Deuxième avis complémentaire de la Commission nationale pour la protection des données relatif au projet de loi n° 6921 portant :
1) modification du Code d'instruction criminelle,
2) modification de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques,
3) modification de la loi du 27 février 2011 sur les réseaux et les services de communications électroniques,
4) adaptation de la procédure pénale face aux besoins liés à la menace terroriste.

Délibération n° 279/2017 du 30 mars 2017

Conformément à l'article 32 paragraphe (3) lettre (e) de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (ci-après « la loi du 2 août 2002 »), la Commission nationale pour la protection des données a notamment pour mission d'aviser *« tous les projets ou propositions de loi portant création d'un traitement de même que sur toutes les mesures réglementaires ou administratives émises sur base de la présente loi »*.

Par courrier du 7 décembre 2016, Monsieur le Ministre de la Justice a fait parvenir à la CNPD des amendements concernant le projet de loi n° 6921 portant 1) modification du Code d'instruction criminelle, 2) modification de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques, 3) modification de la loi du 27 février 2011 sur les réseaux et les services de communications électroniques,4) adaptation de la procédure pénale face aux besoins liés à la menace terroriste.

Pour rappel, la Commission nationale a rendu un premier avis relatif au projet de loi n° 6921 en date du 12 février 2016 (délibération n° 147/2016), ainsi qu'un avis relatif à une première série d'amendements gouvernementaux (délibération n° 803/2016 du 14 septembre 2016).

1) article 24-1 du Code d'instruction criminelle (amendement 1)

La CNPD note avec satisfaction que la modification projetée de l'article 24-1 du Code d'instruction criminelle a été retirée du projet de loi pour être traitée dans le cadre du projet de loi n°6763.

Ledit projet n°6763 devrait d'ailleurs faire l'objet de profondes modifications substantielles, voire être remplacé ou complété par un nouveau projet de loi en raison de l'arrêt rendu par la Cour de justice de l'Union européenne dans les affaires jointes C-203/15 et C-698/15 en date du 21 décembre 2016.

2) article 39 du Code d'instruction criminelle (amendement 2)

La CNPD n'a pas d'observations à formuler concernant cet amendement.

3) article 48-26 projeté du Code d'instruction criminelle (amendement 3)

La CNPD salue que le texte modifié prévoit que l'enquête sous pseudonyme sera réservée aux officiers de police judiciaire spécialement habilités à cette fin par le Procureur Général d'Etat. Il est d'ailleurs fortement recommandé que les officiers de police judiciaire en question bénéficient d'une formation adaptée.

La CNPD partage la position du Conseil d'Etat qui estime que l'enquête sous pseudonyme devrait être réservée aux officiers de police judiciaire de la Police grand-ducale et ne devrait pas pouvoir être effectuée par des officiers de police judiciaire autres que ceux restrictivement énumérés à l'article 10 du code d'instruction criminelle.

De même, elle se rallie au Conseil d'Etat en ce qui concerne l'exigence d'une ordonnance judiciaire pour pouvoir effectuer une enquête sous pseudonyme.

La CNPD regrette cependant que – contrairement à ses suggestions faites au point 4.3. de son avis du 12 février 2016 - il ne soit pas expressément exclu qu'on ait recours, de manière délibérée, aux noms de personnes réellement existantes pour ce qui est des pseudonymes à utiliser.

4) article 48-27 projeté du Code d'instruction criminelle (amendement 4)

4.1.) Types de recherches pouvant être effectuées sur base de l'article 48-27 projeté

Suite aux amendements sous avis, l'accès aux données relatives aux abonnés ou utilisateurs de services de télécommunications et relatives à utilisation de ces services pourra se faire par les deux voies suivantes:

- en requérant le concours d'un opérateur de télécommunications ou d'un fournisseur d'un service de télécommunications
- au moyen d'un accès au fichier créé auprès de l'ILR en vertu de l'article 10bis projeté de la loi modifiée du 30 mai 2005

Dans son avis du 12 février 2016, la CNPD avait rendu attentif au caractère flou du texte en ce qui concerne les recherches pouvant être effectuées sur base de l'article 48-27 projeté.

