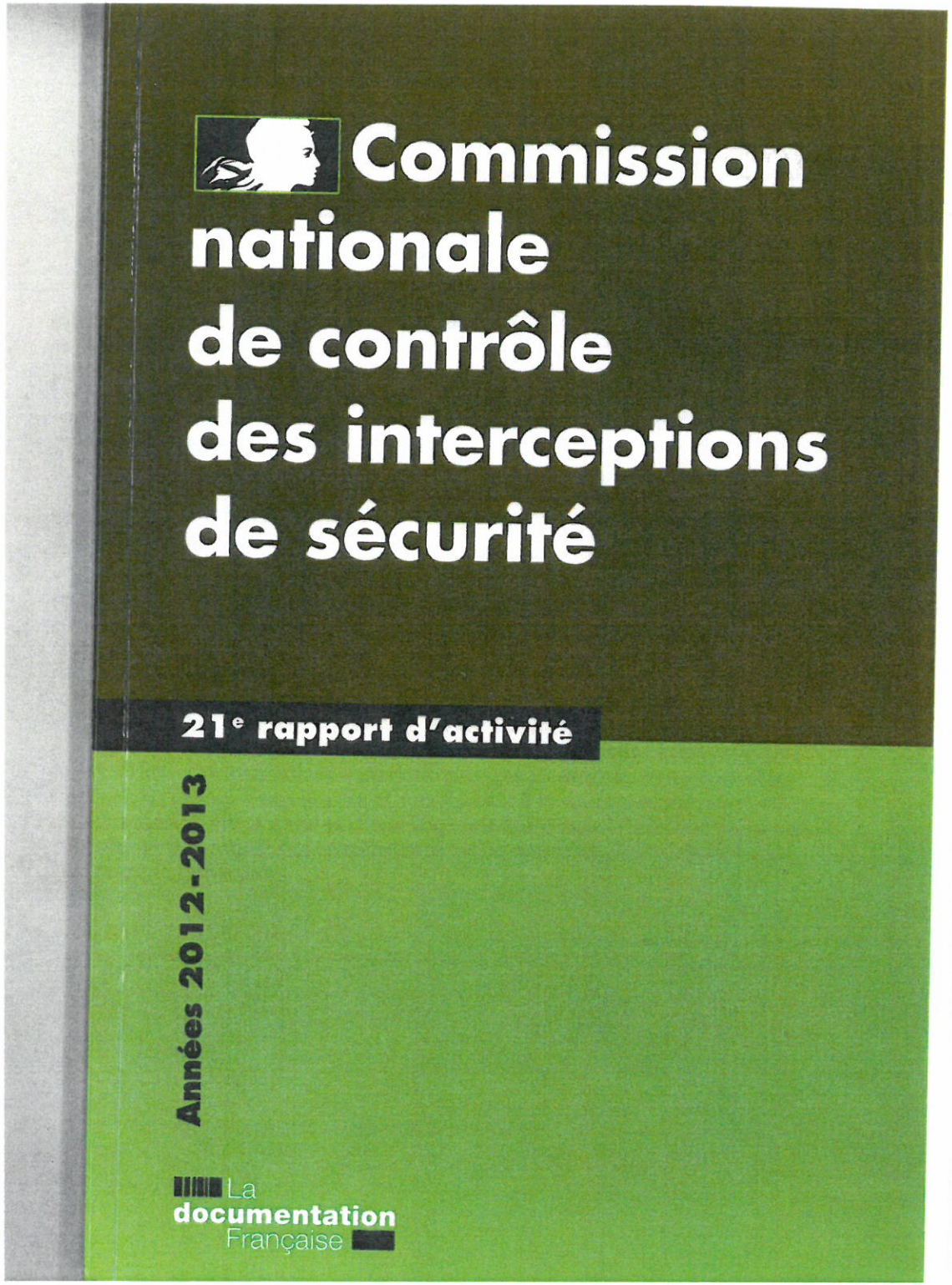
”Pour un approfondissement du cadre juridique des interceptions de sécurité”

Bertrand Warusfel



(pp. 17-23)

Pour un approfondissement du cadre juridique des interceptions de sécurité

Bertrand WARUSFEL
Professeur à l'université Lille 2,
avocat au barreau de Paris

La CNCIS a fêté récemment les vingt ans de la loi du 10 juillet 1991 et de son institution en tant qu'AAI. Une fois passé ces moments de célébration, viennent ceux de ce que l'on me permettra d'appeler la rétro-prospective, c'est-à-dire l'analyse de l'expérience acquise en vue de préparer l'avenir.

