Art. 7. La Secrétaire d'Etat à l'Egalité des chances est chargée de l'exécution du présent arrêté.

Donné à Bruxelles, le 6 décembre 2018.

PHILIPPE

Par le Roi :

La Secrétaire d'Etat à l'Egalité des Chances,
Z. DEMIR

Art. 7. De Staatsecretaris voor Gelijke kansen is belast met de uitvoering van dit besluit.

Gegeven te Brussel, op 6 december 2018.

FILIP

Van Koningswege :

De Staatsecretaris voor Gelijke Kansen,
Z. DEMIR

COUR CONSTITUTIONNELLE

[2019/200144]

Extrait de l'arrêt n° 174/2018 du 6 décembre 2018

Numéro du rôle : 6711

En cause : le recours en annulation des articles 2 et 7 de la loi du 25 décembre 2016 « portant des modifications diverses au Code d'instruction criminelle et au Code pénal, en vue d'améliorer les méthodes particulières de recherche et certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications et créant une banque de données des empreintes vocales », introduit par l'ASBL « Ligue des Droits de l'Homme » et l'ASBL « Liga voor Mensenrechten ».

La Cour constitutionnelle,

composée des présidents F. Daoût et A. Alen, et des juges L. Lavrysen, J.-P. Snappe, J.-P. Moerman, E. Derycke, T. Merckx-Van Goey, P. Nihoul, T. Giet, R. Leysen, J. Moerman et M. Pâques, assistée du greffier F. Meersschaut, présidée par le président F. Daoût,

après en avoir délibéré, rend l'arrêt suivant :

I. *Objet du recours et procédure*

Par requête adressée à la Cour par lettre recommandée à la poste le 17 juillet 2017 et parvenue au greffe le 19 juillet 2017, un recours en annulation des articles 2 et 7 de la loi du 25 décembre 2016 « portant des modifications diverses au Code d'instruction criminelle et au Code pénal, en vue d'améliorer les méthodes particulières de recherche et certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications et créant une banque de données des empreintes vocales » (publiée au *Moniteur belge* du 17 janvier 2017) a été introduit par l'ASBL « Ligue des Droits de l'Homme » et l'ASBL « Liga voor Mensenrechten », assistées et représentées par Me D. Ribant et Me C. Forget, avocats au barreau de Bruxelles, Me J. Heymans, avocat au barreau de Gand, et Me J. Vander Velpen, avocat au barreau d'Anvers.

(...)

II. *En droit*

(...)

Quant à l'objet du recours

B.1.1. Le recours porte sur les articles 2 et 7 de la loi du 25 décembre 2016 « portant des modifications diverses au Code d'instruction criminelle et au Code pénal, en vue d'améliorer les méthodes particulières de recherche et certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications et créant une banque de données des empreintes vocales » (ci-après : la loi du 25 décembre 2016).

B.1.2. Cette loi vise à apporter un certain nombre de modifications au Code d'instruction criminelle concernant l'information et l'instruction pénales, en particulier dans l'application des méthodes particulières de recherche et de certaines autres méthodes d'enquête spécifiques à la recherche sur Internet et aux télécommunications. Les dispositions modifiées par la loi attaquée ont été introduites dans le Code d'instruction criminelle par diverses lois et « n'ont plus été réformées ou adaptées depuis 2000 », ce qui représente « une éternité dans le monde de la technologie de l'information, en évolution rapide » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1966/001, p. 5). Par la loi attaquée, le législateur a dès lors entendu créer « un cadre juridique plus adapté pour la recherche dans un système informatique et l'interception ainsi que la prise de connaissance de communications électroniques » (*ibid.*, p. 7).

B.1.3. Le premier moyen, qui contient cinq branches, vise l'article 2 de cette loi, qui concerne la recherche dans un système informatique. Le second moyen, qui contient trois branches, vise l'article 7 de cette loi, qui concerne l'infiltration sur Internet.

Quant au premier moyen

En ce qui concerne la disposition attaquée

B.2. L'article 2 de la loi du 25 décembre 2016 modifie l'article 39*bis* du Code d'instruction criminelle de la façon suivante :

1° le paragraphe 1er, qui disposait « Sans préjudice des dispositions spécifiques de cet article, les règles de ce code relatives à la saisie, y compris l'article 28*sexies*, sont applicables aux mesures consistant à copier, rendre inaccessibles et retirer des données stockées dans un système informatique », est complété par les mots « ou une partie de celui-ci »;

2° les paragraphes 2 à 6 sont remplacés par les dispositions suivantes :

« § 2. La recherche dans un système informatique ou une partie de celui-ci qui a été saisi, peut être décidée par un officier de police judiciaire.

Sans préjudice de l'alinéa 1er, le procureur du Roi peut ordonner une recherche dans un système informatique ou une partie de celui-ci qui peut être saisi par lui.

Les recherches visées aux alinéas 1er et 2 peuvent uniquement s'étendre aux données sauvegardées dans le système informatique qui est soit saisi, soit susceptible d'être saisi. À cet effet, chaque liaison externe de ce système informatique est empêchée avant que la recherche soit entamée.

§ 3. Le procureur du Roi peut étendre la recherche dans un système informatique ou une partie de celui-ci, entamée sur la base du paragraphe 2, vers un système informatique ou une partie de celui-ci qui se trouve dans un autre lieu que celui où la recherche est effectuée :

- 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.

L'extension de la recherche dans un système informatique ne peut pas excéder les systèmes informatiques ou les parties de tels systèmes auxquels les personnes autorisées à utiliser le système informatique qui fait l'objet de la mesure ont spécifiquement accès.

En ce qui concerne les données recueillies par l'extension de la recherche dans un système informatique, qui sont utiles pour les mêmes finalités que celles prévues pour la saisie, les règles prévues au paragraphe 6 s'appliquent.

Lorsqu'il s'avère que ces données ne se trouvent pas sur le territoire du Royaume, elles peuvent seulement être copiées. Dans ce cas, le procureur du Roi communique sans délai cette information au Service public fédéral Justice, qui en informe les autorités compétentes de l'État concerné, si celui-ci peut raisonnablement être déterminé.

En cas d'extrême urgence, le procureur du Roi peut ordonner verbalement l'extension de la recherche visée à l'alinéa 1er. Cet ordre est confirmé par écrit dans les meilleurs délais, avec mention des motifs de l'extrême urgence.

§ 4. Seul le juge d'instruction peut ordonner une recherche dans un système informatique ou une partie de celui-ci autre que les recherches visées aux paragraphes 2 et 3 :

- si cette recherche 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 recherche, des éléments de preuve soient perdus.

En cas d'extrême urgence, le juge d'instruction peut ordonner verbalement l'extension de la recherche visée à l'alinéa 1er. Cet ordre est confirmé par écrit dans les meilleurs délais, avec mention des motifs de l'extrême urgence.

§ 5. En vue de permettre les mesures visées à cet article, le procureur du Roi ou le juge d'instruction peut également, sans le consentement du propriétaire ou de son ayant droit, ou de l'utilisateur, ordonner, à tout moment :

- la suppression temporaire de toute protection des systèmes informatiques concernés, le cas échéant à l'aide de moyens techniques, de faux signaux, de fausses clés ou de fausses qualités;

- 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.

Toutefois, seul le juge d'instruction peut ordonner cette suppression temporaire de protection ou cette installation de dispositifs techniques lorsque ceci est spécifiquement nécessaire pour l'application du paragraphe 3.

§ 6. Si des données stockées sont trouvées dans les systèmes informatiques concernés qui sont utiles pour les mêmes finalités que celles prévues pour la saisie, mais que la saisie du support n'est néanmoins pas souhaitable, ces données, de même que les données nécessaires pour les comprendre, sont copiées sur des supports qui appartiennent à l'autorité. En cas d'urgence ou pour des raisons techniques, il peut être fait usage de supports qui sont disponibles pour des personnes autorisées à utiliser le système informatique.

En outre, les moyens techniques appropriés sont utilisés pour empêcher l'accès à ces données dans le système informatique, de même qu'aux copies de ces données qui sont à la disposition de personnes autorisées à utiliser le système informatique, de même que pour garantir leur intégrité.

Lorsque la mesure prévue à l'alinéa 1er n'est pas possible, pour des raisons techniques ou à cause du volume des données, le procureur du Roi utilise les moyens techniques appropriés pour empêcher l'accès à ces données dans le système informatique, de même qu'aux copies de ces données qui sont à la disposition de personnes autorisées à utiliser le système informatique, de même que pour garantir leur intégrité.

Si les données forment l'objet de l'infraction ou ont été produites par l'infraction et si elles sont contraires à l'ordre public ou aux bonnes mœurs ou constituent un danger pour l'intégrité des systèmes informatiques ou pour des données stockées, traitées ou transmises par le biais de tels systèmes, le procureur du Roi utilise tous les moyens techniques appropriés pour rendre ces données inaccessibles ou, après en avoir pris copie, les retirer.

Il peut cependant, sauf dans le cas prévu à l'alinéa 4, autoriser l'usage ultérieur de l'ensemble ou d'une partie de ces données, lorsque cela ne présente pas de danger pour l'exercice des poursuites.

En cas d'extrême urgence et s'il s'agit manifestement d'une infraction visée aux articles 137, § 3, 6°, 140*bis* ou 383*bis*, § 1er, du Code pénal, le procureur du Roi peut ordonner verbalement que tous les moyens appropriés soient utilisés pour rendre inaccessibles les données qui forment l'objet de l'infraction ou ont été produites par l'infraction et qui sont contraires à l'ordre public ou aux bonnes mœurs. Cet ordre est confirmé par écrit dans les meilleurs délais, avec mention des motifs de l'extrême urgence »;

3° l'article est complété par les paragraphes 7 et 8 rédigés comme suit :

« § 7. Sauf si son identité ou son adresse ne peuvent être raisonnablement retrouvées, le procureur du Roi ou le juge d'instruction informe dans les plus brefs délais, le responsable du système informatique de la recherche dans le système informatique ou de son extension. Il lui communique le cas échéant un résumé des données qui ont été copiées, rendues inaccessibles ou retirées.

§ 8. Le procureur du Roi utilise les moyens techniques appropriés pour garantir l'intégrité et la confidentialité de ces données.

Des moyens techniques appropriés sont utilisés pour leur conservation au greffe.

La même règle s'applique, lorsque des données qui sont stockées, traitées ou transmises dans un système informatique sont saisies avec leur support, conformément aux articles précédents ».

B.3.1. L'article 39*bis* du Code d'instruction criminelle, ainsi modifié, concerne les recherches dites « non secrètes » dans un système informatique. En effet, en vertu de son paragraphe 7, le responsable du système informatique concerné doit être informé « dans les plus brefs délais » de la recherche dans le système et, le cas échéant, de l'extension de la recherche vers un système informatique qui se trouve dans un autre lieu.

D'après l'exposé des motifs de la loi du 28 novembre 2000 relative à la criminalité informatique, qui a introduit l'article 39*bis* originaire dans le Code d'instruction criminelle, par « système informatique », il faut comprendre « tout système permettant le stockage, le traitement ou la transmission de données » (*Doc. parl.*, Chambre, 1999-2000, DOC 50-0213/001 et 50-0214/001, p. 12).

B.3.2. En principe, une recherche dans un système informatique ou dans une partie de celui-ci ne peut être ordonnée que par un juge d'instruction, à condition que cette recherche soit nécessaire à la manifestation de la vérité à l'égard de l'infraction qui fait l'objet de la recherche et que les autres mesures d'investigation envisageables soient disproportionnées ou qu'il existe un risque que, sans cette recherche, des éléments de preuve soient perdus (§ 4). Il en va de même de l'extension de la recherche vers un système informatique accessible depuis le système qui fait l'objet de la recherche initiale.

B.3.3. La disposition attaquée apporte plusieurs exceptions à la compétence de principe du juge d'instruction en ce qui concerne les recherches non secrètes.

Premièrement, la recherche dans les données stockées dans un système informatique, ou dans une partie de celui-ci, qui fait l'objet d'une saisie peut être effectuée d'initiative par un officier de police judiciaire, à condition qu'il ne soit pas nécessaire, pour accéder aux données, de supprimer une protection ou de décrypter ou décoder les données. Dans l'hypothèse où il est nécessaire, pour accéder aux données stockées, de supprimer leur protection ou de les décrypter ou décoder, l'officier de police judiciaire doit obtenir à cette fin l'autorisation du procureur du Roi.

Deuxièmement, le procureur du Roi peut ordonner une recherche dans les données stockées dans un système informatique, ou dans une partie de celui-ci, qui n'a pas fait l'objet d'une saisie mais qui pourrait être saisi par lui. Dans cette hypothèse, il peut également ordonner la suppression de la protection éventuelle ou le décryptage ou le décodage des données.

Troisièmement, l'extension de la recherche, commencée dans un système informatique saisi ou qui pourrait l'être, à des données stockées dans un autre système informatique qui peut être atteint par connexion, au départ du système dans lequel la recherche a été commencée, peut être ordonnée par le procureur du Roi. Toutefois, si l'accès aux données stockées dans cet autre système informatique est protégé, le procureur du Roi doit obtenir l'autorisation du juge d'instruction pour supprimer la protection ou pour installer un dispositif technique lui permettant de les décrypter ou de les décoder.

B.3.4. Les recherches secrètes, visées par l'article 90*ter* du Code d'instruction criminelle, ne peuvent être ordonnées que par un juge d'instruction, dans des cas exceptionnels, lorsque les nécessités de l'instruction l'exigent, s'il existe des indices sérieux que cela concerne une des infractions énumérées par cet article et si les autres moyens d'investigation ne suffisent pas à la manifestation de la vérité.

En ce qui concerne le droit au respect de la vie privée

B.4.1. La Cour examine d'abord le premier moyen, en ses première, deuxième et quatrième branches, qui sont prises de la violation du droit au respect de la vie privée garanti par l'article 22 de la Constitution et par l'article 8 de la Convention européenne des droits de l'homme ainsi que, pour les première et deuxième branches, de la violation du principe d'égalité et de non-discrimination garanti par les articles 10 et 11 de la Constitution.

B.4.2. Les parties requérantes font grief à l'article 39*bis* du Code d'instruction criminelle, introduit par la disposition attaquée, d'autoriser des ingérences dans le droit au respect de la vie privée commises par les officiers de police judiciaire ou par les magistrats du parquet, sans contrôle d'un juge indépendant et impartial. Elles estiment que les recherches dans un système informatique visées par l'article 39*bis* occasionnent une atteinte à la vie privée comparable à celle qui est occasionnée par une perquisition qui, elle, ne peut être autorisée que par un juge d'instruction (quatrième branche du moyen). Elles sont également d'avis que la différence de traitement entre les recherches secrètes visées par l'article 90*ter* du même Code, qui doivent toujours être autorisées par un juge d'instruction, et les recherches non secrètes visées par la disposition attaquée qui ne doivent pas avoir été autorisées par un juge d'instruction repose sur un critère qui n'est ni objectif ni pertinent (première branche du moyen). Elles considèrent en outre que la différence de traitement entre les recherches effectuées dans un système informatique saisi, qui peuvent être décidées par un officier de police judiciaire, et les recherches effectuées dans un système informatique non saisi mais susceptible de l'être, qui ne peuvent être décidées que par le procureur du Roi, repose aussi sur un critère qui n'est ni objectif, ni pertinent (deuxième branche du moyen).

B.5. Contrairement à ce que soutient le Conseil des ministres, la circonstance que la législation antérieure à la loi attaquée prévoyait déjà, dans une certaine mesure, la compétence du procureur du Roi pour ordonner la saisie de systèmes informatiques et les recherches dans ces systèmes n'entraîne pas l'irrecevabilité, pour tardiveté, du moyen en sa première branche. En effet, par la disposition attaquée, le législateur a légiféré à nouveau dans cette matière et a confirmé et étendu la compétence du procureur du Roi.

B.6.1. L'article 22 de la Constitution dispose :

« Chacun a droit au respect de sa vie privée et familiale, sauf dans les cas et conditions fixés par la loi.

La loi, le décret ou la règle visée à l'article 134 garantissent la protection de ce droit ».

L'article 8 de la Convention européenne des droits de l'homme dispose :

« 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui ».

B.6.2. Le Constituant a recherché la plus grande concordance possible entre l'article 22 de la Constitution et l'article 8 de la Convention européenne précitée (*Doc. parl.*, Chambre, 1992-1993, nº 997/5, p. 2).

La portée de cet article 8 est analogue à celle de la disposition constitutionnelle précitée, de sorte que les garanties que fournissent ces deux dispositions forment un ensemble indissociable.

