. C-167/01**).

2) Directive n° 95/46/CE, article 4 : « Droit national applicable ».

1) Chaque État membre applique les dispositions nationales qu'il arrête en vertu de la présente directive aux traitements de données à caractère personnel lorsque :

a) le traitement est effectué dans le cadre des activités d'un établissement du responsable du traitement sur le territoire de l'État membre ; si un même responsable du traitement est établi sur le territoire de plusieurs États membres, il doit prendre les mesures nécessaires pour assurer le respect, par chacun de ses établissements, des obligations prévues par le droit national applicable ;

b) le responsable du traitement n'est pas établi sur le territoire de l'État membre mais en un lieu où sa loi nationale s'applique en vertu du droit international public ;

c) le responsable du traitement n'est pas établi sur le territoire de la Communauté et recourt, à des fins de traitement de données à caractère personnel, à des moyens, automatisés ou non, situés sur le territoire dudit État membre, sauf si ces moyens ne sont utilisés qu'à des fins de transit sur le territoire de la Communauté.

2) Dans le cas visé au paragraphe 1 point c), le responsable du traitement doit désigner un représentant établi sur le territoire dudit État membre, sans préjudice d'actions qui pourraient être introduites contre le responsable du traitement lui-même.

internationaux de données sont visés et le droit au déréférencement s'applique sur le .com et pas seulement sur les .fr, .de, .uk, etc. De plus, la CJUE, dans l'arrêt *Google Spain* précité, a retenu une définition très large du terme « traitement » : la société Google, en tant que moteur de recherche, a été jugée « responsable de traitement des données », ainsi que ses filiales européennes. Le fait que les données ne soient pas « traitées » dans les centres de traitement européens de Google (Belgique, Irlande, Finlande et, en 2017, les Pays-Bas) n'a pas été jugé déterminant. La Cour considère que, lorsque l'exploitant d'un moteur de recherche crée dans un État membre une succursale ou une filiale destinée à assurer la promotion et la vente des espaces publicitaires proposés par ce moteur et dont l'activité vise les habitants de cet État membre, **un traitement de données à caractère personnel est effectué** *« sur le territoire d'un État membre ».*

La proposition européenne de règlement relatif à la protection des données personnelles élargit le champ d'application des règles européennes[1].

Article 3 – Champ d'application territorial :

1) Le présent règlement s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement de données ou d'un sous-traitant sur le territoire de l'Union.

2) Le présent règlement s'applique au traitement des données à caractère personnel appartenant à des personnes concernées ayant leur résidence sur le territoire de l'Union, par un responsable du traitement qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées : a) à l'offre de biens ou de services à ces personnes concernées dans l'Union ; ou b) à l'observation de leur comportement.

3) Le présent règlement s'applique au traitement de données à caractère personnel par un responsable du traitement qui n'est pas établi dans l'Union, mais dans un lieu où la législation nationale d'un État membre s'applique en vertu du droit international public.

L'article 3.2 de la proposition de règlement introduit le lieu de résidence de la personne à laquelle appartiennent les données comme l'un des critères d'application du droit de l'Union. Ainsi, le responsable de traitement extra-européen ne devra pas seulement se soumettre aux obligations prévues par les instruments ayant autorisé le transfert (*Safe Harbour*, clauses contractuelles ou règles d'entreprises) mais aussi à l'ensemble des obligations découlant du règlement. L'enjeu est d'assurer, pour « ceux qui ont leur résidence sur le territoire de l'Union », l'application des législations assurant l'effectivité de la protection de leurs droits fondamentaux.

1) Proposition adoptée le 12 mars 2014 par le Parlement européen.

La déclaration du groupe de l'article 29[1] reprend à son compte la méthode des lois de police, appliquée à l'ensemble des règles de protection des données de l'Union (article 14) : *« Les règles de protection des données de l'Union sont nécessaires à la sauvegarde de la situation politique, sociale et économique de l'Union et de ceux qui sont soumis à la législation de l'Union. Elles doivent être considérées comme des principes internationaux impératifs en droit international public et privé. Des lois étrangères ou des accords internationaux ne peuvent leur passer outre et les organisations ne peuvent y déroger par contrat »*.

L'étude sur le numérique et les droits fondamentaux du Conseil d'État va dans le même sens : elle recommande de *« promouvoir le principe du pays de destination pour un socle de règles choisies en raison de leur importance particulière dans la protection des droits fondamentaux ou de l'ordre public »* et précise que *« les règles du socle seraient applicables à tous les sites dirigeant leur activité vers la France ou l'Union européenne »*. Elle propose différentes techniques pour *« rendre applicables un socle de règles impératives »* :
– appliquer les règles du droit commun du droit international privé (solution qui ne fonctionne que lorsque ces règles conduisent à appliquer le principe du pays de destination ; ainsi, par exemple, des lois pénales qui définissent les limites de la liberté d'expression) ;
– s'écarter de la loi désignée par les règles de conflit de lois lorsque celle-ci est inadaptée (notamment lorsque la règle de conflit désigne la loi d'autonomie), ce qui est possible grâce aux lois de police.

L'étude estime que la technique des lois de police est plus appropriée que celle de l'exception d'ordre public : *« Les règles relatives à la protection des données personnelles ont vocation à entrer dans cette catégorie, dès lors qu'elles mettent en œuvre un droit garanti par la charte des droits fondamentaux de l'UE et que la protection des données personnelles est regardée comme un enjeu de souveraineté. »*[2]

Le recours aux lois de police pour promouvoir nos valeurs européennes et notre réglementation en matière de données est un pis-aller nécessaire mais dont l'efficacité n'est que relative : comment les imposer aux autres et jusqu'où l'extraterritorialité d'un règlement européen relatif aux données personnelles peut-elle aller[3] ?

---

1) Déclaration précitée dans la première partie de cette étude.
2) Étude préc., p. 240 et s., sp. p. 244, et la proposition n° 43. L'étude relève encore (p. 245) qu'*« un deuxième corps de règles devant s'imposer à tous les acteurs concernés a trait aux obligations de coopération avec les autorités judiciaires, ainsi qu'avec les autorités administratives procédant à des demandes de données de connexion dans le cadre du code de la sécurité intérieure ».*
3) Pour une réflexion d'ensemble sur l'évolution du droit international privé appelé à se transformer « en raison du déclin du territoire », tandis que « le besoin d'articuler des revendications normatives disparates – sectorielles plutôt que territoriales – demeure », v. D. Bureau et H. Muir Watt, *Droit international privé*, tome 1, 3e éd., 2014, p. 37.

Surtout, avec les tensions géopolitiques actuelles aux portes de l'Europe, une réglementation qui nuirait aux capacités opérationnelles du renseignement français risquerait tout simplement d'être ignorée. En pratique, l'obligation de demander aux juges ou à toute autre autorité l'autorisation de procéder légalement à des interceptions de données peut déjà être contournée par l'usage de logiciels malveillants de type Babar, Evil Bunny ou Casper. La paternité de ces programmes espions ne pouvant être prouvée de manière irréfutable[1], comment sanctionner les auteurs de tels *« malwares »* lorsqu'ils violent le cadre réglementaire national ou européen ? Derrière la problématique de l'attribution et de la répartition des responsabilités, c'est celle de l'efficacité du droit dans un monde dominé par les tensions politiques et l'innovation technologique qui resurgit[2]. Ce qui n'empêche pas la société civile ainsi que les juristes de s'emparer de ces questions et de contribuer à promouvoir un modèle humaniste, qui respecte l'individu tout en garantissant un équilibre avec les autres libertés fondamentales et la sécurité.

Un tel projet, idéalement international et non seulement européen, se forme. En 2014, le sommet qui s'est tenu sous l'égide de la présidente brésilienne, a rassemblé près de 900 participants, représentants des gouvernements de 85 pays, du secteur privé, de la société civile ou d'institutions techniques[3]. Les participants ont condamné l'espionnage sur le Web et demandé que la collecte et l'utilisation de données personnelles par des acteurs étatiques et non étatiques soient soumises au cadre international des droits de l'homme. La déclaration finale a posé les jalons d'une gouvernance mondiale d'Internet (NETmundial) et du développement futur du Web. On y lit que la gouvernance d'Internet doit tendre vers « un réseau unique, interopérable, flexible, stable, décentralisé, sûr, interconnecté ». Cette conférence ouvre une voie internationale, dans laquelle l'Europe doit jouer un rôle de premier plan[4].

Les pratiques d'espionnage ont suscité un flux de réprobations venues du monde entier et particulièrement de l'Europe. Une sorte de coutume internationale se forme. Il devient possible de bâtir un cadre

---

1) http://www.lemonde.fr/pixels/article/2015/03/05/casper-le-logiciel-espion-cousin-de-babar-qui-surveillait-la-syrie_4586723_4408996.html

2) L. Lessig, "Code is law", préc.

3) Il s'agit là d'un bel exemple de « gouvernance multiparties prenantes » *(multistakeholders)*, avec aussi toutes ses limites, en matière d'efficacité (voir à cet égard les déceptions exprimées à l'issue de ce sommet, notamment par la Quadrature du Net).

4) La proposition n° 1 du rapport d'information du Sénat préconise « d'inviter les États membres de l'Union européenne à s'entendre pour proposer la consécration des principes du NETmundial de São Paulo, à la fois par un traité international ouvert à tous les États et par une forme de ratification en ligne par les internautes ». Le rapport ajoute : « l'Union européenne devrait prendre l'initiative de le proposer à ses partenaires, à commencer par les États-Unis » (164). Ce rapport insiste sur le rôle de l'Union européenne pour une gouvernance garantissant un Internet ouvert et respectueux des droits fondamentaux et des valeurs démocratiques.

supranational, à valeur de modèle. Comme dans d'autres domaines où les enjeux juridiques se rattachent à des questions économiques et sociales de dimension internationale (environnement, changement climatique, responsabilité sociétale des entreprises, contrats commerciaux, etc.), un modèle international pourrait être élaboré, sous l'égide d'une institution internationale. Dans un premier temps, ce modèle dépourvu de force obligatoire mais non de puissance incitative pourrait prendre la forme de « Principes » spécifiques au renseignement[1], respectueux des droits fondamentaux et de l'idée que l'Internet n'est pas une infrastructure technique parmi d'autres, mais « un nouvel espace commun porteur de libertés nouvelles »[2]. Un jour peut-être, mais nous en sommes loin, il pourrait être transformé en traité international soumis à la ratification des États.

1) Rappr. la recommandation sur « Les opérations de surveillance massives », adoptée par l'Assemblée parlementaire du Conseil de l'Europe, le 21 avril 2015 (Rec. 2067 (2015) provisoire) qui invite le Conseil des ministres à « envisager une initiative visant à la négociation d'un « Code du renseignement ».
2) Rappr. rapport du Sénat préc. note 1, et les auditions des nombreuses personnalités qui ont plaidé pour l'adoption de principes mondiaux, pour encadrer l'évolution de l'Internet et ne pas figer le pouvoir de fait que les États-Unis détiennent sur le réseau pour des raisons historiques (rapport préc., p. 159 et s.).

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 trois 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 ;

• Julien QUÉRÉ, chargé de mission, depuis sa nomination en date du 20 avril 2015.

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, depuis le 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 n° 2012-351 du 12 mars 2012 a abrogé la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques depuis le 1er mai 2012, et rassemblé l'essentiel de ses dispositions à droit constant au sein du 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. Ainsi, 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 les plaintes auxquelles donneraient lieu de tels agissements. 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.

Jusqu'au 31 décembre 2014, la CNCIS était en outre chargée, en application de l'article 6 de la loi n° 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. Il s'agissait des demandes formées, pour la prévention des actes de terrorisme, par les services habilités de police et de gendarmerie, et qui étaient validées par une « personnalité qualifiée » placée auprès du ministre de l'Intérieur.

Toutes les autres demandes relatives au recueil des données techniques de communications étaient formulées par les services habilités des ministères de l'Intérieur, de la Défense et des Finances et traitées par le GIC. Elles relevaient de l'article L. 244-2 du Code de la sécurité intérieure (ancien article 22 de la loi du 10 juillet 1991) et étaient soumises, dans les mêmes conditions que l'article 6 de la loi du 23 janvier 2006, au contrôle de l'autorité administrative indépendante.

Depuis le 1er janvier 2015, ces deux dispositifs ont fusionné conformément aux nouvelles dispositions issues de 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. Les articles L. 246-1 et suivants du Code de la sécurité intérieure prévoient désormais que les demandes de données de connexions de tous les services et pour les cinq motifs légaux soient présentées à une « personnalité qualifiée » placée auprès du Premier ministre. Celle-ci les autorise ou les refuse. La CNCIS dispose d'un contrôle *a posteriori* sur ces mesures. Seule la mesure de géolocalisation en temps réel (article L. 246-3 du Code de la sécurité intérieure) fait l'objet d'une procédure distincte puisque chaque demande est soumise, selon la procédure de l'urgence absolue, à l'avis préalable de la Commission avant décision par le Premier ministre.

La CNCIS est membre de la Commission consultative créée par le décret n° 97-757 du 10 juillet 1997 (article R. 226-2 du Code pénal) 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'exercice 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 2014 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 intitulé « 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 2014 se sont élevés à 567 661 euros (551 673 euros en 2013 et 607 803 euros en 2012) dont 475 269 euros (474 474 euros en 2013 et 529 864 euros en 2012) pour les dépenses du titre II (dépenses de personnel) et 92 392 euros (77 199 euros en 2013 et 77 939 euros en 2012) pour les dépenses de fonctionnement.

Le budget global de la CNCIS a donc connu une augmentation de 15 988 euros, qui a pris en compte les missions nouvelles confiées à la CNCIS par le législateur en 2013. Cette tendance s'est poursuivie pour l'année 2015. Les crédits alloués sont de 568 903 euros dont 468 610 euros pour les dépenses du titre II (dépenses de personnel) et 100 293 euros pour les dépenses de fonctionnement.

L'augmentation des crédits hors titre II, d'environ 8,5 % par rapport à la LFI 2014 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 LPM 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.

Pour autant, le montant alloué pour les dépenses du titre II relatif au personnel bien que calculé comme les années précédentes pour les cinq postes actuellement pourvus (alors que la CNCIS dispose de six ETPT), se situe en légère baisse pour le budget 2015, dont l'exécution est en cours à la date du présent rapport. Toutefois, face à la forte augmentation de son activité depuis le début de l'année 2015, la Commission a dû pourvoir le sixième ETPT vacant en recrutant un second chargé de mission. En parallèle, et en parfait accord avec le Premier ministre, elle conduit le processus de recrutement d'un ingénieur spécialisé dans les réseaux, afin de compléter son pôle juridique actuel par un pôle technique, à même de répondre à la technicisation croissante des problématiques traitées.

Il faut rappeler en effet que la CNCIS a fonctionné 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,

lui-même progressivement alourdi par un recours accru au contrôle des productions, 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 a assuré 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 GIC 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.

Depuis le 1er janvier 2015, comme indiqué ci-dessus, et l'entrée en application des articles L. 246-1 et suivants du Code de la sécurité intérieure tels que résultant de l'article 20 de la loi n° 2013-1168 du 18 décembre 2013 relative à la LPM pour les années 2014 à 2019, la CNCIS contrôle le dispositif unifié de recueil des données de connexion. S'agissant des mesures de géolocalisation en temps réel administratives, elle émet un avis préalable et contrôle leur mise en œuvre.

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[1] et deux secrétaires fonctionnant en binôme. 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

1) Trois magistrats à la date de rédaction du présent rapport.

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 deux autres 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, humains comme matériels, 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 à l'École nationale de la magistrature (ENM) 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

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

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

Depuis l'instauration de cette procédure d'avis *a priori*, les avis défavorables ont été dans leur grande majorité suivis par l'autorité de décision. En ce sens, cette pratique est plus efficace du point de vue de la protection des libertés publiques que la recommandation prévue par la loi et adressée après la notification de la mise en place d'une interception. Dans ce dernier cas, l'atteinte au secret des correspondances, disproportionnée ou inadaptée, est effective, même si elle est de courte durée, 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 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. Ce contrôle préalable est essentiel, tant en termes de respect des libertés publiques que pour éclairer le choix de l'autorité de décision. Il doit pouvoir intervenir dans tous les cas, même les plus urgents, qui représentent actuellement près de 20 % des dossiers. Ainsi la CNCIS a toujours su adapter ses méthodes d'examen aux contraintes opérationnelles des services. Elle se prononce systématiquement en moins d'une heure sur les demandes d'interceptions présentées en urgence absolue, et au besoin en quelques minutes seulement. Elle met en œuvre l'ensemble des moyens de communication modernes et sécurisés existant pour ne jamais retarder le processus de mise en œuvre d'une écoute urgente justifiée.

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

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

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

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

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 79,9 millions au 31 décembre 2014 soit un taux de pénétration (nombre de cartes SIM rapporté à la population française) de 121,5 %, en croissance de 4 points en un an.

Le nombre de cartes s'accroît de 4,1 % au quatrième trimestre 2014, soit une augmentation de 3,1 millions en un an. Cette croissance, qui reste soutenue, est toutefois en léger retrait au quatrième trimestre 2014 par rapport aux cinq trimestres précédents où le taux annuel de croissance atteignait + 5 %.

Par ailleurs, le nombre de messages interpersonnels (SMS et MMS) envoyés par les clients des opérateurs mobiles en 2014 atteint

200,63 milliards. Ce chiffre de messages continue d'augmenter (+ 2,4 %, + 1,2 milliard de messages supplémentaires en un an) même si cet accroissement est moins rapide depuis deux ans (+ 2 % à 3 % sur les cinq derniers trimestres contre + 20 % à + 30 % en 2012). Ce ralentissement ne touche pas le nombre de MMS qui croît de + 36,6 % au quatrième trimestre 2014 (soit 240 millions de messages supplémentaires). Les MMS représentent, avec 900 millions de messages envoyés au cours du quatrième trimestre 2014, près de 2 % de l'ensemble des messages interpersonnels. Les clients des opérateurs ont envoyé, en moyenne, 249 SMS par mois au cours du quatrième trimestre 2014[1].

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 de sécurité prévus par l'article L 242-2 du Code de la sécurité intérieure

	Initial (1991-1996)	1997	2003	2005	2009	2014	2015
Ministère de la Défense	232	330	400	450	285	285	320
Ministère de l'Intérieur	928	1 190	1 190	1 290	1 455	1 785	2235
Ministère du Budget	20	20	80	100	100	120	145
Total	1 180	1 540	1 670	1 840	1 840	2 190	2700

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 2014 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. Lors de cette réforme, 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 paraissait 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

1) Source ARCEP : http://www.arcep.fr

totalité du contingent général, qui était avant les augmentations de 2014 et 2015 de 1 840 objectifs.

Comme il en a été fait état dans le rapport d'activité précédent[1], 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, 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'était posée en 2014. Deux ministères, l'Intérieur et le Budget, avaient 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'était pas opposée à l'augmentation sollicitée, mais avait 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 avait 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, avait eu une conséquence directe sur la méthode d'examen préalable par la Commission des demandes d'interceptions. En effet, l'autorité administrative indépendante n'avait en 2014 bénéficié d'aucun renfort d'effectif pour faire face au surcroît de travail généré par les interceptions supplémentaires. Elle a donc dû, depuis l'an dernier, 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 chaque jour ouvrable (ou au plus tard dans 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.

Cette hausse accordée en 2014 s'est avérée insuffisante dès les premiers mois de l'année 2015 pour certaines directions, en particulier celles qui consacrent une part importante de leurs quotas d'interceptions

1) CNCIS, 22e rapport d'activité, Paris, La Documentation française, 2014, 252 p., p. 73 et sq.

à la prévention du terrorisme. La CNCIS ayant signalé au cours du premier trimestre 2015 des risques de dépassement du contingent, le Premier ministre a de nouveau envisagé une augmentation. Il a recensé les besoins opérationnels nouveaux des services et saisi pour avis la Commission.

Dans son avis, la CNCIS a exprimé une position favorable, assortie de plusieurs conditions. Elle a préconisé une hausse globale plus modérée que celle initialement envisagée (et ce, à plus forte raison, s'agissant d'une hausse intervenant seulement un an après la précédente), une augmentation différenciée en fonction de la nature des activités des services, et un maintien du niveau d'exigence fixé concernant l'exploitation des interceptions de sécurité. En effet, la Commission rappelle avec constance qu'une interception n'a de sens que si les communications sont régulièrement exploitées et transcrites conformément à la loi (article L. 242-5 du Code de la sécurité intérieure).

Le 13 avril 2015, dans son discours de présentation du projet de loi relatif au renseignement devant l'Assemblée nationale le Premier ministre a personnellement annoncé le passage du contingent à 2700 « cibles », soit une hausse de 23 %. Dans sa décision, il a également mentionné que le suivi se ferait non plus par service comme depuis 1960, mais par direction générale. La CNCIS regrette ce suivi moins précis des quotas dévolus à chacun des douze services habilités et entend maintenir quant à elle la vérification quotidienne du respect du contingentement à chaque demande nouvelle d'interception de sécurité.

Cette deuxième hausse en un peu plus d'une année pourrait apparaître comme un signe préoccupant d'une augmentation de la surveillance de la population. Pourtant il n'en est rien, dans la mesure où le chiffre de 2700 interceptions simultanées possibles au maximum reste extrêmement modeste rapporté au chiffre total des terminaux de communication en circulation et où les mesures concernent des « objectifs » clairement ciblés. Cette nouvelle hausse souligne tout au contraire la pertinence de cette règle du contingentement inscrite dans la loi en 1991. Elle permet en effet de s'adapter aux besoins opérationnels des services tout en restant extrêmement vigilant sur le nombre de mesures effectivement exploitées, que le Premier ministre et la CNCIS connaissent en temps réel, et qui leur donne la possibilité de vérifier que les atteintes conservent le caractère « exceptionnel » voulu par la loi.

Dans le cadre des travaux relatifs à la loi sur le renseignement votée en 2015, la CNCIS, prenant appui sur les vertus de ce dispositif en matière d'interceptions depuis 1960, avait préconisé l'extension de la règle du contingentement aux autres techniques de recueil de données, en l'érigeant en principe général. Elle considère que ce moyen de régulation prévu par le législateur est l'un des outils permettant de garder un caractère « exceptionnel » aux atteintes aux droits individuels, moins en ce qu'il opposerait un plafond indépassable (le Premier ministre a

toujours le loisir de le relever) qu'en ce qu'il fonctionne comme un dispositif d'alerte pouvant témoigner d'une « suractivité » des services. Malheureusement, le gouvernement et le Parlement n'ont pas repris cette proposition et ont limité le contingentement à deux techniques seulement, dont les interceptions. Il reviendra à la future CNCTR d'inventer de nouvelles modalités de vérification du nombre simultané de mesures en vigueur afin de s'assurer que l'usage fait de ces techniques par les services ne constitue pas une atteinte disproportionnée aux libertés.