La Commission l'a elle-même souhaité dès l'an dernier en écrivant dans son précédent rapport qu'elle formait le vœu « que le débat soit désormais ouvert sur une réforme de la loi n° 91-546 du 10 juillet 1991, au regard des évolutions technologiques en matière de communications électroniques et des nouvelles formes de menaces qui emportent des conséquences importantes dans l'équilibre entre, d'une part les enjeux de protection du secret des correspondances et de la vie privées, et, d'autre part les exigences de sécurité » (CNCIS, rapport 2011-2012, p. 39). Cette brève contribution s'inscrit dans ce cadre.

S'agissant de la question toujours sensible des interceptions de sécurité, comme l'actualité internationale récente et le scandale *Prism* nous le rappellent clairement, il me semble que l'avenir doit être marqué par une double exigence : suivre efficacement l'évolution rapide des techniques de communication tout en consolidant l'État de droit, et ce dans le contexte plus large de la mise en place d'un véritable droit de la sécurité nationale.

Suivre l'évolution rapide des techniques de communication

Le début du XXIe siècle est indiscutablement marqué par une intensification et une diversification de l'usage des outils numériques de communication et de traitement de l'information. Issu de la fusion

technologique entre l'informatique et les télécommunications, le nouveau domaine des « communications électroniques » – bien qu'assez mal dénommé (puisque c'est en réalité son caractère numérique qui est central et non le fait que les traitements numériques s'effectuent principalement grâce à des moyens électroniques) – a vocation à unifier les usages et les problématiques de traitement et de transmission de l'information, quel que soit l'outil utilisé (ordinateur fixe ou portable, tablette, téléphone mobile, mais aussi tous les systèmes professionnels ou domestiques qui « embarquent » des moyens de traitement et de transmission).

Dès lors que les modes de communication se multiplient et se complètent, le besoin de la puissance publique de pouvoir – dans des cas limitativement prévus et touchant la sécurité nationale – en assurer l'interception, doit également suivre cette évolution. D'où surgit une première interrogation relative à la définition légale du périmètre des communications pouvant faire l'objet d'interceptions de sécurité.

La loi de 1991 a retenu la formule concise des « correspondances émises par la voie des communications électroniques » (aujourd'hui reprise par les articles L. 241-1 et suivants du Code de la sécurité intérieure). Si le renvoi à la notion de « communications électroniques » définie par le Code des postes et des communications électroniques paraît s'imposer (puisque ce sont bien les opérateurs des réseaux de communication électronique, régis par le code du même nom, qui se voient chargés de permettre la réalisation des interceptions sur leurs réseaux), on peut cependant se demander s'il ne serait pas préférable d'harmoniser le texte avec celui du Code pénal (issu de la même loi de 1991) qui sanctionne la violation des « correspondances émises, transmises ou reçues par la voie électronique » (article L. 226-15, 2e alinéa). Cette dernière formulation a en effet l'avantage d'être plus proche de celle donnée par l'article 3 de la convention de Budapest sur la cybercriminalité du 23 novembre 2001 qui vise l'interception « effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique ».

Plus délicate est l'identification des différentes formes de communications électroniques qui doivent être considérées comme des correspondances au sens de l'article L. 241-1 du Code de la sécurité intérieure. Certaines formes en relèvent sans aucune hésitation (appels téléphoniques fixes ou mobiles, visio-communications, télécopies, courriers électroniques, messageries instantanées) mais des pratiques comme les listes de discussions ou de diffusion, le chat ou les forums posent plus de difficultés. Pour pouvoir prévenir des interrogations concernant les nouvelles techniques de communication qui apparaîtront certainement dans les prochaines années, on ne peut que recommander au législateur de fixer un critère simple permettant de distinguer celles qui sont susceptibles de faire l'objet d'une interception. Outre le fait que les interceptions ne peuvent concerner que des « correspondances », c'est-à-dire