B.6.3. Ces dispositions exigent que toute ingérence des autorités dans le droit au respect de la vie privée soit prescrite par une disposition législative, suffisamment précise, corresponde à un besoin social impérieux et soit proportionnée à l'objectif légitime poursuivi par celle-ci.

B.7.1. Ainsi que le souligne la section de législation du Conseil d'État dans son avis relatif à l'avant-projet de loi devenu la loi attaquée, une recherche dans un système informatique peut constituer une ingérence importante dans le droit au respect de la vie privée (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1966/001, p. 126).

B.7.2. La Cour européenne des droits de l'homme a également déjà jugé à plusieurs reprises que « la fouille et la saisie de données électroniques s'analysent en une ingérence dans le droit au respect de la ' vie privée ' et de la ' correspondance ' au sens de [l'article 8 de la Convention] » et que « pareille ingérence méconnaît l'article 8 sauf si, ' prévue par la loi ', elle poursuit un ou des buts légitimes au regard du paragraphe 2 et, de plus, est ' nécessaire dans une société démocratique ' pour les atteindre » (CEDH, 2 avril 2015, *Vinci Construction et GTM Génie Civil et Services c. France*, §§ 63-64).

Dans ce contexte, cette Cour recherche « si la législation et la pratique internes offraient des garanties adéquates et suffisantes contre les abus et l'arbitraire ». Parmi ces garanties figure « l'existence d'un contrôle efficace des mesures attentatoires à l'article 8 de la Convention » (*ibid.*, §§ 66-67).

B.7.3. En considération de l'importance de l'ingérence dans le droit au respect de la vie privée que la recherche dans un système informatique est susceptible d'occasionner, sa mise en œuvre doit faire l'objet d'un contrôle par un juge indépendant et impartial.

En ce qui concerne la recherche dans un système informatique qui fait l'objet d'une saisie

B.8.1. La disposition attaquée permet, en son paragraphe 2, alinéa 1er, à l'officier de police judiciaire de décider l'exécution d'une recherche dans un système informatique qui fait l'objet d'une saisie. La recherche ne peut porter que sur les données stockées dans l'appareil saisi, puisque celui-ci doit être, préalablement à la recherche, empêché de se connecter aux systèmes extérieurs. En outre, si la recherche nécessite la suppression temporaire d'une protection ou le décryptage ou le décodage des données, l'officier de police judiciaire doit obtenir à cette fin l'autorisation du procureur du Roi (§ 5, alinéa 1er).

B.8.2. Il ressort de l'exposé des motifs que l'objectif poursuivi par la disposition attaquée est, en ce qui concerne la recherche dans un système saisi, de confirmer dans la loi la jurisprudence de la Cour de cassation :

« Dans son arrêt du 11 février 2015 (AR P.14 1739.F), la Cour de cassation a en effet indiqué que le droit actuel permet déjà à l'officier de police judiciaire de prendre connaissance des données d'un GSM qui a été saisi. Bien entendu, l'exploitation de ces données se déroule toujours dans les limites de l'enquête pénale et sous le contrôle du magistrat en charge de celle-ci » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1966/001, p. 15).

B.8.3. Par son arrêt précité du 11 février 2015, la Cour de cassation a jugé :

« L'exploitation de la mémoire d'un téléphone portable, dont les messages qui y sont stockés sous forme de *sms*, est une mesure découlant de la saisie, laquelle peut être effectuée dans le cadre d'une information sans autres formalités que celles prévues pour cet acte d'enquête » (Cass., 11 février 2015, P.14 1739.F).

B.8.4. La saisie est un acte d'enquête qui peut être réalisé dans les cas et aux conditions prévues par les dispositions du Code d'instruction criminelle, notamment en cas de flagrant délit ou au cours d'une perquisition régulièrement ordonnée par le juge d'instruction. Elle peut viser tout ce qui semble avoir servi ou avoir été destiné à commettre l'infraction, tout ce qui paraît en avoir été le produit et tout ce qui peut servir à la manifestation de la vérité (art. 35 et suivants du Code d'instruction criminelle).

B.8.5. La personne qui s'estime lésée par la saisie peut en demander mainlevée, selon le cas, au procureur du Roi (article 28*sexies*, § 1er, du Code d'instruction criminelle) ou au juge d'instruction (article 61*quater*, § 1er, du même Code). En cas de refus, la chambre des mises en accusation peut être saisie par la personne lésée.

B.8.6. La recherche dans les données stockées dans la mémoire de l'appareil saisi constitue un accessoire de la saisie elle-même, à l'instar de la prise de connaissance, par l'officier de police judiciaire, du contenu de livres, carnets ou documents saisis sur support physique. Dès lors que l'appareil saisi formant l'objet de la recherche est déconnecté, de sorte que l'officier de police qui effectue la recherche ne peut avoir accès qu'au contenu que le propriétaire ou le possesseur de l'appareil y a enregistré ou sauvegardé, la recherche ne se distingue pas de l'exploitation par les enquêteurs du contenu de documents qui font l'objet d'une saisie.

B.8.7. Il découle de ce qui précède que la recherche dans un système informatique qui a été régulièrement saisi est, à l'instar de l'exploitation de documents régulièrement saisis, entourée de suffisamment de garanties juridictionnelles permettant d'assurer que l'ingérence dans le droit au respect de la vie privée occasionnée par cet acte d'enquête est justifiée au regard des exigences des articles 22 de la Constitution et 8 de la Convention européenne des droits de l'homme.

B.8.8. L'examen au regard des articles 10 et 11 de la Constitution ne mène pas à une autre conclusion en ce qui concerne les recherches dans un système informatique saisi. Le premier moyen, en ses première et quatrième branches, n'est pas fondé en ce qu'il vise les recherches dans un système informatique régulièrement saisi.

En ce qui concerne la recherche dans un système informatique susceptible de faire l'objet d'une saisie

B.9.1. La disposition attaquée permet, en son paragraphe 2, alinéa 2, au procureur du Roi de décider d'effectuer une recherche dans un système informatique qui n'a pas été saisi mais « pour lequel toutes les conditions légales d'une saisie sont réunies » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1966/001, p. 16). La recherche ne peut porter que sur les données stockées dans l'appareil concerné, puisque celui-ci doit être préalablement empêché de se connecter aux systèmes extérieurs. En outre, si la recherche nécessite la suppression temporaire d'une protection ou le décryptage ou le décodage des données, l'officier de police judiciaire doit aussi obtenir à cette fin l'autorisation du procureur du Roi (§ 5, alinéa 1er).

B.9.2. Dans l'hypothèse dans laquelle le système informatique faisant l'objet de l'examen pourrait être saisi par le procureur du Roi, toutes les conditions légales dans lesquelles la saisie peut être décidée sont réunies. Par ailleurs, en vertu du paragraphe 1er de l'article 39*bis* du Code d'instruction criminelle, les règles relatives à la saisie sont applicables aux mesures consistant à copier, rendre inaccessibles et retirer des données stockées dans un système informatique ou une partie de celui-ci. La copie de données livrées par une recherche effectuée dans un système informatique non saisi pour des raisons d'opportunité pratique mais qui aurait pu l'être au regard des conditions légales de la saisie est donc elle-même considérée, au regard des recours et garanties offertes à la personne concernée, comme une saisie.

B.9.3. Par ailleurs, dès lors que l'appareil dans lequel la recherche est effectuée est déconnecté, de sorte que l'officier de police effectuant la recherche ne peut avoir accès qu'au contenu que le propriétaire ou le possesseur de l'appareil y a enregistré ou sauvegardé, cette recherche ne se distingue pas d'une recherche dans des documents préalable à une saisie.

B.9.4. Il en résulte que la personne lésée par la saisie des données opérée dans un système informatique non saisi dispose des mêmes recours et garanties qu'une personne concernée par une perquisition ou par une fouille opérées conformément à la législation.

B.9.5. Il découle de ce qui précède que la recherche dans un système informatique non saisi mais qui pourrait l'être est entourée de suffisamment de garanties juridictionnelles permettant d'assurer que l'ingérence dans le droit au respect de la vie privée occasionnée par cet acte d'enquête est justifiée au regard des exigences des articles 22 de la Constitution et 8 de la Convention européenne des droits de l'homme.

B.9.6. L'examen au regard des articles 10 et 11 de la Constitution ne mène pas à une autre conclusion en ce qui concerne les recherches dans un système informatique non saisi mais qui pourrait l'être. Le premier moyen, en ses première et quatrième branches, n'est pas fondé en ce qu'il vise les recherches effectuées dans un système informatique qui peut être régulièrement saisi.

En ce qui concerne la différence de traitement entre la recherche dans un système informatique saisi et la recherche dans un système informatique susceptible d'être saisi

B.10.1. Dès lors que la possibilité pour l'officier de police judiciaire de décider lui-même d'exécuter une recherche dans un système informatique saisi est justifiée pour les motifs exposés en B.8.1 et suivants, la différence de traitement qui résulte du fait que la recherche envisagée par le procureur du Roi dans un système informatique qui n'est pas saisi mais qui pourrait l'être ne peut être décidée que par celui-ci est justifiée par les mêmes motifs.

B.10.2. Le premier moyen, en sa deuxième branche, n'est pas fondé.

En ce qui concerne l'extension de la recherche

B.11.1. L'article 39*bis*, § 3, du Code d'instruction criminelle, introduit par la disposition attaquée, permet au procureur du Roi de décider d'étendre une recherche, entamée dans un système informatique qui fait ou qui peut faire l'objet d'une saisie, vers un système informatique ou une partie de celui-ci qui se trouve dans un autre lieu que celui où la recherche est effectuée et qui peut être atteint par une connexion. Toutefois, si l'accès aux données est protégé, seul le juge d'instruction peut autoriser la suppression de la protection ou le décryptage ou le décodage des données (§ 5, alinéa 2).

B.11.2. L'extension de la recherche permet aux enquêteurs d'avoir accès non seulement à l'ensemble des données enregistrées ou sauvegardées sur l'appareil qui constitue le point de départ de la recherche, mais également à tous les documents stockés sur les systèmes informatiques atteints par connexion via cet appareil, ainsi qu'à toutes les communications entretenues par son utilisateur avec des tiers, en ce compris les nouveaux messages reçus ou en cours de réception dont l'utilisateur n'a pas encore pris connaissance.

B.12.1. Antérieurement à l'entrée en vigueur de la disposition attaquée, la disposition relative aux recherches sur les réseaux, insérée par l'article 3 de la loi du 28 novembre 2000 relative à la criminalité informatique, se trouvait à l'article 88*ter* du Code d'instruction criminelle. Cet article est abrogé par l'article 13 de la loi attaquée.

B.12.2. L'exposé des motifs de la loi du 28 novembre 2000 indique, au sujet de cet article 88*ter* :

« Une mesure coercitive traditionnelle, telle que la perquisition, est restrictive en ce sens que, par définition, elle ne peut être effectuée que sur le lieu pour lequel elle a été ordonnée. Ce qui caractérise les systèmes informatiques - qu'il s'agisse de systèmes importants dans des sociétés ou d'ordinateurs portables - c'est qu'ils sont de plus en plus connectés en réseaux.

Dans le contexte actuel, lorsque les systèmes informatiques pour lesquels une recherche semble nécessaire sont dispersés en divers endroits, plusieurs mandats de perquisition ou de saisie doivent être délivrés. Pareille approche suscite bien évidemment des problèmes : on court non seulement le risque de voir des éléments de preuve disparaître si l'intervention n'est pas simultanée mais en outre dans de nombreux cas, il ne sera pas possible *a priori* de déterminer les endroits où doivent s'effectuer les recherches, les fichiers pertinents ou même la localisation géographique des ordinateurs.

Pour pallier ces problèmes, le nouvel article fixe les conditions qui permettent l'extension de la recherche dans un système informatique vers des systèmes situés ailleurs. Il doit s'agir de systèmes liés entre eux.

La mesure doit avant tout être nécessaire à la manifestation de la vérité et il faut en outre qu'il y ait un risque de perdre les éléments de preuve ou que la prise d'autres mesures (par exemple plusieurs mandats de perquisition) soit disproportionnée. Il appartient au juge d'instruction d'apprécier raisonnablement ces considérations. En raison du caractère exceptionnel de l'extension de la recherche dans un système informatique, notamment en raison de ses éventuels effets extra territoriaux, une telle recherche ne pourra être étendue que si elle apparaît nécessaire dans le cadre d'une affaire pénale concrète dont le juge est saisi » (*Doc. parl.*, Chambre, 1999-2000, DOC 50-0213/001 et 50-0214/001, pp. 22-23).

B.13.1. Depuis l'entrée en vigueur de la disposition attaquée, l'extension d'une recherche entamée dans un système informatique vers les réseaux qui lui sont connectés ne requiert plus la saisine et l'autorisation du juge d'instruction. Le procureur du Roi est compétent pour ordonner cette extension de la recherche dans la mesure où l'accès aux réseaux n'est pas protégé.

B.13.2. L'exposé des motifs de la loi attaquée indique à ce sujet :

« L'extension de la recherche dans un système informatique peut désormais être ordonnée par le procureur du Roi ou l'auditeur du travail.

Cette extension vise par exemple les situations où un smartphone a été saisi et où il apparaît nécessaire d'avoir accès au compte Hotmail, Facebook ou Dropbox auquel ce smartphone est connecté. Comme indiqué précédemment, le droit actuel permet seulement à l'autorité qui a décidé la saisie de l'appareil de faire une recherche dans l'appareil lui-même, pas dans les données auxquelles cet appareil est connecté dans le cloud par exemple.

Même si l'intervention du juge d'instruction inclut une garantie essentielle en matière d'intrusion dans la vie privée, la modification de loi est justifiée parce que l'article 39*bis* se limite aux recherches non secrètes. Comme il a été dit, l'article 39*bis* est utilisé de manière réactive à la suite du fait que l'on a pu s'emparer légalement d'un système informatique. Il n'y a en aucun cas d'approche ou d'exploitation secrète d'éléments de la vie privée des personnes. Dans ces circonstances, le contrôle du magistrat du parquet offre une garantie suffisante.

En revanche, la pénétration en secret dans un système informatique et sa mise sous surveillance restent soumises à l'intervention du juge d'instruction, conformément aux articles 90*ter* et suivants ou à l'article 89*ter* du Code d'instruction criminelle.

Par ailleurs, le transfert de cette mesure (c'est-à-dire l'extension de la recherche) de l'article 88*ter* vers l'article 39*bis* et donc du juge d'instruction vers le procureur du Roi se justifie par le fait que, avec le développement des nouvelles technologies, la distinction entre ce qui se trouve sur l'appareil et ce qui se trouve dans le cloud devient en partie artificielle.

Toutefois, cette modification doit être lue en combinaison avec le nouveau paragraphe 5 qui concerne l'utilisation de ' fausses clés ' etc. pour accéder aux données. Le dernier alinéa du paragraphe 5 prévoit que seul le juge d'instruction peut ordonner l'usage de ' fausses clés ' dans le cadre de l'application spécifique du § 3 » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1966/001, pp. 18-19).

B.14.1. Compte tenu du développement considérable des réseaux accessibles au départ des systèmes informatiques et de leur utilisation intensive par l'immense majorité des citoyens aussi bien pour y stocker des documents et des données relevant de leur vie privée, en ce compris ce qu'elle a de plus intime, que pour communiquer entre eux, il peut être considéré, à l'heure actuelle, qu'une mesure d'investigation permettant d'accéder à l'ensemble des données et communications situées sur les réseaux connectés à un système informatique appartenant à un individu constitue une ingérence dans son droit au respect de la vie privée à tout le moins comparable à celles qui sont causées, d'une part, par une perquisition dans un domicile ou un lieu privé et, d'autre part, par une interception de ses communications téléphoniques ou de son courrier postal.

B.14.2. En vertu des articles 87 et 88 du Code d'instruction criminelle, les perquisitions relèvent de la compétence du juge d'instruction. En vertu de l'article 88*sexies* du même Code, hors le cas du flagrant délit, seul le juge d'instruction peut prendre connaissance du contenu du courrier confié à un opérateur postal, intercepté et saisi par le procureur du Roi en application de l'article 46*ter* du même Code. En vertu de l'article 90*ter* du même Code, le juge d'instruction est compétent pour « intercepter, prendre connaissance, explorer et enregistrer, à l'aide de moyens techniques, des communications non accessibles au public ou des données d'un système informatique ou d'une partie de celui-ci, ou étendre la recherche dans un système informatique ou une partie de celui-ci ».