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 au droit. À cet effet, la présentation des éléments de fait doit être certes synthétique mais non stéréotypée. Elle doit être sincère et consistante pour permettre à chaque autorité, ministres demandeurs, Commission et Premier ministre, de juger de la pertinence de leur adéquation au motif légal. 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 », qui évoquera également l'extension du nombre et de la portée de ces motifs dans la loi relative au renseignement votée en 2015.

Le cadre des demandes servant à la rédaction de celles-ci par les différents services habilités a été revu en 2006, en 2008, en 2009 et à nouveau en 2015 notamment pour assurer un suivi complet des numéros interceptés simultanément ou successivement durant toute la durée de

l'interception. La CNCIS a en effet 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 limitatif. 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 pour exclure des transcriptions (appelées « productions ») les aspects privés des conversations

ou relevant du secret professionnel attaché à certaines professions, ou encore 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 à la liberté de manifestation.

D'une manière générale, et quel que soit le motif, l'implication personnelle de la cible dans des agissements attentatoires à notre sécurité doit être au moins présumée.

Dans le cadre de son contrôle *a priori*, la Commission dispose d'un moyen d'investigation auquel elle recourt plus souvent depuis quelques années. Elle a la possibilité de demander au service concerné les éléments d'information complémentaires qui lui sont nécessaires pour fonder son avis. Elle peut, en effet, à réception de ces renseignements additionnels, formuler des observations ou rendre un avis défavorable.

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

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 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 pour l'année 2014

• *Évolutions 2013-2014*

6 628 interceptions de sécurité ont été sollicitées en 2014 (4 452 interceptions initiales et 2 176 renouvellements). Pour mémoire, 6 182 interceptions de sécurité avaient été sollicitées en 2013 (4 213 interceptions initiales et 1 961 renouvellements). Cela représente une augmentation modérée de 7,2 %, en cohérence avec la hausse du contingent global des interceptions début 2014 évoquée précédemment.

S'agissant des interceptions initiales, 743 de ces 4 452 demandes ont été présentées selon la procédure dite d'urgence absolue (812 en 2013) soit 16,7 % des dossiers (contre 19,3 % en 2013). Cette diminution du nombre d'urgences absolues est directement liée à la modification en profondeur de la procédure « hors urgence » décidée par la CNCIS l'an dernier et décrite dans le rapport précédent[2].

---

1) Article L. 243-8 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. […] ».

2) CNCIS, 22e rapport d'activité, Paris, la Documentation française, 2014, 252 p., p. 80 et sq.

En effet, jusqu'en 2014, 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 avait 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, avait donc proposé au Premier ministre – qui l'avait accepté – d'introduire plus de fluidité dans le traitement des demandes.

Elle est, depuis le printemps 2014, 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 n'ont pas été renforcés pour autant en 2014, 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.

L'objectif d'un traitement par la Commission des demandes qui continuent d'être présentées en urgence absolue dans un délai inférieur à une heure a toujours été atteint. Le respect de cette contrainte de performance que s'est fixée l'autorité administrative indépendante nécessite, dans le cadre de l'avis *a priori* donné par la Commission, la mise en œuvre d'une permanence 24h/24, tout au long de l'année, qui peut d'une certaine manière être comparée à celle qui est assurée par chaque parquet près les tribunaux de grande instance.

Au final, si l'on impute à ce chiffre global les 67 avis défavorables donnés par la Commission lors des demandes initiales et des demandes de renouvellement suivis par le Premier ministre (sur 75 avis défavorables rendus au total), ce sont donc 6 551 interceptions de sécurité qui ont effectivement été pratiquées au cours de l'année 2014 (6 100 en 2013, soit + 7,4 %).

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 58 %, suivie de la prévention du terrorisme avec 26 % et de la sécurité nationale avec 15 %.

Concernant les renouvellements accordés, on note que la sécurité nationale occupe la première place avec 40 %, suivie de la prévention du terrorisme à 34 % et de la criminalité organisée à 24 %. 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 près 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. Selon ses directives, 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 47 % des requêtes, suivie de celui de la prévention du terrorisme à 28 %, puis celui de la sécurité nationale à 23 %. Ces trois motifs représentent 98 % du total des demandes.

2014 confirme la part majoritaire prise par la criminalité organisée, tout en marquant une nette diminution de cette suprématie (- 7 points par rapport à 2013). Elle marque une stabilisation du nombre de demandes présentées sous le motif « prévention du terrorisme » après la nette hausse relevée en 2013 (+ 5 points par rapport à 2012), qui est évidemment à mettre en relation avec la persistance de la menace terroriste.

L'augmentation de la part de la sécurité nationale (+ 6 points) représente un retour au niveau habituel pour ce motif après une baisse notable (- 7 points) relevée en 2013.

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 4 599 en 2013 dont 259 demandes de renseignements complémentaires et 679 limitations de la durée d'interception sollicitée, à 5 221 en 2014 (79 % des demandes) dont 230 demandes de renseignements complémentaires et 681 limitations de la durée d'interception.

Cette forte augmentation du nombre d'observations (+ 13,5 %), qui intervient après celle déjà observée entre les années 2012 et 2013 (+ 22 %) 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, dans l'ensemble, les services concernés ont 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 75 (1,1 % des demandes), parmi lesquels 32 concernent les demandes initiales (dont 3 portant sur des procédures d'urgence absolue) et 43 les demandes de renouvellement. Cela représente 7 avis défavorables de moins qu'en 2013 (- 9 %). À la différence des années précédentes, ces avis défavorables n'ont pas tous été suivis par le Premier ministre. L'autorité de décision a choisi de passer outre à 8 reprises.

La loi ne contraint nullement le Premier ministre à suivre les avis de la CNCIS, néanmoins, cette situation inédite de décisions non conformes lors d'avis défavorables de l'autorité administrative indépendante a incité cette dernière à accentuer encore sa vigilance dans son contrôle *a posteriori* des lignes concernées, n'hésitant pas à adresser des recommandations de suppression dès que l'analyse des productions de ces interceptions confirmait que leur exploitation était réalisée en méconnaissance des dispositions légales.

À ce chiffre des avis défavorables « bruts », il convient d'ajouter deux techniques d'observation 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 13 reprises en 2014 (contre 16 en 2013). À la différence des années précédentes, par conséquent de manière tout à fait inédite[1], deux d'entre elles n'ont pas été suivies par le Premier ministre et si une troisième a été suivie, c'est avec un délai de près de deux semaines de retard durant lesquelles l'exploitation s'est poursuivie[2] ;

• 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 conduisant à stopper l'exploitation d'interceptions, qui sont susceptibles de présenter des difficultés par rapport aux dispositions légales ou qui s'éloignent du cadre de l'autorisation délivrée par le Premier ministre ou son délégué. 38 préconisations ont été faites en 2014 contre 40 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 2014 à 126 (1,9 % des demandes) contre 138 en 2013.

1) Il est rappelé qu'une recommandation est envoyée lorsqu'une interception se poursuit en dépit des prescriptions légales.
2) L'article L. 243-8 du Code de la sécurité intérieure dispose que, dans le cas où il reçoit une recommandation, « le Premier ministre informe sans délai la commission des suites » qu'il entend lui donner.

Données chiffrées et commentaires pour le premier quadrimestre 2015

Entre le 1er janvier et le 30 avril 2015, 2 509 interceptions de sécurité ont été sollicitées (1 719 interceptions initiales et 790 renouvellements)[1]. Ces chiffres traduisent une hausse de l'activité par rapport au premier quadrimestre 2014, qui est à mettre en relation avec les effets de l'augmentation des quotas intervenue en 2014 et les conséquences des attentats ayant frappé la France en janvier 2015.

S'agissant des interceptions initiales, 428 de ces 1 719 demandes ont été présentées selon la procédure dite d'urgence absolue soit 24,9 % des dossiers, ce qui démontre une forte augmentation, de plus de 8 points, par rapport à la moyenne de l'année 2014 (16,7 %).

L'état de la menace, en particulier terroriste à la suite des attentats du mois de janvier 2015, l'ancrage dans le temps et l'accélération des crises au niveau international, comme leur prolongement prévisible sur le territoire national, constituent sans doute la cause de ce recours plus important à la procédure de l'urgence.

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 spectaculaire des volumes (près de 50 % des demandes initiales en janvier 2015), toujours été atteint.

32 avis défavorables ont été formulés par la Commission lors des demandes initiales et des demandes de renouvellement. 23 ont été suivis. Ce sont donc 2 477 interceptions de sécurité qui ont effectivement été pratiquées au cours du premier quadrimestre 2015.

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 48 %, suivie de la prévention du terrorisme avec 38 % (en augmentation de 12 points par rapport à la moyenne 2014) et de la sécurité nationale avec 12 %.

La part prépondérante prise par la prévention du terrorisme est encore plus marquante si l'on prend en considération les demandes autorisées en urgence absolue, puisque ce motif représente 79 % du total, chiffre à mettre directement en relation avec l'importance de la menace terroriste que subit la France actuellement.

Concernant les renouvellements accordés, on note que la sécurité nationale occupe la première place avec 42 %, suivie de la préven-

1) Soit, par extrapolation, 7 527 en rythme annuel (près de 14 % d'augmentation par rapport à 2014).

tion du terrorisme à 32,5 % et de la criminalité organisée à 22 %, sans changement majeur par rapport à la moyenne 2014.

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 reste le premier avec 40 % des requêtes, talonné de façon inédite par celui de la prévention du terrorisme à 36 %, puis celui de la sécurité nationale à 22 %. Ces trois motifs représentent 98 % du total des demandes.

Le début de l'année 2015 marque surtout une hausse importante du nombre de demandes présentées sous le motif « prévention du terrorisme » (+ 8 points par rapport à la moyenne 2014), qui est évidemment à mettre en relation avec l'acuité de la menace terroriste. La diminution de la part de la criminalité (- 7 points) est la conséquence mécanique de la hausse de la prévention du terrorisme et non pas une tendance liée à la diminution des risques d'atteintes en la matière. La sécurité nationale est un motif stable. Les deux autres motifs légaux « sauvegarde du potentiel scientifique et économique » et « prévention de la reconstitution de groupements dissous » continuent de représenter moins de 2 % des demandes.

• *Observations*

Dans le souci constant d'éviter d'enfermer sa pratique dans une logique purement binaire (avis favorable ou défavorable), la Commission a, de janvier à avril 2015, formulé 1 649 observations dont 67 demandes de renseignements complémentaires et 210 limitations de la durée d'interception sollicitée (soit sur près des deux tiers des demandes).

Les avis défavorables, comptabilisés dans les observations, se sont élevés à 32 (près de 1,3 %), parmi lesquels 11 concernent les demandes initiales (dont 1 en urgence absolue) et 21 les demandes de renouvellement. 9 n'ont pas été suivis par le Premier ministre, qui a autorisé la construction ou la poursuite de l'interception en dépit de la position contraire de l'autorité administrative indépendante. Cela signifie qu'en seulement quatre mois le Premier ministre a décidé de passer outre l'avis négatif de la CNCIS dans un nombre de situations supérieur à toute l'année 2014. Alors que la Commission ne rend pas plus d'avis défavorables qu'avant, et même un peu moins compte tenu de l'augmentation globale du nombre de mesures, l'augmentation du nombre de « passer outre » représente un sujet de préoccupation majeure pour l'autorité de contrôle.

À ce chiffre des avis défavorables « bruts », il convient d'ajouter les deux techniques d'observation qui peuvent s'apparenter, dans le cadre du contrôle *a posteriori*, à « l'avis défavorable » :
– la recommandation adressée au Premier ministre visant à l'interruption de l'interception en cours d'exploitation qui résulte de l'examen exhaustif des « productions » (transcriptions) opérées à partir d'une interception. Il y a été fait recours à une seule reprise pour l'instant en 2015, mais le Premier ministre ne l'a pas suivie, confirmant ainsi l'orientation prise en 2014, qui marque une politique nouvelle dans les relations institutionnelles ;
– la « préconisation d'interruption » adressée par la Commission au service utilisateur en cours d'exploitation. Elle résulte du même examen des productions et procède d'un dialogue constructif mené directement avec les services utilisateurs à stopper l'exploitation d'interceptions, qui sont susceptibles de présenter des difficultés par rapport aux dispositions légales ou qui s'éloignent du cadre de l'autorisation délivrée par le Premier ministre ou son délégué. 34 préconisations ont été faites depuis le début de l'année 2015, toutes suivies par les services titulaires de l'autorisation d'interception.

De fait, si l'on additionne les avis défavorables suivis par le Premier ministre et les « 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'instant à 57 en 2015.

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 512 interceptions en 2014 ont été examinées plus spécifiquement par la Commission, chiffre légèrement inférieur à celui de 2013 (518). 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 2014. Elles ont entraîné des rappels de la part du délégué du Premier ministre en direction du service exploitant. 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 6 553 interceptions accordées en 2014 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

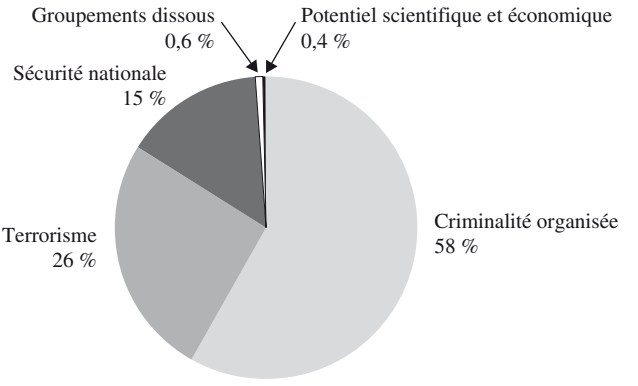
Les demandes initiales d'interceptions

État des demandes initiales d'interceptions (2013 et 2014)

	Demandes initiales		Dont urgences absolues		Accordées	
	2013	2014	2013	2014	2013	2014
TOTAUX	4213	4452	812	743	4176	4420

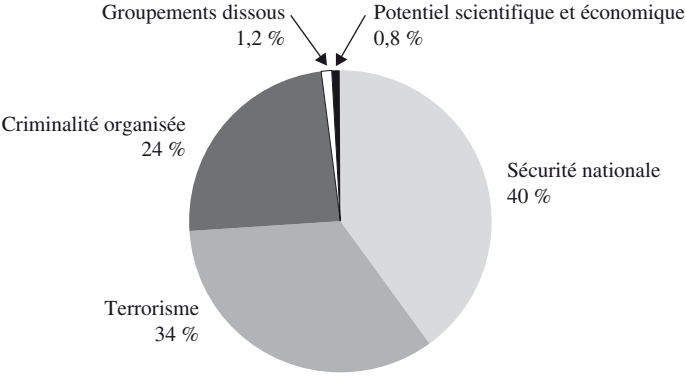
Demandes initiales

Répartition des motifs 2014



Les renouvellements d'interceptions

Total des renouvellements demandés : 2 176
Répartition des motifs des renouvellements accordés en 2014



Activité globale : demandes initiales et renouvellements

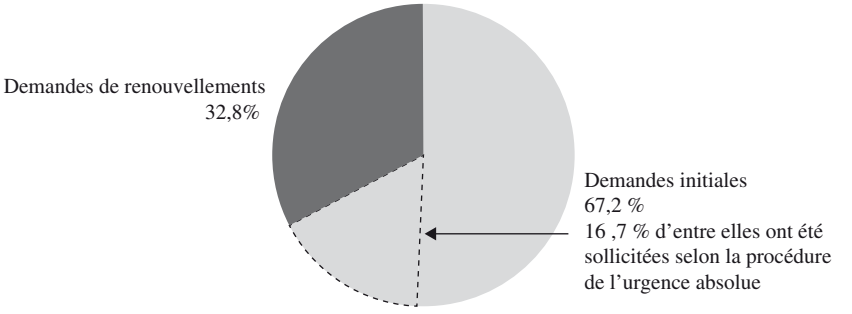
Répartition des demandes entre interceptions et renouvellements d'interceptions

Demandes initiales circuit normal		Demandes initiales en urgence absolue		Demandes de renouvellement	
2013	2014	2013	2014	2013	2014
3 401	3 709	812	743	1 969	2 176

2014

Demandes initiales : 67,2 %. 16,7 % d'entre elles ont été sollicitées selon la procédure de l'urgence absolue

Demandes de renouvellements : 32,8 %

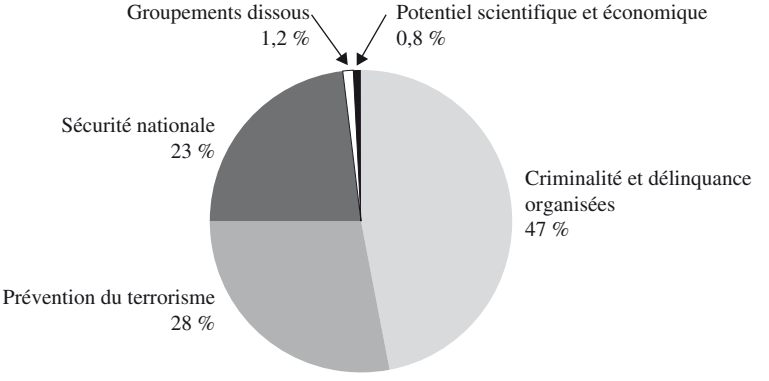


Demandes d'interceptions : tableau récapitulatif global sur neuf ans 2006, 2007, 2008, 2009, 2010, 2011, 2012, 2013 et 2014

	2006	2007	2008	2009	2010	2011	2012	2013	2014
Demandes initiales d'interceptions	4203	4215	4330	3176	3776	4156	4022	4213	4452
Dont « urgences absolues »	714	964	1095	497	522	541	622	812	743
Demandes de renouvellements	1825	1850	1605	1941	2234	2240	2123	1969	2176
Total	6028	6065	5935	5117	6010	6396	6145	6182	6628

Répartitions des motifs d'interceptions de sécurité accordées en 2014

Cumul des demandes initiales et demandes de renouvellements accordées



Répartition entre interceptions et renouvellements accordés

Interceptions accordées en 2014

Interceptions initiales	Renouvellements	Total
4402	2133	6553

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 n° 2002-497 du 12 avril 2002[1], et actuellement dirigé par un officier général, le Groupement interministériel de contrôle 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. Le caractère décisif de cette organisation en quatre « piliers » a déjà été souligné dans les précédents rapports.

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. Lors des travaux relatifs à la loi sur le renseignement votée en 2015, la CNCIS n'a eu de cesse dans les avis qu'elle a portés à la connaissance du Gouvernement ou du législateur de prôner un renforcement du rôle du GIC, tant dans la mise en œuvre des mesures que dans la centralisation des données recueillies.

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

1) CNCIS, 11e rapport d'activité, Paris, La documentation française, 2002, p. 50.

regard de la protection des personnes mises 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.

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. Il apparaît comme une garantie du bon fonctionnement du dispositif technique du recueil du renseignement mis en œuvre sous l'autorité du Premier ministre et le contrôle de la CNCIS.

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, 18 visites de centres d'exploitation et d'échelons centraux ont été effectuées en 2014. Le sous-effectif qui a affecté à plusieurs reprises au cours de l'année la Commission a été compensé par une implication personnelle du président dans la conduite des contrôles et un resserrement du calendrier, permettant ainsi le maintien d'un nombre de visites conforme aux objectifs de performance de l'institution. Les visites se poursuivent en 2015, au rythme d'une à deux chaque mois, annoncées ou inopinées. 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 2014, 110 particuliers ont saisi par écrit la CNCIS. Ils n'étaient que 75 en 2013. Cette hausse de près de 50 %, déjà constatée en 2013, semble se poursuivre en 2015 puisque 45 personnes ont saisi par écrit la Commission au cours des quatre premiers mois de l'exercice. 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 2014 traités un nombre 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 n° 2088 de François MASSOT, 6 juin 1991).

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

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

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

Au cours de l'année 2014 et du premier quadrimestre 2015, la CNCIS n'a pas eu à user des dispositions du 2e alinéa de l'article L. 243-11 du Code de la sécurité intérieure qui précisent que *« conformément au deuxième alinéa de l'article 40 du Code de procédure pénale, la Commission donne avis sans délai au procureur de la République de toute infraction aux dispositions de la présente loi dont elle a pu avoir connaissance à l'occasion du contrôle effectué en application de l'article L. 243-9 »*.

Chapitre III

Le contrôle des opérations portant sur les données de connexion

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 de connexion repose sur un cadre juridique unifié depuis l'entrée en vigueur, le 1er janvier 2015, de l'article 20 de la loi n°2013-1168 du 18 décembre 2013 relative à LPM pour les années 2014 à 2019.

Les dispositions de l'article 20 sont codifiées au chapitre VI du titre IV du livre II du Code de la sécurité intérieure (articles L. 246-1 à L. 246-5).

Elles élargissent aux cinq motifs justifiant des interceptions de sécurité le recueil des données de connexion, définissent les conditions de recueil de ces données « en temps réel » sur sollicitation du réseau (c'est-à-dire de géolocalisation en temps réel), enfin décrivent les procédures de demande, de décision et de contrôle.

Elles constituent un régime spécifique aux données de connexion (I) et à la géolocalisation en temps réel (II), totalement distinct des interceptions de sécurité (III).

Dans ce cadre juridique rénové, la Commission, assistée des services du GIC et de ceux de la « personnalité qualifiée », placée désormais

auprès du Premier ministre et non plus auprès du ministre de l'Intérieur [1], exerce un strict contrôle sur cet accès élargi des services aux données techniques de connexion.

Bien qu'elle ait indéniablement constitué une simplification nécessaire, la refonte opérée par la loi du 18 décembre 2013 laisse toutefois perdurer des disparités qui restent source d'incohérences.

I – L'article 20 de la loi n°2013-116 du 18 décembre 2013 relative à la programmation militaire (articles L. 246-1 et suivants du Code de la sécurité intérieure) et la fin du 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, par la loi n° 2006-64 du 23 janvier 2006, relative à la lutte contre le terrorisme et portant diverses dispositions relatives la sécurité et aux contrôles frontaliers, en son article 6, avait autorisé les seuls services dépendant du ministère de l'Intérieur, spécialisés dans la prévention du terrorisme, à se faire communiquer, sur le fondement d'une réquisition administrative spécifique, les données de connexion détenues par les opérateurs de communications électroniques et les prestataires de la communication au public en ligne (fournisseurs d'accès à Internet et hébergeurs).

Quoique réputée moins intrusive dans le secret des correspondances car ne permettant que le seul accès au contenant des communications électroniques et non au contenu, c'est-à-dire à la conversation proprement dite, cette mesure portait toutefois atteinte au droit à l'intimité de la vie privée et à la liberté d'aller et venir. C'est la raison pour laquelle le législateur avait prévu un certain nombre de garanties au respect desquelles la Commission nationale de contrôle des interceptions de sécurité était pleinement associée.

Il s'agissait d'abord du caractère expérimental du dispositif. La loi avait institué ensuite une personnalité qualifiée auprès du ministre de l'Intérieur, chargée d'autoriser les demandes des services, la Commission étant chargée d'exercer un contrôle *a posteriori* de toutes les demandes autorisées par la personnalité qualifiée.

