Avis n° 21/2016 du 18 mai 2016

Objet: Avis concernant un avant-projet de loi relatif à l'amélioration des méthodes particulières de recherche et certaines méthodes d'enquête concernant Internet, les communications électroniques et les télécommunications (CO-A-2016-021)

La Commission de la protection de la vie privée (ci-après "la Commission") ;

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (ci-après LVP), en particulier l'article 29 ;

Vu la demande d'avis de Monsieur Koen Geens, Ministre de la Justice, reçue le 31/03/2016;

Vu le rapport de Madame Séverine Waterbley Severine et de Monsieur Franck Schuermans ;

Émet, le 18 mai 2016, l'avis suivant :

I. OBJET DE LA DEMANDE D'AVIS

1. La Commission de la protection de la vie privée (ci-après désignée comme "la Commission") a reçu, le 31 mars 2016, une demande d'avis de Monsieur Koen Geens, Ministre de la Justice, concernant un avant-projet de loi relatif à l'amélioration des méthodes particulières de recherche et certaines méthodes d'enquête concernant Internet, les communications électroniques et les télécommunications.

2. Cet avant-projet de loi contient un certain nombre de modifications apportées au Code d'instruction criminelle et au Code pénal et vise surtout à apporter un certain nombre de corrections concernant l'information et l'instruction, d'une part dans l'application des méthodes particulières de recherche et d'autre part dans le cadre de certaines méthodes d'enquête spécifiques à la recherche sur Internet et aux communications électroniques et télécommunications. C'est surtout ce dernier aspect qui constitue l'essentiel de la proposition.

3. En effet, les criminels recourent de plus en plus régulièrement aux possibilités que leur offre la technologie de l'information. Le présent avant-projet de loi entend dès lors créer un cadre juridique plus adapté notamment pour la recherche dans un système informatique, l'activité sur Internet pour les services de police et l'interception ainsi que la prise de connaissance de communications électroniques.

II. INTRODUCTION GÉNÉRALE

4. Au fil des années, le droit à la protection des données à caractère personnel est apparu, à côté du droit à la protection de la vie privée, comme un droit fondamental indépendant et à part entière. Cela s'est traduit de la manière la plus claire dans la "Charte des droits fondamentaux de l'Union européenne du 12 décembre 2007" dans laquelle, outre l'article 7, "Respect de la vie privée et familiale", l'article 8 suivant "Protection des données à caractère personnel" le formule explicitement. La distinction entre la "vie privée" et la "protection des données" est ainsi plus précise que classiquement déduite de l'article 22 de la Constitution belge ou de l'article 8 de la CEDH.[1]

5. Ces deux droits fondamentaux ne sont pas uniquement complémentaires mais font classiquement partie des "libertés" et doivent faire l'objet d'une approche et d'une application conjointes avec les autres droits et libertés. Ce n'est pas un hasard que sous le titre "Libertés" de la Charte, les articles 7 et 8 soient précédés de l'article 6 qui précise cette interférence sous

[1] Voir Dirk De Bot, "Gegevensverwerking in de publieke sector", Brussel 59, ASP/Politea, en particulier la Partie I : "Privacyrecht en gegevensverwerking in de publieke sector" p. 59-132.

le titre "Droit à la liberté et à la sûreté" : "*Toute personne a droit à la liberté et à la sûreté*". D'ailleurs, la Loi Vie Privée ou LVP[2] fait également le lien avec les autres droits fondamentaux en orientant à l'article 2 le droit à la protection des données vers le but : la protection de ses libertés et droits fondamentaux.

6. Le droit de chaque citoyen à la "sûreté" et à l' "intégrité" physique et morale est tout aussi digne de protection que le droit à la protection des données à caractère personnel. On argumente ainsi généralement que ces deux droits et revendications doivent parvenir à un juste équilibre et c'est exact. Mais uniquement en partie : il est tout aussi vrai que ces droits doivent se compléter, se renforcer et se soutenir mutuellement. Ainsi, il n'est pas possible de constituer une protection cohérente des données à caractère personnel et de la vie privée sans prévoir une mise en oeuvre de celle-ci. Le droit pénal général classique et le droit pénal particulier devront également apporter une contribution importante à cet effet. Ce n'est pas pour rien que la LVP actuelle se conclut par un chapitre "Dispositions pénales". D'ici quelques jours, à partir du 24 mai, le nouveau "règlement général de protection des données"[3] sera d'application. Il mise sur cette mission d'application de la loi en imposant des obligations supplémentaires aux autorités en général et à l' "autorité de contrôle" (l'ancienne commission vie privée) en particulier. Ici aussi, le lien avec les autres "libertés et droits fondamentaux" (article 1.2.) est établi et des restrictions sont prévues à l'article 23.