Suite aux amendements gouvernementaux déposés en date du 8 août 2016, les choses semblent claires pour ce qui est des données pouvant être obtenues par le biais de l'accès au fichier créé auprès de l'ILR. En effet, les données détenues au départ par le magistrat ou officier de police judiciaire (fournies pour effectuer la recherche) et celles obtenues par le biais du fichier créé auprès de l'ILR doivent forcément faire partie de celles contenues dans la base de données et énumérées au deuxième paragraphe de l'article 10bis projeté de la loi modifiée du 30 mai 2005.

En revanche, la nature des recherches pouvant être effectuées auprès des opérateurs de télécommunications ou fournisseurs d'un service de télécommunications demeure floue.

Il pourrait s'agir en partie de recherches du même type que celles pouvant être effectuées par le biais de l'accès au fichier créé auprès de l'ILR, comme par exemple:

- la recherche du nom et de l'adresse de la personne [données recherchées] à partir du numéro de téléphone x [donnée de départ]
- la recherche de tous les numéros de téléphone [données recherchées] dont est titulaire une personne dénommée x habitant à une adresse y [données de départ]

Il pourrait cependant aussi s'agir de cas de figure dans lesquelles le lien entre l'information de départ et l'information recherchée ne peut se faire qu'au moyen de données de trafic de communications[1]. A titre d'exemple, on peut mentionner les hypothèses suivantes :

- la recherche du numéro de téléphone, du nom et de l'adresse d'une personne [données recherchées] ayant appelée le numéro de téléphone x [connu, donnée de départ] à telle ou telle heure précise [données de départ].
- la recherche du numéro IMEI de l'appareil [donnée recherchée] à l'origine de l'appel vers le numéro de téléphone x [connu, donnée de départ] à telle ou telle heure précise [données de départ].
- la recherche du numéro de téléphone, du nom et de l'adresse de personnes [données recherchées] ayant effectué des appels téléphoniques à partir du téléphone mobile doté du numéro IMEI x [données de départ]. (Les recherches via le numéro IMEI sont d'ailleurs citées comme exemple de l'utilisation déjà existante de l'article 46bis du Code d'instruction criminelle belge [ayant inspiré l'article 48-27 sous avis] dans les travaux parlementaires relatifs à sa modification en 2007.)[2]
- la recherche de l'adresse IP de l'ordinateur [donnée recherchée] s'étant connectée à messagerie électronique dotée de l'adresse e-mail x à un moment donné [données de départ]. D'ailleurs l'article 46bis du Code d'instruction criminelle belge a justement été modifié en 2007 et a eu la teneur reprise partiellement par l'article 48-27 projeté afin d'inclure les recherches d'adresses IP à partir des temps de connexions exacts[3].

Or, au regard de la jurisprudence récente de la Cour de justice de l'Union européenne en matière de rétention des données de trafic de communications, il semble qu'un tel recours aux données de trafic ne soit possible qu'après un contrôle préalable par une juridiction ou une autorité

---

[1] A l'heure actuelle, les articles 24-1 et 67-1 du Code d'instruction criminelle devraient s'appliquer à ces cas de figure

[2] cf. le projet de loi 3 - 1824/1 (numéro de documents parlementaires du Sénat), commentaire des articles, Article 2, page 8
https://www.senate.be/www/webdriver?MItabObj=pdf&MIcolObj=pdf&MInamObj=pdfid&MItypeObj=application/pdf&MIvalObj=50335352

[3] Loi du 23 janvier 2007 modifiant l'article 46bis du Code d'instruction criminelle, cf. le projet de loi 3 - 1824/1 (numéro de documents parlementaires du Sénat), exposé des motifs, lettre A, page 2
https://www.senate.be/www/webdriver?MItabObj=pdf&MIcolObj=pdf&MInamObj=pdfid&MItypeObj=application/pdf&MIvalObj=50335352

administrative indépendante[4]. Par ailleurs, il n'est guère justifiable qu'on utilise les données de trafic pour des enquêtes concernant tous crimes et délits et non seulement des crimes graves.

4.2.) Les cas d'extrême urgence

Dans son avis du 12 février 2016, la CNPD avait pointé le caractère imprécis de la notion d'extrême urgence alors que c'est la situation d'extrême urgence qui permet à un officier de police judiciaire de recourir aux mesures de l'article 48-27 projeté (avec l'accord oral d'un magistrat).

Selon le commentaire des amendements, le texte inspiré de l'article 46bis du Code d'instruction criminelle belge vise des hypothèses telles que celle d'une victime d'une infraction grave sur le point de se commettre (telle une tentative de meurtre) lançant un appel d'urgence auprès de la Police ou celle d'une alerte à la bombe ou d'une prise d'otages.