B.14.3. Ainsi que l'a observé le Conseil d'État dans l'avis qu'il a rendu au sujet de la disposition attaquée, « le juge d'instruction est un magistrat indépendant qui mène une instruction objective, tant à charge qu'à décharge, alors que le ministère public est partie au procès pénal » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1966/001, p. 127).

B.14.4. Les actes d'information ne peuvent en principe pas porter atteinte aux libertés et droits individuels, de sorte que les mesures d'investigation effectuées au cours de l'enquête pénale comportant de telles atteintes ne peuvent être accomplies que dans le cadre d'une instruction. À tout le moins, les actes visés par l'article 28*septies* du Code d'instruction criminelle qui organise ce qu'il est convenu d'appeler la « mini-instruction » ne peuvent être accomplis qu'avec l'autorisation et sous le contrôle d'un juge d'instruction, même si l'affaire n'est pas mise à l'instruction.

B.14.5. L'information se caractérise par son caractère éminemment secret et non contradictoire, les intéressés disposant de moins de garanties destinées à protéger leurs droits de la défense qu'au cours de l'instruction.

Certes, les personnes directement intéressées ont déjà le droit de demander accès au dossier pénal au cours de l'information (article 21*bis* du Code d'instruction criminelle). À l'inverse de ce qui est le cas pour l'instruction (article 61*ter* du Code d'instruction criminelle), ce droit d'accès au dossier, dans le cadre de l'information, n'est toutefois pas réglé au niveau procédural, de sorte que le ministère public - à défaut de motifs de refus légaux - peut simplement refuser la demande d'accès au dossier et aucune voie de recours n'est ouverte contre une décision de refus ou contre l'absence de décision. Par son arrêt nº 6/2017 du 25 janvier 2017, la Cour a jugé que cette absence de recours contre le refus ou l'absence de décision du ministère public en réponse à une demande d'accès à un dossier au cours de l'information, formulée par un inculpé, violait les articles 10 et 11 de la Constitution. Étant donné que ce constat d'inconstitutionnalité est exprimé en des termes suffisamment précis et complets qui permettent l'application de l'article 21*bis* du Code d'instruction criminelle dans le respect des normes de référence sur la base desquelles la Cour exerce son contrôle, la Cour a aussi jugé que, dans l'attente de l'intervention du législateur, il appartenait au juge de mettre fin à la violation de ces normes, en appliquant par analogie l'article 61*ter* du Code d'instruction criminelle.

En outre, au cours de l'information, les intéressés ne disposent pas d'un droit formel de demander certains actes d'information, alors qu'un droit de demander des actes d'instruction complémentaires est accordé à l'inculpé et à la partie civile au cours de l'instruction (article 61*quinquies* du Code d'instruction criminelle). Il est vrai que les intéressés peuvent toujours adresser une demande informelle au ministère public, mais celui-ci n'est pas tenu d'accéder à cette demande et les parties ne disposent d'aucune voie de recours contre un refus ou une absence de décision.

Enfin, au cours de l'information, la régularité de la procédure n'est pas d'office contrôlée par un juge indépendant et impartial, lequel pourrait purger le dossier d'éventuelles nullités, alors qu'un tel contrôle existe au cours de l'instruction (article 235*bis* du Code d'instruction criminelle).

B.14.6. Il résulte de ce qui précède qu'en ce que la disposition attaquée permet que l'extension de la recherche, entamée dans un appareil saisi ou qui pourrait l'être, vers un système informatique qui se situe à un autre endroit que l'appareil lui-même et auquel l'appareil est connecté, soit ordonnée par le procureur du Roi, sans intervention d'un juge d'instruction, cette mesure d'enquête est entourée de moins de garanties pour le justiciable dont le système informatique fait l'objet de la mesure d'investigation que la perquisition, l'ouverture du courrier postal, l'interception et l'écoute des communications téléphoniques et électroniques et la recherche secrète dans un système informatique.

B.15.1. Cette différence de traitement a été justifiée par le législateur par le caractère non secret de l'investigation :

« Même si l'intervention du juge d'instruction inclut une garantie essentielle en matière d'intrusion dans la vie privée, la modification de la loi est justifiée parce que l'article 39*bis* se limite aux recherches non secrètes. Comme il a été dit, l'article 39*bis* est utilisé de manière réactive à la suite du fait que l'on a pu s'emparer légalement d'un système informatique. Il n'y a en aucun cas d'approche ou d'exploitation secrète d'éléments de la vie privée des personnes. Dans ces circonstances, le contrôle du magistrat du parquet offre une garantie suffisante.

En revanche, la pénétration en secret dans un système informatique et sa mise sous surveillance restent soumises à l'intervention du juge d'instruction, conformément aux articles 90*ter* et suivants ou à l'article 89*ter* du Code d'instruction criminelle.

Par ailleurs, le transfert de cette mesure (c'est-à-dire l'extension de la recherche) de l'article 88*ter* vers l'article 39*bis* et donc du juge d'instruction vers le procureur du Roi se justifie par le fait que, avec le développement des nouvelles technologies, la distinction entre ce qui se trouve sur l'appareil et ce qui se trouve dans le cloud devient en partie artificielle » (*Doc. parl*., Chambre, 2015-2016, DOC 54-1966/001, p. 19).

B.15.2. La différence de traitement exposée en B.14.6 repose dès lors sur le critère du caractère secret ou non de la recherche menée dans les réseaux auxquels l'appareil saisi ou qui pourrait l'être est connecté.

Le caractère non secret de l'ingérence dans le droit au respect de la vie privée de la personne concernée par la mesure est garanti par l'obligation imposée au procureur du Roi, en vertu du paragraphe 7 de la disposition attaquée, d'informer « dans les plus brefs délais » le responsable du système informatique qui fait l'objet de l'investigation.

Puisque l'obligation d'informer le responsable du système informatique de la recherche est utilisée pour distinguer le caractère secret et non secret d'une investigation et que ceci s'inscrit dans le cadre de la protection des justiciables, il faut considérer que la notification au responsable du système informatique concerne aussi le suspect, dont les données stockées dans le système font l'objet de cette recherche, lorsque le suspect n'exerce pas le contrôle effectif du système informatique concerné.

B.15.3. La circonstance que l'ingérence dans le droit au respect de la vie privée d'une personne est effectuée à son insu en augmente la gravité, ce qui implique qu'elle soit entourée des garanties les plus élevées et qu'elle ne puisse en conséquence être effectuée qu'au cours d'une instruction pénale (CEDH, 4 décembre 2015, *Zakharov c. Russie*, §§ 233, 249 et 259; 12 janvier 2016, *Szabó et Vissy c. Hongrie*, § 77; 30 mai 2017, *Trabajo Rueda c. Espagne*, § 33). Toutefois, la circonstance que la même mesure d'investigation est portée à la connaissance de la personne concernée, le cas échéant, après qu'elle a pris fin, comporte également une ingérence importante dans le droit au respect de la vie privée de cette personne. En effet, le fait qu'elle en ait été informée ne signifie pas qu'elle y ait consenti.

B.15.4. L'intervention préalable d'un juge indépendant et impartial permet de garantir que l'ingérence dans le droit au respect de la vie privée est proportionnée aux exigences de l'article 22 de la Constitution et de l'article 8 de la Convention européenne des droits de l'homme.

Ainsi, par son arrêt nº 202/2004 du 21 décembre 2004, la Cour a jugé que la méthode de l'observation avec moyens techniques afin d'avoir une vue dans une habitation et celle du contrôle visuel discret dans un lieu privé sont des mesures qui peuvent être comparées, en ce qui concerne la gravité de l'ingérence dans les droits garantissant la vie privée, à la perquisition et aux écoutes et enregistrements des communications et télécommunications privées et ne peuvent être autorisées que dans les mêmes conditions, soit dans le cadre de l'instruction.

Par son arrêt nº 178/2015 du 17 décembre 2015, la Cour a jugé, à propos de l'extension de la recherche dans un système informatique :

« L'extension de la recherche dans un système informatique est soumise à l'autorisation préalable du juge de l'application des peines, qui doit vérifier si les exigences en matière de légalité, de proportionnalité et de subsidiarité sont respectées et qui doit veiller en particulier à ce qu'aucune atteinte disproportionnée ne soit portée aux droits fondamentaux des intéressés.

Pour garantir un contrôle juridictionnel effectif, le magistrat [qui mène l'enquête pénale d'exécution], lorsqu'il demande une autorisation au juge de l'application des peines, doit aussi indiquer la portée de l'extension de la recherche dans un système informatique, de manière à éviter que l'atteinte portée à la vie privée soit potentiellement illimitée et, partant, disproportionnée (CEDH, 9 décembre 2004, *Van Rossem c.Belgique*, § 45), et de manière à permettre un contrôle de cette atteinte par le juge de l'application des peines. Une autre interprétation des dispositions attaquées ne serait pas conciliable avec le droit au respect de la vie privée et du domicile » (B.48.4).

Par son arrêt nº 148/2017 du 21 décembre 2017, la Cour a jugé à propos de la perquisition dans un domicile, laquelle ne revêt, au demeurant, pas forcément un caractère secret :

« En raison de la gravité de l'ingérence dans le droit au respect de la vie privée et de l'inviolabilité du domicile qu'elle implique, la perquisition ne peut, en l'état actuel de la réglementation en matière de procédure pénale, être autorisée que dans le cadre d'une instruction, au cours de laquelle les personnes intéressées disposent d'un droit organisé de demander un accès au dossier et des actes d'instruction supplémentaires et au cours de laquelle la chambre des mises en accusation peut exercer un contrôle quant à la régularité de la procédure.

En incluant la perquisition, en l'état actuel de la règlementation en matière de procédure pénale, dans le champ d'application de la mini-instruction, sans prévoir des garanties supplémentaires pour protéger les droits de la défense, la disposition attaquée porte une atteinte discriminatoire au droit au respect de la vie privée et au droit à l'inviolabilité du domicile » (B.22.4).

B.15.5. Il découle de ce qui précède que la différence de traitement entre les personnes qui font l'objet d'une mesure d'investigation qui porte sur les réseaux connectés à leur sujet, selon que la recherche est considérée comme secrète ou non secrète, au sens de la disposition attaquée, ne repose pas sur un critère pertinent au regard du principe selon lequel les mesures d'investigation effectuées au cours de l'enquête pénale comportant des atteintes aux libertés et aux droits individuels ne peuvent en principe être accomplies que dans le cadre d'une instruction (article 28*bis*, § 3, alinéa 1er, du Code d'instruction criminelle).

B.16.1. Par ailleurs, la circonstance que si l'accès aux réseaux connectés au système informatique est protégé par une clé ou si les données figurant sur les réseaux ou sur un système informatique connecté sont codées ou cryptées, le procureur du Roi ne peut faire usage de fausses clés ou de techniques de décodage ou de décryptage qu'avec l'autorisation du juge d'instruction ne justifie pas non plus que l'ingérence dans le droit au respect de la vie privée, qui n'est pas moindre dans ce cas, ne soit pas entourée des mêmes garanties lorsque de telles protections n'ont pas été installées.

B.16.2. En outre, la disposition attaquée n'a pas assorti le transfert de la compétence du juge d'instruction vers le procureur du Roi de garanties supplémentaires destinées à protéger de manière effective la vie privée et les droits de la défense de la personne concernée et qui soient de nature à compenser la suppression de l'intervention préalable d'un juge indépendant et impartial (CEDH, 30 septembre 2014, *Prezhdarovi c. Bulgarie*, §§ 45 à 47; 30 mai 2017, *Trabajo Rueda c. Espagne*, § 37). À cet égard, il ressort de la jurisprudence de la Cour européenne des droits de l'homme que l'existence d'un recours effectif est fonction de son caractère adéquat; le recours en question doit de ce fait être en rapport avec la violation alléguée afin de procurer des garanties appropriées et équivalentes sauvegardant les droits en cause de l'individu. Il s'ensuit que l'instance nationale de recours doit être habilitée à connaître en substance du grief fondé sur la Convention pour décider si l'ingérence dans l'exercice du droit de l'intéressé au respect de sa vie privée était en conformité avec l'article 8, paragraphe 2 (CEDH, 1er avril 2008, *Varga c. Roumanie*, §§ 72-73; 3 juillet 2012, *Robathin c. Autriche*, § 21; 30 septembre 2014, *Prezhdarovi c. Bulgarie*, § 47; 2 avril 2015, *Vinci Construction et GTM Génie Civil et Services c. France*, §§ 66-67).

B.16.3. L'article 28*sexies* du Code d'instruction criminelle est certes applicable aux mesures consistant à copier, rendre inaccessibles et retirer des données stockées dans un système informatique ou une partie de celui-ci. Cette disposition permet à toute personne lésée par un acte d'information relatif à ses biens d'en demander la levée au procureur du Roi dont la décision est susceptible de faire l'objet d'un recours devant la chambre des mises en accusation. Cette procédure, également applicable devant le juge d'instruction (article 61*quater*, § 1er, du Code d'instruction criminelle) se limite donc à la possibilité pour la personne concernée d'obtenir la levée de la saisie, et dès lors la restitution, du matériel informatique et des données qui ont été obtenues au moyen d'une recherche dans un système informatique. Elle n'empêche toutefois pas l'ingérence dans la vie privée qui a eu lieu et à laquelle la restitution de l'appareil et des données qui y sont stockées ne remédie pas, ce qui ne satisfait pas aux exigences de la jurisprudence de la Cour européenne des droits de l'homme énoncées en B.16.2.

B.16.4. En raison de la gravité de l'ingérence dans le droit au respect de la vie privée qu'elle implique, la mesure consistant à étendre une recherche dans un système informatique ou une partie de celui-ci, entamée dans un système informatique qui a été saisi ou qui peut être saisi par le procureur du Roi, vers un système informatique ou une partie de celui-ci qui se trouve dans un autre lieu que celui où la recherche est effectuée, ne peut être autorisée que dans les mêmes conditions que celles qui concernent les actes d'instruction visés en B.14.2.

B.17.1. Le premier moyen, en ses première et quatrième branches, est fondé dans cette mesure.

Il y a lieu d'annuler le paragraphe 3 de l'article 39*bis* du Code d'instruction criminelle, inséré par l'article 2 de la loi du 25 décembre 2016 attaquée. Pour éviter de créer un vide juridique quant à la mesure de recherche concernée, il y a lieu également d'annuler l'article 13 de la loi du 25 décembre 2016, qui est indissociablement lié à la disposition attaquée en ce qu'il abroge l'article 88*ter* du Code d'instruction criminelle.

B.17.2. Afin d'éviter l'insécurité juridique qui naîtrait au sujet de la validité des mesures d'extension de recherches dans des systèmes informatiques effectuées conformément à la disposition annulée, il y a lieu de maintenir les effets produits par cette disposition jusqu'à la date de la publication du présent arrêt au *Moniteur belge*.

En ce qui concerne l'information du responsable du système informatique

B.18.1. Le premier moyen, en sa troisième branche, est pris de la violation des articles 12 et 14 de la Constitution, lus en combinaison avec l'article 7 de la Convention européenne des droits de l'homme. Il vise la notion de « responsable du système informatique », inscrit au paragraphe 7 de l'article 39*bis* du Code d'instruction criminelle, introduit par l'article 2 de la loi du 25 décembre 2016 attaquée. Les parties requérantes font grief au législateur de n'avoir pas précisé le contenu de cette notion, de sorte que l'identité des personnes devant être informées de la recherche ou de son extension est floue et indéterminée.

B.18.2. Contrairement à ce que soutient le Conseil des ministres, la circonstance que la législation antérieure à la loi attaquée faisait déjà référence au « responsable du système informatique » n'entraîne pas l'irrecevabilité, pour tardiveté, du moyen en sa troisième branche. En effet, par la disposition attaquée, le législateur a légiféré à nouveau dans cette matière et a confirmé l'obligation faite au procureur du Roi et au juge d'instruction d'informer le « responsable du système informatique ».

B.19.1. L'article 12, alinéa 2, de la Constitution dispose :

« Nul ne peut être poursuivi que dans les cas prévus par la loi, et dans la forme qu'elle prescrit ».

L'article 14 de la Constitution dispose :

« Nulle peine ne peut être établie ni appliquée qu'en vertu de la loi ».

L'article 7, paragraphe 1, de la Convention européenne des droits de l'homme dispose :

« Nul ne peut être condamné pour une action ou une omission qui, au moment où elle a été commise, ne constituait pas une infraction d'après le droit national ou international. De même il n'est infligé aucune peine plus forte que celle qui était applicable au moment où l'infraction a été commise ».