7. Afin de protéger les libertés et droits fondamentaux, non seulement le droit matériel est nécessaire mais également l'instrument, la procédure pénale. Une enquête judiciaire est par excellence invasive dans la vie privée, également lorsque la protection de la vie privée et des données à caractère personne est en cause. Lorsque de nouvelles formes de communication ou des formes de communication en évolution se présentent ou lorsqu'on constate que le besoin d'un examen approfondi ou d'une collecte d'informations est nécessaire, ces méthodes de recherche doivent également être adaptées ou peuvent être appliquées. Et ce en vue de protéger ce même citoyen concerné par ces données à caractère personnel.

---

[2] Ladite Loi vie privée belge est en fait une véritable loi de protection des données et cela ressort également du titre qui l'exprime de manière très précise "loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel"

[3] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE*.

III. EXAMEN QUANT AU FOND

1. Remarque préliminaire

8. Comme précisé ci-dessus, le contenu et la portée de certaines modifications apportées au Code d'Instruction Criminelle et au code pénal toucheront aux droits fondamentaux, tel que le droit fondamental à la vie privée, protégé par l'article 8, alinéa 1 de la CEDH et l'article 22 de la Constitution, et le droit à l'inviolabilité du domicile, tel que protégé par l'article 17 du Pacte international relatif aux droits civils et politiques et l'article 15 de la Constitution.

9. Ces modifications concernant l'information et l'instruction, en particulier dans l'application des dites méthodes particulières de recherche (en abrégé "MPR")[4] et surtout de certaines autres méthodes[5] (de recherche) intrusives en matière de recherche sur Internet et de télécommunications devront passer le test de l'article 8, § 2 de la CEDH, qui pose non seulement l'exigence d'une base légale mais dispose également que l'ingérence dans l'exercice de ce droit doit être proportionnelle et nécessaire dans une société démocratique.

10. La jurisprudence de la Cour européenne des droits de l'Homme met généralement l'accent sur la nécessité impérieuse d'éviter des ingérences arbitraires dans la vie privée des personnes concernées. Il en résulte que toute disposition nationale en la matière doit être suffisamment claire et précise pour indiquer à tous de manière adéquate dans quelles circonstances elle habilite la puissance publique à recourir à des mesures de recherche secrètes. Outre cette exigence commune, la Cour a énoncé d'autres garanties minimales. Les réglementations nationales doivent préciser la nature des infractions susceptibles de donner lieu à un mandat d'interception, indiquer les restrictions subjectives applicables à certaines catégories de personnes, fixer les limites de la durée de cette surveillance, définir la (les) procédure(s) à suivre pour l'examen, l'utilisation, le partage et la conservation des données obtenues, contenir les précautions à prendre lors de la communication de ces informations à des tiers, définir les circonstances dans lesquelles ces informations peuvent être effacées ou détruites[6], et prévoir un examen *ex ante* ou *ex post* par un juge ou tout autre expert véritablement (objectivement et subjectivement) impartial, qui soit indépendant dans les faits et hiérarchiquement de l'organe responsable de l'imposition de pareilles mesures et habilité à

[4] Pour rappel : le Code d'instruction criminelle connaît trois sorte de méthodes particulières de recherche, à savoir l'observation, l'infiltration et le recours aux indicateurs.

[6] Weber et Saravia c. Allemagne (déc.) ; Association for European Integration and Human Rights et Ekimdzhiev c. Bulgarie ; Liberty et autres organisations c. Royaume-Uni.

garantir l'authenticité et la fiabilité des enregistrements. Si la législation nationale omet de faire référence à certains des éléments susmentionnés, la Cour va également étendre son examen à la jurisprudence nationale qui est ou peut être pertinente aux fins de la protection des individus.[7]

2. Analyse de l'article 2 de l'avant-projet – modifications apportées à l'article 39*bis* du Code d'instruction criminelle - la recherche non secrète dans des systèmes informatiques

11. Cet article modifie l'article 39*bis* du Code d'instruction criminelle (CIC) et concerne la recherche non secrète dans des systèmes informatiques. L'article intègre le contenu de l'article 88*ter* du CIC relatif à l'extension de la recherche dans un système informatique ou une partie de celui-ci dans l'article 39*bis* du même code afin d'obtenir un article cohérent sur la recherche non secrète et son extension dans des systèmes informatiques. Le contenu de l'article 88*ter* du CIC étant repris dans son intégralité, l'article n'a plus de raison d'être et est abrogé.

