

I - Mise en conformité du code de la sécurité intérieure à la directive 2016/680

Article 19 bis (nouveau) - Droit à l'information

Amendement

Après l'article 19, il est inséré un article 19 bis ainsi rédigé :

Après l'article L. 822-4 du code de la sécurité intérieure, est créé un article L. 822-5 ainsi rédigé : « Lorsque la mise en œuvre d'une technique de recueil de renseignement prend fin, le service qui l'a réalisée informe promptement la personne concernée de la nature et de la durée de la technique, du type et du volume de renseignements recueillis, de la finalité ayant justifié le recueil et de l'identité du service, ainsi que de ses droits prévus à l'article L. 841-1 du présent code. La transmission de ces informations ne peut être retardée qu'en présence d'un risque manifeste et effectif de compromettre l'objectif qui a initialement justifié la mise en œuvre de la technique, et à la condition que la Commission nationale de contrôle des techniques de renseignement soit dûment informée de ce retard ».

Justifications

Le premier paragraphe de l'article 13 de la directive (UE) 2016/680 exige que le responsable de traitement mette à la disposition des personnes concernées les informations concernant l'identité du responsable, les finalités du traitement et les droits de la personne concernée et ne prévoit aucune dérogation à cette mesure.

Le deuxième paragraphe du même article exige la communication d'autres types d'informations, telle que la nature des données traitées. traitées lorsque la finalité poursuivie les permet.

Le troisième paragraphe du même article prévoit que la loi d'un État membre peut autoriser des dérogations aux obligations posées au deuxième paragraphe, mais ne permet toutefois aucune dérogation aux obligations posées au premier paragraphe.

Or, le code de la sécurité intérieure autorise des traitements de données personnelles dans le but de lutter contre certaines infractions, sans prévoir toutefois que les personnes concernées ne reçoivent la moindre information, en aucune circonstance. Cette absence d'information est donc frontalement contraire à la directive 2016/680 et doit être corrigée.

Article 19 ter (nouveau) - Pouvoirs de contrôle de la CNCTR

Amendement

Après l'article 19, il est inséré un article 19 ter ainsi rédigé :

Au 4° de l'article L. 833-2 du code de la sécurité intérieure, les mots suivants sont supprimés : « communiqués par des services étrangers ou par des organismes internationaux ou ».

Justifications

L'article 46, 1, a), de la directive (UE) 2016/680 exige que, dans chaque État membre, une autorité indépendante « contrôle l'application des dispositions adoptées en application de [cette] directive et de ses mesures d'exécution et veille au respect de celles-ci ». En France, en matière de renseignement, cette autorité de contrôle est définie par l'article L. 833-1 du code de la sécurité intérieure comme étant la Commission nationale de contrôle des techniques de renseignement (CNCTR).

L'article 47, 1, de la même directive exige que « chaque État membre prévoit, par la loi, que chaque autorité de contrôle dispose de pouvoirs d'enquête effectifs. Ces pouvoirs comprennent au moins celui d'obtenir du responsable du traitement ou du sous-traitant l'accès à toutes les données à caractère personnel qui sont traitées ».

Or, l'article L. 833-2, 4°, du code de la sécurité intérieure prévoit que la CNCTR ne peut pas avoir accès aux renseignements collectés, exploités, échangés ou conservés par les services français dès lors que ces renseignements ont initialement été « communiqués par des services étrangers ou par des organismes internationaux ». Cela empêche entièrement la CNCTR de vérifier que les données personnelles collectées et exploitées par les services le sont de façon licite, ce qui est en totale contradiction avec les exigences de la directive et doit être corrigé.

Article 19 quater (nouveau) - Recours effectif

Amendement

Après l'article 19, il est inséré un article 19 ter ainsi rédigé :

À l'article L. 854-9 du code de la sécurité intérieure, avant le dernier alinéa, est ajouté l'alinéa suivant : « Le Conseil d'État, statuant dans les conditions prévues au chapitre III bis du titre VII du livre VII du code de justice administrative, peut aussi être saisi par toute personne souhaitant vérifier qu'aucune technique de renseignement prévue au présent chapitre n'est irrégulièrement mise en œuvre à son égard et justifiant de la mise en œuvre préalable de la procédure prévue au quatrième alinéa du présent article ».