Ce régime expérimental, dont le terme initial était prévu au 31 décembre 2012, avait été prorogé deux fois, une première fois par la loi n° 2008-1245 du 1er décembre 2008 puis une deuxième fois par la loi n°2012-1432 du 21 décembre 2012, jusqu'au 31 décembre 2015.

---

1) Article L. 246-2 II du Code de la sécurité intérieure.

L'article 20 de la loi du 18 décembre 2013, fruit d'un amendement déposé au Sénat, qui a unifié les régimes d'accès aux données de connexion, a donc mis fin prématurément à une expérimentation de plus de sept ans, en prévoyant une entrée en vigueur du nouveau dispositif au 1er janvier 2015.

Les nouvelles dispositions étendent la faculté d'accéder aux données de connexion détenues par les opérateurs de communication électroniques et les prestataires de la communication au public en ligne à l'ensemble des services de renseignement et non plus seulement aux services du ministère de l'Intérieur chargés de la prévention du terrorisme.

Elles élargissent les finalités pour lesquelles cet accès est autorisé en reprenant l'ensemble des motifs énumérés à l'article L. 241-2 du Code de la sécurité intérieure et non plus la seule finalité de prévention du terrorisme.

Ces dispositions nouvelles visent notamment, comme sous le régime de l'article 6 de la loi du 23 janvier 2006, le recueil, *a posteriori*[1], 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.

Pas plus que par le passé, les services ne sont autorisés sous ce régime nouveau à accéder au contenu des communications électroniques.

II – La mise en œuvre d'une procédure administrative de géolocalisation en temps réel

L'article 20 de la loi n°2013-1168 du 18 décembre 2013 a permis également de disposer d'un cadre légal pour la géolocalisation en temps réel puisque les dispositions de l'article L. 246-3 du Code de la sécurité intérieure prévoient que, pour les finalités énumérées à l'article L. 241-2 du même code, les données de connexion peuvent être recueillies « sur sollicitation du réseau » et transmises « en temps réel » par les opérateurs aux services spécialisés et donc permettre une localisation des terminaux, ce que ne permettait pas explicitement la rédaction de l'article 6 de la loi n°2006-64 du 23 janvier 2006.

---

1) L'article L. 34-1-1 du Code des postes et télécommunications, introduit par l'article de la loi n° 2006-64 du 23 janvier 2006, mentionnait « les données conservées et traitées » par les opérateurs de communication électronique ; l'article L. 246-1 du Code de la sécurité intérieure instauré par l'article 20 de la loi 2013-1168 du 18 décembre 2013 mentionne les « informations ou documents traités ou conservés ». Dans les deux régimes, il s'agit donc, pour les services concernés, d'une possibilité de communication *a posteriori* des données.

Compte tenu du caractère plus intrusif dans la vie privée de la géolocalisation en temps réel par rapport aux autres données de connexion, la procédure prévue répond à des conditions d'utilisation restrictives : l'autorisation est accordée par le Premier ministre, sur demande écrite et motivée des ministres de l'Intérieur, de la Défense et du Budget et la durée d'utilisation est limitée à un mois.

La loi prévoit un contrôle *a posteriori* de la CNCIS mais, comme il avait été fait en matière d'interceptions de sécurité dès 1991, le Premier ministre a donné son accord pour que, depuis le 1er janvier 2015, la commission lui fasse connaître son avis préalable à la décision d'autorisation.

Ces demandes sont présentées à l'examen de la Commission suivant un cheminement administratif identique à celui utilisé en matière d'interception en urgence absolue.

Dans le cadre de l'élaboration de ses avis, la CNCIS applique les principes généraux retenus pour les demandes d'interception de sécurité :
– la qualification des faits au regard des motifs légaux ;
– les présomptions d'implication directe et personnelle de l'objectif dans les projets d'atteintes, d'infractions ou de menaces ;
– la proportionnalité, afin de mesurer le rapport entre l'atteinte qui sera portée à l'intimité de la vie privée et le but poursuivi ;
– la subsidiarité qui permet de s'assurer que l'atteinte n'est portée qu'en raison de l'absence de tout autre moyen de parvenir au but recherché.

Comme en matière d'interception de sécurité, la Commission a introduit une certaine gradation dans ses avis, en les modulant quant à la durée de l'autorisation qui devrait être accordée. Elle a également transposé la pratique des renseignements complémentaires, qui lui permet de ne pas enfermer son opinion dans une logique binaire et de veiller à disposer d'une motivation la plus complète possible avant de statuer.

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

Bien qu'elle ait indéniablement constitué une simplification nécessaire, la refonte opérée par la loi du 18 décembre 2013 laisse toutefois perdurer en réalité deux régimes distincts en matière d'accès aux données de connexion, suivant que la demande est accessoire ou non à une interception de sécurité.

La loi n° 91-646 du 10 juillet 1991 est le premier texte en matière d'exploitation des communications électroniques pour la prévention des atteintes les plus graves à la sécurité nationale et aux intérêts fondamentaux de la Nation. L'article 22 de cette loi, devenu, à la faveur de la codification de la loi de 1991 opérée en 2012, l'article L. 244-2 du Code de

la sécurité intérieure, constitue la première référence légale aux données techniques de connexion.

Ce texte prévoit que les 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 plus de soixante-dix opérateurs de réseaux de communications électroniques ou opérateurs virtuels.

Sur ce fondement légal, les demandes d'identification auprès du GIC sont faites par les services dans le but de préparer un projet d'interception de sécurité.

Depuis le 1er janvier 2015 et l'entrée en vigueur des articles L. 246-1 et suivants du Code de la sécurité intérieure, les demandes de données de connexion sans lien *a priori* avec un projet d'interception de sécurité sont présentées sur le fondement de l'article L. 246-1 du Code de la sécurité intérieure et permettent d'ailleurs d'exclure un éventuel projet d'interception de sécurité 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.

S'agissant des projets avérés d'interception de sécurité, c'est sur le fondement de l'article L. 244-2 du Code de la sécurité intérieure que les prestations annexes, portant sur les communications électroniques de l'objectif visé par l'interception (données de trafic, 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 pour tous les services habilités.

Ces données techniques sont recueillies au terme d'une procédure spécifique, organisée conformément aux recommandations de la CNCIS. La Commission a défini une procédure de contrôle reposant sur les principes de la loi du 10 juillet 1991 et adaptée à la nature du recueil des données :

– la centralisation, le traitement et le contrôle *a priori* des demandes des services par le GIC, relevant du Premier ministre ;

– le contrôle *a posteriori* de ces demandes par la CNCIS, qui a accès à l'ensemble de la procédure, à tout instant ;
– la possibilité pour la Commission, de recourir aux mêmes avis et recommandations que ceux adressés au Premier ministre dans le cadre des interceptions de sécurité.

En définitive, ce sont donc bien trois procédures distinctes qui ont été instaurées et l'unification opérée par la loi de programmation militaire est restée partielle, comme l'avait écrit la Commission dans son rapport précédent [1]. En outre, ces trois procédures, dans le schéma résultant de cette réforme, ne sont pas assorties d'un contrôle identique.

En cela, cette réforme est inaboutie, les risques de contradiction et d'incohérence perdurant, comme l'ont souligné tout à la fois la Délégation parlementaire au renseignement dans son rapport pour 2014 [2] et la CNCIS dans son rapport de 2013-2014.

La Commission d'ailleurs a développé de nouveau cette position à l'occasion de l'avis qu'elle a rendu le 23 octobre 2014, en assemblée plénière, sur le projet de décret d'application de l'article 20 de la loi n°2013-1168 du 18 décembre 2013 relative à LPM.

Le décret n°2014-1576 du 24 décembre 2014 relatif à l'accès administratif aux données de connexion.

Pris en application de l'article L. 246-4 du Code de la sécurité intérieure, ce décret précise les conditions dans lesquelles les services spécialisés peuvent accéder aux données de connexion, sous le contrôle de la CNCIS et notamment la procédure de suivi des demandes ainsi que les conditions et durée de conservation des informations ou documents transmis par le GIC aux services spécialisés.

Dans son avis, la CNCIS avait à titre principal émis le vœu que l'on s'en tienne au calendrier initial et que le dispositif de l'article 6 soit prorogé jusqu'au 31 décembre 2015, afin qu'une architecture globale, reposant sur un seul mécanisme d'autorisation et de contrôle, puisse être élaborée dans le cadre du projet de loi sur le renseignement, dont le dépôt devant le Parlement courant 2015 était déjà annoncé.

1) CNCIS, 22e rapport d'activité, Paris, La Documentation française, 2014, 252 p., p. 103.
2) Rapport de M. Jean-Jacques Urvoas, député, relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2014 ; Assemblée Nationale, 18 décembre 2014.

Elle soulignait de nouveau le risque de jurisprudences divergentes que laissait perdurer le dualisme des circuits d'autorisation et de contrôle instauré par l'article 20 de la loi du 18 décembre 2013. Elle déplorait ensuite le principe du maintien d'une procédure d'autorisation délivrée par une « personnalité qualifiée » placée auprès d'une autorité politique, alors même qu'une telle instance de contrôle ne lui paraissait pas présenter les garanties d'indépendance et d'impartialité requises, son positionnement auprès du Premier ministre et non plus auprès du ministre de l'Intérieur étant certes préférable car le ministère de l'Intérieur est un des trois ministères « demandeurs », mais tout de même peu opérant à cet égard.

Il convient d'observer qu'au jour de la rédaction du présent rapport, le texte législatif relatif au renseignement voté en 2015, répond au souhait d'un contrôle unifié puisqu'en matière d'accès aux données de connexion, il supprime la « personnalité qualifiée » au profit d'une procédure d'autorisation par le Premier ministre, après avis préalable de la CNCTR.

À titre subsidiaire, la Commission avait notamment souligné que le délai de conservation de trois ans prévu pour les données de connexion, en régression sur ce point par rapport au régime antérieur (un an), restait à ses yeux tout à la fois superflu pour assurer l'efficacité des services et insuffisamment protecteur des droits des personnes concernées.

Elle avait indiqué qu'un délai d'un an au plus pour les données de connexion obtenues *a posteriori* et de deux mois au plus pour les données obtenues en temps réel sur sollicitation du réseau par les opérateurs lui paraissait plus conforme aux règles européennes applicables en la matière.

Section 2 – Statistiques de l'activité pour l'année 2014. Aperçu de l'activité pour le premier quadrimestre 2015

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

Au cours de l'année 2014, le Groupement interministériel de contrôle a traité 307 839 demandes. 300 535 d'entre elles portaient sur des mesures d'identification (« annuaire inversé »), ainsi que sur des prestations spécifiques comme l'historique d'un identifiant ou l'identification

d'une cellule. 7 304 mesures de détails de trafics ont par ailleurs été examinées (5 451 en 2013). L'ensemble des requêtes satisfaites représente une très légère baisse de 4 % par rapport à l'année 2013, démontrant une stabilité du volume traité.

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

Les demandes concernant les données de trafic se répartissent entre les différents motifs légaux de la façon suivante : 78,5 % d'entre elles portent sur la sécurité nationale, 18 % ont trait à la prévention de la délinquance et de la criminalité organisées, 0,6 % concerne la prévention du terrorisme, 2,4 % sont relatives à la protection du potentiel scientifique et économique et 0,5 % vise la reconstitution de groupements dissous.

Il convient de rappeler que sous le régime de l'article 6 de la loi n° 2006-64 du 23 janvier 2006, applicable jusqu'au 31 décembre 2014, les services du ministère de l'Intérieur ont sollicité par la procédure prévue à l'article L. 244-2 du Code de la sécurité intérieure des données techniques pour l'ensemble des motifs autres que celui de la prévention du terrorisme. Les services qui dépendaient des ministères de la Défense ou du Budget recouraient au GIC pour l'ensemble des cinq motifs légaux, y compris en matière de terrorisme, puisqu'ils ne faisaient pas partie des services habilités au titre de l'article 6.

Comme expliqué précédemment, le dispositif de l'article L. 244-2 a considérablement évolué depuis le 1er janvier 2015. Toutes les demandes de prestations d'identification ou de données de trafics non liées à une interception de sécurité doivent désormais être adressées à la « personnalité qualifiée » de l'article L. 246-2. Le dispositif « historique » de l'article L. 244-2 n'est désormais utilisable par les services que dans le cadre d'une demande d'interception. Les nombres obtenus sur les quatre premiers mois de l'année 2015, 55 000 demandes, ne peuvent donc en aucun cas être comparés avec ceux de 2014.

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

Sur les sept années complètes d'expérimentation (de 2008 à 2014), 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. L'année 2013 montrait une hausse des demandes, quoique le volume atteint soit sans commune mesure avec celui des années précédant 2011.

Parmi les facteurs susceptibles d'expliquer cette baisse, la Commission avait relevé dans son précédent rapport l'obsolescence de l'ancienne plate-forme de traitement des demandes et les lenteurs qu'elle pouvait générer avant l'aboutissement des procédures.

Définitivement arrêtée début 2014, cette plate-forme a été remplacée par une architecture informatique nouvelle, conçue et développée par le GIC, qui a fluidifié et accéléré les échanges entre les agents demandeurs et les opérateurs. Ce nouveau dispositif technique a permis également de procéder à une comptabilisation par « cible », comme pour les interceptions de sécurité, puisque chaque dossier correspond à un « objectif » et peut contenir plusieurs mesures d'identification ou de détail de trafic.

Toutefois, cette évolution en matière informatique, qui a nécessité une période de mise en route au début de 2014 et a imposé un mode de calcul pour l'année 2014 certes amélioré mais différent, conduit à considérer les données statistiques pour l'année 2014 avec un indispensable recul.

Ainsi, avec le nouveau mode de comptage et selon le rapport d'activité 2014 de la personnalité qualifiée de l'article 6 de la loi du 23 janvier 2006, ce sont 16 224 « dossiers » qui ont été examinés en 2014 par ses services, puis, sur ce total, 15 226 dossiers qui ont été autorisés suite à cet examen. S'agissant de la typologie des mesures sollicitées par les services les demandes d'identification d'abonnés ont représenté en 2014 près de 90 % des demandes. Ces mesures sont moins intrusives que les demandes portant sur les détails de trafic qui ont représenté plus de 10 % des dossiers traités.

S'agissant enfin des moyens de communication électronique concernés, la téléphonie mobile reste la technologie qui motive le plus grand nombre de demandes et poursuit la progression importante qu'elle connaît depuis plusieurs années (75,5 % des demandes en 2014) ; le nombre des requêtes concernant la téléphonie fixe reste relativement stable comme au cours des trois dernières années (près de 22 %), celles relatives aux prestations Internet s'établissent à 2,6 % en 2014.

Il importe d'appeler l'attention du lecteur sur le fait que, pour les raisons techniques évoquées ci-dessus, la CNCIS ne s'estime pas en mesure de poursuivre, pour l'année 2014, les comparaisons avec les années antérieures qui avaient permis de retracer l'évolution de l'activité de la personnalité qualifiée au sens de l'article 6 de la loi du 23 janvier 2006.

En particulier, le mode de comptage des demandes de prestations techniques, liées aux dossiers validés, qui sont ensuite adressées aux opérateurs, a pu varier, dans un environnement informatique non stabilisé, et ne sera véritablement affiné qu'en 2015.

III – Concernant les articles L. 246-1 et suivants du Code de la sécurité intérieure

Ce dispositif est entré en vigueur le 1er janvier 2015, la personnalité qualifiée dont les missions sont prévues au II de l'article L. 246-2

ayant été nommée, ainsi que ses adjoints, par décisions de la CNCIS du 26 décembre 2014 publiées au *JO* du 30 décembre 2014.

Les chiffres d'activité disponibles à la date de rédaction du présent rapport portent sur les quatre premiers mois de l'année 2015 et, sous les réserves dues à l'outil informatique de gestion et évoquées ci-dessus, ils illustrent une augmentation importante de l'activité, en relation avec l'élargissement des motifs pour lesquels l'accès administratif aux données de connexion est à présent autorisé et la possibilité qui est faite à l'ensemble des services de bénéficier de cette procédure.

14 448 dossiers[1] ont été examinés par la personnalité qualifiée au cours de cette période, 13 ont fait l'objet d'une décision de refus, soit 0,08 % et 624, soit 4,31 % ont donné lieu à une demande de renseignement complémentaire.

Ces dossiers ont donné lieu à 40 940 demandes de prestations techniques adressées par le GIC aux opérateurs (soit un rapport d'un à 2,8).

On constate donc une tendance à un quasi-triplement de l'activité depuis le 1er janvier 2015 par rapport à l'année 2014.

Pour la première fois, la Commission est en mesure d'observer la répartition entre les motifs légaux :
– 63,2 % des demandes concernent la prévention du terrorisme ;
– 22,4 % la prévention des atteintes à la sécurité nationale ;
– 12 % la prévention de la criminalité et de la délinquance organisée ;
– 2,2 % la prévention du maintien ou de la reconstitution des ligues et mouvements dissous ;
– 0,2 % la sauvegarde du patrimoine scientifique et économique.

S'agissant de la typologie des prestations demandées : près de 80 % sont relatives à des demandes d'identification et plus de 20 % à des demandes portant sur des détails de trafic.

Enfin, s'agissant des moyens de communication électroniques concernés, la téléphonie mobile est majoritaire avec 68,5 % des demandes, 28,7 % concernent la téléphonie fixe et 2,7 % les prestations liées à l'usage d'Internet.

Ces premières tendances mériteront d'être confirmées lorsque le bilan pourra être fait en année pleine, afin de les commenter de façon pertinente.

1) Soit, sur la base de ces nombres, un nombre de dossiers de 43 344 extrapolés en 2015.

IV – Concernant les mesures de géolocalisation en temps réel de l'article L. 246-3 du Code de la sécurité intérieure

Le dispositif permettant aux services de recourir à cette technique de renseignement est entré en vigueur le 1er janvier 2015 et les chiffres disponibles à la date de rédaction du présent rapport portent sur les quatre premiers mois de l'année 2015. Il convient en conséquence de les prendre là aussi avec la prudence qui s'impose.

252 mesures ont été sollicitées au cours de cette période, aucun avis négatif n'a été émis par la Commission.

Toutefois, ainsi qu'il a été exposé *supra*, la Commission a transposé à l'examen de ces demandes la jurisprudence adoptée en matière d'interceptions de sécurité.

Elle examine ainsi, même si la mesure de géolocalisation en temps réel est moins intrusive qu'une interception de sécurité, si cette mesure respecte le principe de proportionnalité. La Commission peut être amenée, à cette fin, à rendre un avis tendant à réduire, lors de la demande initiale ou à l'occasion d'une demande de renouvellement, la durée de la mesure, fixée par la loi à un mois.

Elle a adopté également un principe de différenciation des délais suivant que l'identité de la cible est totalement inconnue ou partiellement déterminée (10 jours pour identifier la cible ou 20 jours pour parfaire l'identification) ou encore lorsqu'il convient de fixer un délai *ad hoc* en fonction de tel événement déterminé.

Ainsi, 56 des avis rendus (entre le cinquième et le quart) l'ont été avec une indication de limitation de la durée.

La Commission se réserve de même la possibilité d'assortir l'avis rendu d'observations, ce qui a été le cas pour 20 (8 %) des demandes examinées, notamment pour rappeler la vocation purement préventive des techniques de renseignement.

Enfin, dans le souci de s'assurer du caractère suffisant et pertinent de la motivation de la demande, la Commission peut adresser au service demandeur une demande de renseignements complémentaires, ce qu'elle a fait à cinq reprises depuis le 1er janvier 2015.

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 de validation que dans celles du contrôle *a posteriori*.

Comme il a déjà été exposé, jusqu'au 1er janvier 2015, les requêtes fondées sur l'article 6 de la loi du 23 janvier 2006 ont été validées préalablement par la « personnalité qualifiée » placée auprès du ministre de l'Intérieur ou par l'un de ses adjoints. Elles étaient sollicitées par des « agents individuellement désignés et dûment habilités ».

Depuis le 1er janvier 2015, les requêtes sont formulées conformément aux dispositions des articles L. 246-1 et suivants du Code de la sécurité intérieure, auprès de la personnalité qualifiée placée auprès du Premier ministre ou par l'un de ses adjoints.

Sous l'un et l'autre de ces régimes juridiques, la loi a conféré à la CNCIS la responsabilité d'un contrôle *a posteriori* et la CNCIS a disposé et dispose de la faculté de saisir le ministre de l'Intérieur (article 6 de la loi du 23 janvier 2006) ou le Premier ministre (article L. 246-4 du Code de la sécurité intérieure) d'une « recommandation » quand elle *« constate un manquement aux règles [...] ou une atteinte aux droits et libertés »*.

Sans changement, 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 GIC, dont la CNCIS a la responsabilité de contrôler *a posteriori* l'activité.

La Commission a adressé une recommandation au ministre de l'Intérieur en 2014, 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 » au sens de l'article 6 de la loi du 23 janvier 2006 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 (0,2 % en 2014).

Les motifs principaux de refus ont été 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. Dans sa décision n°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 directe et personnelle 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.

En 2014, la CNCIS a renforcé sa mission de contrôle en poursuivant les réunions avec la « personnalité qualifiée » et le GIC 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.

Depuis le 1er janvier 2015, cette méthode de travail s'est poursuivie avec la personnalité qualifiée placée auprès du Premier ministre.

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, comme sous le régime qui était celui de l'article 6 de la loi du 23 janvier 2006, 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.

Chapitre IV

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 7 juillet 2009 puis le décret n° 2009-1657 du 24 décembre 2009 ont confié la présidence de cette commission au directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), lui-même rattaché au Secrétaire général de la défense et de la sécurité nationale. Cette mutation structurelle n'a en revanche emporté aucune modification dans l'économie juridique du dispositif existant.

Le régime de contrôle, issu de l'arrêté du 29 juillet 2004 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 n° 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 2014. Sa composition est la suivante :
– le directeur général de l'ANSSI 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 2014, la Commission a connu une hausse significative du nombre de ses décisions, après une année 2013 qui avait marqué une légère diminution après plusieurs années de hausse continue. Elle a ainsi rendu 1 205 décisions (contre 558 en 2009, 643 en 2010, 883 en 2011, 970 en 2012 et 840 en 2013) ventilées comme suit :
- 566 décisions d'autorisation initiale (362 concernant la commercialisation, 204 l'acquisition d'équipements soumis à autorisation) ;
- 171 décisions de renouvellement d'autorisation ;
- 415 décisions d'ajournement ;
- 28 décisions de radiation ou d'annulation ;
- 6 décisions de refus ou de retrait ;

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

- 19 décisions de mise « hors champ » de l'examen pour autorisation.

Le nombre de décisions rendues illustre l'activité soutenue de la commission consultative. Il doit également être souligné que les dossiers qui lui sont soumis sont de plus en plus complexes, comme le démontre l'augmentation du nombre de décisions d'ajournements (+ 38 % par rapport à l'année 2013) 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 2014 ont été traités début 2015. Les premières tendances pour l'exercice en cours laissent d'ailleurs présager une nouvelle et forte hausse du nombre de décisions rendues en 2015. En effet, au cours des deux premières réunions de l'année 2015, pas moins de 526 décisions ont été rendues.