des communications entre un émetteur et un ou plusieurs destinataires identifiés (et non un contenu simplement stocké sur un serveur), il me semble que ce critère distinctif ne peut être que le caractère privé (ou plus exactement « non public » au sens de la convention de Budapest) de l'échange, autrement dit le fait qu'un tiers ne puisse pas accéder sans autorisation au contenu de cette transmission. En effet, à chaque fois que le mécanisme de communication autorise l'accès (même *a posteriori*) d'un tiers, cette dimension publique ou semi-publique permettra d'aménager à l'autorité publique une autre voie d'accès, moins intrusive au regard des libertés publiques que l'interception.

En termes rédactionnels et dans la perspective d'un toilettage des dispositions du Code de la sécurité intérieure issues de la loi de 1991, on pourrait donc envisager que l'article L. 241-1 du Code de la sécurité intérieure vise explicitement les « correspondances non publiques émises, transmises ou reçues par la voie électronique ».

Mais l'évolution récente des pratiques numériques et des méthodes d'enquête nous conduit également à évoquer le domaine connexe du recueil des métadonnées de connexion, à savoir toutes les informations – autres que son contenu même – qu'engendre l'établissement d'une communication électronique privative et dont la trace est conservée durant une certaine période (une année généralement) par l'opérateur ou l'intermédiaire technique par lequel la communication a été établie. Indirectement visées par l'article L. 244-2 du Code de la sécurité intérieure (qui permet d'obtenir des opérateurs « les informations ou documents qui leur sont nécessaires [...] pour la réalisation et l'exploitation des interceptions autorisées par la loi ») mais dans le but premier de préparer une interception, ces données techniques constituent aujourd'hui une source d'informations extrêmement utile et dont l'exploitation peut parfois être presque aussi fructueuse que celles du contenu des communications. C'est d'ailleurs la raison pour laquelle, la loi du 23 janvier 2006 a introduit à titre expérimental une autre procédure (celle du recours à une « personnalité qualifiée ») permettant aux services du ministère de l'Intérieur l'accès à de telles données aux seules fins de la prévention du terrorisme (article L. 34-1-1 du Code des postes et des communications électroniques).

Cette superposition de deux procédures partiellement redondantes ainsi que les rebondissements récents de l'actualité judiciaire en la matière (en l'occurrence, l'affaire dite des « Fadettes ») nous conduisent à approuver l'opinion émise dans ses derniers rapports par la CNCIS selon laquelle une seule procédure réduirait les difficultés de mise en œuvre et faciliterait le travail de recueil et d'exploitation des données (*cf.* notamment, le rapport 2011-2012 de la CNCIS p. 70). Au-delà même de ces raisons opérationnelles invoquées par la Commission, il nous semble en effet que toute l'évolution de l'économie numérique nous montre que la valeur des données de connexion et de leur traitement est égale voire supérieure à celle du contenu même des communications (et les grands

opérateurs du cyberespace comme Google ou Facebook nous en fournissent un exemple permanent).

Dès lors, sans mettre sur le même plan l'interception de correspondances et la récupération des données techniques de connexion, il serait justifié de fondre ensemble les actuels articles L. 34-1-1 du Code des postes et des communications électroniques et L. 244-2 du Code de la sécurité intérieure dans un nouvel article du même code qui mettrait sous le contrôle de la CNCIS (et dans le cadre d'une procédure adaptée à définir) toutes les demandes effectuées par les services de renseignement et de sécurité touchant aux données techniques de connexion. Il conviendrait alors de s'interroger sur le fait de savoir si ce renforcement du contrôle par la CNCIS ne justifierait pas, en contrepartie, de supprimer la distinction actuellement faite entre le motif de prévention du terrorisme et les autres domaines et d'autoriser sans distinction les demandes de tous les services concernés pour l'ensemble des motifs de sécurité nationale.