Justifications

L'article 54 de la directive (UE) 2016/680 exige, sans aucune exception possible, que les États membres offrent aux particuliers une voie de recours juridictionnel pour contester la licéité d'un traitement portant sur leur données personnelles. L'article précise explicitement que cette voie de recours juridictionnel doit être ouverte seraient aussi ouvertes par ailleurs des voies administratives.

Or, l'article L. 854-9 du code de la sécurité intérieure prévoit que, en matière de surveillance internationale, les particuliers ne peuvent pas agir en justice pour contester la licéité d'une mesure mise en œuvre à leur égard - seule la CNCTR a ce pouvoir, étant entièrement libre d'agir ou non. Cette absence de voie de recours juridictionnel est parfaitement contraire aux exigences de la directive et doit être corrigée.

Article 19 quinquies (nouveau) - Transferts

Amendement

Après l'article 19, il est inséré un article 19 ter ainsi rédigé :

À l'article L. 863-2, à la fin du premier alinéa, est ajoutée la phrase suivante : « Ces services ne peuvent transmettre ou obtenir des renseignements à d'autres services, français ou étrangers, que dans les conditions prévues au chapitre Ier du titre II du présent livre ainsi que, s'agissant des autorités d'un État n'appartenant pas à l'Union européenne, dans les conditions prévues à l'article 70-25 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ».

Justifications

Le code de la sécurité intérieure n'impose aucune condition ni contrôle s'agissant des échanges de renseignement par les autorités françaises avec d'autres autorités, françaises ou étrangères. Le code doit ainsi être modifié, non seulement pour imposer aux autorités françaises de respecter le cadre des transferts hors-UE posé par la directive (UE) 2016/680, mais aussi pour exiger que ces échanges, avec des autorités françaises, européennes ou hors-UE, poursuivent un des intérêts fondamentaux de la Nation prévus à l'article L. 811-3 du code (tel que doit le faire n'importe quelle autre collecte de renseignement) et que la CNCTR soit en mesure d'en assurer le contrôle.

II - Adaptation du droit français au RGPD

Article 7 - Données sensibles

Amendement

L'article 7 est ainsi modifié :

1° Avant le 2° est inséré un 1° bis ainsi rédigé : « Le 4° du II est complété par les mots suivants : «, dès lors que ces données révèlent à elles-seules les informations visées au I ».

2° Au 5°, la phrase ajoutée est complétée par les mots suivants : « et dont le traitement poursuit l'une des finalités visées aux b), g) et j) du paragraphe 2 de l'article 9 du règlement (UE) 2016/679 ».

Justifications

L'objectif de cet amendement est d'une part, d'apporter les précisions manquantes au RGPD et, d'autre part, de corriger certaines contradictions entre le projet de loi et le règlement.

1° L'article 9 du RGPD manque de précision en n'interdisant pas explicitement les traitements qui, recoupant des données non-sensibles que la personne concernée a publiées, visent à reconstituer des données sensibles qui, elles, n'ont jamais été publiées par la personne.

2° L'article 9 du RGPD n'autorise le traitement de données sensibles que pour certaines finalités dont il fait la liste exhaustive. Or, l'article 8, III, de la loi de 1978 (tel que modifié par le projet de loi) autoriserait les traitements de données sensibles poursuivant n'importe quelle finalité, pour la simple raison qu'une mesure technique serait appliquée : l'anonymisation à bref délai. Ceci n'est pas autorisé par le RGPD : cette autorisation doit être limitée à des finalités précises. Cette contradiction doit par conséquent être supprimée.

Pour autant, cette mesure d'anonymisation à bref délai n'est pas sans intérêt. En effet, l'article 9 du RGPD prévoit que, s'agissant de certaines finalités, le traitement de données sensibles n'est licite qu'en présence de « mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée ». Pour certaines de ces finalités, la loi de 1978 prévoit effectivement des garanties qui pourraient correspondre à ces « mesures appropriées ». Néanmoins, s'agissant d'autres finalités (celles visées au b), g) et j) du 2 de l'article 9 du règlement), la loi n'en prévoit aucune. Ainsi, dans ce cas précis, la mesure d'anonymisation à bref délai pourrait être une des « mesures appropriées » autorisant la poursuite de ces finalités.