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 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 a impliqué 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.

---

1) Voir 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).

S'agissant de l'actualité réglementaire, il doit être également précisé que le décret n°2012-1266 du 23 octobre 2014 relatif aux exceptions à l'application du principe « silence vaut acceptation » a fixé un délai de neuf mois à l'expiration duquel le silence gardé par l'administration sur les demandes d'autorisation prévues par les articles R. 226-3 et R. 226-7 du Code pénal vaut décision implicite de rejet.

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 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, qu'offrent 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. La loi relative au renseignement aurait pu en être le support, mais le législateur n'a pas souhaité intégrer dans le texte de nouvelles mesures portant sur 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 du 10 juillet 1991 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. Les modifications apportées par la loi relative au renseignement de 2015 ne sont pas présentées ici puisqu'elles n'ont pas encore été mises en œuvre. Or il s'agit, dans le présent chapitre, de rendre compte de l'application concrète des critères définis par le législateur aux dossiers soumis à l'autorité de contrôle. 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 depuis 1994 et dénommées « atteintes aux intérêts fondamentaux de la Nation ».

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

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

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

Dès l'entrée en vigueur du nouveau Code pénal en 1994, la CNCIS a estimé que la notion de sécurité nationale devait être définie par

référence à ces dispositions pénales (article 410-1 du Code pénal) portant sur les intérêts fondamentaux de la Nation en intégrant les notions d'intégrité du territoire, de forme républicaine des institutions ou des moyens de la défense.

S'il s'agit là d'un élargissement notable de la notion antérieure de sûreté de l'État, on ne saurait y voir pour autant une extension par assimilation aux atteintes les plus courantes à la sécurité des personnes ou des biens. La Commission a toujours rappelé qu'il ne suffit pas d'invoquer la crainte générale d'un trouble à l'ordre public, comme y expose plus ou moins toute manifestation, pour répondre aux exigences de motivation résultant de la loi. Pour ce faire, il doit être justifié, avec la précision nécessaire, d'une menace particulièrement grave à la sécurité nationale.

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

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

Enfin, la Commission opère une appréciation *in concreto* de la notion « d'intérêts fondamentaux de la Nation », la notion de sécurité étant appréhendée en un instant donné et dans un contexte géopolitique donné par rapport aux besoins vitaux du pays. Ainsi la Commission

considère depuis plusieurs années que la sécurité énergétique fait désormais intégralement partie de la sécurité nationale.

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

La sauvegarde des éléments essentiels du potentiel scientifique et économique de la France est, avec la 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 susvisé permet d'étendre la protection du Code pénal non seulement aux différents secteurs de l'économie au sens étroit du terme mais également à la recherche scientifique et aux innovations techniques ou technologiques sur lesquelles reposent précisément la force ou la compétitivité du pays ».

L'article 410-1 du Code pénal est suivi des articles 411-1 à 411-11 qui incriminent les différentes atteintes à ces intérêts au titre desquelles on relève plus particulièrement les infractions des articles 411-5 à 411-8 relatives aux différentes formes d'intelligence avec une puissance

étrangère (article 411-5) et à la livraison d'informations à celle-ci (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 physique[1] 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 (désormais inséré dans le code monétaire et financier aux articles R-153-1 et suivants) 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

1) En aucun cas il ne peut s'agir en effet d'une « surveillance générale » de l'activité d'une entreprise ou de l'ensemble de son équipe dirigeante de façon indifférenciée. Il faut que l'objectif soit soupçonné d'implication directe et personnelle dans des activités en lien avec le motif légal.

l'acte peut être commis par un homme seul, il doit avoir été entrepris dans le but d'intimider ou de terroriser tout ou partie de la population.

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

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

Un certain nombre d'actes relevant de l'expression politique violente pourraient répondre à cette définition comme l'organisation d'incidents en fin de manifestations, le démontage ou le sac symbolique de locaux publics ou privés. Toutefois, pour recevoir la qualification de terroristes, ces actes doivent avoir été commis avec la volonté de troubler gravement l'ordre public par l'intimidation ou la terreur, la gravité du trouble consistant dans la peur collective que l'on cherche à répandre dans la population ou une 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 alinéa 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 n° 2012-1432 du 21 décembre 2012 relative à la sécurité et à la lutte contre le terrorisme 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 n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme 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. La tendance observée depuis plusieurs années, qui consiste pour le champ judiciaire à gagner sur celui de l'administratif, se vérifie une nouvelle fois avec cette loi de 2014.

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 a cependant 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'Office central pour la répression du banditisme (OCRB)[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 préparation, caractérisée par un ou plusieurs faits matériels, d'une ou plusieurs infractions »*. Cette définition est également celle de l'association de malfaiteurs.

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

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

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

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

---

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

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 7 ans d'emprisonnement et le vol en bande organisée de 15 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 courant 2015.

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 pas 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.

1) Par l'ordonnance n°2012-351 du 12 mars 2012

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[1].

L'évolution du nombre et de la nature des motifs légaux en 2015

Depuis plusieurs années, certains, parmi les universitaires[2] ou les praticiens, plaidaient pour une évolution du nombre ou de la définition des motifs légaux adoptés par le législateur en 1991. La CNCIS n'était pas hostile par principe à améliorer l'adéquation des définitions aux besoins des services de renseignement.

La loi relative au renseignement de 2015 a complété la liste et modifié la définition de certains motifs de 1991. Cette révision des motifs légaux, sûrement utile, notamment pour prendre en considération des phénomènes mal couverts jusqu'à présent, comme les violences collectives préméditées et concertées qui n'entraient parfaitement dans aucun des cinq anciens motifs, a toutefois pris une ampleur inattendue, élargissant les domaines possibles d'investigations d'une façon qui peut légitimement inquiéter.

Il reviendra à la CNCTR de se montrer extrêmement vigilante quant au maintien de définitions « jurisprudentielles » précises et restrictives, afin de respecter le caractère exceptionnel des raisons pouvant autoriser le recours à une interception de sécurité et de rester ainsi fidèle à « l'esprit de la loi du 10 juillet 1991 », qui a démontré, à travers un quart de siècle de pratique de la CNCIS, toute sa pertinence.

---

1) 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.

2) Parmi lesquels le professeur Bertrand Warusfel, qui avait évoqué sa vision du motif « sécurité nationale » dans le 21e rapport d'activité, Paris, La Documentation française, 2013, 172 p., p. 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, du 23 janvier 2006, et désormais du 18 décembre 2013[1], lesquelles donnent compétence à la CNCIS pour rendre des avis et exercer son contrôle.

La Commission a régulièrement rappelé les limites de ce champ d'application, 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.

1) Depuis le 1er janvier 2015, tous les textes sont rassemblés au titre IV du livre II du Code de la sécurité intérieure.

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. 244-2, et L. 246-1 et suivants 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 (articles L. 244-2, L. 246-1 et suivants du Code de la sécurité intérieure).

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, envisagée de façon assez consensuelle dans le cadre des travaux relatifs à la loi sur le renseignement de 2015, n'a finalement pas été votée par le Parlement, ce qui est particulièrement regrettable.

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 étaient mis en œuvre jusqu'au 31 décembre 2014 :
– 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.

Comme expliqué dans la première partie de ce rapport, depuis le 1er janvier 2015, ces deux régimes sont unifiés (article L. 246-1 et suivants du Code de la sécurité intérieure). La décision d'autoriser ou non ces mesures est prise par une « personnalité qualifiée » placée auprès du Premier ministre. L'article L. 244-2 demeure, mais n'est utilisé que pour les mesures d'identification intervenant dans le cadre d'une interception de sécurité. La CNCIS poursuit son rôle de contrôleur *a posteriori*. Seule la mesure de géolocalisation en temps réel prévue à l'article L. 246-3 fait l'objet, au même titre qu'une interception de sécurité, d'un avis préalable de la CNCIS et d'une décision par le Premier ministre ou son délégué.

La Commission a, sur le fondement des dispositions précitées, défini une procédure de contrôle reposant sur les principes suivants :
– la centralisation, le traitement, et la validation, par le GIC pour les demandes fondées sur l'article L. 244-2 du Code de la sécurité intérieure ; par la « personnalité qualifiée » pour les demandes relevant des articles L. 246-1 et suivants ;

– le contrôle *a posteriori* de l'intégralité de ces demandes par la CNCIS ;
le contrôle *a priori* et *a posteriori* des géolocalisations en temps réel ;
– la possibilité pour le GIC s'agissant des identifications de l'article L. 244-2, la « personnalité qualifiée » pour les prestations d'identifications ou de données de trafic, ou la Commission s'agissant de la seule géolocalisation en temps réel, de solliciter des renseignements complémentaires, et pour la CNCIS de recourir aux avis, aux recommandations, et aux droits de suite comme en matière d'interceptions de sécurité.

Les mesures sont classées dans une nomenclature qui a été définie par voie réglementaire selon la nature des informations qu'elles permettent de recueillir et l'importance de leur caractère intrusif dans la correspondance et la vie privées. Il faut préciser que la gradation du caractère intrusif a perdu beaucoup de sa pertinence aujourd'hui, dans la mesure où plusieurs prestations réputées « peu intrusives » employées simultanément peuvent en révéler davantage sur un objectif que le contenu de ses communications. Néanmoins, les exigences de rédaction, d'informations et de motivation des demandes demeurent, faute de mieux, déclinées en fonction de cette classification. Elles sont graduées en fonction de la catégorie des données concernées, selon qu'il s'agit de simples mesures d'identification ou de recueillir l'historique, la localisation des cellules ou le détail du trafic.

La nature des contrôles exercés par la Commission pour chaque requête portant sur les données de connexion, est également, en l'état, 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 de connexion, 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.

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

Une motivation suffisante

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

• En quantité

Quelques lignes ne sauraient suffire. Les développements doivent permettre de cerner la personnalité de la « cible », de développer précisément 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.

Si les informations initiales sont insuffisantes, les « renseignements complémentaires » fournis à la demande de la Commission pourront emporter la conviction de cette dernière.

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

La Commission a poursuivi son inscription dans une volonté de dialogue avec les services demandeurs. Cette démarche s'est traduite par une nette augmentation des réunions bilatérales au plus haut niveau 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 en 2014.

Les avis défavorables sont relativement stables (légère diminution en 2014, légère augmentation sur le premier quadrimestre de 2015), et restent très peu nombreux au regard de l'augmentation du volume global des mesures sollicitées. La CNCIS déplore toutefois que le Premier ministre décide de passer outre son avis défavorable de manière de plus en plus fréquente depuis 2014.

À ce chiffre des avis négatifs « 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. En moyenne, depuis 1991, il y est fait recours dix à quinze fois par an. Elles étaient toujours suivies par le Premier ministre jusqu'en 2013. Depuis 2014, le Premier ministre marque une propension à y donner suite au terme d'un délai prolongé, en contradiction avec les termes de la loi, voire à refuser de suivre les recommandations de la Commission, au risque de maintenir une interruption illégale. Il s'agit d'un motif d'inquiétude pour les membres de la CNCIS qui ont tenu à le mentionner dans le rapport public.
• 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.

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

Le caractère illégal de l'interception et les suites pénales qui sont susceptibles d'en découler en matière d'atteintes au secret des correspondances sont identiques lorsque certaines informations soutenant la demande sont partiellement exactes, sont amplifiées, ou lorsque des hypothèses ou des soupçons sont présentés 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 n° 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 n° 2002-1138 du 9 septembre 2002 et 2004-204 du 9 mars 2004, modifiée par la loi n° 2011-267 du 11 mars 2011.

En effet, aux interceptions en matière criminelle et correctionnelle prévues par les articles 100 à 100-7 du Code de procédure pénale, s'ajoutent celles prévues par les dispositions suivantes du même code :
– article 74-2 (recherche d'une personne en fuite) ;

– article 80-4 (recherche des causes de la mort ou d'une disparition présentant un caractère inquiétant) ;
– article 706-95 (criminalité et délinquance organisées) ;
– article 727-1 (écoute, enregistrement et interruption des conversations téléphoniques des détenus).

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

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

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

Les interceptions ordonnées en matière criminelle et correctionnelle

Code de procédure pénale

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

Titre III : Des juridictions d'instruction

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

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

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

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

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

Article 100-1 – « La décision prise en application de l'article 100 doit comporter tous les éléments d'identification de la liaison à intercepter,

l'infraction qui motive le recours à l'interception ainsi que la durée de celle-ci. »

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

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

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

Les enregistrements sont placés sous scellés fermés. »

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

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

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

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

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

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

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

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

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

Les interceptions ordonnées pour recherche d'une personne en fuite

Code de procédure pénale

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

Titre II : Des enquêtes de contrôle d'identité

Chapitre Ier : Des crimes et des délits flagrants

Article 74-2 – « Les officiers de police judiciaire, assistés le cas échéant des agents de police judiciaire, peuvent, sur instructions du procureur de la République, procéder aux actes prévus par les articles 56 à 62 aux fins de rechercher et de découvrir une personne en fuite dans les cas suivants :
1° personne faisant l'objet d'un mandat d'arrêt délivré par le juge d'instruction, le juge des libertés et de la détention, la chambre de l'instruction ou son président ou le président de la cour d'assises, alors qu'elle est renvoyée devant une juridiction de jugement ;
2° personne faisant l'objet d'un mandat d'arrêt délivré par une juridiction de jugement ou par le juge de l'application des peines ;
3° personne condamnée à une peine privative de liberté sans sursis supérieure ou égale à un an, lorsque cette condamnation est exécutoire ou passée en force de chose jugée. »

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

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

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

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

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

Titre III : Des juridictions d'instruction

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

Section I : Dispositions générales

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

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

Les interceptions ordonnées en matière de criminalité et délinquance organisées

Code de procédure pénale

Livre IV : De quelques procédures particulières

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

Chapitre II : Procédure

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

Article 706-95 – « Si les nécessités de l'enquête de flagrance ou de l'enquête préliminaire relative à l'une des infractions entrant dans le champ d'application de l'article 706-73 l'exigent, le juge des libertés et de la détention du tribunal de grande instance peut, à la requête du procureur de la République, autoriser l'interception, l'enregistrement et la transcription de correspondances émises par la voie des télécommunications selon les modalités prévues par les articles 100 deuxième alinéa, 100-1 et 100-3 à 100-7, pour une durée maximum d'un mois[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 n° 2007-297 du 5 mars 2007 – article 72 *JORF* du 7 mars 2007

« Aux fins de prévenir les évasions et d'assurer la sécurité et le bon ordre des établissements pénitentiaires ou des établissements de santé habilités à recevoir des détenus, les communications téléphoniques "des personnes détenues"[2] peuvent, à l'exception de celles avec leur avocat, être écoutées, enregistrées et interrompues par l'administration pénitentiaire sous le contrôle du procureur de la République territorialement compétent, dans des conditions et selon des modalités qui sont précisées par décret[3].

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

---

1) La loi n° 2011-267 du 11 mars 2011 a fait passer la durée légale de quinze jours à un mois, renouvelable une fois.
2) Loi n° 2009-1436 du 24 novembre 2009, article 97-II.
3) Décret n° 2010-1635 du 23 décembre 2010 portant application de la loi pénitentiaire et modifiant le Code de procédure pénale (troisième partie : Décrets).

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 n° 91-646 du 10 juillet 1991 consolidée) :
DES INTERCEPTIONS DE SÉCURITÉ

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

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

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

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

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

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

Article 6 – « L'autorisation mentionnée à l'article 3 est donnée pour une durée maximum de quatre mois. Elle cesse de plein droit de produire

effet à l'expiration de ce délai. Elle ne peut être renouvelée que dans les mêmes conditions de forme et de durée. »

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

Cette transcription est effectuée par les personnels habilités. »

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

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

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

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

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

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

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

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

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

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

Article 13 – « Il est institué une Commission nationale de contrôle des interceptions de sécurité. Cette Commission est une autorité administrative indépendante. Elle est chargée de veiller au respect des dispositions du présent titre. Elle est présidée par une personnalité désignée, pour une durée de six ans, par le Président de la République, sur une liste, de quatre noms, établie conjointement par le vice-président du Conseil d'État et le premier président de la Cour de cassation.

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

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

Les membres de la Commission désignés en remplacement de ceux dont les fonctions ont pris fin avant leur terme normal achèvent le mandat de ceux qu'ils remplacent. À l'expiration de ce mandat, par dérogation au septième alinéa ci-dessus, ils peuvent être nommés comme membre de la Commission s'ils ont occupé ces fonctions de remplacement pendant moins de deux ans.

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

Article 14 – « La décision motivée du Premier ministre mentionnée à l'article 4 est communiquée dans un délai de 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 n° 2006-64 du 23 janvier 2006* – « La Commission remet chaque année au Premier ministre un rapport sur les conditions d'exercice et les résultats de son activité, qui précise notamment le nombre de recommandations qu'elle a adressées

au Premier ministre en application de l'article 14 de la présente loi et au ministre de l'Intérieur en application de l'article L. 34-1-1 du Code des postes et des communications électroniques et de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, ainsi que les suites qui leur ont été données. Ce rapport est rendu public.

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

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

DISPOSITIONS COMMUNES AUX INTERCEPTIONS JUDICIAIRES ET DE SÉCURITÉ

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

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

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

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

Le fait, en violation du premier alinéa, de refuser de communiquer les informations ou documents, ou de communiquer des renseignements erronés est puni de six mois d'emprisonnement et de 7 500 euros

d'amende. Les personnes morales peuvent être déclarées responsables pénalement dans les conditions prévues par l'article 121-2 du Code pénal de l'infraction définie au présent alinéa. Les peines encourues par les personnes morales sont l'amende, suivant les modalités prévues par l'article 131-38 du Code pénal. »

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

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

Article 226-3 – « Est puni des mêmes peines [un an d'emprisonnement et 45 000 euros d'amende] la fabrication, l'importation, la détention, l'exposition, l'offre, la location ou la vente, en l'absence d'autorisation ministérielle dont les conditions d'octroi sont fixées par décret en Conseil d'État, d'appareils "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 (ex-article 186-1 du même code)

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

Est puni des mêmes peines le fait, par une personne visée à l'alinéa précédent ou un agent d'un exploitant de réseau de "ouvert au public de communications électroniques" ou d'un fournisseur de services de

---

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

"communications électroniques", agissant dans l'exercice de ses fonctions, d'ordonner, de commettre ou de faciliter, hors les cas prévus par la loi, l'interception ou le détournement des correspondances émises, transmises ou reçues par la voie des télécommunications, l'utilisation ou la divulgation de leur contenu. »

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

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

COMMUNICATION DES DONNÉES TECHNIQUES RELATIVES À DES COMMUNICATIONS ÉLECTRONIQUES

Article 27 – « La Commission nationale de contrôle des interceptions de sécurité exerce les attributions définies à l'article L. 34-1-1 du Code des postes et des communications électroniques et à l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique en ce qui concerne les demandes de communication de données formulées auprès des opérateurs de communications électroniques et personnes mentionnées à l'article L. 34-1 du code précité ainsi que des prestataires mentionnés aux 1 et 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 précitée. »

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

Titre V (de la loi n° 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[1]

1) Il s'agit du texte applicable depuis le 1er mai 2012, date de l'abrogation de la loi du 10 juillet 1991, après la ratification, par le Parlement, de l'ordonnance n° 2012-351 du 12 mars 2012. Le titre IV est intitulé, depuis la loi du 18 décembre 2013, « Interceptions de sécurité et accès administratif aux données de connexion ».

TITRE IV Interceptions de sécurité

Chapitre Ier : Dispositions générales

Article L. 241-1

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

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

Article L. 241-2

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

Article L. 241-3

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

Article L. 241-4

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

Chapitre II : Conditions des interceptions

Article L. 242-1

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

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

Article L. 242-2

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

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

Article L. 242-3

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

Article L. 242-4

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

Article L. 242-5

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

Article L. 242-6

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

Article L. 242-7

Les transcriptions d'interceptions doivent être détruites dès que leur conservation n'est plus indispensable à la réalisation des fins mentionnées à l'article L. 241-2. Il est dressé procès-verbal de l'opération de destruction. Les opérations mentionnées aux alinéas précédents sont effectuées sous l'autorité du Premier ministre.

Article L. 242-8

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

Article L. 242-9

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

Chapitre III : Commission nationale de contrôle des interceptions de sécurité

Section 1 : Composition et fonctionnement

Article L. 243-1

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

Article L. 243-2

La Commission nationale de contrôle des interceptions de sécurité est présidée par une personnalité désignée, pour une durée de six ans, par le Président de la République, sur une liste de quatre noms établie conjointement par le vice-président du Conseil d'État et le premier président de la Cour de cassation.

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

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

Article L. 243-3

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

Les membres de la Commission désignés en remplacement de ceux dont les fonctions ont pris fin avant leur terme normal achèvent le mandat de ceux qu'ils remplacent. À l'expiration de ce mandat, par dérogation au précédent alinéa, ils peuvent être nommés comme membre de la Commission s'ils ont occupé ces fonctions de remplacement pendant moins de deux ans.

Article L. 243-4

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

Article L. 243-5

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

Article L. 243-6

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

Article L. 243-7

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

Section 2 : Missions

Article L. 243-8

La décision motivée du Premier ministre mentionnée à l'article L. 242-1 est communiquée dans un délai de 48 heures au plus tard au président de la Commission nationale de contrôle des interceptions de sécurité. Si celui-ci estime que la légalité de cette décision au regard des dispositions du présent titre n'est pas certaine, il réunit la Commission,

qui statue dans les sept jours suivant la réception par son président de la 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° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique en ce qui concerne les demandes de communication de données formulées auprès des opérateurs de communications électroniques et personnes mentionnées à l'article L. 34-1 du code précité ainsi que des prestataires mentionnés aux 1 et 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 précitée.

Chapitre IV : Obligations des opérateurs et prestataires de services

Article L. 244-1

Les personnes physiques ou morales qui fournissent des prestations de cryptologie visant à assurer une fonction de confidentialité sont tenues de remettre aux agents autorisés dans les conditions prévues à l'article L. 242-1, sur leur demande, les conventions permettant le déchiffrement des données transformées au moyen des prestations qu'elles ont fournies. Les agents autorisés peuvent demander aux fournisseurs de prestations susmentionnés de mettre eux-mêmes en œuvre ces conventions, sauf si ceux-ci démontrent qu'ils ne sont pas en mesure de satisfaire à ces réquisitions.

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

Article L. 244-2

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

Article L. 244-3

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

Chapitre V : Dispositions pénales

Article L. 245-1

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

Article L. 245-2

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

Article L. 245-3

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

• Les textes réglementaires récents visant le titre IV du livre II du Code de la sécurité intérieure (ex-loi du 10 juillet 1991)

Code de la sécurité intérieure
Partie réglementaire
LIVRE II : ORDRE ET SÉCURITÉ PUBLICS
TITRE IV : INTERCEPTIONS DE SÉCURITÉ
Chapitre 1er : Dispositions générales

Article R. 241-1 – *(créé par décret n°2014-1576 du 24 décembre 2014 – art. 1)*

Le Groupement interministériel de contrôle est un service du Premier ministre chargé des interceptions de sécurité et de l'accès administratif aux données de connexion dans les conditions fixées aux chapitres II et VI du présent titre.