Concilier l'usage des interceptions avec l'État de droit

Quel qu'en soit le périmètre, la prérogative régalienne que constitue le recours par l'État aux interceptions de sécurité représente une atteinte réelle à l'exercice des libertés publiques (et particulièrement à la protection de la vie privée, telle qu'elle est garantie constitutionnellement ainsi que par l'article 8 de la CEDH). Il convient donc de s'assurer en permanence qu'un équilibre satisfaisant est établi entre l'intérêt public de sécurité et les garanties des libertés individuelles. C'est à quoi s'attache depuis l'origine le régime instauré par la loi du 10 juillet 1991 dont les principes essentiels ne semblent donc pas à remettre en question, ni le rôle central que joue l'intervention d'une AAI, en l'occurrence la CNCIS.

Tout au plus peut-on tirer de l'expérience des vingt années de pratique et de jurisprudence de la CNCIS quelques enseignements que le législateur pourrait utilement retraduire afin de perfectionner le dispositif.

S'agissant tout d'abord des motifs justifiant le recours aux interceptions, la CNCIS a souvent relevé dans ses rapports annuels la filiation qui existe historiquement entre la rédaction originelle de l'article 3 de la loi de 1991 (aujourd'hui codifié à l'article L. 241-2 du Code de la sécurité intérieure) et celle de l'article 410-1 du Nouveau Code pénal de 1992 qui a défini les « intérêts fondamentaux de la nation ». Par ailleurs, plus récemment, a été établie par le législateur de 2009 la nouvelle notion de « sécurité nationale » (article L. 1111-1 du Code de la défense) que l'article 3 de la loi de 1991 avait, par anticipation, visée sans la définir et que l'article 8 de la CEDH cite également.

Il nous semble que ces trois textes partagent une logique commune. Ce sont en effet les impératifs de la sécurité nationale dont l'État est le garant qui justifient le recours à ce moyen dérogatoire de l'interception de sécurité et qui font l'objet d'une protection pénale particulière. Dès lors, l'objectif d'intelligibilité du droit (souvent rappelé par le Conseil constitutionnel) ainsi que de sa cohérence nous invite à une nouvelle rédaction de l'article 3 qui renverrait explicitement aux deux autres textes du Code pénal et du Code de la défense. Sans vouloir ici se lancer dans un exercice rédactionnel approfondi, on pourrait imaginer que l'article vise désormais les « interceptions justifiées par un motif de sécurité nationale touchant à la protection des intérêts fondamentaux de la nation et en particulier à la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, ou à 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 ». En croisant la sécurité nationale (qui ne serait plus un domaine parmi d'autres, mais le facteur commun qui – comme l'indique le Code de la défense – vise à « identifier l'ensemble des menaces et des risques susceptibles d'affecter la vie de la Nation ») et les domaines couverts par l'article 410-1 du Code pénal, on affirmerait mieux l'exigence d'une motivation en relation directe avec ces seuls intérêts nationaux majeurs (par différence avec les interceptions judiciaires qui peuvent, pour leur part, se prévaloir des motifs de sûreté publique ou de défense de l'ordre et de prévention du crime, également prévus par l'article 8 CEDH) tandis que le rappel des domaines précédemment visés en 1991 préserverait les motifs traditionnels du recours aux interceptions sans exclure tout à fait qu'un autre intérêt fondamental de nation puisse également être invoqué.

Au-delà de la révision des motifs, une autre évolution renforçant l'État de droit paraît aujourd'hui prête à rentrer dans notre droit positif. Il s'agirait de conférer à la commission de contrôle indépendante un réel pouvoir d'autorisation et non plus seulement consultatif. On sait en effet que les avis supposés consultatifs de la CNCIS sont dans leur immense majorité suivis par le Premier ministre et – surtout – qu'en réalité la procédure mise en œuvre n'est plus aujourd'hui une procédure d'intervention *a posteriori* (comme le prévoyait la lettre de la loi de 1991) mais une procédure d'examen *a priori*, laquelle « a transformé *de facto*, le pouvoir de recommandation en un quasi-pouvoir de décision » comme le soulignait l'ancien président Dewost dans le rapport 2011-2012 de la CNCIS (p. 12).