Article 10 bis (nouveau) - Chiffrement

Amendement

Après l'article 10, il est inséré un article 10 bis ainsi rédigé :

Le premier alinéa de l'article 34 de la même loi est complété par la phrase suivante : « Cela implique notamment que, chaque fois que cela est possible, les données soient chiffrées de sorte à n'être accessibles qu'au moyen d'une clef mise à la seule disposition des personnes autorisées à accéder à ces données. »

Justifications

Cet amendement vise à rendre explicite que l'obligation de sécurité prévue dans le règlement se traduit en obligation de chiffrer de bout en bout chaque fois que cela est possible. En effet, le chiffrement de bout en bout où seules les personnes autorisées à accéder aux données (par exemple l'expéditeur et le/les destinataire/s d'un message) ont la clef limite considérablement les risques d'intrusion.

Article 14 AAA (nouveau) - Consentement

Amendement

Avant l'article 14, il est inséré un article 13 bis ainsi rédigé :

L'article 7 de la même loi est complété par l'alinéa suivant :

« Pour être valide, le consentement de la personne concernée doit être donné de façon explicite, libre, spécifique et informée. Cela implique notamment que son consentement ne soit pas exigé en contrepartie d'un bien ou d'un service, à moins que le traitement faisant l'objet du consentement ne soit indispensable à la fourniture de ce bien ou service. »

Justifications

Cet amendement vise à intégrer la définition déterminante donnée par la CNIL et le G29 du caractère libre du consentement (voir les dernières propositions de lignes directrices produites par le G29 à ce sujet : http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849).

Article 21 - Liberté d'expression

Amendement

L'article 21 est ainsi modifié :

1° Après le 6° est inséré un 6° bis ainsi rédigé : « Le titre du chapitre XI est remplacé par le titre suivant : « Publication de données à caractère personnel. » ».

2° Le 7°, a), est remplacé par le point suivant : « Le premier alinéa est remplacé par l'alinéa suivant : « Les traitements qui consistent à mettre des données personnelles à disposition du public ne sont licites qu'avec le consentement de la personne concernée ou si ces données contribuent à un débat d'intérêt général. Le 5° de l'article 6, les articles 8, 9, 32, et 39 et les articles 68 à 70 ne s'appliquent pas à de tels traitements, de même que le e) du 1 de l'article 4, les articles 10, 13 et 14 et le chapitre V du règlement (UE) 2016/679. » ».

Justifications

L'article 85 du RGPD exige que « les États membres concilient, par la loi, le droit à la protection des données à caractère personnel au titre du présent règlement et le droit à la liberté d'expression et d'information ».

Or, la loi de 1978 se contente de prévoir une série de dérogations (à l'interdiction de traiter des données sensibles ou à l'obligation de déclaration, par exemple) en faveur des seuls traitements mis en œuvre aux fins d'expression littéraire et artistique ou d'exercice de la profession de journaliste. Ce faisant, la loi ne concilie qu'une partie particulièrement réduite de la liberté d'expression avec le droit à la protection des données, omettant entièrement de concilier toutes les autres façons dont la liberté d'expression et d'information peut être mise en œuvre (débats politiques publics entre particuliers, investigations réalisées par d'autres personnes que des journalistes professionnels, etc.). La loi est trop restreinte et se conformer au règlement exige donc de viser le champ complet des activités mettant en œuvre la liberté d'expression et d'information : la publication de données personnelles, par n'importe quelle personne.

Ensuite, la loi de 1978 est floue sur la base légale qui autorise la publication de données personnelles (par des journalistes ou autres). Dans la plus part des cas, cette base est l'intérêt légitime du public à avoir accès à l'information publiée (le 5° de l'article 7 de la loi de 1978 autorisant les traitements pour la réalisation de l'intérêt légitime du destinataire des données). Ce flou rend la loi trop imprévisible pour concilier efficacement la liberté d'expression et le droit à la protection des données. L'amendement proposé vise à corriger ce défaut en intégrant explicitement la jurisprudence très claire de la Cour européenne des droits de l'Homme, qui réalise cette conciliation en autorisant uniquement les atteintes à la vie privée qui sont une « contribution à un débat d'intérêt général », en considérant « qu'ont trait à [cet] intérêt général les questions qui touchent le public dans une mesure telle qu'il peut légitimement s'y intéresser, qui éveillent son attention ou le préoccupent sensiblement notamment parce qu'elles concernent le bien-être des citoyens ou la vie de la collectivité » (CEDH, Grande chambre, 10 novembre 2015, Couderc et Hachette Filipacchi associés c. France, req. n°40454/07, § 103).