12. Par ailleurs, les modifications apportées à l'article 39*bis* du CIC visent à clarifier les compétences des différents acteurs en matière de recherche dans un système informatique ou une partie de celui-ci. L'article 39*bis* du CIC actuel manque en effet de clarté à cet égard.

13. Un régime à quatre niveaux est dès lors prévu.

14. Le premier niveau est celui de la recherche dans un système informatique qui a été saisi dans le cadre d'une instruction en matière pénale (qui peut donc être aussi bien une information qu'une instruction). Cette recherche peut être exécutée par l'officier de police judiciaire sans autorisation préalable du procureur du Roi ou du juge d'instruction (art. 39*bis*, § 2 du CIC en avant-projet).

15. La Commission constate que la Cour de Cassation a indiqué dans son arrêt du 11 février 2015[8] que le droit actuel permet déjà aux fonctionnaires de police de prendre connaissance des données d'un GSM qui a été saisi. La Cour met ainsi un terme à un flou datant de plusieurs années concernant les compétences policières exactes de "lecture" lorsqu'un GSM ou un smartphone a été saisi.

---

[7] Ivana Roagna, La protection du droit au respect de la vie privée et familiale par la Convention européenne des droits de l'homme.

[8] Cass., 11 février 2015 (AR P.14.1739.F), juridat..

16. Le deuxième niveau concerne la recherche dans un système informatique qui n'a pas été saisi mais pour lequel les conditions d'une saisie sont réunies. Dans ce cas, la recherche doit être autorisée par le procureur du Roi.[9] (art. 39*bis*, § 2, 2e alinéa et § 3 du CIC en avant-projet).

17. La Commission constate que cela est déjà prévu en substance par l'article 39*bis*, § 2 du CIC actuel.

18. Le troisième niveau concerne la recherche non secrète et l'extension dans des systèmes informatiques. L'article 39*bis*, § 4 du CIC en avant-projet fixe les limites de l'extension de la recherche non secrète dans un système informatique ou une partie de celui-ci qui se trouve dans un autre lieu que celui où la recherche est effectuée.

19. L'extension de la recherche dans un système informatique ou une partie de celui-ci peut être ordonnée par le procureur du Roi :
    - si cette extension est nécessaire pour la manifestation de la vérité à l'égard de l'infraction qui fait l'objet de la recherche ; et
    - si d'autres mesures seraient disproportionnées, ou s'il existe un risque que, sans cette extension, des éléments de preuve soient perdus.

20. L'avant-projet justifie l'intervention du procureur du Roi (de manière à qu'ainsi, il ne s'agisse pas d'une compétence exclusive du juge d'instruction) au motif que l'article 39*bis* du CIC se limite aux recherches non secrètes. Il n'y a ainsi, en aucune façon, violation secrète de la vie privée de personnes et/ou d'inculpés. Au contraire, le ministère public doit informer le responsable du système informatique de la recherche. Par ailleurs, le transfert de cette mesure (c'est-à-dire l'extension de la recherche) de l'article 88*ter* du CIC vers l'article 39*bis* du CIC, conférant ainsi cette compétente non seulement au juge d'instruction mais aussi au procureur du Roi, se justifie par le fait que, avec le développement de nouvelles technologies, la distinction entre ce qui se trouve sur l'appareil et ce qui se trouve dans le cloud (ce qui rend nécessaire une extension de la recherche) devient en partie artificielle.

21. Si la Commission estime que l'intervention d'un juge d'instruction inclut davantage de garanties contre l'intrusion dans la vie privée, elle ne s'oppose pas au fait que le ministère public soit compétent en matière de recherche non secrète dans des systèmes informatiques étant donné qu'en la matière, comme précisé, le magistrat du parquet est tenu d'informer "le responsable du système informatique de la recherche effectuée dans le système informatique ou de son extension, sauf si son identité ou son adresse ne peuvent être raisonnablement

[9] La Commission part du principe que chaque fois que l'avant-projet parle du "procureur du Roi", on vise également le procureur fédéral, l'auditeur du travail et le procureur général, selon le cas.

retrouvées, et lui communique le cas échéant un résumé des données qui ont été copiées, rendues inaccessibles ou retirées" (art. 39*bis*, § 5 du CIC dans l'avant-projet). De manière plus générale, la Commission rappelle d'ailleurs que le ministère public est également indépendant dans l'exercice des recherches et poursuites individuelles (art. 151 de la Constitution) et doit veiller à la légalité des moyens de preuve ainsi qu'à la loyauté avec laquelle ils sont rassemblés (art. 28*bis*, § 3, dernier alinéa du CIC). Ce principe de loyauté implique, selon la Cour de cassation, que toutes les données collectées par le parquet sont jointes au dossier répréssif, en particulier les données à décharge[10]. Ainsi, la Cour de cassation adhère également à l'avis de la Cour constitutionnelle qui a déjà affirmé à plusieurs reprises ce qui suit : "*Il existe, entre le ministère public et l'inculpé, une différence fondamentale qui repose sur un critère objectif : le premier accomplit, dans l'intérêt de la société, les missions de service public relatives à la recherche et à la poursuite des infractions (...) et il exerce l'action publique (...) ; le second défend son intérêt personnel*"[11].