B.19.2. En ce qu'il garantit le principe de légalité en matière pénale, l'article 7, paragraphe 1, de la Convention européenne des droits de l'homme a une portée analogue à celle des articles 12, alinéa 2, et 14 de la Constitution.

B.19.3. Il découle des dispositions précitées que la loi pénale doit être formulée en des termes qui permettent à chacun de connaître, au moment où il adopte un comportement, si ce comportement est punissable ou non et la peine éventuellement encourue. Les principes de légalité et de prévisibilité sont applicables à l'ensemble de la procédure pénale. Ces dispositions entendent ainsi exclure tout risque d'intervention arbitraire de la part du pouvoir exécutif ou du pouvoir judiciaire dans l'établissement et l'application des peines.

Le principe de légalité en matière pénale ne va pas jusqu'à obliger le législateur à régler lui-même chaque aspect de l'incrimination, de la peine ou de la procédure pénale. Plus précisément, il n'empêche pas que le législateur attribue un pouvoir d'appréciation au juge ou au ministère public. Il faut en effet tenir compte du caractère de généralité des dispositions législatives, de la diversité des situations auxquelles elles s'appliquent et de l'évolution des comportements qu'elles répriment.

B.19.4. En l'espèce, ce n'est pas la légalité de l'incrimination ou de la peine qui est en cause mais celle de la procédure pénale.

Une délégation au pouvoir exécutif n'est pas contraire à ce principe, pour autant que l'habilitation soit définie en des termes suffisamment précis et porte sur l'exécution de mesures dont les éléments essentiels ont été fixés préalablement par le législateur.

L'exigence de prévisibilité de la procédure pénale garantit à tout justiciable qu'il ne peut faire l'objet d'une information, d'une instruction et de poursuites que selon une procédure dont il peut prendre connaissance avant sa mise en œuvre.

B.20. Dès lors que la disposition attaquée impose d'informer le « responsable du système informatique » de la recherche, c'est à cette personne qu'elle permet de prendre les dispositions nécessaires pour la sauvegarde de ses droits, de sorte que cette notion est un élément essentiel de la procédure pénale en matière de recherches dans les systèmes informatiques.

B.21.1. À ce sujet, la section de législation du Conseil d'État a observé :

« Mais la disposition ne donne pas une définition de ce qu'il faut entendre par ' le responsable du système informatique '.

Au sens de la recommandation nº R(95)13 [du Comité des ministres du Conseil de l'Europe du 11 septembre 1995], la notion englobe toutes les personnes qui, lors de la perquisition ou de la saisie, paraissent disposer formellement ou réellement du contrôle sur le système informatique, objet de la perquisition. Il peut s'agir du propriétaire du système, d'un opérateur de ce système ou même du gardien (locataire ou occupant) des locaux abritant le système informatique.

La disposition en projet doit, en conséquence, définir expressément les personnes concernées par l'information.

Par ailleurs, la saisie de données peut également concerner des tierces personnes. C'est ainsi que la recommandation nº R(95)13, précitée, invite les États membres à organiser ce type d'information et ce dans le respect des impératifs de l'enquête.

Cette exigence est importante car, en vertu des articles 28*sexies* et 61*quater* du Code d'instruction criminelle, toute personne qui s'estime lésée par un acte d'information ou par un acte d'instruction relatif à ses biens peut en demander la levée soit au procureur du Roi, soit au juge d'instruction » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1966/001, pp. 129-130).

B.21.2. L'exposé des motifs indique, au sujet de cette observation :

« Le Conseil d'État estime également (et renvoie à cet égard à l'avis nº 28 029/2 du 31 mai 1999) que le texte de l'avant-projet de loi doit lui-même contenir une définition du ' responsable du système informatique '. Le but de la communication de la mesure est toutefois d'établir clairement qu'il ne s'agit pas d'une mesure secrète (cf. la compétence de perquisitionner). La terminologie de l'avant-projet comporte dans cette optique une certaine souplesse pour ce qui est de la personne à contacter : en effet, il n'est pas possible de déterminer *a priori* pour tous les cas et de manière univoque qui exerce le contrôle réel ou juridique sur le système (*Doc. parl.*, Chambre, 1999-2000, nº 0213/001, p. 21) » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1966/001, p. 24).

B.22.1. Au-delà de l'établissement du caractère secret ou non secret de la mesure d'investigation, la communication de l'exécution de cette mesure a également pour conséquence de permettre à la personne ou aux personnes concernée(s) d'exercer les droits procéduraux qui ont notamment pour fonction de contrôler la proportionnalité de l'ingérence occasionnée dans le droit au respect de la vie privée de cette personne ou de ces personnes.

B.22.2. Il en découle que la notion de « responsable du système informatique » doit être comprise comme désignant la personne ou les personnes responsables des données ou des communications enregistrées sur l'appareil saisi ou qui peut l'être et des données ou des communications dont il peut être pris connaissance via les réseaux qui sont visés par l'extension de la recherche entamée dans l'appareil précité, cette ou ces personnes n'étant pas nécessairement les propriétaires ou les détenteurs des appareils concernés. Comme il est dit en B.15.2, cette notion vise également le suspect dont les données font l'objet de la recherche lorsqu'il n'exerce pas lui-même le contrôle effectif du système informatique concerné.

B.23. Sous réserve que la notion de « responsable du système informatique » soit interprétée comme il est dit en B.15.2 et B.22.2, le premier moyen, en sa troisième branche, n'est pas fondé.

En ce qui concerne les systèmes informatiques des avocats et des médecins

B.24.1. Le premier moyen, en sa cinquième branche, est pris de la violation des articles 10, 11 et 22 de la Constitution, lus en combinaison avec l'article 6 de la Convention européenne des droits de l'homme. Les parties requérantes font grief au législateur de n'avoir pas prévu, à l'article 39*bis* du Code d'instruction criminelle qui règle les recherches non secrètes dans un système informatique, des garanties équivalentes à celles qui sont inscrites à l'article 90*octies* du même Code et qui concernent les recherches secrètes dans un système informatique.

B.24.2. L'article 90*octies* du Code d'instruction criminelle dispose :

« § 1er. La mesure ne pourra porter sur les locaux utilisés à des fins professionnelles, la résidence, les moyens de communication ou les systèmes informatiques d'un avocat ou d'un médecin que si celui-ci est lui-même soupçonné d'avoir commis une des infractions visées à l'article 90*ter* ou d'y avoir participé, ou si des faits précis laissent présumer que des tiers soupçonnés d'avoir commis une des infractions visées à l'article 90*ter*, utilisent ses locaux, sa résidence, ses moyens de communication ou ses systèmes informatiques.

§ 2. La mesure ne peut être exécutée sans que le bâtonnier ou le représentant de l'ordre provincial des médecins, selon le cas, en soit averti.

Ces personnes sont tenues au secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.

§ 3. Le juge d'instruction évalue, après concertation avec le bâtonnier ou le représentant de l'ordre provincial des médecins, quelles parties des communications non accessibles au public ou données d'un système informatique visées à l'article 90*sexies*, § 3, qu'il estime pertinentes pour l'instruction, relèvent du secret professionnel et quelles sont celles qui n'en relèvent pas.

Seules les parties des communications ou données visées à l'alinéa 1er qui sont estimées ne pas relever du secret professionnel sont transcrites ou reproduites et, le cas échéant, traduites. Le juge d'instruction en fait dresser procès-verbal. Les fichiers contenant ces communications ou données sont déposés au greffe sous pli scellé.

Toutes les autres communications ou données sont déposées au greffe dans un autre fichier sous pli scellé séparé ».

B.24.3. Cette disposition a été introduite dans le Code d'instruction criminelle par l'article 22 de la loi attaquée. L'exposé des motifs indique à son sujet :

« L'exception pour les avocats et les médecins était dictée par la considération que ces catégories professionnelles sont par excellence exposées au risque d'être confrontées à des suspects avec qui, en raison de leur situation professionnelle, elles entretiennent une relation de confiance qui doit tout particulièrement être préservée. Il s'agit de la clause de protection classique telle qu'elle apparaît également dans des mesures d'investigation similaires comme l'ouverture de courrier (article 88*sexies* du Code d'instruction criminelle), une observation afin d'avoir une vue dans un domicile (article 56*bis* du Code d'instruction criminelle) ou un contrôle visuel discret (article 89*ter* du Code d'instruction criminelle) » (*Doc. parl.*, 2015-2016, DOC 54-1966/001, pp. 72-73).

B.25. Le secret professionnel auquel sont astreints les avocats et les médecins n'entend pas leur conférer un quelconque privilège mais vise, principalement, à protéger le droit fondamental au respect de la vie privée de la personne qui se confie à eux, parfois dans ce qu'elle a de plus intime. En outre, les informations confidentielles confiées à un avocat, dans l'exercice de sa profession et en raison de cette qualité, bénéficient aussi, dans certaines hypothèses, de la protection découlant, pour le justiciable, des garanties inscrites à l'article 6 de la Convention européenne des droits de l'homme, dès lors que la règle du secret professionnel imposée à l'avocat est un élément fondamental des droits de la défense du justiciable qui se confie à lui.

B.26.1. Il n'est pas justifié que la clause de protection du secret professionnel des avocats et des médecins ne soit prévue que lorsque la recherche dans un système informatique qu'ils utilisent à titre professionnel est menée en secret et non lorsqu'elle est portée à leur connaissance. En effet, l'ingérence dans le droit au respect de la vie privée des personnes qui leur ont confié des informations couvertes par leur secret professionnel intervient de la même manière, que la recherche soit menée à l'insu ou non de l'avocat ou du médecin concerné.

B.26.2. Il est exact, ainsi que le soutient le Conseil des ministres, que lorsque la recherche a lieu dans un système informatique dans le cadre d'une perquisition, les dispositions relatives aux perquisitions dans les locaux professionnels d'avocats ou de médecins sont applicables et permettent de garantir le secret professionnel. Les possibilités de recherche non secrètes prévues par l'article 39*bis* du Code d'instruction criminelle vont toutefois au-delà de cette hypothèse précise et peuvent être menées en dehors de l'hypothèse de la perquisition de locaux professionnels.

B.27. Le premier moyen, en sa cinquième branche, est fondé. Il y a lieu d'annuler l'article 39*bis* du Code d'instruction criminelle, introduit par l'article 2 de la loi attaquée, en ce qu'il ne prévoit pas de disposition spécifique en vue de protéger le secret professionnel des médecins et des avocats.

Afin de garantir la sécurité juridique relativement aux recherches effectuées dans des systèmes informatiques appartenant à des médecins ou à des avocats, les effets de la disposition annulée doivent être maintenus ainsi qu'il est indiqué dans le dispositif.

Quant au second moyen

En ce qui concerne la disposition attaquée

B.28.1. Le second moyen porte sur l'article 7 de la loi du 25 décembre 2016, qui insère dans le Code d'instruction criminelle un article 46*sexies* qui dispose :

« Art. 46*sexies*. § 1er. Dans la recherche des crimes et délits, si les nécessités de l'enquête l'exigent et que les autres moyens d'investigation ne semblent pas suffire à la manifestation de la vérité, le procureur du Roi peut autoriser les services de police visés à l'alinéa 2 à entretenir, le cas échéant sous une identité fictive, des contacts sur Internet avec une ou plusieurs personnes concernant lesquelles il existe des indices sérieux qu'elles commettent ou commettraient des infractions pouvant donner lieu à un emprisonnement correctionnel principal d'un an ou à une peine plus lourde.

Le Roi détermine les conditions, y compris pour ce qui concerne la formation, et les modalités de désignation des services de police habilités à exécuter la mesure visée au présent article.

Dans des circonstances exceptionnelles et moyennant l'autorisation expresse du procureur du Roi, le fonctionnaire des services de police visés à l'alinéa 2 peut, dans le cadre d'une opération déterminée, recourir momentanément à l'expertise d'une personne qui ne fait pas partie des services de police si cela s'avère strictement nécessaire à la réussite de sa mission. L'autorisation et l'identité de cette personne sont conservées dans le dossier visé au paragraphe 3, alinéa 7.

Le présent article ne s'applique pas à l'interaction personnelle de fonctionnaires de police, dans l'exercice de leurs missions de police judiciaire, avec une ou plusieurs personnes sur Internet, qui n'a pour finalité directe qu'une vérification ciblée ou une arrestation, et ceci sans utiliser d'identité fictive crédible.

§ 2. La mesure visée au § 1er est ordonnée par le procureur du Roi par une autorisation écrite et motivée préalable. Cette autorisation est valable pour une période de trois mois, sous réserve de renouvellement.

En cas d'urgence, l'autorisation peut être donnée verbalement. Elle doit être confirmée dans les plus brefs délais dans la forme prévue à l'alinéa 1er.

§ 3. Sont exemptés de peine, les fonctionnaires de police qui, dans le cadre de leur mission et en vue de la réussite de celle-ci ou afin de garantir leur propre sécurité ou celle d'autres personnes concernées par la mesure, commettent des infractions strictement nécessaires, ce avec l'accord exprès du procureur du Roi.

Ces infractions ne peuvent être plus graves que celles pour lesquelles la mesure est utilisée et doivent nécessairement être proportionnelles à l'objectif visé.

Les alinéas 1er et 2 sont également d'application aux personnes qui ont fourni directement une aide ou une assistance nécessaire à l'exécution de cette mission ainsi qu'aux personnes visées au § 1er, alinéa 3.

Le magistrat qui autorise, dans le respect du présent Code, un fonctionnaire de police et la personne visée à l'alinéa 3 à commettre des infractions dans le cadre de l'exécution de la mesure, n'encourt aucune peine.

Les fonctionnaires de police communiquent, par écrit et préalablement à l'exécution de la mesure, au procureur du Roi les infractions qu'eux-mêmes ou les personnes visées à l'alinéa 3 ont l'intention de commettre.

Si cette notification préalable n'a pas pu avoir lieu, les fonctionnaires de police informent sans délai le procureur du Roi des infractions qu'eux-mêmes ou les personnes visées à l'alinéa 3 ont commises et en donnent ensuite confirmation par écrit.

Le procureur du Roi indique dans une décision écrite séparée les infractions pouvant être commises par les services de police et les personnes visées à l'alinéa 3 dans le cadre de la mesure qu'il a ordonnée. Cette décision est conservée dans un dossier séparé et confidentiel. Il est le seul à avoir accès à ce dossier, sans préjudice du droit de consultation du juge d'instruction et de la chambre des mises en accusation visé respectivement à l'article 56*bis* et aux articles 235*ter*, § 3, et 235*quater*, § 3. Le contenu de ce dossier est couvert par le secret professionnel.

§ 4. L'officier de police judiciaire chargé de l'enquête rédige le procès-verbal des différentes phases de l'exécution de cette mesure, y compris les contacts pertinents. Ces procès-verbaux sont joints au dossier au plus tard après la fin de la mesure.

Les contacts visés au paragraphe 1er sont enregistrés avec les moyens techniques appropriés et joints au dossier ou déposés au greffe, sous forme numérique ou non, au plus tard après la fin de la mesure.

§ 5. Le procureur du Roi est chargé de l'exécution des autorisations de la mesure visée au § 1er, alinéa 1er, accordées par le juge d'instruction dans le cadre d'une instruction, conformément à l'article 56*bis*.

Le procureur du Roi indique à ce moment dans une décision écrite séparée les infractions pouvant être commises par les services de police et les personnes visées au § 3, alinéa 3, dans le cadre de la mesure ordonnée par le juge d'instruction. Cette décision est conservée dans le dossier visé au § 3, alinéa 7 ».

B.28.2. L'exposé des motifs relatif à cette disposition mentionne :

« Cet article introduit la possibilité de procéder à une infiltration ou à une interaction sur Internet qui ne vise pas uniquement une vérification ciblée ou une arrestation.

Étant donné que l'infiltration sur Internet a un caractère moins intrusif que l'infiltration ' classique ' et que les différents contacts durant l'exécution de cette mesure sont enregistrés, un régime plus souple est justifié » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1966/001, p. 36).

En ce qui concerne la différence de régime avec l'infiltration dans le monde réel

B.29.1. Le second moyen, en sa première branche, est pris de la violation des articles 10 et 11 de la Constitution. Les parties requérantes estiment que le critère tiré du caractère virtuel ou réel de la mesure d'infiltration ne permet pas de justifier, d'une part, que le procureur du Roi ne puisse pas, dans le cadre d'une infiltration sur Internet, prendre des mesures en vue de garantir la sécurité et l'intégrité physique, psychique et morale de l'infiltrant et, d'autre part, que le contrôle sur l'exécution de la méthode, prévu par les articles 235*ter* et 235*quater* du Code d'instruction criminelle, ne s'applique pas à l'infiltration sur Internet.