Enfin, la loi de 1978 (dans son état actuel et telle que modifiée par l'actuel projet de loi) prévoit une dérogation injustifiable à l'article 40, I : dès lors qu'un traitement de données à caractère personnel bénéficie d'une dérogation pour liberté d'expression, les personnes concernées ne peuvent pas exiger du responsable de traitement que des informations les concernant soient corrigées ou effacées lorsqu'elles sont inexacts ou que leur publication est illicite. Cette dérogation doit être supprimée.

De l'applicabilité de la directive 2016/680 au livre VIII du code de la sécurité intérieure

I. Les activités couvertes par la directive

L'article premier de la directive 2016/680 définit son champ d'application comme couvrant tout « *traitement des données à caractère personnel par les autorités compétentes à des fins de **prévention et de détection des infractions pénales, d'enquêtes et de poursuites** en la matière ou d'exécution de **sanctions pénales*** ».

Il précise explicitement que font partis de ces traitements ceux concernant « **la protection contre les menaces pour la sécurité publique et la prévention de telles menaces** ».

Son considérant 14 précise que, « *étant donné que la présente directive ne devrait pas s'appliquer au traitement de données à caractère personnel effectué dans le cadre d'**une activité ne relevant pas du champ d'application du droit de l'Union**, il convient que les activités relatives à la **sécurité nationale** [...] ne soient pas considérées comme des activités relevant du champ d'application de la présente directive* ». Aussi, il apparaît clairement que toute activité relative à la sécurité nationale n'entre pas dans le champ d'application du droit de l'Union et que, réciproquement, toute activité entrant dans ce champ ne saurait être qualifiée de relative à la sécurité nationale.

Or, il doit être rappelé que l'Union européenne et ses États Membres ont systématiquement considéré que la **lutte contre le terrorisme** entrait dans le champ d'application du droit de l'Union, prenant de nombreux actes européens à son sujet : règlement 603/2013, décisions-cadres 2002/475/JAI, 2002/465/JAI, 2002/584/JAI et 2006/960/JAI, décisions du Conseil 2005/671/JAI et 2008/615/JAI).

La dernière directive 2017/541 « *relative à la lutte contre le terrorisme* », qui « *énumère de manière exhaustive un certain nombre d'infractions graves, telles que les atteintes à la vie d'une personne, en tant qu'actes intentionnels pouvant être qualifiés d'infractions terroristes* » (considérant 8), en est un exemple manifeste.

Ainsi, en droit de l'Union, **la lutte contre le terrorisme n'est pas liée à la notion juridique de « sécurité nationale »** telle que visée par la directive 2016/680, et entre donc entièrement dans le champ de cette dernière.

II. Les activités autorisées par le code de la sécurité intérieure

Le livre VIII du code de la sécurité intérieure détermine les conditions dans lesquelles les services de renseignement peuvent collecter de informations sur des individus –

ces collectes sont des traitements de données personnelles au sens de la directive 2016/680.

L'article L. 811-3 du code de la sécurité intérieure liste les finalités que peuvent licitement poursuivre ces traitements. Le Conseil constitutionnel (dans sa décision n° 2015-713 DC, considérant 10) a explicitement défini certaines de ces finalité comme consistant en la **prévention d'infractions** déjà définies en droit pénal, de sorte que :

- la prévention du **terrorisme**, visée au 4° de l'article L. 811-3, concerne les infractions définies aux articles 421-1 à 421-6 du code pénal (atteintes aux personnes, aux biens ou aux systèmes informatiques dans le but de troubler l'ordre public par intimidation ; blanchiment et financement liés) ;
- la prévention de la **criminalité et de la délinquance organisées**, visée au 6° de l'article L. 811-3, concerne les infractions énumérées à l'article 706-73 du code de procédure pénale (trafic de stupéfiants, blanchiment d'argent, contrefaçon de monnaie, proxénétisme, extorsion avec arme...) ;
- la prévention des **violences collectives**, visée au c) du 5°, concerne les infractions définies aux articles 431-1 à 431-10 du code pénal (organisation d'une manifestation interdite ou non déclarée, participation à une émeute...) ;
- la prévention des **atteintes à la forme républicaine des institutions**, visée au a) du 5°, concerne les infractions définies aux articles 412-1 à 412-8 du code pénal (organisation et participation à un mouvement insurrectionnel) ;