22. La Commission constate par ailleurs que la pénétration en secret dans un système informatique et sa mise sous surveillance restent soumises à l'intervention du juge d'instruction (art. 90ter et suivants CIC).

23. La Commission constate également que seul le juge d'instruction peut ordonner l'usage de "*fausses clés* [12]". Le législateur précise toutefois dans le commentaire de l'article 2 en avant-projet que : "*cela ne vaut que pour les données qui ne sont pas situées dans le système informatique qui a été saisi ou qui pourrait être saisi. Si l'usage de "fausses clés" additionnelles à celles pour accéder au contenu général du système informatique est nécessaire pour accéder à certaines parties spécifiques du stockage interne du système informatique, le procureur du Roi reste compétent pour ordonner l'usage de ces "fausses clés" ".* La répartition des compétences entre le parquet et le juge d'instruction dans le cadre de la recherche informatique non secrète en devient assurément complexe dans un environnement informatique qui évolue rapidement. Si la Commission a bien compris, le parquet est habilité à effectuer une recherche informatique non secrète ainsi qu'une extension de celle-ci. Si nécessaire, le parquet peut utiliser de "fausses clés" pour réaliser cette recherche informatique non secrète (§ 4*ter*, 1er alinéa en avant-projet), mais dès qu'il s'agit d'une extension (en d'autres termes, qu'il y a donc des connexions en réseau, ce qui sera quasi toujours le cas), un juge d'instruction doit être requis (§ 4*ter*, 2e alinéa en projet).

---

[10] Voir notamment Cour de cassation du 19 décembre 2012, n° P. 12.1310.F/1

[11] Voir notamment Cour constitutionnelle du 1er décembre 1994, n° 82/1994 ; voir également les arrêts n° 22/95, n° 43/95, n° 76/95, n° 49/97, n° 29/98, n° 58/98, n° 12/2000, n° 58/2001, n° 69/2001, n° 5/2002, n° 70/2005, n° 191/2005, n° 182/2008, http://www.const-court.be/fr/common/home.html.

[12] L'installation de dispositifs techniques dans les systèmes informatiques concernés en vue du décryptage et du décodage de données stockées, traitées ou transmises par ce système.

24. La Commission en prend acte.

25. Le quatrième niveau concerne les systèmes informatiques qui ne sont pas susceptibles de saisie. Dans ce cas, la recherche nécessitera l'autorisation d'un juge d'instruction, le cas échéant dans le cadre de la mini-instruction.

26. La Commission en prend acte.

3. Analyse des articles 3 et 4 de l'avant-projet – insertion des articles 39*ter* et 39*quater* du Code d'instruction criminelle – conservation et divulgation rapides de données informatiques

27. Le nouvel article 39*ter* du CIC matérialise la transposition des articles 16 et 17 de la Convention sur la cybercriminalité[13] concernant la conservation et la divulgation rapides de données informatiques au niveau national.

28. Le nouvel article 39*quater* est la transposition des articles 29 et 30 de la Convention sur la cybercriminalité concernant la conservation et la divulgation rapides de données informatiques au niveau international.

29. Ces articles prévoient qu'il peut être ordonné à une ou plusieurs personnes physiques ou personnes morales de conserver les données qui sont en leur possession ou sous leur contrôle "*s'il existe des raisons de croire que des données stockées, traitées ou transmises par un système informatique au moyen d'un système informatique sont particulièrement susceptibles de perte ou de modification* ».

30. La Commission constate que cette mesure peut être prise par le ministère public au niveau international. Elle prend acte du fait que la mesure pourra être ordonnée au niveau national "*par tout officier de police judiciaire*" et n'a aucune remarque particulière à cet égard

4. Analyse des articles 6 et 15 de l'avant-projet - modifications apportées aux articles 46*quinquies* et 89 du Code d'instruction criminelle – contrôle visuel discret

[13] Convention sur la cybercriminalité (STE 185), Budapest, Conseil de l'Europe, 23 décembre 2001.

31. Outre la pénétration dans un lieu privé, il devient désormais possible, lors d'un contrôle visuel discret, de prendre connaissance du contenu des objets fermés qui s'y trouvent, comme les armoires fermées à clé ou les coffres-forts par exemple.