B.29.2. Les parties requérantes ayant intérêt à l'annulation de la disposition attaquée, il n'y a pas lieu de s'interroger sur leur intérêt à ce moyen, en sa première branche, contrairement à ce que soutient le Conseil des ministres.

La sécurité des « cyberinfiltrants »

B.30.1. L'article 47*octies* du Code d'instruction criminelle, qui concerne l'infiltration dans le monde réel, précise en son paragraphe 2, alinéa 3, que si c'est justifié, le procureur du Roi accorde l'autorisation de prendre les mesures nécessaires en vue de garantir la sécurité, ainsi que l'intégrité physique, psychique et morale de l'infiltrant.

B.30.2. En réponse à une observation du Conseil d'État sur ce point, l'exposé des motifs précise :

« Le Conseil d'État se demande aussi, au point 25 de l'avis, pourquoi le procureur du Roi, contrairement à ce qui est le cas pour l'infiltration classique, ne peut pas prendre des mesures en vue de garantir la sécurité, ainsi que l'intégrité physique, psychique et morale du cyberinfiltrant (voir l'article 47*octies*, § 2, dernier alinéa, du Code d'instruction criminelle). Le gouvernement estime que ceci est superflu lorsqu'une infiltration est réalisée uniquement via Internet. Il n'y a tout d'abord pas de contact physique avec d'éventuels suspects. En outre, il va de soi que les cyberinfiltrants continueront de faire l'objet d'un suivi. Aucune base légale n'est requise pour garantir leur intégrité psychique et morale » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1966/001, p. 42).

B.30.3. L'infiltration réalisée uniquement sur Internet ne présente pas les mêmes risques, pour la sécurité physique de l'infiltrant, qu'une infiltration dans le monde réel. Le législateur a dès lors pu raisonnablement estimer qu'il n'était pas nécessaire de prévoir les mêmes possibilités de prendre des mesures pour garantir la sécurité physique de l'infiltrant qui n'agit que dans le monde virtuel. La différence de traitement attaquée repose dès lors, à cet égard, sur un critère pertinent.

B.30.4. Au surplus, la disposition n'interdit pas la mise en œuvre, au sein des services de police concernés, de mesures de suivi et de soutien psychologiques adaptées à la situation des personnes qui effectuent des infiltrations sur Internet de sorte que la disposition attaquée n'a pas de conséquences disproportionnées pour les cyberinfiltrants, en ce qui concerne leur sécurité psychique et morale.

Le contrôle par la chambre des mises en accusation

B.31.1. L'article 235*ter* du Code d'instruction criminelle charge la chambre des mises en accusation de contrôler la mise en œuvre, notamment, des infiltrations effectuées dans le monde réel. En vertu de la même disposition, la chambre des mises en accusation ne contrôle la mise en œuvre des infiltrations sur Internet que si un dossier confidentiel a été ouvert dans ce cadre.

Un dossier confidentiel doit toujours être ouvert lors de l'autorisation d'une infiltration dans le monde réel. Il contient l'autorisation d'infiltration, les décisions de modification, d'extension ou de prolongation, ainsi que les rapports établis par l'officier de police judiciaire sur chaque phase de l'exécution des infiltrations qu'il dirige. En revanche, dans le cas d'une infiltration sur Internet, un dossier confidentiel ne doit être ouvert que dans deux hypothèses : lorsque l'infiltrant recourt à l'expertise d'une personne extérieure aux services de police et lorsque le procureur du Roi autorise la commission d'une infraction.

B.31.2. L'établissement du dossier confidentiel découle de la nécessité, dans certains procès pénaux, de protéger l'anonymat des témoins ou de garder le secret sur des méthodes d'enquête mises en œuvre, intérêts qui doivent être mis en balance avec les droits de la défense du prévenu qui impliquent en principe que celui-ci puisse contester en connaissance de cause tout moyen de preuve retenu contre lui. L'intervention de la chambre des mises en accusation en vertu des articles 235*ter* et 235*quater* du Code d'instruction criminelle vise spécifiquement le dossier confidentiel et constitue la garantie qu'un juge indépendant et impartial exerce un contrôle sur la régularité de la mise en œuvre des méthodes particulières de recherche et des preuves qu'elles ont permis de produire lorsque les intérêts précités justifient que l'accusé n'ait pas accès à l'intégralité du dossier pénal.

B.31.3. Contrairement à ce qui est le cas dans le monde réel, en vertu du paragraphe 4, alinéa 2, de la disposition attaquée, tous les contacts établis dans le cadre de l'infiltration sur Internet sont enregistrés et joints au dossier ou déposés au greffe. Les personnes poursuivies sur la base de preuves récoltées au cours d'une infiltration sur Internet ont donc accès à l'ensemble de la mise en œuvre de l'infiltration. Elles sont à même de contester le recours à cette méthode et ses modalités d'exécution et elles peuvent inviter la juridiction d'instruction ou la juridiction de fond à en contrôler la régularité. Il ne s'impose donc pas, dans ce cas, qu'un dossier confidentiel soit ouvert et qu'un contrôle spécifique soit exercé sur celui-ci par la chambre des mises en accusation. La différence de traitement repose, à cet égard également, sur un critère pertinent.

B.31.4. Le second moyen, en sa première branche, n'est pas fondé.

En ce qui concerne les modalités de désignation des services de police habilités à exercer une infiltration sur Internet

B.32.1. Le second moyen, en sa deuxième branche, est pris de la violation des articles 12 et 14 de la Constitution, lus en combinaison avec l'article 6 de la Convention européenne des droits de l'homme et vise le paragraphe 1er, alinéa 2, de l'article 7 attaqué. Les parties requérantes font grief au législateur d'avoir délégué au Roi, en violation du principe de légalité en matière pénale, le pouvoir de déterminer les modalités de désignation des services de police habilités à exécuter la mesure d'infiltration sur Internet.

B.32.2. L'exposé des motifs indique, au sujet de cette délégation :

« S'agissant des services de police qui vont pouvoir réaliser la nouvelle mesure, il n'est pas nécessaire d'avoir un régime aussi strict que pour l'infiltration telle qu'elle existe actuellement. Cette dernière est réservée aux membres des unités spéciales de la police fédérale (DSU). Cela est justifié par la dangerosité de la mesure, y compris et surtout pour l'agent infiltrant. Cette limitation n'est pas justifiée pour la mesure se déroulant uniquement sur Internet. Cela ne signifie toutefois pas que tout enquêteur pourra se voir charger d'exécuter une telle interaction ou infiltration. Seuls les services de police spécifiquement désignés pourront exécuter la mesure. Une formation spécifique sera prévue tant pour protéger la vie privée des personnes visées que pour assurer le bon déroulement des enquêtes. Dans l'avant-projet, cette désignation était déléguée au ministre de la Justice. Le Conseil d'État observe qu'une telle délégation n'est pas autorisée et que les services de police compétents devraient être repris dans la loi. Le gouvernement fait remarquer qu'une telle délégation au ministre de la Justice existe déjà dans le cadre de l'application des méthodes particulières de recherche (art. 47*ter*, § 1er, alinéa 2, CIC) et qu'il n'appartient pas au législateur d'élaborer un règlement détaillé. Une formation spécifique sera en effet prévue pour les services de police visés, en vue aussi bien de la protection de la vie privée des personnes visées que de l'assurance du bon déroulement des enquêtes. Pour ces raisons, le gouvernement prend l'option de faire déterminer les conditions, y compris pour ce qui concerne la formation, et modalités de la désignation des services de police compétents par le Roi » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1966/001, p. 40).

B.33.1. En attribuant au pouvoir législatif la compétence, d'une part, de déterminer dans quels cas et sous quelle forme des poursuites pénales sont possibles, et, d'autre part, d'adopter une loi en vertu de laquelle une peine peut être établie et appliquée, les articles 12, alinéa 2, et 14 de la Constitution garantissent à tout justiciable qu'aucun comportement ne sera punissable, qu'aucune peine ne sera infligée et qu'aucune procédure pénale ne sera établie qu'en vertu de règles adoptées par une assemblée délibérante, démocratiquement élue.

B.33.2. Le principe de légalité en matière pénale ne va pas jusqu'à obliger le législateur à régler lui-même chaque aspect de la procédure pénale. Une délégation au pouvoir exécutif n'est pas contraire à ce principe, pour autant que l'habilitation soit définie en des termes suffisamment précis et porte sur l'exécution de mesures dont les éléments essentiels ont été fixés préalablement par le législateur.

B.34.1. En l'espèce, il peut être admis que le législateur ait considéré qu'il était nécessaire d'habiliter le Roi à désigner les services de police compétents pour effectuer des infiltrations sur Internet. Dans une matière en perpétuel développement comme l'Internet, il est en effet indiqué qu'une certaine souplesse permette aux autorités d'adapter régulièrement le contenu de la formation permettant aux policiers de mettre en œuvre la mesure d'infiltration sur Internet, ce qui suppose également de pouvoir adapter la désignation des officiers de police habilités en fonction des formations disponibles et suivies par les membres des services concernés.

Par ailleurs, l'article 46*sexies* du Code d'instruction criminelle définit les conditions dans lesquelles l'infiltration sur Internet peut être ordonnée. Par la disposition attaquée, le législateur a habilité le Roi à adopter des dispositions portant sur des mesures dont il a donc lui-même fixé les éléments essentiels.

B.34.2. Le second moyen, en sa deuxième branche, n'est pas fondé.

En ce qui concerne l'exclusion de la notion d'infiltration de certaines mesures ciblées

B.35.1. Le second moyen, en sa troisième branche, est pris de la violation des articles 12 et 14 de la Constitution et vise le paragraphe 1er, alinéa 4, de l'article 46*sexies* du Code d'instruction criminelle. Les parties requérantes font grief au législateur d'avoir négligé de définir, en violation du principe de légalité en matière pénale, les actes d'enquête accomplis sur Internet qui ne doivent pas faire l'objet d'une autorisation du procureur du Roi et qui peuvent donc être posés d'initiative par les policiers. Elles estiment que l'expression « interaction [...] qui n'a pour finalité directe qu'une vérification ciblée ou une arrestation » permet aux officiers de police judiciaire de détourner ou de méconnaître les conditions strictes de l'infiltration sur Internet.

B.35.2. L'exigence de prévisibilité de la procédure pénale, inscrite à l'article 12, alinéa 2, de la Constitution, garantit à tout justiciable qu'il ne peut faire l'objet d'une information, d'une instruction et de poursuites que selon une procédure dont il peut prendre connaissance avant sa mise en œuvre.

B.36. L'exposé des motifs relatif à la disposition attaquée mentionne :

« Cette précision vise à éviter de créer une situation où les services de police voient leur capacité d'action sur Internet réduite par rapport à ce qui existe actuellement que ce soit sur Internet ou dans le monde physique » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1966/001, p. 38).

Les exemples suivants sont ensuite cités : un contact pour prendre un rendez-vous afin de voir un bien mis en vente via une « petite annonce » publiée dans un journal ou placée sur un site de vente d'occasion, une brève interaction avec une personne qui a posté un message sur Internet pour déterminer s'il s'agit d'une personne sérieusement radicalisée ou d'un malheureux plaisantin, la fixation d'un lieu de rencontre physique avec une personne afin de pouvoir l'arrêter. Le texte précise que dans ces cas, le policier ne mentionne pas son statut, mais qu'il n'utilise pas non plus de fausse identité et que ce type d'interaction « ne vise qu'un aspect spécifique et très limité » (*ibid.*, p. 39).

B.37.1. Il apparaît suffisamment du texte de la disposition attaquée, éclairé par les précisions mentionnées dans l'exposé des motifs précité, que l'infiltration sur Internet qui ne peut être mise en œuvre que moyennant l'autorisation du procureur du Roi consiste en « l'entretien » de contacts avec un ou plusieurs suspects, sous couvert d'une identité fictive. De même, l'article 47*octies* du Code d'instruction criminelle, qui concerne l'infiltration dans le monde réel, définit celle-ci comme le fait « d'entretenir, sous une identité fictive, des relations durables » avec un ou plusieurs suspects. L'infiltration, sous ces deux formes, suppose donc, d'une part la construction d'une identité fictive crédible pour l'infiltrant et, d'autre part, une interaction d'une certaine durée avec une ou plusieurs personnes soupçonnées de commettre ou de pouvoir commettre des infractions d'une certaine gravité. Les contacts ponctuels en vue de convenir d'un rendez-vous ou d'opérer une vérification ciblée, qui permettent à la police judiciaire d'exercer ses missions conformément à l'article 15 de la loi du 5 août 1992 sur la fonction de police, ne répondent pas à cette définition et ne doivent donc pas avoir été préalablement autorisés par le procureur du Roi.

B.37.2. Le second moyen, en sa troisième branche, n'est pas fondé.

Par ces motifs,

la Cour

1. annule :

- l'article 39*bis*, § 3, du Code d'instruction criminelle, inséré par l'article 2 de la loi du 25 décembre 2016 « portant des modifications diverses au Code d'instruction criminelle et au Code pénal, en vue d'améliorer les méthodes particulières de recherche et certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications et créant une banque de données des empreintes vocales »;

- l'article 13 de la loi du 25 décembre 2016 précitée;

- l'article 39*bis* du Code d'instruction criminelle, inséré par l'article 2 de la loi du 25 décembre 2016 précitée, en ce qu'il ne prévoit pas de disposition spécifique en vue de protéger le secret professionnel des médecins et des avocats;

2. maintient les effets produits par les dispositions annulées jusqu'à la date de la publication du présent arrêt au *Moniteur belge*;

3. sous réserve des interprétations mentionnées en B.15.2 et en B.22.2, rejette le recours pour le surplus.

Ainsi rendu en langue française, en langue néerlandaise et en langue allemande, conformément à l'article 65 de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle, le 6 décembre 2018.

Le greffier, Le président,

F. Meersschaut F. Daoût

GRONDWETTELIJK HOF

[2019/200144]

Uittreksel uit arrest nr. 174/2018 van 6 december 2018

Rolnummer 6711

In zake : het beroep tot vernietiging van de artikelen 2 en 7 van de wet van 25 december 2016 « houdende diverse wijzigingen van het Wetboek van strafvordering en het Strafwetboek, met het oog op de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet en elektronische en telecommunicaties en tot oprichting van een gegevensbank stemafdrukken », ingesteld door de vzw « Ligue des Droits de l'Homme » en de vzw « Liga voor Mensenrechten ».

Het Grondwettelijk Hof,

samengesteld uit de voorzitters F. Daoût en A. Alen, en de rechters L. Lavrysen, J.-P. Snappe, J.-P. Moerman, E. Derycke, T. Merckx-Van Goey, P. Nihoul, T. Giet, R. Leysen, J. Moerman en M. Pâques, bijgestaan door de griffier F. Meersschaut, onder voorzitterschap van voorzitter F. Daoût,

wijst na beraad het volgende arrest :

I. *Onderwerp van het beroep en rechtspleging*

Bij verzoekschrift dat aan het Hof is toegezonden bij op 17 juli 2017 ter post aangetekende brief en ter griffie is ingekomen op 19 juli 2017, is beroep tot vernietiging ingesteld van de artikelen 2 en 7 van de wet van 25 december 2016 « houdende diverse wijzigingen van het Wetboek van strafvordering en het Strafwetboek, met het oog op de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet en elektronische en telecommunicaties en tot oprichting van een gegevensbank stemafdrukken » (bekendgemaakt in het *Belgisch Staatsblad* van 17 januari 2017) door de vzw « Ligue des Droits de l'Homme » en de vzw « Liga voor Mensenrechten », bijgestaan en vertegenwoordigd door Mr. D. Ribant en Mr. C. Forget, advocaten bij de balie te Brussel, Mr. J. Heymans, advocaat bij de balie te Gent, en Mr. J. Vander Velpen, advocaat bij de balie te Antwerpen.

(...)

II. *In rechte*

(...)

Ten aanzien van het onderwerp van het beroep

B.1.1. Het beroep heeft betrekking op de artikelen 2 en 7 van de wet van 25 december 2016 « houdende diverse wijzigingen van het Wetboek van strafvordering en het Strafwetboek, met het oog op de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet en elektronische en telecommunicaties en tot oprichting van een gegevensbank stemafdrukken » (hierna : de wet van 25 december 2016).