Ensuite, quand il ne s'agit pas de lutter contre des infractions pénales, l'article L. 811-3 autorise généralement des traitements poursuivant des finalités ordinaires pour l'administration, soumises de façon normale au règlement général sur la protection des données (RGPD) qui prévoit des règles au moins aussi stricte que la directive 2016/680. Ces finalités sont :

- « les intérêts majeurs de la **politique étrangère** » ;
- « l'exécution des **engagements européens et internationaux** de la France ;
- « les « **intérêts économiques, industriels et scientifiques** majeurs de la France ».

Enfin, seules certaines finalités résiduelles visées par l'article L. 811-3 pourraient être débattues comme concernant la « sécurité nationale ». Il s'agirait de :

- « **l'indépendance** nationale, **l'intégrité du territoire** et la défense nationale » ;
- « la prévention de toute forme d'**ingérence étrangère** ».

Toutefois, que ces finalités concernent la sécurité nationale ou non, elles restent soumises au droit européen. En effet, l'article 23 du RGPD prévoit qu'une loi nationale

peut déroger à certaines des obligations prévues par ce règlement si est en jeu « la sécurité nationale », mais à la stricte condition que cette loi « **respecte l'essence des libertés et droits fondamentaux** et qu'elle constitue une **mesure nécessaire et proportionnée** dans une société démocratique ». Cette formulation est une reprises directe de l'article 52 de la Charte des droits fondamentaux de l'Union européenne.

Dès lors, les traitements réalisés pour la sécurité nationale doivent respecter les conditions générales que le RGPD comme la Charte imposent, et ce sans aucune dérogation. Or, une absence total de droit d'information, de droit au recours ou de contrôle par une autorité indépendante, tel que le code de la sécurité le prévoit en certaines dispositions, constitue indiscutablement des **atteintes à l'essence des droits fondamentaux** à la vie privée et à la protection des données personnelles.

Dans tous les cas, même à accepter que certaines finalités résiduelles de l'article L. 811-3 échapperaient au champ de la directive 2016/680 (tout en restant soumises au RGPD et à la Charte de l'UE), cela ne justifierait en rien que l'ensemble du livre VIII du code de la sécurité intérieure, dont l'écrasante majorité des finalités est bien soumise à la directive 2016/680, viole entièrement cette dernière.