32. Le commentaire de l'article 6 précise que : "*par "objet fermé", on ne vise toutefois pas un système informatique. Pour pouvoir explorer des systèmes informatiques (comme des laptops ou des smartphones), une ordonnance du juge d'instruction est toujours requise. Les services de recherche peuvent néanmoins pénétrer dans un système informatique si cela a pour seule finalité de placer, de réparer ou de retirer un moyen technique dans le cadre d'une observation.*»

33. La Commission observe que la prise d'échantillons est déjà possible. En effet, comme indiqué dans l'exposé des motifs de la loi du 6 janvier 2003, "*il peut être indiqué que les fonctionnaires de police qui, à l'occasion d'un contrôle visuel discret, découvrent une quantité suspecte de poudre blanche ou de substances liquides en prélèvent un échantillon afin de pouvoir déterminer avec certitude s'il s'agit ou non de drogue ou d'une préparation d'hormones* [14]».

34. Le § 5 de l'article 46*quinquies* du CIC en projet octroie désormais la possibilité pour le service de police d'emporter un objet, et non un simple échantillon, si l'examen de l'objet en question ne peut se faire sur place et si l'information ne peut être obtenue d'une autre manière. Il est précisé *in fine* que "*l'objet en question est remis en place dans les plus brefs délais, à moins que cela n'entrave le bon déroulement de l'enquête* ».

35. La Commission en prend acte.

36. L'article 89ter du CIC en projet instaure également une nouvelle possibilité de recherche en secret
dans un système informatique, mais uniquement aux fins mentionnées à l'article 46*quinquies*, § 2 du CIC.

37. La finalité de cette mesure est de vérifier si des preuves existent mais pas de les collecter. Seuls des échantillons peuvent être prélevés. Dans le cadre d'un contrôle visuel discret dans un système informatique, cela signifie qu'il peut être pris une copie ciblée de certaines données.

[14] Doc. Parl. 50-1688/001, p. 59.

38. La distinction entre la recherche en secret dans un système informatique conformément à l'article 89*ter* du CIC et la recherche en secret dans un système informatique conformément à l'article 90*ter* du CIC réside principalement dans la finalité de la mesure. La finalité de l'article 89*ter* du CIC est de permettre la recherche de preuves d'infractions, mais les preuves découvertes ne peuvent pas être collectées, ni utilisées, et seuls des échantillons peuvent être prélevés. En d'autres termes, le contrôle visuel discret dans un système informatique est un instrument orienté qui permet une intrusion graduelle dans la vie privée et la prise de prélèvements qui, le cas échéant, peuvent justifier une mesure encore plus intrusive.

39. II a été décidé de classer le contrôle visuel discret (pour d'autres finalités que le simple placement, la simple réparation ou la simple récupération d'un moyen technique visant à pouvoir réaliser une observation) dans un système informatique sous l'article 89*ter* et non sous l'article 46*quinquies*, bien que l'on puisse en principe défendre le fait qu'un système informatique - par exemple un compte Hotmail, un compte Facebook, un compte iCloud... - est un lieu privé qui n'est pas un domicile. Vu l'étendue et le caractère sensible de la vie privée de personnes en ligne ou dans le "cloud", combinés au fait que cette vie privée peut faire l'objet d'une approche "en secret" lors d'un contrôle visuel discret, cette opération doit s'effectuer de manière cohérente sous le contrôle du juge d'instruction.

40. À la lecture de ces dispositions, la Commission constate que les systèmes informatiques se voient octroyer la même protection que le domicile dans le cadre du contrôle visuel discret et en prend acte.

5. Analyse de l'article 7 de l'avant-projet – insertion de l'article 46*sexies* du Code d'instruction criminelle – interactions et infiltrations qui ont uniquement lieu sur Internet

41. Cet article introduit la possibilité de procéder à une infiltration ou à une interaction sur Internet[15] qui ne vise pas uniquement une vérification ciblée ou une arrestation. On parle parfois également de ce qu'on appelle un "infiltration-light".

42. Le procureur du Roi peut l'autoriser si "*les nécessités de l'enquête l'exigent" ;* si *"les autres moyens d'investigations ne semblent pas suffire à la manifestation de la vérité*" et s'il "existe des indices sérieux qu'une ou plusieurs personnes commettent ou commettraient des infractions pouvant donner lieu à un emprisonnement correctionnel principal d'un an ou à une

[15] La notion d'Internet doit être comprise au sens large et comprend notamment le "dark web".

peine plus lourde ».