Article R. 241-2 – *(créé par décret n°2014-1576 du 24 décembre 2014 – art. 1)*

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

Section 1 : Groupement interministériel de contrôle

Article R. 242-2 – *(créé par décret n°2013-1113 du 4 décembre 2013)*

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.

Section 2 : Réalisation des opérations matérielles nécessaires à la mise en place des interceptions – (créé par décret n°2013-1113 du 4 décembre 2013)

Article R. 242-4

Ne peuvent être tenus pour qualifiés, pour répondre à l'ordre du ministre chargé des « communications électroniques » prévu par l'article L. 242-9, que les agents techniquement compétents qui :
1° sont employés depuis au moins deux ans chez le même opérateur de communications électroniques ;
2° n'ont fait l'objet d'aucune condamnation pénale inscrite au bulletin n° 2 de leur casier judiciaire.

La liste des agents ne relevant pas du statut de la fonction publique pressentis est adressée au procureur de la République, qui indique ceux des agents qui satisfont à cette dernière condition.

Article R. 242-5

L'ordre du ministre chargé des « communications électroniques » prévu par l'article L. 242-9 est adressé par écrit au responsable spécialement désigné par l'opérateur de communications électroniques, figurant sur la liste prévue à l'article R. 242-6.

L'ordre doit indiquer tous les éléments d'identification de la liaison à intercepter ainsi que la durée de l'interception.

Le responsable intimé désigne par écrit l'un des agents mentionnés à l'article R. 242-4.

Article R. 242-6

Le ministre chargé des « communications électroniques » établit la liste des responsables compétents pour recevoir l'ordre prévu par l'article L. 242-9, en application de l'article R. 242-5.

Ne peuvent être retenus que des responsables :
1° employés depuis au moins deux ans chez le même opérateur de communications électroniques ;

2° qui n'ont fait l'objet d'aucune condamnation pénale inscrite au bulletin n° 2 de leur casier judiciaire.

La liste des responsables pressentis par l'opérateur de communications électroniques est adressée au procureur de la République, qui indique ceux des agents qui satisfont à cette dernière condition.

Article R. 242-7

Le responsable figurant sur la liste prévue à l'article R. 242-6 assure la confidentialité des informations relatives à l'identité des agents mentionnés à l'article R. 242-4 et désignés en application du dernier alinéa de l'article R. 242-5.

Article R. 242-8

Le responsable figurant sur la liste prévue à l'article R. 242-6 rappelle à l'agent, lorsqu'il le désigne en application du dernier alinéa de l'article R. 242-5, les obligations découlant de l'article L. 245-1 du présent code et de l'article 432-9 du Code pénal ainsi que les peines encourues.

Deuxième mission : les opérations de recueil de données techniques de communications et de géolocalisation en temps réel

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

Au sein de ce texte, l'article 6 concernait directement la Commission jusqu'au 1er janvier 2015. Les dispositions de l'article L. 34-1-1 sont abrogées depuis cette date :

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 n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, il est inséré un II bis ainsi rédigé :

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

Les demandes des agents sont motivées et soumises à la décision de la personnalité qualifiée instituée par l'article L. 34-1-1 du Code des postes et des communications électroniques selon les modalités prévues

par le même article. La Commission nationale de contrôle des interceptions de sécurité exerce son contrôle selon les modalités prévues par ce même article.

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

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

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

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

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

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

COMMUNICATION DES DONNÉES TECHNIQUES RELATIVES À DES COMMUNICATIONS ÉLECTRONIQUES

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 étaient 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 était 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 entre interceptions judiciaires (article 100 à 100-7 du Code de procédure pénale) et interceptions administratives rappelée régulièrement par la CNCIS dans ses avis et rapports publics (3e rapport 1994, p. 19 ; 7e rapport 1998, p. 23 ; 8e rapport 1999, p. 14).

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

Article unique

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

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

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

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 ».

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

Au titre IV du livre II du Code de la sécurité intérieure, intitulé « Interceptions de sécurité et accès administratif aux données de connexions » à compter du 1er janvier 2015, figure désormais un nouveau chapitre :

Chapitre VI : Accès administratif aux données de connexion

Article L. 246-1 – *(créé par loi n°2013-1168 du 18 décembre 2013 – art. 20)*

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.

Article 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.

Article 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 ».

Article 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.

Article 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.

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 IER : DISPOSITIONS RELATIVES AUX RÉQUISITIONS JUDICIAIRES PRÉVUES PAR LE II DE L'ARTICLE 6 DE LA LOI N° 2004-575 DU 21 JUIN 2004

Article 1

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

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

d) les dates et heure de début et de fin de la connexion ;
e) les caractéristiques de la ligne de l'abonné ;

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

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

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

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

Article 2

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

Article 3

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

Article 4

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

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

CHAPITRE II : DISPOSITIONS RELATIVES AUX DEMANDES ADMINISTRATIVES PRÉVUES PAR LE II BIS DE L'ARTICLE 6 DE LA LOI N° 2004-575 DU 21 JUIN 2004 (Abrogé par le décret n°2014-1576 du 24 décembre 2014)

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.

Code de la sécurité intérieure

LIVRE II : ORDRE ET SÉCURITÉ PUBLICS

TITRE IV : INTERCEPTIONS DE SÉCURITÉ ET ACCÈS ADMINISTRATIF AUX DONNÉES DE CONNEXION (Créé par décret n°2014-1576 du 24 décembre 2014)

Chapitre VI : Accès administratif aux données de connexion

Article R. 246-1

Pour l'application de l'article L. 246-1, les informations et les documents pouvant faire, à l'exclusion de tout autre, l'objet d'une demande de recueil sont ceux énumérés aux articles R. 10-13 et R. 10-14 du Code des postes et des communications électroniques et à l'article 1er du décret n° 2011-219 du 25 février 2011 modifié 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.

Article R. 246-2

I.-Pour l'application du I de l'article L. 246-2, les services relevant des ministres chargés de la Sécurité intérieure, de la Défense, de l'Économie et du Budget dont les agents peuvent solliciter les informations et les documents mentionnés à l'article L. 246-1 sont :

1° Au ministère de l'Intérieur :

a) à la Direction générale de la sécurité intérieure ;

b) à la Direction générale de la police nationale :

– l'unité de coordination de la lutte antiterroriste ;

– la Direction centrale de la police judiciaire ;

– à la Direction centrale de la sécurité publique : le service central du renseignement territorial ; les services départementaux du renseignement territorial et les sûretés départementales au sein des directions départementales de la sécurité publique ;

– à la Direction centrale de la police aux frontières : l'Office central pour la répression de l'immigration irrégulière et de l'emploi d'étrangers sans titre au sein de la sous-direction de l'immigration irrégulière et des services territoriaux ;

c) à la Direction générale de la gendarmerie nationale :

– à la Direction des opérations et de l'emploi : la sous-direction de la police judiciaire ; la sous-direction de l'anticipation opérationnelle ;

– au pôle judiciaire : le service technique de recherches judiciaires et de documentation ;

– les sections de recherches ;

d) à la préfecture de police :

– la Direction du renseignement ;

– la Direction régionale de la police judiciaire ;

– à la Direction de la sécurité de proximité de l'agglomération parisienne : le service transversal d'agglomération des événements au sein de la sous-direction des services spécialisés de l'agglomération ; la cellule de suivi du plan de lutte contre les bandes au sein de la sous-direction de la police d'investigation territoriale ; la sûreté régionale des transports au sein de la sous-direction régionale de la police des transports ; les sûretés territoriales au sein des directions territoriales de sécurité de proximité ;

2° Au ministère de la Défense :

a) à la Direction générale de la sécurité extérieure ;

b) à la Direction de la protection et de la sécurité de la défense ;

c) à la Direction du renseignement militaire ;

3° au ministère des Finances et des Comptes publics :

a) le service à compétence nationale dénommé Direction nationale du renseignement et des enquêtes douanières ;

b) le service à compétence nationale dénommé traitement du renseignement et action contre les circuits financiers clandestins.

II.-Seuls peuvent solliciter ces informations et ces documents les agents individuellement désignés et dûment habilités par le directeur dont ils relèvent.

Article R. 246-3

Afin de permettre la désignation de la personnalité qualifiée mentionnée au II de l'article L. 246-2 et de ses adjoints, le Premier ministre transmet à la Commission nationale de contrôle des interceptions de sécurité, pour chaque poste à pourvoir, une liste d'au moins trois personnes choisies en raison de leur compétence et de leur impartialité. Ces propositions sont motivées. Elles sont adressées à la Commission au moins trois mois avant le terme du mandat de la personnalité qualifiée et de ses adjoints. La Commission désigne, au sein des listes, la personnalité qualifiée et ses adjoints deux mois au plus tard après avoir reçu les propositions.

Toute décision désignant la personnalité qualifiée et ses adjoints est notifiée sans délai au Premier ministre par la Commission et publiée au *Journal officiel de la République française*.

Les adjoints de la personnalité qualifiée sont au maximum au nombre de quatre.

Nota : ces dispositions entrent en vigueur le 1er janvier 2015. Toutefois, les délais mentionnés à l'article R. 246-3 du Code de la sécurité intérieure ne sont pas applicables à la première désignation, après l'entrée en vigueur du décret n° 2014-1576 du 24 décembre 2014, de la personnalité qualifiée et de ses adjoints mentionnés au II de l'article L. 246-2 du même code.

Article R. 246-4

Les demandes de recueil d'informations ou de documents prévues à l'article L. 246-2 comportent :

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 précise des informations ou des documents dont le recueil est demandé et, le cas échéant, la période concernée ;

c) la date de la demande et sa motivation au regard des finalités mentionnées à l'article L. 241-2.

Article R. 246-5

Le Premier ministre enregistre et conserve pendant une durée maximale de trois ans, dans un traitement automatisé qu'il met en œuvre, les demandes des agents et les décisions de la personnalité qualifiée ou de ses adjoints.

Ces demandes et ces décisions sont automatiquement effacées du traitement, sous l'autorité du Premier ministre, à l'expiration de la durée de conservation. Le directeur du Groupement interministériel de contrôle adresse chaque année à la Commission nationale de contrôle des interceptions de sécurité un procès-verbal certifiant que l'effacement a été effectué.

Article R. 246-6

Les demandes approuvées par la personnalité qualifiée ou par ses adjoints sont adressées par le Groupement interministériel de contrôle, sans les éléments mentionnés aux a et c de l'article R. 246-4, aux opérateurs et aux personnes mentionnés à l'article L. 246-1. Ces derniers transmettent sans délai les informations ou les documents demandés au Groupement interministériel de contrôle, qui les met à disposition de l'auteur de la demande pour exploitation.

La transmission des informations ou des documents par les opérateurs et les personnes mentionnés à l'article L. 246-1 au Groupement

interministériel de contrôle est effectuée selon des modalités assurant leur sécurité, leur intégrité et leur suivi.

Le Premier ministre enregistre et conserve pendant une durée maximale de trois ans, dans un traitement automatisé qu'il met en œuvre, les informations ou les documents transmis par les opérateurs et les personnes mentionnés à l'article L. 246-1. Ces informations ou ces documents sont automatiquement effacés du traitement dans les conditions prévues à l'article R. 246-5.

Article R. 246-7

Les demandes de recueil d'informations ou de documents, impliquant sollicitation du réseau et transmission en temps réel, prévues à l'article L. 246-3 comportent, outre leur date et leur motivation au regard des finalités mentionnées à l'article L. 241-2, la nature précise des informations ou des documents dont le recueil est demandé et la durée de ce recueil.

Les demandes des ministres ou des personnes spécialement désignées par eux et les décisions du Premier ministre ou des personnes spécialement désignées par lui sont enregistrées, conservées et effacées dans les conditions prévues à l'article R. 246-5.

Les demandes approuvées par le Premier ministre ou par les personnes spécialement désignées par lui sont adressées par le Groupement interministériel de contrôle, sans leur motivation, aux opérateurs et aux personnes mentionnés à l'article L. 246-1.

La sollicitation du réseau prévue à l'article L. 246-3 est effectuée par l'opérateur qui exploite le réseau. Les informations ou les documents demandés sont transmis, enregistrés, conservés et effacés dans les conditions prévues à l'article R. 246-6.

Article R. 246-8

La Commission nationale de contrôle des interceptions de sécurité dispose d'un accès permanent aux traitements automatisés mentionnés aux articles R. 246-5, R. 246-6 et R. 246-7.

L'autorité ayant approuvé une demande de recueil d'informations ou de documents fournit à la Commission tous éclaircissements que celle-ci sollicite sur cette demande.

Article R. 246-9

Les coûts identifiables et spécifiques supportés par les opérateurs et les personnes mentionnés à l'article L. 246-1 pour la transmission des informations ou des documents font l'objet d'un remboursement par l'État par référence aux tarifs et selon des modalités fixés par un arrêté des ministres chargés de la Sécurité intérieure, de la Défense, de l'Économie, du Budget et des Communications électroniques.

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 n° 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 n° 2009-619 du 6 juin 2009 relatif à certaines commissions administratives à caractère consultatif relevant du Premier ministre ;

• Le décret n° 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 ;

---

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

– 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 n° 2009-1657 du 24 décembre 2009 relatif au Conseil de défense et de sécurité nationale et au Secrétariat général de la défense et de la sécurité nationale :

– article 5 :

– **I** : À l'article 2 du décret du 7 juillet 2009 susvisé, la référence : « L'article D * 1132-10 » est remplacée par la référence « le 7°de l'article R*1132-3 ».

– **II** : Dans les articles R. 226-2, R. 226-4 et R. 226-8 du Code pénal, les mots : « Le Secrétariat général de la défense nationale » sont remplacés par les mots : « L'Agence nationale de la sécurité des systèmes d'information ».

– **III** : Dans toutes les dispositions à caractère réglementaire, sous réserve des dispositions du II du présent article, les références au Conseil de défense, au Secrétariat général de la défense nationale et au Secrétaire général de la défense nationale sont remplacés respectivement par les références au Conseil de défense et de sécurité nationale, au Secrétariat général de la défense et de la sécurité nationale et au 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 :

ARRÊTE

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

Version consolidée au 22 mai 2015

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 n° 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 micro-émetteurs 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 micro-émetteurs 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° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme

NOR : INTX1414166L

L'Assemblée nationale et le Sénat ont adopté,

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

Chapitre Ier : Création d'un dispositif d'interdiction de sortie du territoire

Article 1

Le livre II du Code de la sécurité intérieure est ainsi modifié :

1° Le titre II est complété par un chapitre IV ainsi rédigé :

« Chapitre IV

« Interdiction de sortie du territoire

« Art. L. 224-1. – Tout Français peut faire l'objet d'une interdiction de sortie du territoire lorsqu'il existe des raisons sérieuses de penser qu'il projette :
– « 1°des déplacements à l'étranger ayant pour objet la participation à des activités terroristes ;
– « 2°ou des déplacements à l'étranger sur un théâtre d'opérations de groupements terroristes, dans des conditions susceptibles de le conduire à porter atteinte à la sécurité publique lors de son retour sur le territoire français.

« L'interdiction de sortie du territoire est prononcée par le ministre de l'Intérieur pour une durée maximale de six mois à compter de sa notification. La décision est écrite et motivée. Le ministre de l'intérieur ou son représentant met la personne concernée en mesure de lui présenter ses observations dans un délai maximal de huit jours après la notification de la décision. Cette personne peut se faire assister par un conseil ou représenter par un mandataire de son choix.

« Lorsque les conditions en sont réunies, l'interdiction de sortie du territoire peut être renouvelée par décision expresse et motivée. Elle est levée aussitôt que ces conditions ne sont plus satisfaites. Les renouvellements consécutifs d'une interdiction initiale ne peuvent porter la durée globale d'interdiction au-delà de deux années.

« La personne qui fait l'objet d'une interdiction de sortie du territoire peut, dans le délai de deux mois suivant la notification de la décision et suivant la notification de chaque renouvellement, demander au tribunal administratif l'annulation de cette décision. Le tribunal administratif statue dans un délai de quatre mois à compter de sa saisine. Ces recours s'exercent sans préjudice des procédures ouvertes aux articles L. 521-1 et L. 521-2 du Code de justice administrative.

« L'interdiction de sortie du territoire emporte dès son prononcé et à titre conservatoire l'invalidation du passeport et de la carte nationale d'identité de la personne concernée ou, le cas échéant, fait obstacle à la délivrance d'un tel document. L'autorité administrative informe la personne concernée par tout moyen.

« Dès notification de l'interdiction de sortie du territoire, et au plus tard dans les 24 heures à compter de celle-ci, la personne concernée est tenue de restituer son passeport et sa carte nationale d'identité.

« Un récépissé valant justification de son identité est remis à la personne concernée en échange de la restitution de son passeport et de sa carte nationale d'identité ou, à sa demande, en lieu et place de la délivrance d'un tel document. Ce récépissé suffit à justifier de l'identité de la personne concernée sur le territoire national en application de l'article 1er de la loi n° 2012-410 du 27 mars 2012 relative à la protection de l'identité.

« Le fait de quitter ou de tenter de quitter le territoire français en violation d'une interdiction de sortie du territoire prise en application du présent article est puni de trois ans d'emprisonnement et de 45 000 euros d'amende.

« Le fait, pour toute personne s'étant vu notifier une décision d'interdiction de sortie du territoire, de se soustraire à l'obligation de restitution de son passeport et de sa carte nationale d'identité est puni de deux ans d'emprisonnement et de 4 500 euros d'amende.

« Un décret en Conseil d'État précise les modalités de mise en œuvre du présent article, s'agissant notamment des modalités d'établissement du récépissé mentionné au neuvième alinéa. »

2° Le chapitre II du titre III est complété par un article L. 232-8 ainsi rédigé :

« Art. L. 232-8. – Lorsque l'autorité administrative constate que les données transmises en application du présent chapitre permettent d'identifier une personne faisant l'objet d'une interdiction de sortie du territoire mentionnée à l'article L. 224-1, elle notifie à l'entreprise de transport concernée, par un moyen tenant compte de l'urgence, une décision d'interdiction de transport de cette personne.

« En cas de méconnaissance de l'interdiction de transport par une entreprise de transport, l'amende prévue à l'article L. 232-5 est applicable, dans les conditions prévues au même article.

« Les conditions d'application du présent article sont précisées par décret en Conseil d'État. »

Chapitre II : Création d'un dispositif d'interdiction administrative du territoire

Article 2

I. – Le Code de l'entrée et du séjour des étrangers et du droit d'asile est ainsi modifié :

1° Le titre I^er^ du livre II est complété par un chapitre IV ainsi rédigé :

« Chapitre IV

« Interdiction administrative du territoire

« Art. L. 214-1. – Tout ressortissant d'un État membre de l'Union européenne, d'un autre État partie à l'accord sur l'Espace économique européen ou de la Confédération suisse ou tout membre de la famille d'une telle personne peut, dès lors qu'il ne réside pas habituellement en France et ne se trouve pas sur le territoire national, faire l'objet d'une interdiction administrative du territoire lorsque sa présence en France constituerait, en raison de son comportement personnel, du point de vue de l'ordre ou de la sécurité publics, une menace réelle, actuelle et suffisamment grave pour un intérêt fondamental de la société.

« Art. L. 214-2. – Tout ressortissant étranger non mentionné à l'article L. 214-1 peut, dès lors qu'il ne réside pas habituellement en France et ne se trouve pas sur le territoire national, faire l'objet d'une interdiction administrative du territoire lorsque sa présence en France constituerait une menace grave pour l'ordre public, la sécurité intérieure ou les relations internationales de la France.

« Art. L. 214-3. – L'interdiction administrative du territoire fait l'objet d'une décision du ministre de l'Intérieur écrite et rendue après une

procédure non contradictoire. Elle est motivée, à moins que des considérations relevant de la sûreté de l'État ne s'y opposent.

« Si l'étranger est entré en France alors que la décision d'interdiction administrative du territoire prononcée antérieurement ne lui avait pas déjà été notifiée, il est procédé à cette notification sur le territoire national.

« Lorsque la décision a été prise en application de l'article L. 214-1 et que l'intéressé est présent en France à la date de sa notification, il bénéficie à compter de cette date d'un délai pour quitter le territoire qui, sauf urgence, ne peut être inférieur à un mois.

« Art. L. 214-4. – L'étranger qui fait l'objet d'une interdiction administrative du territoire et qui s'apprête à entrer en France peut faire l'objet d'un refus d'entrée, dans les conditions prévues au chapitre III du présent titre.

« Lorsque l'étranger qui fait l'objet d'une interdiction administrative du territoire est présent sur le territoire français, il peut être reconduit d'office à la frontière, le cas échéant à l'expiration du délai prévu à l'article L. 214-3. L'article L. 513-2, le premier alinéa de l'article L. 513-3 et les titres V et VI du livre V sont applicables à la reconduite à la frontière des étrangers faisant l'objet d'une interdiction administrative du territoire.

« Art. L. 214-5. – L'autorité administrative peut à tout moment abroger l'interdiction administrative du territoire. L'étranger peut introduire une demande de levée de la mesure après un délai d'un an à compter de son prononcé. Le silence gardé pendant plus de quatre mois sur la demande de levée vaut décision de rejet.

« Art. L. 214-6. – Sans préjudice des dispositions de l'article L. 214-5, les motifs de l'interdiction administrative du territoire donnent lieu à un réexamen tous les cinq ans à compter de la date de la décision.

« Art. L. 214-7. – Le second alinéa de l'article L. 214-4 n'est pas applicable à l'étranger mineur. »

2° L'article L. 213-1 est complété par les mots : «, soit d'une interdiction administrative du territoire ».

3° Le livre V est ainsi modifié :

a) Le 7° de l'article L. 551-1 est complété par les mots : « ou d'une interdiction administrative du territoire ».

b) À la seconde phrase de l'article L. 552-4, après les mots : « de retour sur le territoire français en vigueur, », sont insérés les mots : « d'une interdiction administrative du territoire en vigueur, ».

c) À l'intitulé du chapitre V du titre V, le mot : « mesure » est remplacé par le mot : « peine ».

d) Après le 5° de l'article L. 561-1, il est inséré un 6° ainsi rédigé :

« 6° Si l'étranger doit être reconduit à la frontière en exécution d'une interdiction administrative du territoire. »

e) L'article L. 571-1 est ainsi modifié :
– au premier alinéa, après les mots : « retour sur le territoire français, », sont insérés les mots : « d'interdiction administrative du territoire, » et après le mot : « pénale », la fin de l'alinéa est supprimée ;
– les trois derniers alinéas sont supprimés ;

4° Le chapitre IV du titre II du livre VI est ainsi modifié :

a) L'article L. 624-1 est ainsi modifié :
– au premier alinéa, après les mots : « de quitter le territoire français », sont insérés les mots : «, d'une interdiction administrative du territoire » ;
– au deuxième alinéa, après les mots : « d'entrée en France, » et les mots : « judiciaire du territoire, », sont insérés les mots : « d'une interdiction administrative du territoire, ».

b) Au dernier alinéa de l'article L. 624-4, la référence : « ou L. 541-3 » est remplacée par les références : «, L. 541-3 ou du 6° de l'article L. 561-1 ».