B.1.2. Die wet beoogt in het Wetboek van strafvordering een aantal wijzigingen aan te brengen in het opsporingsonderzoek en het gerechtelijk onderzoek, meer in het bijzonder in de toepassing van de bijzondere opsporingsmethoden en bepaalde andere onderzoeksmethoden die in het bijzonder betrekking hebben op de internetrecherche en elektronische en telecommunicaties. De bepalingen die bij de bestreden wet worden gewijzigd, werden bij verschillende wetten in het Wetboek van strafvordering ingevoerd en « [zijn] niet meer hervormd of aangepast [sinds 2000] », hetgeen « een eeuwigheid » is « in de snel evoluerende wereld van de informatietechnologie » (*Parl. St.*, Kamer, 2015-2016, DOC 54-1966/001, p. 5). Met de bestreden wet wilde de wetgever dan ook « een meer aangepast juridisch kader ontwerpen voor de zoeking in een informaticasysteem en het onderscheppen en kennisnemen van elektronische communicatie » (*ibid.*, p. 7).

B.1.3. Het eerste middel, dat uit vijf onderdelen bestaat, heeft betrekking op artikel 2 van die wet, dat de zoeking in een informaticasysteem betreft. Het tweede middel, dat drie onderdelen bevat, beoogt artikel 7 van die wet, dat betrekking heeft op de infiltratie op internet.

Ten aanzien van het eerste middel

Wat de bestreden bepaling betreft

B.2. Bij artikel 2 van de wet van 25 december 2016 wordt artikel 39*bis* van het Wetboek van strafvordering als volgt gewijzigd :

1° in paragraaf 1, die bepaalde « Onverminderd de specifieke bepalingen van dit artikel, zijn de regels van dit wetboek inzake inbeslagneming, met inbegrip van artikel 28*sexies*, van toepassing op het kopiëren, ontoegankelijk maken en verwijderen van in een informaticasysteem opgeslagen gegevens », worden de woorden « of een deel ervan » ingevoegd tussen de woorden « een informaticasysteem » en de woorden « opgeslagen gegevens »;

2° de paragrafen 2 tot 6 worden vervangen door de volgende bepalingen :

« § 2. Tot de zoeking in een informaticasysteem of een deel ervan dat in beslag genomen is, kan beslist worden door een officier van gerechtelijke politie.

Onverminderd het eerste lid, kan de procureur des Konings een zoeking bevelen in een informaticasysteem of een deel ervan dat door hem in beslag kan worden genomen.

De zoekingen bedoeld in het eerste en het tweede lid kunnen zich enkel uitstrekken tot de gegevens die opgeslagen zijn op het informaticasysteem dat, respectievelijk, in beslag genomen is of in beslag kan worden genomen. Met het oog daarop wordt elke externe verbinding van dit informaticasysteem verhinderd, alvorens de zoeking wordt aangevat.

§ 3. De procureur des Konings kan de zoeking in een informaticasysteem of een deel ervan, aangevat op grond van paragraaf 2, uitbreiden naar een informaticasysteem of een deel ervan dat zich op een andere plaats bevindt dan daar waar de zoeking plaatsvindt :

- indien deze uitbreiding noodzakelijk is om de waarheid aan het licht te brengen ten aanzien van het misdrijf dat het voorwerp uitmaakt van de zoeking; en

- indien andere maatregelen disproportioneel zouden zijn, of indien er een risico bestaat dat zonder deze uitbreiding bewijselementen verloren gaan.

De uitbreiding van de zoeking in een informaticasysteem mag zich niet verder uitstrekken dan tot de informaticasystemen of de delen ervan waartoe de personen die gerechtigd zijn het onderzochte informaticasysteem te gebruiken, in het bijzonder toegang hebben.

Inzake de door uitbreiding van de zoeking in een informaticasysteem aangetroffen gegevens, die nuttig zijn voor dezelfde doeleinden als de inbeslagneming, wordt gehandeld zoals bepaald in paragraaf 6.

Wanneer blijkt dat deze gegevens zich niet op het grondgebied van het Rijk bevinden, worden ze enkel gekopieerd. In dat geval deelt de procureur des Konings dit onverwijld mee aan de Federale Overheidsdienst Justitie, dat de bevoegde overheid van de betrokken Staat hiervan op de hoogte brengt, indien deze redelijkerwijze kan worden bepaald.

In geval van uiterst dringende noodzakelijkheid kan de procureur des Konings de uitbreiding van de zoeking bedoeld in het eerste lid mondeling bevelen. Dit bevel wordt zo spoedig mogelijk schriftelijk bevestigd, met vermelding van de redenen van de uiterst dringende noodzakelijkheid.

§ 4. Enkel de onderzoeksrechter kan een andere zoeking bevelen in een informaticasysteem of een deel ervan dan de zoekingen voorzien in de paragrafen 2 en 3 :

- indien deze zoeking noodzakelijk is om de waarheid aan het licht te brengen ten aanzien van het misdrijf dat het voorwerp uitmaakt van de zoeking; en

- indien andere maatregelen disproportioneel zouden zijn, of indien er een risico bestaat dat zonder deze zoeking bewijselementen verloren gaan.

In geval van uiterst dringende noodzakelijkheid kan de onderzoeksrechter de uitbreiding van de zoeking bedoeld in het eerste lid mondeling bevelen. Dit bevel wordt zo spoedig mogelijk schriftelijk bevestigd, met vermelding van de redenen van de uiterst dringende noodzakelijkheid.

§ 5. Teneinde de maatregelen bedoeld in dit artikel mogelijk te maken, kan de procureur des Konings of de onderzoeksrechter bevelen om, te allen tijde, ook zonder de toestemming van hetzij de eigenaar of zijn rechthebbende, hetzij de gebruiker :

- elke beveiliging van de betrokken informaticasystemen tijdelijk op te heffen, desgevallend met behulp van technische hulpmiddelen, valse signalen, valse sleutels of valse hoedanigheden;

- technische middelen in de betrokken informaticasystemen aan te brengen teneinde de door dat systeem opgeslagen, verwerkte of doorgestuurde gegevens te ontcijferen en te decoderen.

Evenwel kan enkel de onderzoeksrechter deze tijdelijke opheffing van de beveiliging of deze aanbrenging van technische middelen bevelen wanneer dit in het bijzonder noodzakelijk is voor de toepassing van paragraaf 3.

§ 6. Indien in de betrokken informaticasystemen opgeslagen gegevens aangetroffen worden die nuttig zijn voor dezelfde doeleinden als de inbeslagneming, maar de inbeslagneming van de drager daarvan evenwel niet wenselijk is, worden deze gegevens, evenals de gegevens noodzakelijk om deze te kunnen verstaan, gekopieerd op dragers, die toebehoren aan de overheid. In geval van dringendheid of om technische redenen, kan gebruik gemaakt worden van dragers, die ter beschikking staan van personen die gerechtigd zijn om het informaticasysteem te gebruiken.

Bovendien worden passende technische middelen aangewend om de toegang tot deze gegevens in het informaticasysteem, evenals tot de kopieën daarvan die ter beschikking staan van personen die gerechtigd zijn om het informaticasysteem te gebruiken, te verhinderen en hun integriteit te waarborgen.

Wanneer de in het eerste lid vermelde maatregel niet mogelijk is om technische redenen of wegens de omvang van de gegevens, wendt de procureur des Konings de passende technische middelen aan om de toegang tot deze gegevens in het informaticasysteem, evenals tot de kopieën daarvan die ter beschikking staan van personen die gerechtigd zijn om het informaticasysteem te gebruiken, te verhinderen en hun integriteit te waarborgen.

Indien de gegevens het voorwerp van het misdrijf vormen of voortgekomen zijn uit het misdrijf en indien de gegevens strijdig zijn met de openbare orde of de goede zeden, of een gevaar opleveren voor de integriteit van informaticasystemen of gegevens die door middel daarvan worden opgeslagen, verwerkt of overgedragen, wendt de procureur des Konings alle passende technische middelen aan om deze gegevens ontoegankelijk te maken of, na hiervan kopie te hebben genomen, te verwijderen.

Hij kan evenwel, behoudens in het geval bedoeld in het vierde lid, het verdere gebruik van het geheel of een deel van deze gegevens toestaan, wanneer dit geen gevaar voor de strafvordering oplevert.

In geval van uiterst dringende noodzakelijkheid en wanneer het kennelijk gaat om een strafbaar feit bedoeld in de artikelen 137, § 3, 6°, 140*bis* of 383*bis*, § 1, van het Strafwetboek, kan de procureur des Konings mondeling bevelen dat alle passende technische middelen worden aangewend om de gegevens, die het voorwerp van het misdrijf vormen of voortgekomen zijn uit het misdrijf en die strijdig zijn met de openbare orde of de goede zeden, ontoegankelijk te maken. Dit bevel wordt zo spoedig mogelijk schriftelijk bevestigd, met vermelding van de redenen van de uiterst dringende noodzakelijkheid »;

3° het artikel wordt aangevuld met de paragrafen 7 en 8, luidende :

« § 7. Tenzij diens identiteit of woonplaats redelijkerwijze niet achterhaald kan worden, brengt de procureur des Konings of de onderzoeksrechter de verantwoordelijke van het informaticasysteem zo spoedig mogelijk op de hoogte van de zoeking in het informaticasysteem of van de uitbreiding ervan. Hij deelt hem in voorkomend geval een samenvatting mee van de gegevens die zijn gekopieerd, ontoegankelijk gemaakt of verwijderd.

§ 8. De procureur des Konings wendt de passende technische middelen aan om de integriteit en de vertrouwelijkheid van deze gegevens te waarborgen.

Gepaste technische middelen worden aangewend voor de bewaring hiervan op de griffie.

Hetzelfde geldt, wanneer gegevens die worden opgeslagen, verwerkt of overgedragen in een informaticasysteem, samen met hun drager in beslag worden genomen, overeenkomstig de vorige artikelen ».

B.3.1. Het aldus gewijzigde artikel 39*bis* van het Wetboek van strafvordering betreft de zogenoemde « niet-geheime » zoekingen in een informaticasysteem. Krachtens paragraaf 7 ervan moet de verantwoordelijke van het betrokken informaticasysteem immers « zo spoedig mogelijk » op de hoogte worden gebracht van de zoeking in het systeem en, in voorkomend geval, van de uitbreiding van de zoeking naar een informaticasysteem dat zich op een andere plaats bevindt.

Volgens de memorie van toelichting bij de wet van 28 november 2000 inzake informaticacriminaliteit, waarbij het oorspronkelijke artikel 39*bis* in het Wetboek van strafvordering is ingevoerd, dient onder « informaticasysteem » te worden begrepen « alle systemen voor de opslag, verwerking of overdracht van data » (*Parl. St.*, Kamer, 1999-2000, DOC 50-0213/001 en DOC 50-0214/001, p. 12).

B.3.2. In beginsel kan een zoeking in een informaticasysteem of in een deel ervan enkel worden bevolen door een onderzoeksrechter, op voorwaarde dat die zoeking noodzakelijk is om de waarheid aan het licht te brengen ten aanzien van een misdrijf dat het voorwerp uitmaakt van de zoeking en dat de andere denkbare onderzoeksmaatregelen disproportioneel zijn of dat er een risico bestaat dat zonder die zoeking bewijselementen verloren gaan (§ 4). Hetzelfde geldt voor de uitbreiding van de zoeking naar een informaticasysteem dat toegankelijk is vanaf het systeem dat het voorwerp uitmaakt van de oorspronkelijke zoeking.

B.3.3. Bij de bestreden bepaling wordt voorzien in verscheidene uitzonderingen op de principiële bevoegdheid van de onderzoeksrechter wat de niet-geheime zoekingen betreft.

Ten eerste kan de zoeking in de gegevens die zijn opgeslagen in een informaticasysteem, of in een deel ervan, dat het voorwerp uitmaakt van een inbeslagneming, op eigen initiatief worden verricht door een officier van gerechtelijke politie, op voorwaarde dat het, om toegang te hebben tot de gegevens, niet noodzakelijk is een beveiliging op te heffen of de gegevens te ontcijferen of te decoderen. In het geval dat het, om toegang te hebben tot de opgeslagen gegevens, noodzakelijk is de beveiliging op te heffen of de gegevens te ontcijferen of te decoderen, moet de officier van gerechtelijke politie daartoe de toestemming van de procureur des Konings verkrijgen.

Ten tweede kan de procureur des Konings een zoeking bevelen in de gegevens die zijn opgeslagen in een informaticasysteem, of in een deel ervan, dat niet het voorwerp heeft uitgemaakt van een inbeslagneming maar dat door hem in beslag zou kunnen worden genomen. In dat geval kan hij ook bevelen dat de eventuele beveiliging wordt opgeheven of dat de gegevens worden ontcijferd of gedecodeerd.

Ten derde kan de procureur des Konings bevelen dat de zoeking, die is begonnen in een informaticasysteem dat in beslag is of zou kunnen worden genomen, wordt uitgebreid naar gegevens die zijn opgeslagen in een ander informaticasysteem dat via verbinding kan worden bereikt vanaf het systeem waarin de zoeking is opgestart. Indien de toegang tot de gegevens die zijn opgeslagen in dat andere informaticasysteem is beveiligd, moet de procureur des Konings evenwel de machtiging van de onderzoeksrechter verkrijgen om de beveiliging op te heffen of om technische middelen aan te brengen die hem de mogelijkheid bieden die gegevens te ontcijferen of te decoderen.

B.3.4. De geheime zoekingen beoogd in artikel 90*ter* van het Wetboek van strafvordering kunnen enkel door een onderzoeksrechter worden bevolen in uitzonderlijke gevallen, wanneer het onderzoek zulks vereist, indien er ernstige aanwijzingen bestaan dat het een van de in dat artikel opgesomde strafbare feiten betreft, en indien de overige middelen van onderzoek niet volstaan om de waarheid aan het licht te brengen.

Wat het recht op eerbiediging van het privéleven betreft

B.4.1. Het Hof onderzoekt eerst het eerste, tweede en vierde onderdeel van het eerste middel, die zijn afgeleid uit de schending van het recht op eerbiediging van het privéleven, gewaarborgd bij artikel 22 van de Grondwet en bij artikel 8 van het Europees Verdrag voor de rechten van de mens, alsook, voor het eerste en het tweede onderdeel, die zijn afgeleid uit de schending van het beginsel van gelijkheid en niet-discriminatie, gewaarborgd bij de artikelen 10 en 11 van de Grondwet.

B.4.2. De verzoekende partijen klagen aan dat artikel 39*bis* van het Wetboek van strafvordering, ingevoerd bij de bestreden bepaling, inmengingen door officieren van gerechtelijke politie of door parketmagistraten in het recht op eerbiediging van het privéleven toestaat, zonder toezicht door een onafhankelijke en onpartijdige rechter. Zij zijn van mening dat de in artikel 39*bis* beoogde zoekingen in een informaticasysteem een schending van het privéleven veroorzaken die vergelijkbaar is met die welke wordt veroorzaakt door een huiszoeking, die, harerzijds, enkel door een onderzoeksrechter kan worden toegestaan (vierde onderdeel van het middel). Zij zijn ook van oordeel dat het verschil in behandeling tussen de bij artikel 90*ter* van hetzelfde Wetboek beoogde geheime zoekingen, die steeds door een onderzoeksrechter moeten worden toegestaan, en de bij de bestreden bepaling beoogde niet-geheime zoekingen, die niet door een onderzoeksrechter moeten zijn toegestaan, op een criterium berust dat noch objectief, noch relevant is (eerste onderdeel van het middel). Zij gaan bovendien ervan uit dat het verschil in behandeling tussen de zoekingen in een in beslag genomen informaticasysteem, waartoe door een officier van gerechtelijke politie kan worden beslist, en de zoekingen in een informaticasysteem dat niet in beslag is maar kan worden genomen, waartoe enkel door de procureur des Konings kan worden beslist, ook op een criterium berust dat noch objectief, noch relevant is (tweede onderdeel van het middel).

B.5. In tegenstelling tot hetgeen de Ministerraad betoogt, leidt de omstandigheid dat in de wetgeving die voorafgaat aan de bestreden wet, in een bepaalde mate, reeds was voorzien in de bevoegdheid van de procureur des Konings om de inbeslagneming van informaticasystemen en de zoekingen in die systemen te bevelen, niet tot de niet-ontvankelijkheid, wegens het niet-tijdig indienen van het beroep, van het eerste onderdeel van het middel. Met de bestreden bepaling is de wetgever in die aangelegenheid immers opnieuw wetgevend opgetreden en heeft hij de bevoegdheid van de procureur des Konings bevestigd en uitgebreid.