Mettre ainsi le droit en accord avec le fait aurait là encore des avantages de cohérence et de clarté tout en renforçant le caractère incontestable de notre procédure nationale au regard des impératifs toujours plus stricts de la jurisprudence, européenne en particulier. Cela n'empêcherait pas la nouvelle loi de prévoir que le Premier ministre puisse en cas d'urgence et pour un motif d'intérêt national particulier, obtenir un réexamen rapide de la demande et, dans l'intervalle, une suspension

temporaire de la décision de refus d'autorisation. La sécurité nationale et ses impératifs ne seraient donc pas affectés de ce fait mais on aurait ainsi procédé à un rééquilibrage juridiquement et symboliquement important entre la règle (l'autorisation préalable indépendante) et l'exception (la décision discrétionnaire imposée par les circonstances).

Le troisième aspect qui mériterait de retenir l'attention d'un futur législateur pourrait avoir trait à la difficile question de la judiciarisation des interceptions. L'article L. 242-8 du Code de la sécurité intérieure prescrit en effet que « les renseignements recueillis ne peuvent servir à d'autres fins que celles mentionnées à l'article L. 241-2 », ce qui – cumulé avec la classification systématique de toutes les décisions et transcriptions d'interception – empêche, sauf exception, que l'existence et les résultats des interceptions de sécurité puissent être transmis à l'autorité judiciaire et verser en procédure. Certes, cette interdiction est tempérée par le fait qu'elle s'exerce « sans préjudice de l'application du deuxième alinéa de l'article 40 du Code de procédure pénale », ce qui permet aux services concernés de dénoncer au parquet des faits nouveaux susceptibles de révéler la commission d'un délit ou d'un crime. On pourrait cependant souhaiter qu'il soit plus facile à l'autorité administrative d'exploiter judiciairement des résultats de renseignement lorsqu'il s'agit d'un domaine donnant lieu à répression pénale. L'argument qui est souvent opposé à une telle production en procédure tient au fait que ces interceptions n'ont pas le caractère d'un acte de procédure effectué par un officier de police judiciaire et sous le contrôle d'un juge et que la loyauté et la crédibilité d'un tel renseignement pourraient facilement être contestées par la défense. Mais cet argument n'est pas totalement convaincant.

On connaît déjà en effet des cas dans lesquels les résultats d'un acte techniquement couvert par le secret de la défense nationale peuvent être produits en justice : c'est le cas du décryptement de certains fichiers utiles à l'enquête pénale et pour lequel la juridiction concernée choisit de recourir à des moyens couverts par le secret de la défense nationale (articles 230-1 à 230-5 du Code de procédure pénale). Dans un tel cas, est prévue une procédure particulière permettant de concilier le respect du secret et la nécessaire information des juges et des parties. On pourrait donc s'en inspirer pour permettre que la transcription d'une interception de sécurité utile à la justice puisse être déclassifiée (après avis favorable de la CCSDN) et qu'un minimum d'éléments d'information touchant aux conditions d'exécution de l'interception soit communiqué, en respectant les règles fixées par la jurisprudence de la cour de Strasbourg en ce qui concerne le recours aux preuves secrètes.

En conclusion, et pour compléter les différentes pistes de réforme évoquées plus haut, il faut être conscient de ce que la réforme de la loi de 1991 s'inscrira nécessairement dans un mouvement plus vaste de constitution d'un véritable droit de la sécurité nationale, dont la décision fondatrice du Conseil constitutionnel du 10 novembre 2011 (censurant les dispositions de 2009 instaurant une classification de certains lieux,

et non plus seulement des informations qu'ils contiendraient) a marqué sans doute la première étape. Le nouvel équilibre qui s'instaurera entre les nécessités de la sécurité nationale justifiant une interception et la garantie des libertés individuelles aura ainsi valeur de référence pour toutes les autres dispositions légales applicables à l'usage dérogatoire de certains moyens spéciaux par les services d'État ayant une mission de sécurité et de renseignement.

De plus, et si l'on suit les perspectives ouvertes par le rapport parlementaire de la mission d'information de la Commission des lois de l'Assemblée nationale consacrée à l'évolution du cadre juridique applicable aux services de renseignement, cette modernisation du cadre légal des interceptions de sécurité pourrait se doubler d'une extension des missions de la CNCIS afin de faire de cette autorité expérimentée le socle d'un nouveau dispositif de contrôle indépendant des activités des services de renseignement.