L'amendement 4 remplace la formulation « *En cas d'extrême urgence* » par le passage suivant : « *Lorsqu'il existe une nécessité urgente de prévenir une atteinte grave à la vie, à la liberté ou à l'intégrité physique d'une personne ou lorsqu'il est impératif que les autorités qui procèdent à l'enquête agissent immédiatement pour éviter de compromettre sérieusement une procédure pénale ...* ».

La CNPD comprend l'opportunité d'introduire une dérogation pour les cas de figure énumérés dans le commentaire des amendements (victime d'une infraction grave sur le point de se commettre telle une tentative de meurtre lançant un appel d'urgence auprès de la Police ou celles d'une alerte à la bombe ou d'une prise d'otages).

Ces hypothèses correspondent au premier cas d'ouverture de l'exception « *Lorsqu'il existe une nécessité urgente de prévenir une atteinte grave à la vie, à la liberté ou à l'intégrité physique d'une personne* ».

En revanche le deuxième cas d'ouverture « *lorsqu'il est impératif que les autorités qui procèdent à l'enquête agissent immédiatement pour éviter de compromettre sérieusement une procédure pénale* » semble très large et non justifiée au regard des finalités de cet alinéa telles qu'énoncées dans le commentaire des amendements. Cela est d'autant plus problématique que l'article 48-27 projeté s'applique à tous les crimes et délits indépendamment de leur gravité et non seulement aux crimes ayant trait au terrorisme.

Enfin, la CNPD partage la position du Conseil d'Etat qui estime que la mesure ne devrait pas pouvoir être effectuée par des officiers de police judiciaire autres que ceux énumérés à l'article 10 du Code d'instruction criminelle.

4.3.) Divers

La CNPD déplore que sa suggestion de soumettre le recours aux mesures de l'article 48-27 projeté à la condition qu'il soit «*nécessaire à la manifestation de la vérité*» n'a pas été retenu.

[4] Voir l'arrêt rendu le 8 avril 2014 dans les affaires jointes C-293/12 et C-594/12, point 62 et l'arrêt rendu le 21 décembre 2016 dans les affaires jointes C-203/15 et C-698/15, point 120

Par ailleurs, elle constate que le texte amendé ne comporte toujours pas de disposition particulière relative aux titulaires d'un secret professionnel.

5) articles 88-1 à 88-4 projetés du Code d'instruction criminelle (amendement 5)

5.1.) Protection du « *Kernbereich privater Lebensgestaltung* »

Dans son avis du 12 février 2016, la CNPD avait rendu attentif au concept d'un noyau dur de la vie privée, le « *Kernbereich privater Lebensgestaltung* » qui doit bénéficier d'une protection particulière aussi bien en matière de sonorisation qu'en matière de captation de données informatiques.

L'amendement 5 tente d'y répondre par l'alinéa qui suit : « *Les éléments de la communication qui ne sont pas pertinents pour l'instruction préparatoire ne peuvent être utilisés et leur enregistrement et leur transcription sont immédiatement détruits par le juge d'instruction.* »

Si l'insertion d'une disposition prévoyant l'effacement de données non nécessaires est louable, le texte amendé ne garantit pourtant pas une protection équivalente à celle du «*Kernbereich privater Lebensgestaltung*» existant en Allemagne.

Comme il a été relevé dans l'avis du 12 février 2016[5], suite à un arrêt de la Cour constitutionnelle allemande de 2004, la législation allemande s'appliquant en matière de sonorisation oblige d'une part l'autorité décidant de la mesure d'apprécier, dès le départ, l'atteinte à la vie privée et, d'autre part, impose le cas échéant une interruption de la mesure en fonction des circonstances.

En ce qui concerne la captation de données informatiques, un récent arrêt du Bundesverfassungsgericht[6] du 20 avril 2016 pose des conditions concernant la loi « BKA » dans le domaine de la lutte préventive contre le terrorisme, alors que la captation de données informatiques n'est pas prévue par le Code de procédure pénal allemand[7].

Ledit arrêt exige notamment que les informations obtenues par le biais de la captation soient visionnées par un organe indépendant avant de pouvoir être utilisées par les autorités répressives.