B.6.1. Artikel 22 van Grondwet bepaalt :

« Ieder heeft recht op eerbiediging van zijn privéleven en zijn gezinsleven, behoudens in de gevallen en onder de voorwaarden door de wet bepaald.

De wet, het decreet of de in artikel 134 bedoelde regel waarborgen de bescherming van dat recht ».

Artikel 8 van het Europees Verdrag voor de rechten van de mens bepaalt :

« 1. Eenieder heeft recht op eerbiediging van zijn privé-leven, zijn gezinsleven, zijn huis en zijn briefwisseling.

2. Geen inmenging van enig openbaar gezag is toegestaan met betrekking tot de uitoefening van dit recht dan voor zover bij de wet is voorzien en in een democratische samenleving nodig is in het belang van 's lands veiligheid, de openbare veiligheid, of het economisch welzijn van het land, de bescherming van de openbare orde en het voorkomen van strafbare feiten, de bescherming van de gezondheid of de goede zeden, of voor de bescherming van de rechten en vrijheden van anderen ».

B.6.2. De Grondwetgever heeft gestreefd naar een zo groot mogelijke concordantie tussen artikel 22 van de Grondwet en artikel 8 van het voormeld Europees Verdrag (*Parl. St.*, Kamer, 1992-1993, nr. 997/5, p. 2).

De draagwijdte van dat artikel 8 is analoog aan die van de voormelde grondwetsbepaling, zodat de waarborgen die beide bepalingen bieden, een onlosmakelijk geheel vormen.

B.6.3. Die bepalingen vereisen dat elke overheidsinmenging in het recht op eerbiediging van het privéleven wordt voorgeschreven in een voldoende precieze wettelijke bepaling, beantwoordt aan een dwingende maatschappelijke behoefte en evenredig is met de daarin nagestreefde wettige doelstelling.

B.7.1. Zoals de afdeling wetgeving van de Raad van State onderstreept in haar advies met betrekking tot het voorontwerp van wet dat de bestreden wet is geworden, kan een zoeking in een informaticasysteem een belangrijke inmenging vormen in het recht op eerbiediging van het privéleven (*Parl. St.*, Kamer, 2015-2016, DOC 54-1966/001, pp. 126-127).

B.7.2. Het Europees Hof voor de Rechten van de Mens heeft ook reeds herhaaldelijk geoordeeld dat « het doorzoeken en het in beslag nemen van elektronische gegevens worden beschouwd als een inmenging in het recht op eerbiediging van het ' privéleven ' en de ' briefwisseling ' in de zin van [artikel 8 van het Verdrag] » en dat « een dergelijke inmenging artikel 8 schendt, behalve indien zij, ' bij de wet [...] voorzien ', een of meer wettige doelstellingen ten aanzien van lid 2 nastreeft en, bovendien, ' in een democratische samenleving nodig ' is om ze te bereiken » (EHRM, 2 april 2015, *Vinci Construction en GTM Génie Civil et Services t. Frankrijk*, §§ 63-64).

In die context onderzoekt dat Hof « of de interne wetgeving en praktijk afdoende en toereikende waarborgen bieden tegen misbruik en willekeur ». Tot die waarborgen behoort « het bestaan van een ' doeltreffend toezicht ' op de maatregelen die afbreuk doen aan artikel 8 van het Verdrag » (*ibid.*, §§ 66-67).

B.7.3. Gelet op de omvang van de inmenging in het recht op eerbiediging van het privéleven die de zoeking in een informaticasysteem kan veroorzaken, moet de toepassing ervan het voorwerp uitmaken van een controle door een onafhankelijke en onpartijdige rechter.

Wat betreft de zoeking in een informaticasysteem dat het voorwerp uitmaakt van een inbeslagneming

B.8.1. De bestreden bepaling biedt, in paragraaf 2, eerste lid, ervan, de officier van gerechtelijke politie de mogelijkheid om te beslissen tot het uitvoeren van een zoeking in een informaticasysteem dat het voorwerp uitmaakt van een inbeslagneming. De zoeking kan enkel betrekking hebben op de gegevens die zijn opgeslagen in het in beslag genomen toestel, aangezien voorafgaandelijk aan de zoeking dient te worden verhinderd dat dat toestel verbinding maakt met externe systemen. Bovendien, indien de zoeking vereist dat een beveiliging tijdelijk wordt opgeheven of dat de gegevens worden ontcijferd of gedecodeerd, moet de officier van gerechtelijke politie daartoe de machtiging van de procureur des Konings verkrijgen (§ 5, eerste lid).

B.8.2. Uit de memorie van toelichting blijkt dat de met de bestreden bepaling nagestreefde doelstelling, wat de zoeking in een in beslag genomen systeem betreft, erin bestaat in de wet de rechtspraak van het Hof van Cassatie te bevestigen :

« In zijn arrest van 11 februari 2015 (P.14.1739.F) stelde het Hof van Cassatie immers dat het huidige recht de officier van gerechtelijke politie reeds toestaat om kennis te nemen van de gegevens die zijn opgeslagen in een in beslag genomen gsm. Uiteraard gebeurt de exploitatie van de gegevens steeds binnen de grenzen van het strafrechtelijk onderzoek en onder controle van de magistraat die ermee is belast » (*Parl. St.*, Kamer, 2015-2016, DOC 54-1966/001, p. 15).

B.8.3. Bij zijn voormelde arrest van 11 februari 2015 heeft het Hof van Cassatie geoordeeld :

« Het uitlezen van het geheugen van een mobiele telefoon, waaronder de berichten die erin opgeslagen zijn in de vorm van tekstberichten, is een maatregel die voortvloeit uit de inbeslagneming die kan worden uitgevoerd in het kader van een opsporingsonderzoek zonder andere vormvereisten dan die welke bepaald zijn voor die onderzoekshandeling » (Cass., 11 februari 2015, P.14.1739.F).

B.8.4. De inbeslagneming is een onderzoeksdaad die kan worden verricht in de gevallen en onder de voorwaarden waarin is voorzien bij de bepalingen van het Wetboek van strafvordering, met name in geval van ontdekking op heterdaad of tijdens een regelmatig door de onderzoeksrechter bevolen huiszoeking. Zij kan betrekking hebben op alles wat lijkt te hebben gediend of te zijn bestemd om het strafbaar feit te plegen, alles wat eruit lijkt te zijn voortgekomen en alles wat kan dienen om de waarheid aan het licht te brengen (artikel 35 en volgende van het Wetboek van strafvordering).

B.8.5. Een persoon die zich geschaad acht door de inbeslagneming kan de opheffing ervan vragen, naar gelang van het geval, aan de procureur des Konings (artikel 28*sexies*, § 1, van het Wetboek van strafvordering) of aan de onderzoeksrechter (artikel 61*quater*, § 1, van hetzelfde Wetboek). In geval van weigering kan de geschade persoon zich tot de kamer van inbeschuldigingstelling wenden.

B.8.6. De zoeking in de gegevens die zijn opgeslagen in het geheugen van het in beslag genomen toestel is een accessorium van de inbeslagneming zelf, net zoals de kennisneming, door de officier van gerechtelijke politie, van de inhoud van de in beslag genomen boeken, notitieboekjes of documenten op fysieke drager. Aangezien het in beslag genomen toestel dat het voorwerp uitmaakt van de zoeking is losgekoppeld, zodat de politieofficier die de zoeking uitvoert, enkel toegang kan hebben tot de inhoud die de eigenaar of de bezitter van het toestel erin heeft opgeslagen of bewaard, onderscheidt de zoeking zich niet van de exploitatie, door de speurders, van de inhoud van documenten die het voorwerp uitmaken van een inbeslagneming.

B.8.7. Uit het voorgaande vloeit voort dat aan de zoeking in een informaticasysteem dat regelmatig in beslag is genomen, net zoals aan de exploitatie van regelmatig in beslag genomen documenten, voldoende jurisdictionele waarborgen zijn verbonden die het mogelijk maken te verzekeren dat de door die onderzoekshandeling veroorzaakte inmenging in het recht op eerbiediging van het privéleven is verantwoord ten aanzien van de vereisten van artikel 22 van de Grondwet en van artikel 8 van het Europees Verdrag voor de rechten van de mens.

B.8.8. Het onderzoek ten aanzien van de artikelen 10 en 11 van de Grondwet leidt niet tot een andere conclusie wat betreft de zoekingen in een in beslag genomen informaticasysteem. Het eerste middel, in zijn eerste en vierde onderdeel, is niet gegrond, in zoverre daarbij de zoekingen in een regelmatig in beslag genomen informaticasysteem worden beoogd.

Wat betreft de zoeking in een informaticasysteem dat het voorwerp kan uitmaken van een inbeslagneming

B.9.1. De bestreden bepaling biedt, in paragraaf 2, tweede lid, ervan, de procureur des Konings de mogelijkheid om te beslissen tot een zoeking in een informaticasysteem dat niet in beslag is genomen maar « waarvoor alle wettelijke voorwaarden voor een inbeslagneming zijn vervuld » (*Parl. St.*, Kamer, 2015-2016, DOC 54-1966/001, p. 16). De zoeking kan enkel betrekking hebben op de gegevens die zijn opgeslagen in het desbetreffende toestel, aangezien vooraf dient te worden verhinderd dat dat toestel verbinding maakt met externe systemen. Bovendien, indien de zoeking vereist dat een beveiliging tijdelijk wordt opgeheven of dat de gegevens worden ontcijferd of gedecodeerd, moet de officier van gerechtelijke politie daartoe ook de machtiging van de procureur des Konings verkrijgen (paragraaf 5, eerste lid).

B.9.2. In het geval waarin het informaticasysteem dat het voorwerp uitmaakt van het onderzoek, door de procureur des Konings in beslag zou kunnen worden genomen, zijn alle wettelijke voorwaarden waaronder tot de inbeslagneming kan worden beslist, vervuld. Daarenboven zijn, krachtens paragraaf 1 van artikel 39*bis* van het Wetboek van strafvordering, de regels inzake inbeslagneming van toepassing op het kopiëren, ontoegankelijk maken

en verwijderen van in een informaticasysteem of een deel ervan opgeslagen gegevens. Het kopiëren van gegevens afkomstig van een zoeking in een informaticasysteem dat om opportuniteitsredenen van praktische aard niet in beslag is genomen maar dat, ten aanzien van de wettelijke voorwaarden voor een inbeslagneming, in beslag had kunnen worden genomen, wordt dus, ten aanzien van de aan de betrokken persoon geboden rechtsmiddelen en waarborgen, zelf als een inbeslagneming beschouwd.

B.9.3. Daarenboven, aangezien het toestel waarin de zoeking wordt uitgevoerd is losgekoppeld, zodat de politieofficier die de zoeking uitvoert enkel toegang kan hebben tot de inhoud die de eigenaar of de bezitter van het toestel erin heeft opgeslagen of bewaard, onderscheidt die zoeking zich niet van een aan een inbeslagneming voorafgaande zoeking in documenten.

B.9.4. Daaruit volgt dat de persoon die wordt geschaad door de inbeslagneming van gegevens die in een niet in beslag genomen informaticasysteem wordt verricht, over dezelfde rechtsmiddelen en waarborgen beschikt als een persoon die door een wetgevingsconforme verrichte huiszoeking of fouillering wordt geraakt.

B.9.5. Uit het voorgaande vloeit voort dat aan de zoeking in een informaticasysteem dat niet in beslag is genomen maar dat in beslag zou kunnen worden genomen, voldoende jurisdictionele waarborgen zijn verbonden die het mogelijk maken te verzekeren dat de door die onderzoekshandeling veroorzaakte inmenging in het recht op eerbiediging van het privéleven is verantwoord ten aanzien van de vereisten van artikel 22 van de Grondwet en van artikel 8 van het Europees Verdrag voor de rechten van de mens.

B.9.6. Het onderzoek ten aanzien van de artikelen 10 en 11 van de Grondwet leidt niet tot een andere conclusie wat betreft de zoekingen in een informaticasysteem dat niet in beslag is genomen maar dat in beslag zou kunnen worden genomen. Het eerste middel, in zijn eerste en vierde onderdeel, is niet gegrond, in zoverre daarbij de zoekingen in een informaticasysteem dat regelmatig in beslag kan worden genomen, worden beoogd.

Wat betreft het verschil in behandeling tussen de zoeking in een in beslag genomen informaticasysteem en de zoeking in een informaticasysteem dat in beslag kan worden genomen

B.10.1. Aangezien de mogelijkheid voor de officier van gerechtelijke politie om zelf te beslissen tot het uitvoeren van een zoeking in een in beslag genomen informaticasysteem is verantwoord om de in B.8.1 en volgende uiteengezette redenen, is het verschil in behandeling dat het gevolg is van het feit dat de door de procureur des Konings overwogen zoeking, in een informaticasysteem dat niet in beslag is genomen maar dat in beslag zou kunnen worden genomen, enkel door hem kan worden beslist, om dezelfde redenen verantwoord.

B.10.2. Het eerste middel, in zijn tweede onderdeel, is niet gegrond.

Wat de uitbreiding van de zoeking betreft

B.11.1. Artikel 39*bis*, § 3, van het Wetboek van strafvordering, ingevoerd bij de bestreden bepaling, biedt de procureur des Konings de mogelijkheid te beslissen om een zoeking die is aangevat in een informaticasysteem dat het voorwerp uitmaakt of kan uitmaken van een inbeslagneming, uit te breiden naar een informaticasysteem of een deel ervan dat zich op een andere plaats bevindt dan daar waar de zoeking plaatsvindt en dat door een verbinding kan worden bereikt. Indien de toegang tot de gegevens is beveiligd, kan echter enkel de onderzoeksrechter de opheffing van de beveiliging of het ontcijferen of het decoderen van de gegevens toestaan (paragraaf 5, tweede lid).

B.11.2. De uitbreiding van de zoeking biedt de speurders de mogelijkheid toegang te hebben niet alleen tot alle gegevens die zijn opgeslagen of bewaard op het toestel dat het vertrekpunt vormt van de zoeking, maar ook tot alle op de informaticasystemen opgeslagen documenten die door verbinding via dat toestel worden bereikt, alsook tot alle communicatie die door de gebruiker ervan met derden wordt gevoerd, met inbegrip van de nieuwe ontvangen of onderweg zijnde berichten waarvan de gebruiker nog geen kennis heeft genomen.

B.12.1. Vóór de inwerkingtreding van de bestreden bepaling bevond de bepaling met betrekking tot de zoekingen op netwerken, ingevoegd bij artikel 3 van de wet van 28 november 2000 inzake informaticacriminaliteit, zich in artikel 88*ter* van het Wetboek van strafvordering. Dat artikel is opgeheven bij artikel 13 van de bestreden wet.

B.12.2. In de memorie van toelichting bij de wet van 28 november 2000 wordt, in verband met dat artikel 88*ter*, vermeld :

« Een beperking bij een traditionele dwangmaatregel zoals de huiszoeking is dat ze, per definitie, enkel mag worden uitgevoerd ten aanzien van de plaats waarvoor ze wordt bevolen. Kenmerkend voor informaticasystemen - of het nu gaat om grote systemen binnen bedrijven of om handige draagbare computers - is dat ze meer en meer verbonden zijn in netwerken.

Wanneer de informaticasystemen waarin onderzoek noodzakelijk blijkt te zijn, zich op verschillende locaties bevinden, zijn derhalve in de bestaande context meerdere bevelen tot huiszoeking of inbeslagneming vereist. Het is duidelijk dat een dergelijke benadering problematisch is : niet alleen bestaat het risico dat bij niet gelijktijdig optreden bewijsmateriaal verloren gaat, maar bovendien zal in veel gevallen niet *a priori* vastgesteld kunnen worden op welke plaatsen de zoeking moet plaatsvinden, welke bestanden relevant zijn, of zelfs waar de computers geografisch gesitueerd zijn.

Om hieraan te verhelpen bepaalt het nieuwe artikel de voorwaarden waarin de uitbreiding van de zoeking in een informaticasysteem naar elders gesitueerde systemen toegelaten is. Hierbij moet het gaan om onderling verbonden systemen.

De maatregel moet vooreerst noodzakelijk zijn voor de waarheidsvinding, en bovendien moet, hetzij een risico bestaan dat de bewijsgaring in het gedrang komt, hetzij het nemen van andere maatregelen (bijvoorbeeld meerdere huiszoekingsbevelen) disproportioneel zijn. Het komt aan de onderzoeksrechter toe om dit in redelijkheid te beoordelen. Omwille van het uitzonderlijke karakter van de uitbreiding van de zoeking in een informaticasysteem, meer bepaald het mogelijke extraterritoriale effect ervan, mag een dergelijke zoeking enkel uitgebreid worden inzoverre dit noodzakelijk is in het kader van de concrete strafzaak waarmee de onderzoeksrechter is gelast » (*Parl. St.*, Kamer, 1999-2000, DOC 50-0213/001 en DOC 50-0214/001, pp. 22-23).