II. – A la première phrase du premier alinéa de l'article 729-2 du Code de procédure pénale, après les mots : « d'interdiction du territoire français, », sont insérés les mots : « d'interdiction administrative du territoire français, ».

Chapitre III : Renforcement des mesures d'assignation à résidence

Article 3

I. – Le titre VI du livre V du Code de l'entrée et du séjour des étrangers et du droit d'asile est complété par un chapitre III ainsi rédigé :

« Chapitre III

« Assignation à résidence avec interdiction de se trouver en relation avec une personne nommément désignée

« Art. L. 563-1. – L'étranger astreint à résider dans les lieux qui lui sont fixés en application des articles L. 523-3, L. 523-4 ou L. 541-3 qui a été condamné à une peine d'interdiction du territoire pour des actes de terrorisme prévus au titre II du livre IV du Code pénal ou à l'encontre duquel un arrêté d'expulsion a été prononcé pour un comportement lié à des activités à caractère terroriste peut, si la préservation de la sécurité publique l'exige, se voir prescrire par l'autorité administrative compétente pour prononcer l'assignation à résidence une interdiction de se trouver en relation, directement ou indirectement, avec certaines personnes nommément désignées dont le comportement est lié à des activités à caractère terroriste. La décision est écrite et motivée. Elle peut être prise pour une durée maximale de six mois et renouvelée, dans la même limite de durée, par une décision également motivée. Cette interdiction

est levée dès que les conditions ne sont plus satisfaites ou en cas de levée de l'assignation à résidence.

« La violation de cette interdiction est sanctionnée dans les conditions prévues à l'article L. 624-4 du présent code. »

II. – L'article L. 624-4 du même code est complété par un alinéa ainsi rédigé :

« La même peine d'emprisonnement d'un an est applicable aux étrangers qui n'ont pas respecté les interdictions qui leur sont prescrites en application de l'article L. 563-1. »

Chapitre IV : Renforcement des dispositions de nature répressive

Article 4

Au 4° de l'article 421-1 du Code pénal, après la première occurrence des mots : « définies par », sont insérées les références : « les articles 322-6-1 et 322-11-1 du présent code, ».

Article 5

I. – Après l'article 421-2-4 du même code, il est inséré un article 421-2-5 ainsi rédigé :

« Art. 421-2-5. – Le fait de provoquer directement à des actes de terrorisme ou de faire publiquement l'apologie de ces actes est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende.

« Les peines sont portées à sept ans d'emprisonnement et à 100 000 euros d'amende lorsque les faits ont été commis en utilisant un service de communication au public en ligne.

« Lorsque les faits sont commis par la voie de la presse écrite ou audiovisuelle ou de la communication au public en ligne, les dispositions particulières des lois qui régissent ces matières sont applicables en ce qui concerne la détermination des personnes responsables. »

II. – La loi du 29 juillet 1881 sur la liberté de la presse est ainsi modifiée :

1° le sixième alinéa de l'article 24 est supprimé ;

2° au premier alinéa de l'article 24 bis, les mots : « des peines prévues par le sixième alinéa de l'article 24 » sont remplacés par les mots : « d'un an d'emprisonnement et de 45 000 euros d'amende » ;

3° au premier alinéa de l'article 48-1, la référence : « (alinéa 8) » est remplacée par la référence : « (alinéa 7) » ;

4° au premier alinéa des articles 48-4,48-5 et 48-6, le mot : « neuvième » est remplacé par le mot : « huitième » ;

5° à l'article 52, les mots : « et sixième » sont supprimés ;

6° au premier alinéa de l'article 63, les références : « 6,8 et 9 » sont remplacées par les références : « 7 et 8 » ;

7° à l'article 65-3, les mots : « sixième, huitième et neuvième » sont remplacés par les mots : « septième et huitième ».

Article 6

I. – Après l'article 421-2-4 du Code pénal, il est inséré un article 421-2-6 ainsi rédigé :

« Art. 421-2-6.-I.-Constitue un acte de terrorisme le fait de préparer la commission d'une des infractions mentionnées au II, dès lors que la préparation de ladite infraction est intentionnellement en relation avec une entreprise individuelle ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur et qu'elle est caractérisée par :

« 1° le fait de détenir, de rechercher, de se procurer ou de fabriquer des objets ou des substances de nature à créer un danger pour autrui ;

« 2° et l'un des autres faits matériels suivants :

« a) recueillir des renseignements sur des lieux ou des personnes permettant de mener une action dans ces lieux ou de porter atteinte à ces personnes ou exercer une surveillance sur ces lieux ou ces personnes ;

« b) s'entraîner ou se former au maniement des armes ou à toute forme de combat, à la fabrication ou à l'utilisation de substances explosives, incendiaires, nucléaires, radiologiques, biologiques ou chimiques ou au pilotage d'aéronefs ou à la conduite de navires ;

« c) consulter habituellement un ou plusieurs services de communication au public en ligne ou détenir des documents provoquant directement à la commission d'actes de terrorisme ou en faisant l'apologie ;

« d) avoir séjourné à l'étranger sur un théâtre d'opérations de groupements terroristes.

« II. – Le I s'applique à la préparation de la commission des infractions suivantes :

« 1° soit un des actes de terrorisme mentionnés au 1° de l'article 421-1 ;

« 2° soit un des actes de terrorisme mentionnés au 2° du même article 421-1, lorsque l'acte préparé consiste en des destructions, dégradations ou détériorations par substances explosives ou incendiaires devant être réalisées dans des circonstances de temps ou de lieu susceptibles d'entraîner des atteintes à l'intégrité physique d'une ou plusieurs personnes ;

« 3° soit un des actes de terrorisme mentionnés à l'article 421-2, lorsque l'acte préparé est susceptible d'entraîner des atteintes à l'intégrité physique d'une ou plusieurs personnes. »

II. – Après le troisième alinéa de l'article 421-5 du même code, il est inséré un alinéa ainsi rédigé :

« L'acte de terrorisme défini à l'article 421-2-6 est puni de dix ans d'emprisonnement et de 150 000 euros d'amende. »

Article 7

Au premier alinéa de l'article 227-24 du même code, après le mot : « violent », le mot : « ou » est remplacé par les mots : «, incitant au terrorisme, ».

Article 8

Le Code de procédure pénale est ainsi modifié :

1° Au début de la section 2 du titre XV du livre IV, il est rétabli un article 706-23 ainsi rédigé :

« Art. 706-23. – L'arrêt d'un service de communication au public en ligne peut être prononcé par le juge des référés pour les faits prévus à l'article 421-2-5 du Code pénal lorsqu'ils constituent un trouble manifestement illicite, à la demande du ministère public ou de toute personne physique ou morale ayant intérêt à agir. »

2° L'article 706-24-1 est ainsi rétabli :

« Art. 706-24-1. – Les articles 706-88 à 706-94 du présent code ne sont pas applicables aux délits prévus à l'article 421-2-5 du Code pénal. »

3° L'article 706-25-1 est complété par un alinéa ainsi rédigé :

« Le présent article n'est pas applicable aux délits prévus à l'article 421-2-5 du Code pénal. »

4° L'article 706-25-2 est abrogé.

Chapitre V : Renforcement des moyens de prévention et d'investigations

Article 9

L'article 706-16 du Code de procédure pénale est complété par deux alinéas ainsi rédigés :

« La section 1 du présent titre est également applicable à la poursuite, à l'instruction et au jugement des infractions commises en détention par une personne détenue, prévenue, condamnée, recherchée dans le cadre d'un mandat d'arrêt européen ou réclamée dans le cadre d'une extradition pour des actes de terrorisme incriminés par les articles 421-1 à 421-6 du Code pénal.

« Ces dispositions sont également applicables à la poursuite, à l'instruction et au jugement des infractions d'évasion incriminées par les articles 434-27 à 434-37 du même code, des infractions d'association de malfaiteurs prévues à l'article 450-1 dudit code lorsqu'elles ont pour objet

la préparation de l'une des infractions d'évasion précitées, des infractions prévues à l'article L. 624-4 du Code de l'entrée et du séjour des étrangers et du droit d'asile ainsi que des infractions prévues à l'article L. 224-1 du Code de sécurité intérieure, lorsqu'elles sont commises par une personne détenue, prévenue, condamnée, recherchée dans le cadre d'un mandat d'arrêt européen ou réclamée dans le cadre d'une extradition pour des actes de terrorisme incriminés par les articles 421-1 à 421-6 du Code pénal. »

Article 10

I. – Le paragraphe 2 de la section 3 du chapitre IV du titre X du livre IV du même code est complété par un article 695-28-1 ainsi rédigé :

« Art. 695-28-1. – Pour l'examen des demandes d'exécution d'un mandat d'arrêt européen concernant les auteurs d'actes de terrorisme, le procureur général près la cour d'appel de Paris, le premier président de la cour d'appel de Paris ainsi que la chambre de l'instruction de la cour d'appel de Paris et son président exercent une compétence concurrente à celle qui résulte de l'application des articles 695-26 et 695-27. »

II. – La section 2 du chapitre V du titre X du livre IV du même code est complétée par un article 696-24-1 ainsi rédigé :

« Art. 696-24-1. – Pour l'examen des demandes d'extradition concernant les auteurs d'actes de terrorisme, le procureur général près la cour d'appel de Paris, le premier président de la cour d'appel de Paris ainsi que la chambre de l'instruction de la cour d'appel de Paris et son président exercent une compétence concurrente à celle qui résulte de l'application des articles 696-9, 696-10 et 696-23. »

Article 11

I. – Le Code monétaire et financier est ainsi modifié :

1° À la première phrase de l'article L. 562-1, le mot : « peut » est remplacé par les mots : « et le ministre de l'Intérieur peuvent, conjointement, ».

2° L'article L. 562-5 est ainsi modifié :

a) À la première phrase, le mot : « peut » est remplacé par les mots : « et le ministre de l'Intérieur peuvent, conjointement, ».

b) À la fin de la seconde phrase, les mots : « du ministre » sont supprimés.

3° À l'article L. 562-6, les mots : « du ministre » sont remplacés par les mots : « des ministres ».

II. – Le présent article entre en vigueur le premier jour du quatrième mois suivant la promulgation de la présente loi.

Article 12

I. – Le 7 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique est ainsi modifié :

1° Au troisième alinéa, après le mot : « humanité, », sont insérés les mots : « de la provocation à la commission d'actes de terrorisme et de leur apologie, », les mots : « huitième et neuvième » sont remplacés par les mots : « septième et huitième » et la référence : « et 227-24 » est remplacée par les références : «, 227-24 et 421-2-5 ».

2° Les cinquième et sixième alinéas sont supprimés.

3° Au dernier alinéa, les mots : «, cinquième et septième » sont remplacés par les mots : « et cinquième ».

II. – Après l'article 6 de la même loi n° 2004-575 du 21 juin 2004, il est inséré un article 6-1 ainsi rédigé :

« Art. 6-1. – Lorsque les nécessités de la lutte contre la provocation à des actes terroristes ou l'apologie de tels actes relevant de l'article 421-2-5 du Code pénal ou contre la diffusion des images ou des représentations de mineurs relevant de l'article 227-23 du même code le justifient, l'autorité administrative peut demander à toute personne mentionnée au III de l'article 6 de la présente loi ou aux personnes mentionnées au 2 du I du même article 6 de retirer les contenus qui contreviennent à ces mêmes articles 421-2-5 et 227-23. Elle en informe simultanément les personnes mentionnées au 1 du I de l'article 6 de la présente loi.

« En l'absence de retrait de ces contenus dans un délai de 24 heures, l'autorité administrative peut notifier aux personnes mentionnées au même 1 la liste des adresses électroniques des services de communication au public en ligne contrevenant auxdits articles 421-2-5 et 227-23. Ces personnes doivent alors empêcher sans délai l'accès à ces adresses. Toutefois, en l'absence de mise à disposition par la personne mentionnée au III du même article 6 des informations mentionnées à ce même III, l'autorité administrative peut procéder à la notification prévue à la première phrase du présent alinéa sans avoir préalablement demandé le retrait des contenus dans les conditions prévues à la première phrase du premier alinéa du présent article.

« L'autorité administrative transmet les demandes de retrait et la liste mentionnées, respectivement, aux premier et deuxième alinéas à une personnalité qualifiée, désignée en son sein par la Commission nationale de l'informatique et des libertés pour la durée de son mandat dans cette Commission. Elle ne peut être désignée parmi les personnes mentionnées au 1° du I de l'article 13 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. La personnalité qualifiée s'assure de la régularité des demandes de retrait et des conditions d'établissement, de mise à jour, de communication et d'utilisation de la liste. Si elle constate une irrégularité, elle peut à tout moment recommander

à l'autorité administrative d'y mettre fin. Si l'autorité administrative ne suit pas cette recommandation, la personnalité qualifiée peut saisir la juridiction administrative compétente, en référé ou sur requête.

« L'autorité administrative peut également notifier les adresses électroniques dont les contenus contreviennent aux articles 421-2-5 et 227-23 du Code pénal aux moteurs de recherche ou aux annuaires, lesquels prennent toute mesure utile destinée à faire cesser le référencement du service de communication au public en ligne. La procédure prévue au troisième alinéa du présent article est applicable.

« La personnalité qualifiée mentionnée au même troisième alinéa rend public chaque année un rapport d'activité sur les conditions d'exercice et les résultats de son activité, qui précise notamment le nombre de demandes de retrait, le nombre de contenus qui ont été retirés, les motifs de retrait et le nombre de recommandations faites à l'autorité administrative. Ce rapport est remis au Gouvernement et au Parlement.

« Les modalités d'application du présent article sont précisées par décret, notamment la compensation, le cas échéant, des surcoûts justifiés résultant des obligations mises à la charge des opérateurs.

«Tout manquement aux obligations définies au présent article est puni des peines prévues au 1 du VI de l'article 6 de la présente loi. »

III. – Le premier alinéa du 1 du VI de l'article 6 de la même loi n° 2004-575 du 21 juin 2004 est ainsi modifié :

1° Les mots : «, cinquième et septième » sont remplacés par les mots : « et cinquième ».

2° Après la référence : « 7 du I », sont insérés les mots : « du présent article ni à celles prévues à l'article 6-1 de la présente loi ».

3° Après la référence : « II », sont insérés les mots : « du présent article ».

Article 13

L'article 57-1 du Code de procédure pénale est ainsi modifié :

1° Après le premier alinéa, il est inséré un alinéa ainsi rédigé :

« Ils peuvent également, dans les conditions de perquisition prévues au présent code, accéder par un système informatique implanté dans les locaux d'un service ou d'une unité de police ou de gendarmerie à des données intéressant l'enquête en cours et stockées dans un autre système informatique, si ces données sont accessibles à partir du système initial. »

2° Sont ajoutés quatre alinéas ainsi rédigés :

« Les officiers de police judiciaire peuvent, par tout moyen, requérir toute personne susceptible :
– « 1° d'avoir connaissance des mesures appliquées pour protéger les données auxquelles il est permis d'accéder dans le cadre de la perquisition ;
– « 2° de leur remettre les informations permettant d'accéder aux données mentionnées au 1°.

« À l'exception des personnes mentionnées aux articles 56-1 à 56-3, le fait de s'abstenir de répondre dans les meilleurs délais à cette réquisition est puni d'une amende de 3 750 euros. »

Article 14

Le premier alinéa des articles 60-1 et 77-1-1 du même code est ainsi modifié :

1° À la première phrase, deux fois, et à la seconde phrase, le mot : « documents » est remplacé par le mot : « informations ».

2° À la première phrase, les mots : « ceux issus » sont remplacés par les mots : « celles issues ».

Article 15

Le même code est ainsi modifié :

1° L'article 230-1 est ainsi modifié :
a) au premier alinéa, après le mot : « comprendre, », sont insérés les mots : « ou que ces données sont protégées par un mécanisme d'authentification, » et les mots : « la version en clair de ces informations » sont remplacés par les mots : « l'accès à ces informations, leur version en clair » ;
b) aux premier et dernier alinéas, après les mots : « d'instruction », sont insérés les mots : «, l'officier de police judiciaire, sur autorisation du procureur de la République ou du juge d'instruction, » ;
c) à la première phrase du deuxième alinéa, après le mot : « République », sont insérés les mots : «, de l'officier de police judiciaire » ;
d) à la seconde phrase du deuxième alinéa, après le mot : « prévu », est insérée la référence : « au deuxième alinéa de l'article 60 et », et la référence : « au premier alinéa de » est remplacée par le mot : « à ».

2° L'article 230-2 est ainsi modifié :

a) Le premier alinéa est ainsi modifié :
– à la première phrase, après le mot : « instruction », sont insérés les mots : «, l'officier de police judiciaire, sur autorisation du procureur de la République ou du juge d'instruction, » et les mots : « au service national de police judiciaire chargé de la lutte contre la criminalité liée aux technologies de l'information » sont remplacés par les mots : « à un organisme technique soumis au secret de la défense nationale, et désigné par décret » ;

– à la dernière phrase, les mots : « l'autorité judiciaire requérante » sont remplacés par les mots : « le procureur de la République, la juridiction d'instruction, l'officier de police judiciaire, sur autorisation du procureur de la République ou du juge d'instruction, ou la juridiction de jugement saisie de l'affaire ou ayant requis l'organisme technique ».

b) La première phrase du second alinéa est supprimée.

3° L'article 230-3 est ainsi modifié :

a) La première phrase du premier alinéa est ainsi rédigée :

« Dès l'achèvement des opérations ou dès qu'il apparaît que ces opérations sont techniquement impossibles ou à l'expiration du délai prescrit ou à la réception de l'ordre d'interruption émanant du procureur de la République, de la juridiction d'instruction, de l'officier de police judiciaire, sur autorisation du procureur de la République ou du juge d'instruction, ou de la juridiction de jugement saisie de l'affaire, les résultats obtenus et les pièces reçues sont retournés par le responsable de l'organisme technique à l'auteur de la réquisition. »

b) Le deuxième alinéa est supprimé.

4° À l'article 230-4, le mot : « judiciaires » est supprimé.

Article 16

Au premier alinéa de l'article 323-3 du Code pénal, la première occurrence du mot : « ou » est remplacée par les mots : «, d'extraire, de détenir, de reproduire, de transmettre, ».

Article 17

I. – Après l'article 323-4 du même code, il est inséré un article 323-4-1 ainsi rédigé :

« Art. 323-4-1. – Lorsque les infractions prévues aux articles 323-1 à 323-3-1 ont été commises en bande organisée et à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État, la peine est portée à dix ans d'emprisonnement et à 150 000 euros d'amende. »

II. – Au 1° de l'article 704 du Code de procédure pénale, la référence : « 323-4 » est remplacée par la référence : « 323-4-1 ».

Article 18

Le titre XXIV du livre IV du Code de procédure pénale est ainsi rétabli :

« Titre XXIV

« DE LA PROCÉDURE APPLICABLE AUX ATTEINTES AUX SYSTÈMES DE TRAITEMENT AUTOMATISÉ DE DONNÉES

« Art. 706-72.-Les articles 706-80 à 706-87-1, 706-95 à 706-103 et 706-105 du présent code sont applicables à l'enquête, à la poursuite, à l'instruction et au jugement des délits prévus à l'article 323-4-1 du Code pénal.

« Les articles mentionnés au premier alinéa du présent article sont également applicables à l'enquête, à la poursuite, à l'instruction et au jugement du blanchiment des mêmes délits ainsi qu'à l'association de malfaiteurs lorsqu'elle a pour objet la préparation de l'un desdits délits. »

Article 19

Après la section 2 du chapitre II du titre XXV du livre IV du même code, est insérée une section 2 bis ainsi rédigée :

« Section 2 bis

« De l'enquête sous pseudonyme

« Art. 706-87-1. – Dans le but de constater les infractions mentionnées aux articles 706-72 et 706-73 et, lorsque celles-ci sont commises par un moyen de communication électronique, d'en rassembler les preuves et d'en rechercher les auteurs, les officiers ou agents de police judiciaire agissant au cours de l'enquête ou sur commission rogatoire peuvent, s'ils sont affectés dans un service spécialisé désigné par arrêté du ministre de l'intérieur et spécialement habilités à cette fin, procéder aux actes suivants sans en être pénalement responsables :

« 1° Participer sous un pseudonyme aux échanges électroniques.

« 2° Être en contact par le moyen mentionné au 1° avec les personnes susceptibles d'être les auteurs de ces infractions ;

« 3° Extraire, acquérir ou conserver par ce moyen les éléments de preuve et les données sur les personnes susceptibles d'être les auteurs de ces infractions ;

« 4° Extraire, transmettre en réponse à une demande expresse, acquérir ou conserver des contenus illicites, dans des conditions fixées par décret.

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

Article 20

I. – Le même code est ainsi modifié :

1° L'article 706-35-1 est ainsi modifié :

a) à la première phrase du premier alinéa, les références : « 225-4-1 à 225-4-9, 225-5 à 225-12 » sont remplacées par les références : « 225-4-1, 225-4-8, 225-4-9, 225-5, 225-6 » ;

b) après le 2°, il est inséré un 2° bis ainsi rédigé :

« 2° bis extraire, acquérir ou conserver par ce moyen les éléments de preuve et les données sur les personnes susceptibles d'être les auteurs de ces infractions ; » ;

2° Après le 2° de l'article 706-47-3, il est inséré un 2° bis ainsi rédigé :

« 2° bis extraire, acquérir ou conserver par ce moyen les éléments de preuve et les données sur les personnes susceptibles d'être les auteurs de ces infractions ; ».

II. – L'article 59 de la loi n° 2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne est ainsi modifié :

1° Au 2°, les mots : « des données » sont remplacés par les mots : « les éléments de preuve et les données » ;

2° Après le même 2°, il est inséré un 3° ainsi rédigé :

« 3° extraire, transmettre en réponse à une demande expresse, acquérir ou conserver des contenus illicites dans des conditions fixées par décret. »

Article 21

À la fin de la première phrase de l'article 706-102-1 du Code de procédure pénale, les mots : « ou telles qu'il les y introduit par saisie de caractères » sont remplacés par les mots : «, telles qu'il les y introduit par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques audiovisuels ».

Article 22

Le troisième alinéa de l'article 706-161 du même code est complété par une phrase ainsi rédigée :

« L'agence peut également verser à l'État des contributions destinées au financement de la lutte contre la délinquance et la criminalité. »

Article 23

Le chapitre Ier du titre IV du livre III de la sixième partie du Code des transports est complété par un article L. 6341-4 ainsi rédigé :

« Art. L. 6341-4. – En cas de menace pour la sécurité nationale, l'autorité administrative peut imposer aux entreprises de transport aérien desservant le territoire national au départ d'aérodromes étrangers la mise en œuvre de mesures de sûreté dont la durée d'application ne peut excéder trois mois. Ces mesures peuvent être reconduites dans les mêmes conditions.