« *Der Gesetzgeber hat insofern dem Schutzbedarf der Betroffenen durch Sicherungen auf der Aus- und Verwertungsebene Rechnung zu tragen und die Auswirkungen eines solchen Zugriffs zu minimieren. Entscheidende Bedeutung hierfür kommt dabei einer Sichtung durch eine*

---

[5] Point 7.1.

[6] BVerfG, Urteil des Ersten Senats vom 20. April 2016
- 1 BvR 966/09 - Rn. (1-29)
http://www.bverfg.de/e/rs20160420_1bvr096609.html

[7] Et il semble que, selon la jurisprudence du Bundesgerichtshof, les dispositions existentes de la Strafprozessordnung ne permettent pas la captation des données informatiques
Cf. BGH, 31.01.2007 - StB 18/06
http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=38779&pos=0&anz=1

unabhängige Stelle zu, die kernbereichsrelevante Informationen vor ihrer Kenntnisnahme und Nutzung durch das Bundeskriminalamt herausfiltert.»[8]

Cette commission composée principalement de personnes indépendantes des autorités de sécurité visionnera et filtrera les données obtenues afin d'assurer la protection du «Kernbereich privater Lebensgestaltung» :

« *Die verfassungsrechtlich gebotene Sichtung durch eine unabhängige Stelle dient neben der Rechtmäßigkeitskontrolle maßgeblich dem Ziel, kernbereichsrelevante Daten so frühzeitig herauszufiltern, dass sie den Sicherheitsbehörden nach Möglichkeit nicht offenbar werden. Dies setzt voraus, dass die Kontrolle im Wesentlichen von externen, nicht mit Sicherheitsaufgaben betrauten Personen wahrgenommen wird*»[9].

5.2.) Sécurité en matière de captation de données informatiques

Dans son avis du 12 février 2016[10], la CNPD avait rendu attentif aux problèmes de sécurité considérables engendrés par la captation de données informatiques.

Les auteurs du projet tentent d'y remédier par le paragraphe suivant introduit par l'amendement 5: «*Dans les cas visés à l'article 88-1, le jour, l'heure, la durée et, si nécessaire, le lieu de surveillance et du contrôle des télécommunications ou de la correspondance postale, de la sonorisation de certains lieux ou véhicules ou de la captation de données informatiques, ainsi que l'identité des personnes y ayant procédé sont indiqués et consignés dans un procès-verbal.*»

Si l'alinéa cité ci-dessus constitue un avantage en termes de transparence, voire de procès équitable, il ne répond pourtant pas aux risques relatives à la sécurité des traitements effectués, ni ne permet de dissiper un certain flou entourant les scellés des enregistrements[11].

A titre de comparaison, on peut citer le futur article 269quater du Code de procédure pénale suisse[12] qui dispose ce qui suit :
« *Art. 269quater Exigences posées aux programmes informatiques spéciaux de surveillance de la correspondance par télécommunication*
1 Seuls peuvent être utilisés des programmes informatiques spéciaux qui génèrent un procès-verbal complet et inaltérable de la surveillance. Le procès-verbal est joint au dossier de la procédure.
2 Le transfert des données du système informatique surveillé à l'autorité de poursuite pénale compétente est sécurisé.
3 L'autorité de poursuite pénale s'assure que le code source peut être contrôlé, dans le but de vérifier que le programme ne contient que des fonctions admises par la loi.»

Si l'article susmentionné du Code de procédure pénale suisse est loin de résoudre tous les problèmes de sécurité liés à la captation de données informatiques, il a le mérite d'imposer au

[8] Point 220 de l'arrêt
[9] Point 224 de l'arrêt
[10] Point 7.3.
[11] Cf l'avis de la CNPD du 12 février 2016, point 7.5.
[12] Article 269quater du Code de procédure pénale introduit par la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT) du 18 mars 2016
https://www.admin.ch/opc/fr/federal-gazette/2016/1821.pdf

moins certaines exigences pour ce qui est des programmes informatiques utilisés par les autorités.

5.3.) Contenu des décisions ordonnant les mesures des articles 88-1 et suivants

Dans son avis du 12 février 2016[13], la CNPD avait suggéré que la loi exige que les décisions ordonnant la captation de données informatiques contiennent des informations relatives aux données à capter. En effet, le caractère attentatoire à la vie privée est très différent selon le type de données captées et les mesures précises de contrôle absolument nécessaires dans une affaire ne sont pas forcément les mêmes que celles nécessaires dans une autre affaire.