43. La Commission estime que des interactions sur Internet peuvent avoir un impact sur la vie privée de la personne concernée. La Commission note que l'article 46*sexies*, § 4, al. 2 du CIC prévoit que les contacts pertinents soient enregistrés. Cette mesure rend la mesure beaucoup plus transparente a posteriori et évite les risques d'abus. Par ailleurs, l'inculpé, le prévenu, la partie civile ou leur conseil peuvent être autorisés par le procureur du Roi à consulter l'ensemble ou des parties des contacts enregistrés.

44. À la lecture de l'article 46*sexies* du CIC en projet et du commentaire de l'article, la Commission ne perçoit cependant pas ce qui est visé par "*une infiltration ou à une interaction sur Internet qui ne vise pas uniquement une vérification ciblée ou une arrestation*". L'exclusion de l'application de l'article 46*sexies* du CIC à "*l'interaction personnelle de fonctionnaires de police avec une ou plusieurs personnes sur Internet, qui n'a pour finalité directe qu'une vérification ciblée ou une arrestation"* apparait pour le moins énigmatique au regard du fait que la mesure visée par l'article 46sexies du CIC ne peut absolument être ordonnée par le procureur du Roi que s'il existe, entre autres, "*des indices sérieux qu'une ou plusieurs personnes commettent ou commettraient des infractions pouvant donner lieu à un emprisonnement correctionnel principal d'un an ou à une peine plus lourde* ». Il semble qu'avec la dispositon d'exception envisagée, il soit possible pour des fonctionnaires de police d'entreprendre de manière autonome une interaction sur Internet, ayant pour but une vérification ciblée ou une arrestation d'une personne.

45. La Commission présume donc qu'avec ce passage, tel que formulé au § 1, 3e alina, les fonctionnaires de police pourront "patrouiller" sur Internet. Dans ce cas, l'article 46*sexies* du CIC doit toutefois être libellé de manière plus claire. La question est en effet de savoir si cette disposition d'exception est en soi suffisamment claire et si cette compétence autonome de la police telle qu'envisagée ne doit pas en soi être inscrite soit dans le Code d'instruction criminelle, soit dans la Loi sur la fonction de police.

46. À cet égard, la Commission attire l'attention du demandeur d'avis sur son avis n° 13/2015 du 13 mai 2015 concernant des avant-projets de loi portant dispositions diverses – modifications de la loi portant création d'un organe de recours en matière d'habilitations de sécurité, de la loi sur la fonction de police et de la loi du 18 mars 2014 relative à la gestion de l'information policière.

47. Une des modifications envisagées de la loi du 5 août 1992 *sur la fonction de police* visait précisément à définir à l'article 26 que soient "*considérés comme lieux accessibles au public,*

tous les lieux de connexion à Internet, ou à d'autres réseaux de communication électronique, accessibles au public, quelles que soient les conditions formelles d'accès à accomplir. Les fonctionnaires de police sont autorisés à visiter, et à analyser ces lieux, de même qu'à prendre des copies ».

48. Eu égard à une telle définition des "lieux accessibles au public", les fonctionnaires de police pourraient être amenés à "patrouiller" sur Internet afin notamment d'effectuer une vérification ciblée ou une arrestation. Cette compétence doit cependant être formulée clairement dans une loi afin de respecter les principes de légitimité et de prévisibilité. La Commission ne comprend pas pourquoi il n'est apparemment plus question de la modification envisagée de l'article 26 de la loi sur la fonction de police au sens où on semble manifestement quand même vouloir indirectement la mettre en oeuvre via l'article 46*sexies* du CIC en projet.

6. Analyse de l'article 14 de l'avant-projet - modifications apportées à l'article 88*quater* du Code d'instruction criminelle - obligation de collaboration

49. L'article 14 impose des peines plus sévères aux personnes qui ne collaborent pas à la recherche dans un système informatique ou à son extension. L'Exposé des motifs motive cet article comme suit : "*Cette sanction plus sévère doit envoyer un signal clair aux personnes qui ne prêtent pas leur collaboration ou qui sapent l'enquête. (..) Compte tenu de l'état actuel de la technologie et de son évolution attendue dans ce domaine, il est souvent particulièrement difficile pour les services de recherche, voire impossible, d'accéder à des données d'un système informatique sans l'aide d'externes qui en connaissent le fonctionnement, qui savent quel est le cryptage utilisé, etc.*"

50. La Commission fait remarquer que cette obligation de collaboration peut dans certains cas être contraire à ce que prescrit l'article 48 de la loi *relative aux communications électroniques* du 13 juin 2005 (ci-après la "LCE"). Cette dernière disposition affirme notamment que l'utilisation du cryptage est libre. On peut également en déduire que les utilisateurs de cryptages ne sont pas obligés de conservés les clés. Les utilisateurs qui n'ont pas conservé les clés peuvent évidemment fournir peu d'informations utiles aux services de recherche dans le cadre de leur obligation de collaboration telle que prévue à l'article 88*quater* du CIC et il semble contestable qu'ils pourraient en être sanctionné, justement vu l'article 48 LCE précité.