« Les mesures de sûreté mentionnées au premier alinéa sont celles dont la mise en œuvre peut être imposée aux entreprises de transport

aérien en application du règlement (CE) n° 300/2008 du Parlement européen et du Conseil, du 11 mars 2008, relatif à l'instauration de règles communes dans le domaine de la sûreté de l'aviation civile et abrogeant le règlement (CE) n° 2320/2002, des règlements pris pour son application par la Commission européenne et des normes de sûreté prévues par la réglementation nationale.

« Les modalités d'application du présent article sont fixées par décret en Conseil d'État. »

Article 24

[…]

Article 25

I. – Le dernier alinéa du II de l'article L. 222-1 du Code de la sécurité intérieure est supprimé.

II. – Le 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 est supprimé.

Chapitre VI : Dispositions relatives à l'outre-mer

Article 26, 27 et 28

[…]

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

Fait à Paris, le 13 novembre 2014.

François Hollande

Par le Président de la République :

Le Premier ministre,

Manuel Valls

La ministre de l'Écologie, du Développement durable et de l'Énergie,

Ségolène Royal

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

La ministre des Outre-mer,

George Paul Langevin

Décret n° 2014-1576 du 24 décembre 2014 relatif à l'accès administratif aux données de connexion

NOR : PRMD1422750D

Objet : procédure applicable à l'accès, au titre de la sécurité nationale, de la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France ou de la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous, aux données de connexion détenues par les opérateurs de télécommunications électroniques.

Entrée en vigueur : le texte entre en vigueur le 1er janvier 2015.

Notice : le décret crée un chapitre intitulé « Accès administratif aux données de connexion » au titre IV du livre II de la partie réglementaire du Code de la sécurité intérieure. Il définit les données de connexion pouvant être recueillies et dresse la liste des services dont les agents individuellement désignés et dûment habilités peuvent demander à accéder aux données de connexion. Il prévoit les conditions de désignation et d'habilitation de ces agents ainsi que celles de désignation de la personnalité qualifiée placée auprès du Premier ministre à laquelle sont soumises les demandes d'accès en temps différé. Il précise également les modalités de présentation des demandes d'accès en temps différé comme en temps réel, de conservation de ces demandes ainsi que de décision. En cas de décision favorable, il prévoit les conditions de transmission et de conservation des données recueillies. Il fixe les modalités de transmission des demandes à la CNCIS ainsi que celles du suivi général et du contrôle du dispositif par la Commission. Enfin, l'indemnisation des coûts supportés par les opérateurs de communications électroniques, les fournisseurs d'accès à Internet et les hébergeurs lors de la mise en œuvre de la procédure est prévue. Le décret se substitue, en s'en inspirant, aux dispositions jusqu'alors prévues aux articles R. 10-15 à R. 10-21 du Code des postes et des communications électroniques et à celles du chapitre II du décret n° 2011-219 du 25 février 2011.

Le Premier ministre,

Sur le rapport du ministre des Finances et des Comptes publics, du ministre de la Défense, du ministre de l'Intérieur et du ministre de l'Économie, de l'Industrie et du Numérique,

Vu le Code de la sécurité intérieure, notamment ses articles L. 246-1 et suivants ;

Vu le Code des postes et des communications électroniques, notamment ses articles L. 34-1 et R. 10-12 et suivants ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 26 et 34 ;

Vu la loi n° 2004-575 du 21 juin 2004 modifiée pour la confiance dans l'économie numérique, notamment son article 6 ;

Vu 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 ses articles 20 et 57 ;

Vu le décret n° 2011-219 du 25 février 2011 modifié 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 contrôle des interceptions de sécurité en date du 23 octobre 2014 ;

Vu l'avis de l'Autorité de régulation des communications électroniques et des postes en date du 18 novembre 2014 ;

Vu l'avis de la Commission nationale de l'informatique et des libertés en date du 4 décembre 2014 ;

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

Décrète :

Article 1

Le livre II de la partie réglementaire du Code de la sécurité intérieure est ainsi modifié :

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

2° Au chapitre Ier du titre IV, il est créé deux articles R. 241-1 et R. 241-2 ainsi rédigés :

« Art. R. 241-1.-Le Groupement interministériel de contrôle est un service du Premier ministre chargé des interceptions de sécurité et de l'accès administratif aux données de connexion dans les conditions fixées aux chapitres II et VI du présent titre.

« Art. R. 241-2.-Le directeur du Groupement interministériel de contrôle est nommé par arrêté du Premier ministre. »

3° Au titre IV, il est ajouté un chapitre VI ainsi rédigé :

« Chapitre VI

« Accès administratif aux données de connexion

« Art. R. 246-1. – Pour l'application de l'article L. 246-1, les informations et les documents pouvant faire, à l'exclusion de tout autre, l'objet d'une demande de recueil sont ceux énumérés aux articles R. 10-13 et R. 10-14 du Code des postes et des communications électroniques et à l'article 1er du décret n° 2011-219 du 25 février 2011 modifié 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.

« Art. R. 246-2.-I.-Pour l'application du I de l'article L. 246-2, les services relevant des ministres chargés de la Sécurité intérieure, de la Défense, de l'Économie et du Budget dont les agents peuvent solliciter les informations et les documents mentionnés à l'article L. 246-1 sont :

« 1° Au ministère de l'Intérieur :

« a) la Direction générale de la sécurité intérieure ;

« b) à la Direction générale de la police nationale :

« – l'Unité de coordination de la lutte antiterroriste ;

« – la Direction centrale de la police judiciaire ;

« – à la Direction centrale de la sécurité publique : le service central du renseignement territorial ; les services départementaux du renseignement territorial et les sûretés départementales au sein des directions départementales de la sécurité publique ;

« – à la Direction centrale de la police aux frontières : l'Office central pour la répression de l'immigration irrégulière et de l'emploi d'étrangers sans titre au sein de la sous-direction de l'immigration irrégulière et des services territoriaux ;

« c) à la Direction générale de la gendarmerie nationale :

« – à la Direction des opérations et de l'emploi : la sous-direction de la police judiciaire ; la sous-direction de l'anticipation opérationnelle ;

« – au pôle judiciaire : le service technique de recherches judiciaires et de documentation ;

« – les sections de recherches ;

« d) à la préfecture de police :

« – la Direction du renseignement ;

« – la Direction régionale de la police judiciaire ;

« – à la Direction de la sécurité de proximité de l'agglomération parisienne : le service transversal d'agglomération des événements au sein de la sous-direction des services spécialisés de l'agglomération ; la cellule de suivi du plan de lutte contre les bandes au sein de la sous-direction de la police d'investigation territoriale ; la sûreté régionale des transports au sein de la sous-direction régionale de la police des

transports ; les sûretés territoriales au sein des directions territoriales de sécurité de proximité ;

« 2° Au ministère de la Défense :

« a) la Direction générale de la sécurité extérieure ;

« b) la Direction de la protection et de la sécurité de la défense ;

« c) la Direction du renseignement militaire ;

« 3° Au ministère des finances et des comptes publics :

« a) le service à compétence nationale dénommé « Direction nationale du renseignement et des enquêtes douanières » ;

« b) Le service à compétence nationale dénommé « traitement du renseignement et action contre les circuits financiers clandestins ».

« II. – Seuls peuvent solliciter ces informations et ces documents les agents individuellement désignés et dûment habilités par le directeur dont ils relèvent.

« Art. R. 246-3. – Afin de permettre la désignation de la personnalité qualifiée mentionnée au II de l'article L. 246-2 et de ses adjoints, le Premier ministre transmet à la Commission nationale de contrôle des interceptions de sécurité, pour chaque poste à pourvoir, une liste d'au moins trois personnes choisies en raison de leur compétence et de leur impartialité. Ces propositions sont motivées. Elles sont adressées à la Commission au moins trois mois avant le terme du mandat de la personnalité qualifiée et de ses adjoints. La Commission désigne, au sein des listes, la personnalité qualifiée et ses adjoints deux mois au plus tard après avoir reçu les propositions.

«Toute décision désignant la personnalité qualifiée et ses adjoints est notifiée sans délai au Premier ministre par la Commission et publiée au Journal officiel de la République française.

« Les adjoints de la personnalité qualifiée sont au maximum au nombre de quatre.

« Art. R. 246-4. – Les demandes de recueil d'informations ou de documents prévues à l'article L. 246-2 comportent :
« 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 précise des informations ou des documents dont le recueil est demandé et, le cas échéant, la période concernée ;

« c) la date de la demande et sa motivation au regard des finalités mentionnées à l'article L. 241-2.

« Art. R. 246-5. – Le Premier ministre enregistre et conserve pendant une durée maximale de trois ans, dans un traitement automatisé

qu'il met en œuvre, les demandes des agents et les décisions de la personnalité qualifiée ou de ses adjoints.

« Ces demandes et ces décisions sont automatiquement effacées du traitement, sous l'autorité du Premier ministre, à l'expiration de la durée de conservation. Le directeur du groupement interministériel de contrôle adresse chaque année à la Commission nationale de contrôle des interceptions de sécurité un procès-verbal certifiant que l'effacement a été effectué.

« Art. R. 246-6.-Les demandes approuvées par la personnalité qualifiée ou par ses adjoints sont adressées par le groupement interministériel de contrôle, sans les éléments mentionnés aux a et c de l'article R. 246-4, aux opérateurs et aux personnes mentionnés à l'article L. 246-1. Ces derniers transmettent sans délai les informations ou les documents demandés au groupement interministériel de contrôle, qui les met à disposition de l'auteur de la demande pour exploitation.

« La transmission des informations ou des documents par les opérateurs et les personnes mentionnés à l'article L. 246-1 au groupement interministériel de contrôle est effectuée selon des modalités assurant leur sécurité, leur intégrité et leur suivi.

« Le Premier ministre enregistre et conserve pendant une durée maximale de trois ans, dans un traitement automatisé qu'il met en œuvre, les informations ou les documents transmis par les opérateurs et les personnes mentionnés à l'article L. 246-1. Ces informations ou ces documents sont automatiquement effacés du traitement dans les conditions prévues à l'article R. 246-5.

« Art. R. 246-7. – Les demandes de recueil d'informations ou de documents, impliquant sollicitation du réseau et transmission en temps réel, prévues à l'article L. 246-3 comportent, outre leur date et leur motivation au regard des finalités mentionnées à l'article L. 241-2, la nature précise des informations ou des documents dont le recueil est demandé et la durée de ce recueil.

« Les demandes des ministres ou des personnes spécialement désignées par eux et les décisions du Premier ministre ou des personnes spécialement désignées par lui sont enregistrées, conservées et effacées dans les conditions prévues à l'article R. 246-5.

« Les demandes approuvées par le Premier ministre ou par les personnes spécialement désignées par lui sont adressées par le Groupement interministériel de contrôle, sans leur motivation, aux opérateurs et aux personnes mentionnés à l'article L. 246-1.

« La sollicitation du réseau prévue à l'article L. 246-3 est effectuée par l'opérateur qui exploite le réseau. Les informations ou les documents demandés sont transmis, enregistrés, conservés et effacés dans les conditions prévues à l'article R. 246-6.

« Art. R. 246-8. – La Commission nationale de contrôle des interceptions de sécurité dispose d'un accès permanent aux traitements automatisés mentionnés aux articles R. 246-5, R. 246-6 et R. 246-7.

« L'autorité ayant approuvé une demande de recueil d'informations ou de documents fournit à la Commission tous éclaircissements que celle-ci sollicite sur cette demande.

« Art. R. 246-9. – Les coûts identifiables et spécifiques supportés par les opérateurs et les personnes mentionnés à l'article L. 246-1 pour la transmission des informations ou des documents font l'objet d'un remboursement par l'État par référence aux tarifs et selon des modalités fixés par un arrêté des ministres chargés de la Sécurité intérieure, de la Défense, de l'Économie, du Budget et des Communications électroniques. »

4° La ligne :

figurant dans le tableau des articles R. 285-1, R. 286-1 et R. 287-1 est remplacée par les lignes suivantes :

R. 241-1 et R. 241-2	Résultant du décret n° 2014-1576 du 24 décembre 2014 relatif à l'accès administratif aux données de connexion
R. 242-2, R. 242-4 à R. 242-8 et R. 244-1 à R. 244-6	Résultant du décret n° 2013-1113 relatif aux dispositions des livres Ier, II, IV et V de la partie réglementaire du Code de la sécurité intérieure (décrets en Conseil d'État et décrets simples)
R. 246-1 à R. 246-9	Résultant du décret n° 2014-1576 du 24 décembre 2014 relatif à l'accès administratif aux données de connexion

5° La ligne :

R. 242-1 à R. 244-6	Résultant du décret n° 2013-1113 relatif aux dispositions des livres Ier, II, IV et V de la partie réglementaire du Code de la sécurité intérieure (décrets en Conseil d'État et décrets simples)

figurant dans le tableau de l'article R. 288-1 est remplacée par les lignes suivantes :

R. 241-1 et R. 241-2	Résultant du décret n° 2014-1576 du 24 décembre 2014 relatif à l'accès administratif aux données de connexion
R. 242-2	Résultant du décret n° 2013-1113 relatif aux dispositions des livres Ier, II, IV et V de la partie réglementaire du Code de la sécurité intérieure (décrets en Conseil d'État et décrets simples)
R. 246-1 à R. 246-9	Résultant du décret n° 2014-1576 du 24 décembre 2014 relatif à l'accès administratif aux données de connexion

Article 2

I. – Sont abrogés :

1° Les articles R. 242-1 et R. 242-3 du Code de la sécurité intérieure ;

2° Les articles R. 10-15 à R. 10-21 du Code des postes et des communications électroniques ;

3° Le chapitre II du décret du 25 février 2011 susvisé.

II. – La seconde phrase de l'article R. 10-22 du Code des postes et des communications électroniques est supprimée.

III. – À l'article 12 du décret du 25 février 2011 susvisé, le mot : « 10 » est supprimé.

Article 3

Le présent décret s'applique sur l'ensemble du territoire de la République.

Il entre en vigueur le 1er janvier 2015.

Toutefois, les délais mentionnés à l'article R. 246-3 du Code de la sécurité intérieure ne sont pas applicables à la première désignation, après l'entrée en vigueur du présent décret, de la personnalité qualifiée et de ses adjoints mentionnés au II de l'article L. 246-2 du même code.

Article 4

Le ministre des Finances et des Comptes publics, le ministre de la Défense, le ministre de l'Intérieur, le ministre de l'Économie, de l'Industrie et du Numérique et la ministre des Outre-mer 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 24 décembre 2014

Manuel Valls
Par le Premier ministre :

Le ministre des Finances et des Comptes publics,
Michel Sapin

Le ministre de la Défense,
Jean-Yves Le Drian

Le ministre de l'Intérieur,
Bernard Cazeneuve

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

La ministre des Outre-mer,
George Pau-Langevin

Chapitre III

Jurisprudence et actualités parlementaires

Arrêt n° 5658 du 15 octobre 2014 (14-85.056 ; 12-82.391) – Cour de cassation – chambre criminelle – ECLI : FR : CCASS : 2014 : CR05658

Convention européenne des droits de l'homme

Rejet

Demandeur(s) : M. Daouda X...

I – Sur le pourvoi formé contre l'arrêt du 2 mars 2012 :

Sur le moyen unique de cassation, pris de la violation des articles 8 de la Convention européenne des droits de l'homme, préliminaire, 14, 19, 31, 40, 75, 591 et 593 du Code de procédure pénale ;

« en ce que la chambre de l'instruction a refusé de prononcer l'annulation des procès-verbaux relatifs à la géolocalisation du véhicule "Renault Trafic" par pose de balise géolocalisation par satellite (GPS) ;

« aux motifs que sur la nullité alléguée du dispositif de géolocalisation au regard de la violation de l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales ; qu'il résulte des articles 171 et 802 du Code de procédure pénale que la méconnaissance d'une formalité substantielle ne peut être invoquée à l'appui d'une demande d'annulation d'acte ou de pièce de procédure que si elle a porté atteinte aux intérêts de la partie qu'elle concerne ; que M. Daouda X... sollicite l'annulation de procès-verbaux relatifs à la mise en place d'un procédé de géolocalisation par satellite sur un véhicule utilisé par

M. Malek Y... en violation des dispositions relatives au respect de la vie privée de ce dernier ; que le requérant est sans qualité pour se prévaloir d'un droit, soit le respect de la vie privée de M. Y..., qui appartient en propre à ce dernier et ne lui appartient donc pas ; qu'il n'y a pas lieu en conséquence de faire droit à ce moyen ; que cependant, il résulte de l'examen de la procédure que le recours au procédé de géolocalisation a porté atteinte aux intérêts de M. X..., même si cela a été de façon indirecte, puisque l'ADN du requérant a été découvert sur un des objets placés sous scellé suite à la perquisition opérée lors de l'interpellation de M. Y... ; qu'il y a donc lieu d'examiner les autres moyens de la requête ; que sur la nullité alléguée du dispositif de géolocalisation au regard de la violation du principe de légalité ; qu'il est soutenu que le procédé de géolocalisation mis en place par les fonctionnaires de police de la brigade de répression du banditisme, n'est prévu par aucune disposition légale et qu'il ne peut en particulier se fonder sur les dispositions de l'article 14 du Code de procédure pénale ; que ce procédé, qui ne répond pas non plus aux principes de prévisibilité, de clarté et de précision, a été effectué en dehors de tout contrôle de l'autorité judiciaire, principes pourtant rappelés par la jurisprudence européenne et celle de la Cour de cassation ; qu'il résulte de l'examen de la procédure, que suite à la découverte, en stationnement dans le bois de Vincennes (Paris 12e), par un effectif de la brigade anti-criminalité du commissariat de police de Vincennes (94), dans l'après-midi du 18 mai 2010, d'un véhicule utilitaire "Renault Master" faussement immatriculé [...], un déplacement était effectué par les enquêteurs de la brigade de répression du banditisme, les caractéristiques du véhicule correspondant à ceux habituellement utilisés par des malfaiteurs spécialisés dans les attaques de fourgons blindés et ce lieu étant un lieu récurant de remise de véhicules volés ; que ceux-ci découvraient dans les environs immédiats de ce véhicule, deux autres utilitaires de même gabarit, également volés et faussement immatriculés ; que sur l'un d'eux, un véhicule de marque "Renault Trafic" faussement immatriculé [...] et estampillé air climat, il était remarqué un léger prééquipement par découpage d'une fenêtre d'observation dans une des vitres arrières opaques, laissant penser aux policiers qu'ils avaient affaire à un véhicule destiné à la surveillance ; qu'un dispositif de surveillance physique par les fonctionnaires de police était mis en place jusqu'au 19 mai 2010 à 0 heure 40 sur les trois véhicules suspects et que parallèlement à ces observations, un engin de localisation était placé sur une partie extérieure du véhicule "Renault Trafic" [...] le 19 mai 2010 à 0 heure 13 ; que cet engin était récupéré après remorquage du véhicule, le 21 mai 2010 à 21 heures 51 ; qu'il est joint à la procédure, l'historique complet de la balise indiquant les dates et heures de localisation, les distances parcourues, les temps de trajets et pauses ainsi que les adresses d'arrêts ; que ce véhicule était retrouvé à Champigny-sur-Marne (94) le 20 mai 2010 à 21 heures 40 ; que les surveillances effectuées sur les lieux permettaient de repérer un individu s'affairant au niveau de la porte latérale droite puis quittant le véhicule, porteur d'un sac manifestement lourd en direction d'une impasse ; qu'il était perdu de vue puis

repéré à nouveau sortant d'un pavillon pour se diriger vers un véhicule 4x4 stationné à proximité avant de retourner dans le pavillon ; qu'ayant été aperçus par une femme présente à l'intérieur du pavillon et qui s'enquérait auprès d'eux de la raison de leur présence, les policiers l'invitaient à venir sur le perron, le groupe étant ensuite rejoint par un homme qui était alors interpellé à 22 heures 55 ; que celui-ci déclarait se nommer M. Malek Y... et résider à cette adresse ; que les opérations de perquisition amenaient la découverte de deux sacs renfermant notamment des cagoules, des gilets pare-balles, des armes, des grenades et des munitions que l'intéressé reconnaissait avoir déposé dans le jardin mitoyen après les avoir sortis du véhicule "Renault Trafic" ; que l'analyse des scellés par le laboratoire de police scientifique de Paris amenait la mise à jour de plusieurs profils génétiques dont celui de M. X... ; que qu'il résulte des investigations que le véhicule "Renault Trafic", faussement immatriculé [...] et initialement immatriculé sous le numéro [...], appartenait à la société Selasa Services sise [...] à Paris (12e) et qu'il avait été déclaré volé auprès de la brigade de gendarmerie de Fosse (95) depuis le 29 mars 2010 ; qu'au surplus, l'utilisation d'un système de géolocalisation par satellite (GPS) installé sur un véhicule afin de surveiller ses déplacements ne fait l'objet d'aucun texte spécifique en l'état du droit français ; qu'il convient, en conséquence, d'analyser ce dispositif au regard des textes de procédure pénale en vigueur à ce jour ; que les articles 12, 14 et 41 du Code de procédure pénale confient à la police judiciaire le soin de «constater les infractions à la loi pénale, d'en rassembler les preuves et d'en rechercher les auteurs» sous le contrôle du procureur de la République ; que les techniques de filatures et de surveillances effectuées par les policiers dans le cadre de leurs enquêtes trouvent leur fondement dans ces dispositions ; que le système de balise ne procède pas d'une autre nature dans la mesure où tant la mise en place que le retrait de l'appareil n'ont nécessité d'intrusion dans le véhicule en question ou dans un quelconque lieu privé ; que le relevé des données collectées informatiquement ne présente pas de caractère de contrainte ni de coercition s'agissant de données techniques qui auraient pu être de la même façon recueillies "de visu" par les fonctionnaires de police ; que les investigations effectuées selon ce procédé sont moins susceptibles de porter atteinte aux droits d'une personne que des méthodes de surveillance par des moyens visuels ou acoustiques qui révèlent plus d'informations sur la conduite, les opinions ou les sentiments de la personne qui en fait l'objet ; que la base légale de la géolocalisation n'est donc pas contestable, que l'exigence normative est donc remplie et qu'il est légitime qu'elle fasse l'objet d'une interprétation judiciaire ; que s'agissant de surveillances secrètes par les autorités publiques, il convient donc de vérifier les circonstances de la cause, en particulier au regard de la nature, de l'étendue et la durée des mesures, les raisons de leur mise en place ou le type de recours fourni par le droit interne ; qu'en l'espèce, la mise en place d'une surveillance par le moyen d'une balise de géolocalisation s'est effectuée sur un véhicule qui, après vérifications, s'est avéré volé et faussement immatriculé ; qu'il était