Selon les considérations générales des amendements gouvernements sous avis, une telle exigence se heurterait à des difficultés pratiques.

Si la CNPD comprend qu'il n'est pas opportun de déterminer, à l'avance, les données à capter de manière trop détaillée et précise, elle estime néanmoins qu'il serait indiqué d'exiger que la décision du juge d'instruction comprenne au moins une indication du type ou des catégories de données recherchées.

A titre d'exemple, on peut mentionner le futur article 269ter du Code de procédure pénale suisse[14] qui exige que l'ordre d'opérer la captation de données informatiques contienne le « *type de données qu'il*[15] *souhaite obtenir* ».

Le même article 269ter exige par ailleurs de manière expresse qu'en cas d'introduction dans un lieu non accessible au public, l'ordre d'opérer la mesure indique «*le local qui n'est pas public dans lequel il est, le cas échéant, nécessaire de pénétrer pour introduire des programmes informatiques spéciaux de surveillance de la correspondance par télécommunication dans le système informatique considéré* », alors que l'article 88-3 projeté du Code d'instruction criminelle semble moins explicite à ce sujet. La CNPD suggère dès lors que l'ordonnance autorisant une introduction doive au moins indiquer l'adresse (en cas d'introduction dans une maison) ou le numéro d'immatriculation (en cas d'introduction dans une voiture).

5.4.) Information des personnes concernées

Dans son avis du 12 février 2016[16], la CNPD avait recommandé que la loi exige que doivent être informées non seulement la personne surveillée en vertu de l'ordonnance du juge d'instruction, mais aussi les autres personnes concernées comme par exemple des membres de famille cohabitant dans le même logement (faisant l'objet d'une sonorisation) ou utilisant le même ordinateur (faisant l'objet d'une captation de données informatiques) que la personne surveillée, dans l'hypothèse où ces autres personnes concernées sont connues.

Le texte amendé prévoit que soit informé également «*l'occupant des lieux soumis à une sonorisation*». Selon le commentaire des amendements, il s'agit d'«*informer les habitants des*

[13] point 7.2.
[14] Article 269ter du Code de procédure pénale introduit par la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT) du 18 mars 2016
https://www.admin.ch/opc/fr/federal-gazette/2016/1821.pdf
[15] [le Procureur]
[16] point 7.6.1.

lieux». La désignation de «*l'occupant*» (au singulier) dans le texte de l'amendement peut cependant prêter à confusion et pourrait ne viser qu'une personne déterminée (le locataire, l'occupant à titre précaire, le conjoint occupant le logement conjugal après une séparation ...) et non tous les personnes habitant un logement et concernées par les mesures de sonorisation.

La CNPD regrette par ailleurs qu'en matière de captation de données informatiques, l'information reste limitée à la personne directement visée par l'ordonnance, alors que l'atteinte à la vie privée d'autres personnes concernées (par exemple cohabitant et utilisant le même ordinateur) inhérente à ce type de mesure peut être grave.

Il semble aussi y avoir une incohérence dans la mesure où des personnes habitant avec la personne surveillée seraient informées, si on a enregistré leurs conversations par le biais de microphones installés dans leur logement (sonorisation), mais qu'elles ne seraient pas informées si un résultat similaire est obtenu en activant les microphones des ordinateurs ou smartphones (captation de données informatiques) à l'intérieur de leur logement.

Enfin, la CNPD partage le souci du Conseil d'Etat concernant le risque que l'exercice d'un recours soit rendu impossible de fait, dans le cas où les données sont effacées avant que n'ait lieu l'information des intéressés eu égard aux délais de douze mois s'appliquant d'un côté à la destruction des enregistrements et de l'autre à l'information de la personne surveillée. Dès lors le texte devrait prévoir que l'information doit intervenir avant la destruction des enregistrements. Par ailleurs, un espace de temps permettant à la personne concernée d'exercer un recours devrait séparer le moment de l'information et celui de la destruction des enregistrements.

Pour le surplus la CNPD n'a pas d'autres observations à formuler.

Ainsi décidé à Esch-sur-Alzette en date du 30 mars 2017.

La Commission nationale pour la protection des données

Tine A. Larsen Présidente	Thierry Lallemang Membre effectif	Christophe Buschmann Membre effectif