III. L'activité concrète des services de renseignement

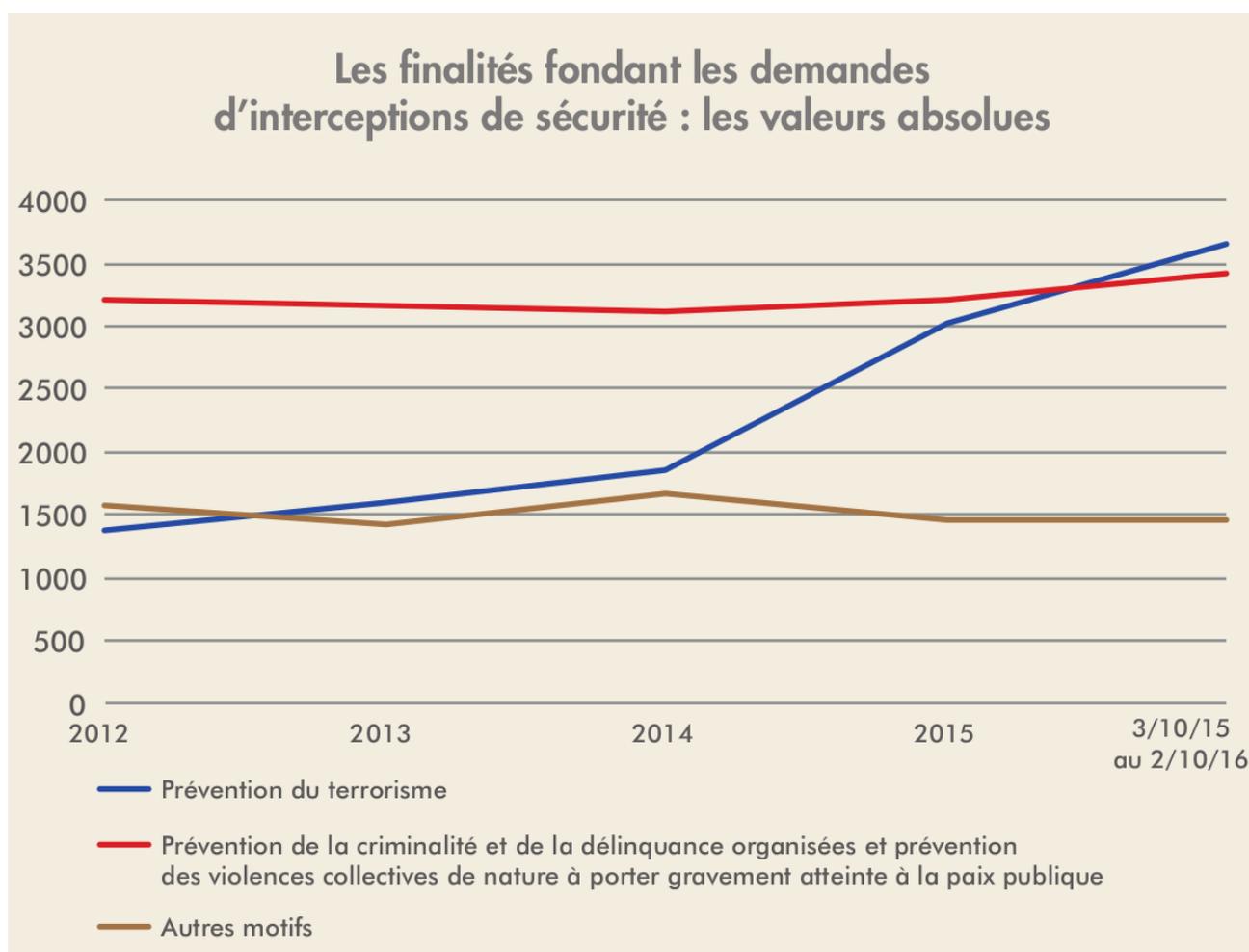
Dans son 22^e rapport d'activité, la Commission nationale de contrôle des interceptions de sécurité (CNCIS) expliquait (page 80) que « *6 182 interceptions de sécurité ont été sollicitées en 2013 (4 213 interceptions initiales et 1 969 renouvellements)* », précisant que, « *au stade des autorisations initiales, la prévention de la criminalité et délinquance organisées reste le premier motif des demandes initiales avec 60 %, suivie de la prévention du terrorisme avec 24 % et de la **sécurité nationale avec 15 %*** ».

Dans son 23^e rapport, elle expliquait (page 84) que « *6 628 interceptions de sécurité ont été sollicitées en 2014 (4 452 interceptions initiales et 2 176 renouvellements)* », précisant que, « *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 %*** ».

Dans le même rapport, elle ajoutée que, « *entre le 1^{er} janvier et le 30 avril 2015, 2 509 interceptions de sécurité ont été sollicitées (1 719 interceptions initiales et 790 renouvellements)* », précisant que, « *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 %*** ».

Jusqu'à 2015, la prévention de la criminalité et de la délinquance organisée est donc resté la principale raison justifiant la collecte de renseignements, la « sécurité nationale » restant une finalité marginale.

Dans son premier rapport d'activité, la CNCTR explique que, « entre le 3 octobre 2015 et le 2 octobre 2016, 43 % des demandes ont été motivées par la prévention du terrorisme et 40 % par la prévention de la criminalité et de la délinquance organisées ainsi que des violences collectives de nature à porter gravement atteinte à la paix publique. L'analyse des chiffres mensuels des demandes montre que c'est au mois de janvier 2015 que la prévention du terrorisme a, pour la première fois, été le fondement légal le plus fréquemment invoqué ». Elle joint le graphique suivant, représentant l'évolution du nombre de demandes d'interception en fonction de leur finalité :



Il ressort de ces chiffres que les activités autorisées par le livre VIII du code de la sécurité intérieure n'ont, en pratique, qu'un lien faible avec la protection de la sécurité nationale.

Conclusion

L'examen tant de la pratique que du droit révèle que la très grande majorité des activités autorisées par le livre VIII du code de la sécurité intérieure entre dans le champ d'application tant du droit de l'Union que de la directive 2016/680.