stationné dans un lieu particulièrement passant (bois de Vincennes), proche de nombreux axes routiers empruntés habituellement par les convoyeurs de fonds pour alimenter les nombreuses banques aux alentours, desservant tout l'est parisien et pouvant servir de base stratégique pour des malfaiteurs susceptibles de préparer des projets criminels ; que ce véhicule présentait, à travers ses caractéristiques et notamment la présence d'une ouverture suspecte dans la carrosserie, tous les signes d'un instrument destiné à être utilisé pour la commission d'infractions pénales ; qu'il a été constaté la présence, à proximité de ces lieux, de deux autres véhicules de même type signalés volés ; que l'utilisation de la balise a donc été justifiée par la nécessité de vérifier l'usage et la destination d'un véhicule frauduleusement soustrait à son propriétaire et l'existence d'une éventuelle préparation d'actes criminels, en particulier d'attaques de fourgons blindés ou d'agences bancaires régulièrement commis en région parisienne, d'en rechercher l'organisation, d'en identifier les participants et de prévenir leur commission et ce de manière discrète et efficace, en raison du professionnalisme de ce type de délinquance ; que les infractions de cette nature, troublent de façon évidente l'ordre public par les conséquences tant financières qu'humaines à travers l'utilisation d'armes et la détermination de leurs auteurs dont la dangerosité concerne non seulement les victimes directes de leurs méfaits mais aussi les personnes se trouvant à proximité ainsi que les services de police intervenants pour faire cesser l'infraction ou procéder à l'arrestation des auteurs ; qu'en conséquence, la mesure a répondu à une finalité légitime proportionnée à la gravité des infractions commises ou suspectées au regard de l'ordre public et strictement limitée aux nécessités de la manifestation de la vérité dans la mesure où la brigade de répression du banditisme, service de police spécialisé dans le grand banditisme, était au fait des modes opératoires mis en place par des équipes de malfaiteurs professionnels et dont la soustraction de véhicules utilitaires constitue un des actes préparatoires aux infractions projetées ; que contrairement aux assertions de la requête, on ne peut reprocher aux enquêteurs, au vu des éléments qu'ils ont constatés, la mise en place de moyens destinés à exercer pleinement la mission générale de police judiciaire qui leur est confiée par la loi sous le contrôle du procureur de la République, parmi lesquels la surveillance par une nouvelle technologie ; que cette mesure, dont l'aspect technique est connu par l'ensemble des malfaiteurs qui ont conscience qu'ils peuvent faire l'objet de surveillances et en prévoir les conséquences, a été parfaitement circonscrite dans le temps puisqu'elle a été mise en place pour une durée de l'ordre de 48 heures, durée n'excédant pas le temps nécessaire à la manifestation de la vérité qui s'imposait pour parvenir au démantèlement d'un réseau structuré de délinquants ; que les procès-verbaux relatifs à la mise en place de la balise et à son exploitation figurent au dossier (D1433, D1434 et D1471) et peuvent être contradictoirement discutés à tout moment de la procédure et soumis au contrôle de légalité de la chambre de l'instruction, les conditions d'exercice des droits de la défense n'étant donc aucunement compromis ; que les circonstances de

la cause démontrent que le dispositif présente des garanties adéquates et suffisantes contre l'arbitraire où les abus dans l'utilisation des techniques de surveillance, qu'il n'est en rien attentatoire à la vie privée ou aux droits de la personne et répond aux exigences d'accessibilité et prévisibilité de la loi pénale, donc de sécurité juridique ; qu'en conséquence, les dispositions légales internes comme les dispositions conventionnelles ayant été respectées au regard du principe de légalité, le moyen sera rejeté ; que sur la nullité alléguée du dispositif de géolocalisation au regard du principe de loyauté de l'administration de la preuve, l'article 6, § 1, de la Convention européenne des droits de l'homme énonce que "Toute personne a droit à ce que sa cause soit entendue équitablement par un tribunal qui décidera du bien-fondé de toute accusation en matière pénale dirigée contre elle" *; qu'il est soutenu que le dispositif de surveillance par géolocalisation par satellite (GPS), interdit par la loi, a méconnu l'exigence de loyauté dans la mesure où la preuve recueillie en violation de l'article 8 a irrémédiablement vicié la procédure en ce qu'elle a influencé de manière décisive notamment la mise en cause de M. X..., et donc porté atteinte à l'équité du procès protégé par l'article 6 ; que cette équité comporte aussi une exigence de légalité relative au déroulement de la procédure visant à protéger la personne poursuivie contre les abus de pouvoir ; qu'en complément des motifs développés pour écarter le premier moyen fondé sur la violation de l'article 8 de la Convention européenne des droits de l'homme auxquels il convient de se référer, l'utilisation par les services de police d'un moyen de géolocalisation par satellite au cours de l'enquête de flagrance a été faite sans aucun artifice ni stratagème ; que de façon générale, l'efficacité des investigations suppose le plus souvent qu'elles soient conduites de manière discrète, voire secrète, l'emploi de telles méthodes n'étant pas considéré par lui-même, comme étant incompatible avec les exigences du procès équitable ; que les enquêteurs n'ont pas outrepassé leurs droits en ayant utilisé une possibilité technique existante, même si elle n'est pas encore expressément prévue par la loi mais qui s'inscrit dans des textes plus généraux sachant qu'il n'existe pas de liste limitative des moyens d'investigation ; que dans un domaine couvert par le droit écrit, la loi est le texte en vigueur tel que les juridictions compétentes l'interprètent en ayant eu égard au besoin, à des techniques nouvelles ; que ce procédé n'a pas, par nature, pour résultat de compromettre les conditions d'exercice des droits de la défense ; que si l'admissibilité des preuves en tant que telles relève en premier chef du droit interne, la jurisprudence européenne n'exclut cependant pas par principe et* in abstracto *d'examiner la recevabilité de preuves dont la légalité est contestée au regard du caractère équitable du procès, contrairement à ce qu'affirme le conseil du requérant ; que l'examen concret du dossier ne révèle ni ruse ni détournement de procédure et qu'il convient de rappeler que figurent en procédure les procès-verbaux relatifs à la mise en place de la balise sur un véhicule frauduleusement soustrait et faussement immatriculé, et à son exploitation ; que l'exigence de loyauté, garante de l'équité du procès pénal a été respectée ; que contrairement aux affirmations de la requête, figurent au dossier les*

procès-verbaux initiaux de surveillance (D3, D6, D10 et D11), les procès-verbaux relatant la pose de la balise et son exploitation (D1433 et D1434) ainsi que sous cote judiciaire n°17, l'historique complet de la balise (D1471) ; que ces pièces peuvent donc être contradictoirement discutées ; que le moyen sera, en conséquence, rejeté ;

« 1°) alors qu'aux termes de la jurisprudence de la chambre criminelle, la technique dite de géolocalisation constitue une ingérence dans la vie privée, qui, en raison de sa gravité, doit être exécutée sous le contrôle d'un juge ; que la chambre de l'instruction ne pouvait dès lors considérer que la géolocalisation constitue un dispositif "qui n'est en rien attentatoire à la vie privée ou aux droits de la personne" pour refuser de constater la violation de l'article 8 de la Convention européenne résultant de la mise en place d'un tel procédé sous le seul contrôle du procureur de la République dans le cadre d'une enquête préliminaire ;

« 2°) alors qu'en vertu de l'article 8, § 2, de la Convention européenne, toute ingérence dans le droit au respect de la vie privée doit reposer sur une base légale suffisamment claire et précise ; que "dans le contexte de mesures de surveillance secrète la loi doit user de termes assez clairs pour indiquer à tous de manière suffisante en quelles circonstances et sous quelles conditions elle habilité la puissance publique à recourir à de telles mesures" *(CEDH, Ch. 2 août 1984,* Malone c. Royaume-Uni, *n° 8691/79, § 67) ; que les articles 12, 14 et 41 du Code de procédure pénale confient à la police judiciaire le soin de constater les infractions à la loi pénale, d'en rassembler les preuves et d'en rechercher les auteurs sous le contrôle du procureur de la République ; qu'en conséquence, en l'espèce, le droit français applicable à l'époque de l'enquête n'indiquait pas avec suffisamment de clarté l'étendue et les modalités d'exercice du pouvoir d'appréciation des autorités dans le domaine considéré, de sorte qu'il y a eu violation de l'article 8 de la Convention européenne ; »*

Attendu que, pour écarter le moyen de nullité, tiré de l'atteinte à l'intimité de la vie privée et du défaut de qualité du procureur de la République pour autoriser la pose d'une balise sur un véhicule s'avérant être volé et permettre de retrouver ses déplacements ultérieurs, l'arrêt prononce par les motifs repris au moyen ;

Attendu qu'en se déterminant ainsi, la chambre de l'instruction a justifié sa décision, dès lors que la pose d'un procédé de géolocalisation à l'extérieur d'un véhicule volé et faussement immatriculé est étrangère aux prévisions de l'article 8, § 2, de la Convention européenne des droits de l'homme ;

D'où il suit que le moyen ne saurait être admis ;

II – Sur le pourvoi formé contre l'arrêt du 3 juillet 2014 :

Sur le moyen unique de cassation, pris de la violation des articles 6 de la Convention européenne des droits de l'homme, préliminaire, 175, 591 et 593 du Code de procédure pénale ;

« en ce que la chambre de l'instruction a confirmé la mise en accusation de M. X... des chefs de tentative de vol avec armes commis en bande organisée, association de malfaiteurs en vue de commettre ce crime, acquisition, détention, transport d'armes et de munitions de 1re et 4e catégories, détention et transport d'explosifs et de produits incendiaires, recel en bande organisée de vol, tentative de meurtre sur personne dépositaire de l'autorité publique commis en bande organisée, tentative de meurtre commis en bande organisée, destructions, dégradations, détériorations de véhicules par l'effet de substances explosives, d'un incendie ou d'un moyen de nature à créer un danger pour les personnes commis en bande organisée, meurtre en bande organisée sur personne dépositaire de l'autorité publique ;

« aux motifs que M. X... était mis en examen des chefs d'association de malfaiteurs en vue de la préparation d'un ou plusieurs crimes notamment de vol avec arme en bande organisée, détention ou transport d'armes de 1re catégorie, de munitions en bande organisée ; qu'il était mis en examen supplétivement le 31 mai 2011 des chefs de meurtre avec préméditation d'une personne dépositaire de l'autorité publique dans l'exercice de ses fonctions en bande organisée, tentatives de meurtres avec préméditation de personnes dépositaires de l'autorité publique dans l'exercice de leurs fonctions en bande organisée, tentatives de meurtres avec préméditation en bande organisée, vols sous la menace d'une arme en bande organisée, destructions volontaires par incendie ou moyen dangereux en bande organisée, acquisition d'armes de 1re catégorie, de munitions, d'explosifs et engins explosifs en bande organisée, recels en bande organisée de vols en bande organisée ; qu'il était de nouveau mis en examen supplétivement du chef de tentative de vol avec arme en bande organisée ; qu'au soutien du renvoi de M. X... devant la cour d'assises de Paris (appelant, appel parquet non soutenu), les magistrats instructeurs ont retenu dans leur ordonnance de clôture du 2 avril 2014 les motifs suivants :« M. X... paraît lui aussi être l'un des membres du commando impliqué dans la fusillade. En effet, M. X... présente par ailleurs des brûlures occasionnées en mai 2010 (cf. audition de M. Mathieu Z...) pouvant correspondre, notamment concernant leur localisation, à celles décrites par l'un des témoins de Villiers sur Marne (cf. audition de M. Hicham A...). Ses explications concernant la présence de son ADN sur un pistolet-mitrailleur découvert suite à l'interpellation de M. Y... sont contredites tant par les retranscriptions d'écoutes téléphoniques communiquées par le juge d'instruction de Senlis que par les déclarations des témoins qui ont participé à la promenade en vélo et qui tous déclarent que M. X... n'étaient pas avec eux. Quant à ses explications sur l'origine de ses blessures, aucun élément ne permet de les confirmer, sachant que s'il avait effectivement incendié un véhicule, une procédure aurait été établie par les pompiers ou les forces de l'ordre. Enfin, lors de leur première audition, aucun des proches de M. X... n'a parlé de son départ au Sénégal au moment des faits, ce qui aurait pu prouver dès le début de la procédure son innocence alors qu'il était soupçonné de faits

gravissimes. Au contraire, certains d'entre eux ont même indiqué qu'il n'avait pas quitté la France en mai 2010; que ce n'est que trois ans plus tard qu'il a raconté un périple en Afrique effectué sous couvert du passeport de son frère. Ce voyage a ensuite été confirmé par ses proches, sachant que certains d'entre eux bénéficiaient de permis de visite depuis longtemps. Dès lors, aucun élément objectif ne permet de confirmer cet alibi, d'autant plus que les renseignements recueillis auprès des autorités des pays qu'il dit avoir traversé permettent de douter de la véracité de son récit, que son retour en avion sous l'identité de son frère n'a pu être confirmé, que l'un de ses entraîneurs (cf. M. Emmanuel B…) se souvient de sa présence au mois de mai. En conséquence, il y a lieu de suivre les réquisitions du procureur de la République concernant M. X…, en suivant la même analyse que celle développée au sujet de M. Olivier C…, et d'ordonner la mise en accusation et le renvoi du mis en examen devant la cour d'assises des chefs de tentative de vol avec armes commis en bande organisée au préjudice de la société Loomis, association de malfaiteurs en vue de commettre un crime de vol avec arme en bande organisée, acquisition, détention, transport d'armes et de munitions de 1re et 4e catégories, classées désormais sous la nouvelle catégorie A, détention et transport d'explosifs et de produits incendiaires, recel en bande organisée de vol (deux véhicules "Renault Trafic"), tentative de meurtre sur personne dépositaire de l'autorité publique commis en bande organisée au préjudice de MM. Benoit D…, Gaëtan E…, Franck F…, Rony G…, Arnaud H…, tentative de meurtre commis en bande organisée commis sur les personnes de Mme Marie Hélène I…, M. Clément J…, Mme Martine K…, M. Bernard L…, destructions, dégradations, détériorations de véhicules par l'effet de substances explosives d'un incendie ou d'un moyen de nature à crée un danger pour les personnes commis en bande organisée commis au préjudice du commissariat de Villeneuve-Saint-Georges (véhicule de police "Peugeot 308"), de la compagnie de sécurisation et d'intervention du Val-de-Marne (véhicule de police "Renault Scénic"), de Mme Marie-hélène I… ("Renault Clio"), de Mme Martine K… ("Peugeot 308"), de Mme Nathalie M… ("Citroën C3"), de M. Bernard M… et de la société Vin Malin (véhicule semi-remorque "Scannia"), de M. Jean Sébastien N… (véhicule "Peugeot 406"), de M. Mickël O… (véhicule "Mercedes"), de M. Gregory P… (véhicule "Toyota"), meurtre en bande organisée commis sur Aurélie Q…, personne dépositaire de l'autorité publique, tentative de meurtre sur personne dépositaire de l'autorité publique commis en bande organisée au préjudice de M. Thierry R…, vol d'un véhicule "Hyundai" avec armes en bande organisée commis au préjudice de M. Guillaume S…, tentative de vol d'un véhicule "Toyota" avec armes en bande organisée commis au préjudice de M. Jean Louis T…, et de Mme Nathalie U…, vol d'un véhicule "Peugeot 206" avec arme et en bande organisée commis au préjudice de M. Franck V…, destructions, dégradations, détérioration de véhicules par l'effet de substances explosives, d'un incendie ou d'un moyen de nature à créer un danger pour les personnes commis en bande organisée commis au préjudice de la société Selsa Service ("Renault Trafic" volé), de la

commune de Villiers-sur-Marne (véhicule de police municipale "Peugeot 307") de M. Guillaume S... (véhicule "Hyundai"), de M. Jean Louis T... et de Mme Nathalie U... (véhicule "Toyota"), vol d'un véhicule "Mercedes" avec armes en bande organisée commis au préjudice de M. Sylvain W... et de Mme Brigitte XX... ; que M. X... nie toute implication dans les faits reprochés ; qu'en dépit de ses dénégations, la présence de son ADN sur la queue de détente du pistolet-mitrailleur hk découvert dans un sac de sport que M. Y... avait dissimulé dans le jardin de son voisin ; que ses explications contredites tant par les retranscriptions d'écoutes téléphoniques communiquées par le juge d'instruction de Senlis que par les déclarations des témoins ayant participé à la promenade en vtt ; que ses déclarations quant à l'origine de ses blessures qu'aucun élément ne permet de confirmer, blessures contemporaines à la tentative de vol à mains armées, éléments à mettre en parallèle avec la déposition du témoin de Villiers-sur-Marne ayant assisté à l'incendie du véhicule "Renault Trafic" durant lequel un des malfaiteurs avait été brûlé au bras gauche ; que son changement de version sur la genèse de ses blessures, les divergences d'appréciation de son entourage ainsi que son alibi quant à la date des faits, alibi tardif et non confirmé par les investigations effectuées, sont autant d'éléments venant conforter sa participation aux faits reprochés ; qu'en conséquence et nonobstant les éléments du mémoire, il existe à l'encontre de M. X... des charges suffisantes d'avoir commis les crimes et délits justifiant son renvoi devant la cour d'assises de Paris ;

« alors qu'il appartenait à la chambre de l'instruction de caractériser la matérialité des infractions reprochées à M. X..., et notamment des faits de meurtre ; qu'en procédant à sa mise en accusation sur le seul fondement de la présence de ses traces ADN sur une arme retrouvée chez M. Y..., dont il n'est pas mentionné qu'elle ait servi au meurtre, et de brûlures dont M. X... faisait état et dont il a été péremptoirement déduit qu'elles avaient été causées par l'incendie provoqué par un véhicule utilitaire au moment des faits, la cour d'appel n'a pas légalement justifié sa décision » ;

Attendu que les motifs de l'arrêt attaqué mettent la Cour de cassation en mesure de s'assurer que la chambre de l'instruction, après avoir exposé les faits et répondu comme elle le devait aux articulations essentielles du mémoire dont elle était saisie, a relevé l'existence de charges qu'elle a estimé suffisantes contre M. X... pour ordonner son renvoi devant la cour d'assises sous les accusations susvisées ;

Qu'en effet, les juridictions d'instruction apprécient souverainement si les faits retenus à la charge de la personne mise en examen sont constitutifs d'une infraction, la Cour de cassation n'ayant d'autre pouvoir que de vérifier si, à supposer ces faits établis, la qualification justifie la saisine de la juridiction de jugement ;

Que, dès lors, le moyen ne peut qu'être écarté ;

Et attendu que la procédure est régulière et que les faits, objet principal de l'accusation, sont qualifiés crime par la loi ;

REJETTE les pourvois ;

DIT n'y avoir lieu à application de l'article 618-1 du Code de procédure pénale

Président : M. Guérin

Rapporteur : M. Moreau, conseiller

Avocat général : M. Lacan

Avocat(s) : SCP Spinosi et Sureau ; SCP Waquet, Farge et Hazan

Arrêt n° 617 du 6 mars 2015 (14-84.339) – Cour de cassation – assemblée plénière – ECLI : FR : CCASS : 2015 : AP00617

Preuve

Cassation

Demandeur(s) : M. Meshal X… ; M. Abdelgrani Y…

Sur le pourvoi formé par M. Y…

Attendu que le demandeur n'a produit aucun mémoire à l'appui de son pourvoi ;

Sur le pourvoi formé par M. X… :

Attendu, selon l'arrêt attaqué, rendu sur renvoi après cassation (chambre criminelle, 7 janvier 2014, n° 13-85.246), qu'à la suite d'un vol avec arme, une information a été ouverte au cours de laquelle le juge d'instruction a, par ordonnance motivée 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 deux cellules contiguës d'un commissariat de police en vue du placement en garde à vue de MM. Z… et X…, soupçonnés d'avoir participé aux faits ; que ceux-ci ayant communiqué entre eux pendant leurs périodes de repos, des propos de M. X… par lesquels il s'incriminait lui-même ont été enregistrés ; que celui-ci, mis en examen et placé en détention provisoire, a déposé une requête en annulation de pièces de la procédure ;

Sur le premier moyen :

Vu l'article 6 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales ainsi que les articles préliminaire et 63-1 du Code de procédure pénale, ensemble le principe de loyauté des preuves et le droit de ne pas contribuer à sa propre incrimination ;

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 que, pour rejeter la demande d'annulation, présentée par M. X..., des procès-verbaux de placement et d'auditions en garde à vue, de l'ordonnance autorisant la captation et l'enregistrement des paroles prononcées dans les cellules de garde à vue, des pièces d'exécution de la commission rogatoire technique accompagnant celle-ci et de sa mise en examen, prise de la violation du droit de se taire, d'un détournement de procédure et de la déloyauté dans la recherche de la preuve, l'arrêt retient que plusieurs indices constituant des raisons plausibles de soupçonner que M. X... avait pu participer aux infractions poursuivies justifient son placement en garde à vue, conformément aux exigences de l'article 62-2, alinéa 1, du Code de procédure pénale, que l'interception des conversations entre MM. Z... et X... a eu lieu dans les conditions et formes prévues par les articles 706-96 à 706-102 du Code de procédure pénale, lesquelles n'excluent pas la sonorisation des cellules de garde à vue contrairement à d'autres lieux visés par l'article 706-96, alinéa 3, du même code, que les intéressés, auxquels a été notifiée l'interdiction de communiquer entre eux, ont fait des déclarations spontanées, hors toute provocation des enquêteurs, et que le droit au silence ne s'applique qu'aux auditions et non aux périodes de repos ;

Attendu qu'en statuant ainsi, alors qu'au cours d'une mesure de garde à vue, le placement, durant les périodes de repos séparant les auditions, de deux personnes retenues dans des cellules contiguës préalablement sonorisées, de manière à susciter des échanges verbaux qui seraient enregistrés à leur insu pour être utilisés comme preuve, constitue un procédé déloyal d'enquête mettant en échec le droit de se taire et celui de ne pas s'incriminer soi-même et portant atteinte au droit à un procès équitable, la chambre de l'instruction a violé les textes et principes susvisés ;

PAR CES MOTIFS, et sans qu'il y ait lieu de statuer sur le second moyen :

Sur le pourvoi formé par M. Y... :

Le rejette ;

Sur le pourvoi formé par M. X... :

CASSE ET ANNULE, en toutes ses dispositions, l'arrêt rendu le 5 juin 2014, entre les parties, par la chambre de l'instruction de la cour d'appel de Paris ; remet, en conséquence, la cause et les parties dans l'état où elles se trouvaient avant ledit arrêt et, pour être fait droit, les renvoie devant la chambre de l'instruction de la cour d'appel de Paris, autrement composée.

Président : M. Terrier, président de chambre le plus ancien faisant fonction de premier président

Rapporteur : M. Zanoto, assisté de M. Cardini, auditeur au service de documentation, des études et du rapport

Avocat général : M. Boccon-Gibod, premier avocat général

Avocat(s) : SCP Spinosi et Sureau