7. Analyse des articles 17 et sv. de l'avant-projet - modifications apportées à l'article 90*ter* du Code d'instruction criminelle – recherche en secret dans un système informatique et prise de connaissance en secret de communications

51. L'article 90*ter* du CIC (relatif à l'interception de télécommunications) a été revu en profondeur en :
    - introduisant la recherche en secret dans des systèmes informatiques ;
    - rassemblant en une seule mesure la recherche en secret dans des systèmes informatiques et l'interception de télécommunications[16]. En effet, du fait de l'évolution technologique, il n'est souvent plus possible de faire la distinction entre les deux. Il est préférable de parler à présent de la prise de connaissance en secret de communications et d'informations ;
    - étendant la liste des infractions pour lesquelles la mesure de l'article 90*ter* est possible

52. L'alinéa 1er, § 1er de l'article 90*ter* du CIC décrit la mesure que le juge d'instruction peut ordonner. Celle-ci comprend l'interception, la prise de connaissance, l'exploration et l'enregistrement de communications non accessibles au public[17] ou de données d'un système informatique ou d'une partie de celui-ci, ainsi que l'extension d'une recherche dans un système informatique.

53. La Commission rappelle que la Cour Européenne des droits de l'Homme considère que les conversations téléphoniques se trouvent comprises dans les notions de "vie privée" et de "correspondance" au sens de l'article 8 CEDH[18].

54. La Commission constate que cette mesure ne peut être ordonnée que dans des cas exceptionnels, lorsque les nécessités de l'instruction l'exigent, s'il existe des indices sérieux que cela concerne une infraction déterminée et si les autres moyens d'investigation ne suffisent pas à la manifestation de la vérité.

55. La Commission constate également que dans l'arrêt n° 202/2004 du 21 décembre 2004 de la Cour constitutionnelle relatif à la loi du 6 janvier 2003 *concernant les méthodes particulières de recherche et quelques autres méthodes d'enquête*, la Cour a estimé que le contrôle visuel discret (article 89*ter* du CIC) et l'observation effectuée à l'aide de moyens techniques afin d'avoir une vue dans un domicile (article 56*bis*, alinéa 2 du CIC) sont des mesures qui peuvent être comparées, en ce qui concerne l'ingérence dans le droit à la vie privée, à la perquisition

[17] Selon le commentaire des articles, il convient d'entendre par "communications non accessibles au public" des communications ou communications électroniques qui ont lieu dans la sphère privée. Il s'agit d'une notion globale qui recouvre également les termes "communications ou télécommunications" privées" de l'ancien article 90*ter*.

[18] Voir, notamment, Klass et autres, précité, § 41, Malone c. Royaume-Uni, 2 août 1984, § 64, série A no 82, et Lambert c. France, 24 août 1998, § 21, Recueil des arrêts et décisions 1998-V.

et aux écoutes et enregistrements des communications et télécommunications privées. Selon la Cour, ces mesures ne peuvent être autorisées qu'aux mêmes conditions que celles appliquées à l'égard de la perquisition et des écoutes téléphoniques.

56. C'est la raison pour laquelle le contrôle visuel discret et l'observation effectuée à l'aide de moyens techniques afin d'avoir une vue dans un domicile sont exclus du champ d'application de la mini-instruction.

57. Cette exclusion s'applique à la mesure d'enquête de la recherche en secret et de la prise de connaissance en secret de communications. C'est pourquoi cette mesure est intégrée dans l'article 90*ter*, § 1*er* du CIC, qui présente les mêmes caractéristiques. La modification n'aboutit pas seulement à ajouter la recherche secrète dans un système informatique à côté de la mesure déjà existante de l'interception des communications. Elle aboutit plutôt à fusionner les deux mesures en une seule afin de s'adapter aux évolutions technologiques qui rendent difficile la distinction entre, d'une part, la recherche dans un système informatique et, d'autre part, l'interception des communications.

58. La Commission prend acte du fait que des recherches "au hasard" ou "exploratoires" ne peuvent être effectuées. En effet, l'article 90*ter*, § 1er, al. 4 du CIC en projet décrit la finalité de la mesure : la mesure ne pourra uniquement être ordonnée qu'afin de rechercher des données pouvant servir à la manifestation de la vérité.

59. La Commission estime cependant que la mesure élargit considérablement l'éventail des domaines de nature à faire l'objet d'une recherche en secret et souhaite attirer l'attention du législateur sur le fait que cette extension doit faire l'objet d'un débat parlementaire approfondi.

60. Au niveau des mesures garantissant la sécurité et la confidentialité des données à caractère personnel, la Commission prend acte que l'article 90*septies* du CIC prévoit que "les moyens appropriés sont utilisés pour garantir l'intégrité et la confidentialité des communications non accessibles au public ou données d'un système informatique qui ont été enregistrées" et que l'article 90*octies*, § 2 du CIC stipule que "toute violation du secret est punie conformément à l'article 458 du Code pénal".

61. La Commission prend acte du fait que toute personne ayant fait l'objet de la mesure visée à l'article 90*ter* du CIC sera avisée de la nature de la mesure et des dates auxquelles elle a été effectuée (sauf si l'identité ou l'adresse de cette personne ne peut raisonnablement être retrouvée).

62. Cette information à la personne concernée est conforme à la jurisprudence de la Cour européenne des droits de l'Homme qui énonce que "*la question de la notification ultérieure de mesures de surveillance est indissolublement liée au caractère effectif des recours judiciaires et donc à l'existence de garanties effectives contre les abus des pouvoirs de surveillance ; si on ne l'avise pas des mesures prises à son insu, l'intéressé ne peut guère, en principe, en contester rétrospectivement la légalité en justice* »[19].

8. Analyse de l'article 33 de l'avant-projet – création d'une banque de données d'empreintes vocales

63. L'article 33 de l'avant-projet crée une banque de données des empreintes vocales qui a pour finalité d'aider à identifier, via un logiciel, sur la base de leurs voix, des suspects et des personnes condamnées, dont l'empreinte vocale a déjà été enregistrée dans le cadre de dossiers pour lesquels une écoute téléphonique ou un enregistrement d'une communication est ou a été approuvé par le magistrat compétent.

64. La Commission estime qu'une telle base de donnée doit en effet être prévue par la loi.

65. La Commission observe que seules pourront être conservées les empreintes vocales de personnes qui font ou ont fait l'objet d'une mesure d'écoute et qui sont visées à l'article 44/5, § 3, 1°, de la loi sur la fonction de police[20] (suspects et personnes condamnées). Les empreintes vocales d'autres personnes dont la voix est enregistrée lors d'une écoute téléphonique ou d'un enregistrement d'une communication, comme les témoins ou les personnes impliquées tout à fait par hasard, ne peuvent pas être établies ou conservées.

66. La Commission rappelle que dans sa jurisprudence, la Cour européenne des droits de l'Homme a maintes fois constaté que "*l'interception secrète de conversations téléphoniques entrait dans le champ d'application de l'article 8 pour ce qui est du droit au respect tant de la vie privée que de la correspondance. Certes, les enregistrements sont en général effectués dans le but d'utiliser le contenu de conversations d'une manière ou d'une autre, mais la Cour n'est pas convaincue que des enregistrements destinés à servir d'échantillons de voix puissent passer pour échapper à la protection qu'offre l'article 8. La voix de la personne concernée a tout de même été enregistrée sur un support permanent et soumise à un processus d'analyse directement destiné à identifier cette personne à la lumière d'autres données personnelles.*

[19] Weber et Saravia c. Allemagne ; Klass et autres c. Allemagne.

[20] Loi du 5 août 1992 *sur la fonction de police*, *M.B.* du 22 décembre 1992.

(...) l'enregistrement et l'analyse de leurs voix à cette occasion doivent cependant être considérés comme relevant des données personnelles les concernant »[21].

67. La Commission prend acte du fait que cette banque de données des empreintes vocales fait partie de la Banque de données Nationale Générale (BNG), dont les finalités sont prévues à l'article 44/7 de la loi sur la fonction de police. Les règles de gestion de la BNG prévues dans les articles 44/7 à 44/11/1 de la loi sur la fonction de police sont donc d'application. À cet égard, un délai de conservation de 10 ans est également prévu. En outre, le contrôle de cette banque de donnée est aussi garanti par l'Organe de contrôle de l'information policière.

PAR CES MOTIFS,
la Commission,

émet un avis ***favorable*** concernant l'avant-projet de loi relatif à l'amélioration des méthodes particulières de recherche et certaines méthodes d'enquête concernant Internet, les communications électroniques et les télécommunications moyennant la prise en compte des remarques émises aux points 44 à 48, 50 et 59.

L'Administrateur f.f., Le Président,

(sé) An Machtens (sé) Willem Debeuckelaere

[21] P.G. et J.H. c. Royaume-Uni - 44787/98. Arrêt 25.9.2001.