B.13.1. Sinds de inwerkingtreding van de bestreden bepaling vereist de uitbreiding van een aangevatte zoeking in een informaticasysteem naar de netwerken die ermee verbonden zijn, niet langer de saisine en de machtiging van de onderzoeksrechter. De procureur des Konings is bevoegd om die uitbreiding van de zoeking te bevelen in zoverre de toegang tot de netwerken niet is beveiligd.

B.13.2. In de memorie van toelichting bij de bestreden wet wordt in dat verband vermeld :

« De uitbreiding van de zoeking in een informaticasysteem kan voortaan worden bevolen door de procureur des Konings of de arbeidsauditeur.

Deze uitbreiding beoogt bijvoorbeeld de situaties waarin een smartphone in beslag genomen werd en waarin het noodzakelijk blijkt om toegang te krijgen tot de Hotmail-, Facebook- of Dropbox-account waarmee deze smartphone is verbonden. Zoals eerder aangehaald, staat het huidige recht slechts toe aan de instantie die de inbeslagneming van het toestel bevolen heeft om een zoeking uit te voeren in het toestel zelf, dus niet ten aanzien van de gegevens waarmee het apparaat is verbonden in - bijvoorbeeld - de cloud.

Ofschoon de tussenkomst van de onderzoeksrechter een essentiële waarborg inhoudt bij het inbreken op de privacy, is de wetwijziging verantwoord omdat artikel 39*bis* zich beperkt tot de niet-heimelijke zoekingen. Artikel 39*bis* wordt zoals gezegd reactief gebruikt naar aanleiding van het feit dat op een wettige wijze de hand kon worden gelegd op een informaticasysteem. De privacy van personen wordt op geen enkele wijze heimelijk benaderd of geëxploiteerd. In die omstandigheden is de controle van de parketmagistraat een voldoende waarborg.

Het heimelijk inbreken op een informaticasysteem en het onder bewaking stellen ervan blijft daarentegen onderworpen aan de tussenkomst van de onderzoeksrechter, thans overeenkomstig artikel 90*ter* e.v. of artikel 89*ter* van het Wetboek van Strafvordering.

Daarnaast is de overdracht van deze maatregel (namelijk de uitbreiding van de zoeking) van artikel 88*ter* naar artikel 39*bis*, en dus van de onderzoeksrechter naar de procureur des Konings, gerechtvaardigd door het feit dat, wegens de ontwikkeling van nieuwe technologieën, het onderscheid tussen hetgeen zich op het toestel bevindt en hetgeen zich in de cloud bevindt voor een deel artificieel wordt.

Evenwel moet deze wijziging samengelezen worden met de nieuwe paragraaf 5 die het gebruik betreft van ' valse sleutels ' en dergelijke om toegang te krijgen tot de gegevens. De laatste alinea van paragraaf 5 voorziet dat enkel de onderzoeksrechter het gebruik van ' valse sleutels ' kan bevelen, in het kader van de specifieke toepassing van § 3 » (*Parl. St.*, Kamer, 2015-2016, DOC 54-1966/001, pp. 18-19).

B.14.1. Rekening houdend met de aanzienlijke ontwikkeling van de netwerken die toegankelijk zijn vanaf informaticasystemen en met het intensieve gebruik ervan door de overgrote meerderheid van de burgers, zowel om er documenten en gegevens op te slaan die tot hun privéleven behoren, met inbegrip van heel persoonlijke zaken, als om met elkaar te communiceren, kan thans ervan worden uitgegaan dat een onderzoeksmaatregel die het mogelijk maakt toegang te hebben tot alle gegevens en communicatie die zich op de netwerken bevinden die verbonden zijn met een informaticasysteem dat aan een individu toebehoort, een inmenging vormt in zijn recht op eerbiediging van het privéleven die op zijn minst vergelijkbaar is met de inmengingen die worden veroorzaakt, enerzijds, door een huiszoeking in een woonplaats of een private plaats en, anderzijds, door het onderscheppen van zijn telefoongesprekken of zijn briefwisseling.

B.14.2. Krachtens de artikelen 87 en 88 van het Wetboek van strafvordering behoren de huiszoekingen tot de bevoegdheid van de onderzoeksrechter. Krachtens artikel 88*sexies* van hetzelfde Wetboek kan, buiten het geval van ontdekking op heterdaad, alleen de onderzoeksrechter kennisnemen van de inhoud van aan een postoperator toevertrouwde, onderschepte en door de procureur des Konings met toepassing van artikel 46*ter* van hetzelfde Wetboek in beslag genomen post. Krachtens artikel 90*ter* van hetzelfde Wetboek is de onderzoeksrechter bevoegd om « niet voor het publiek toegankelijke communicatie of gegevens van een informaticasysteem of een deel ervan met technische hulpmiddelen [te] onderscheppen, er kennis van [te] nemen, [te] doorzoeken en [op te nemen] of de zoeking in een informaticasysteem of een deel ervan [uit te breiden] ».

B.14.3. Zoals de Raad van State heeft opgemerkt in het advies dat hij heeft uitgebracht over de bestreden bepaling, « [is] de onderzoeksrechter een onafhankelijk magistraat [...] die een objectief onderzoek voert, zowel *à charge* als *à décharge*, terwijl het openbaar ministerie partij in het strafproces is » (*Parl. St.*, Kamer, 2015-2016, DOC 54-1966/001, p. 127).

B.14.4. Opsporingshandelingen mogen in beginsel geen schending van individuele rechten en vrijheden inhouden, zodat de onderzoeksmaatregelen uitgevoerd tijdens het strafrechtelijk onderzoek die dergelijke aantastingen inhouden, enkel in het kader van een gerechtelijk onderzoek kunnen worden uitgevoerd. Op zijn minst mogen de handelingen beoogd in artikel 28*septies* van het Wetboek van strafvordering, waarin het zogeheten « mini-onderzoek » wordt geregeld, enkel worden uitgevoerd met de toestemming en onder de controle van een onderzoeksrechter, zelfs indien voor de zaak geen gerechtelijk onderzoek wordt ingesteld.

B.14.5. Het opsporingsonderzoek wordt gekenmerkt door zijn uitgesproken geheim en niet-contradictoir karakter, waarbij de belanghebbenden over minder waarborgen ter bescherming van hun rechten van verdediging beschikken dan tijdens het gerechtelijk onderzoek.

Weliswaar hebben de rechtstreeks belanghebbenden reeds tijdens het opsporingsonderzoek het recht om toegang tot het strafdossier te vragen (artikel 21*bis* van het Wetboek van strafvordering). Anders dan voor het gerechtelijk onderzoek (artikel 61*ter* van het Wetboek van strafvordering) is dat recht op toegang tot het dossier voor het opsporingsonderzoek evenwel niet procedureel geregeld, zodat het openbaar ministerie - bij gebrek aan wettelijk bepaalde weigeringsgronden - het verzoek om toegang tot een dossier zonder meer kan weigeren en er geen rechtsmiddel tegen een weigeringsbeslissing of de ontstentenis van beslissing voorhanden is. Bij zijn arrest nr. 6/2017 van 25 januari 2017 heeft het Hof geoordeeld dat die ontstentenis van een rechtsmiddel tegen de weigering of de ontstentenis van een beslissing door het openbaar ministerie ten aanzien van een door een verdachte geformuleerd verzoek om toegang tot een dossier in het opsporingsonderzoek de artikelen 10 en 11 van de Grondwet schendt. Aangezien die ongrondwettigheid is uitgedrukt in voldoende precieze en volledige bewoordingen die toelaten artikel 21*bis* van het Wetboek van strafvordering toe te passen met inachtneming van de referentienormen op grond waarvan het Hof zijn toetsingsbevoegdheid uitoefent, heeft het Hof ook geoordeeld dat het, in afwachting van het optreden van de wetgever, aan de rechter toekomt een einde te maken aan de schending van die normen, door artikel 61*ter* van het Wetboek van strafvordering bij analogie toe te passen.

Voorts beschikken de belanghebbenden tijdens het opsporingsonderzoek niet over een formeel recht om een bepaalde opsporingshandeling te vragen, terwijl een recht om bijkomende onderzoekshandelingen te vragen wel aan de inverdenkinggestelde en de burgerlijke partij wordt toegekend tijdens het gerechtelijk onderzoek (artikel 61*quinquies* van het Wetboek van strafvordering). De belanghebbenden kunnen weliswaar steeds een informeel verzoek aan het openbaar ministerie richten, doch het openbaar ministerie is geenszins verplicht op dat verzoek in te gaan en de partijen beschikken niet over enig rechtsmiddel tegen een weigeringsbeslissing of de ontstentenis van beslissing.

Tot slot is er tijdens het opsporingsonderzoek geen ambtshalve toezicht op de regelmatigheid van de procedure door een onafhankelijke en onpartijdige rechter, die het dossier van eventuele nietigheden kan zuiveren, terwijl een dergelijk toezicht wel voorhanden is tijdens het gerechtelijk onderzoek (artikel 235*bis* van het Wetboek van strafvordering).

B.14.6. Uit het voorgaande volgt dat in zoverre de bestreden bepaling het mogelijk maakt dat de uitbreiding van de zoeking die is aangevat in een toestel dat in beslag is genomen of dat in beslag zou kunnen worden genomen, naar een informaticasysteem dat zich op een andere plaats bevindt dan het toestel zelf en waarmee het toestel is verbonden, door de procureur des Konings wordt bevolen zonder het optreden van een onderzoeksrechter, aan die onderzoeksmaatregel, voor de rechtzoekende van wie het informaticasysteem het voorwerp uitmaakt van de onderzoeksmaatregel, minder waarborgen verbonden zijn dan aan de huiszoeking, de opening van de briefwisseling, het onderscheppen en het afluisteren van telefonische en elektronische communicaties en de geheime zoeking in een informaticasysteem.

B.15.1. Dat verschil in behandeling is door de wetgever verantwoord door het niet-geheime karakter van het onderzoek :

« Ofschoon de tussenkomst van de onderzoeksrechter een essentiële waarborg inhoudt bij het inbreken op de privacy, is de wetwijziging verantwoord omdat artikel 39*bis* zich beperkt tot de niet-heimelijke zoekingen. Artikel 39*bis* wordt zoals gezegd reactief gebruikt naar aanleiding van het feit dat op een wettige wijze de hand kon worden gelegd op een informaticasysteem. De privacy van personen wordt op geen enkele wijze heimelijk benaderd of geëxploiteerd. In die omstandigheden is de controle van de parketmagistraat een voldoende waarborg.

Het heimelijk inbreken op een informaticasysteem en het onder bewaking stellen ervan blijft daarentegen onderworpen aan de tussenkomst van de onderzoeksrechter, thans overeenkomstig artikel 90*ter* e.v. of artikel 89*ter* van het Wetboek van Strafvordering.

Daarnaast is de overdracht van deze maatregel (namelijk de uitbreiding van de zoeking) van artikel 88*ter* naar artikel 39*bis*, en dus van de onderzoeksrechter naar de procureur des Konings, gerechtvaardigd door het feit dat, wegens de ontwikkeling van nieuwe technologieën, het onderscheid tussen hetgeen zich op het toestel bevindt en hetgeen zich in de cloud bevindt voor een deel artificieel wordt » (*Parl. St.*, Kamer, 2015-2016, DOC 54-1966/001, p. 19).

B.15.2. Het in B.14.6 uiteengezette verschil in behandeling berust derhalve op het criterium van het al dan niet geheime karakter van de zoeking in de netwerken waarmee het toestel dat in beslag is genomen of dat in beslag zou kunnen worden genomen, verbonden is.

Het niet-geheime karakter van de inmenging in het recht op eerbiediging van het privéleven van de persoon die door de maatregel wordt geraakt, wordt gewaarborgd door de verplichting die krachtens paragraaf 7 van de bestreden bepaling aan de procureur des Konings wordt opgelegd om de verantwoordelijke van het informaticasysteem dat het voorwerp uitmaakt van het onderzoek, « zo spoedig mogelijk » op de hoogte te brengen.

Nu de verplichting om de verantwoordelijke van het informaticasysteem op de hoogte te brengen van de zoeking gehanteerd wordt om het onderscheid te maken tussen een geheim en een niet-geheim onderzoek, en zulks strookt met de bescherming van de rechtsonderhorigen, dient ervan te worden uitgegaan dat de kennisgeving aan de verantwoordelijke van het informaticaysteem ook de verdachte betreft wiens daarin opgeslagen gegevens het voorwerp uitmaken van die zoeking, wanneer die verdachte zelf niet de effectieve controle heeft over het desbetreffende informaticasysteem.

B.15.3. De omstandigheid dat de inmenging in het recht op eerbiediging van het privéleven van een persoon buiten zijn medeweten gebeurt, verhoogt de ernst ervan, hetgeen impliceert dat de hoogste waarborgen eraan dienen te worden verbonden en dat zij bijgevolg enkel kan gebeuren tijdens een strafrechtelijk onderzoek (EHRM, 4 december 2015, *Zakharov t. Rusland*, §§ 233, 249 en 259; 12 januari 2016, *Szabó en Vissy t. Hongarije*, § 77; 30 mei 2017, *Trabajo Rueda t. Spanje*, § 33). De omstandigheid dat dezelfde onderzoeksmaatregel ter kennis van de betrokken persoon wordt gebracht, in voorkomend geval nadat hij is beëindigd, houdt echter ook een aanzienlijke inmenging in het recht op eerbiediging van het privéleven van die persoon in. Het feit dat hij ervan op de hoogte is gebracht, betekent immers niet dat hij ermee heeft ingestemd.

B.15.4. Het voorafgaand optreden van een onafhankelijke en onpartijdige rechter maakt het mogelijk te waarborgen dat de inmenging in het recht op eerbiediging van het privéleven evenredig is met de vereisten van artikel 22 van de Grondwet en van artikel 8 van het Europees Verdrag voor de rechten van de mens.

Zo heeft het Hof, bij zijn arrest nr. 202/2004 van 21 december 2004, geoordeeld dat de methode van de observatie met gebruik van technische hulpmiddelen om zicht te verwerven in een woning en die van de inkijkoperatie in een private plaats, maatregelen zijn die, wat betreft de ernst van de inmenging in het recht op eerbiediging van het privéleven, kunnen worden vergeleken met de huiszoeking en met het afluisteren en opnemen van privécommunicatie en -telecommunicatie, en enkel onder dezelfde voorwaarden kunnen worden toegestaan, dat wil zeggen in het kader van het gerechtelijk onderzoek.

Bij zijn arrest nr. 178/2015 van 17 december 2015 heeft het Hof, in verband met de uitbreiding van de zoeking in een informaticasysteem, geoordeeld :

« De uitbreiding van de zoeking in een informaticasysteem is onderworpen aan de voorafgaande machtiging van de strafuitvoeringsrechter, die moet nagaan of voldaan is aan de vereisten inzake wettigheid, proportionaliteit en subsidiariteit en die in het bijzonder erover dient te waken dat niet op onevenredige wijze afbreuk wordt gedaan aan de fundamentele rechten van de betrokkenen.

Om een daadwerkelijke rechterlijke controle te waarborgen, moet de magistraat [die het strafrechtelijk uitvoeringsonderzoek voert], wanneer hij een machtiging vraagt aan de strafuitvoeringsrechter, ook de reikwijdte van de uitbreiding van de zoeking in een informaticasysteem aangeven, zodat wordt verhinderd dat de aantasting van het privéleven potentieel onbeperkt en bijgevolg onevenredig is (EHRM, 9 december 2004, *Van Rossem t. België*, § 45) en zodat een controle daarop door de strafuitvoeringsrechter mogelijk is. Een andere interpretatie van de bestreden bepalingen zou niet verzoenbaar zijn met het recht op eerbiediging van het privéleven en de woning » (B.48.4).

Bij zijn arrest nr. 148/2017 van 21 december 2017 heeft het Hof, in verband met de huiszoeking in een woonplaats, die overigens niet noodzakelijk een geheim karakter heeft, geoordeeld :

« Vanwege de ernst van de erdoor teweeggebrachte inmenging in het recht op eerbiediging van het privéleven en de onschendbaarheid van de woning, kan de huiszoeking, in de huidige stand van de regelgeving inzake de strafrechtspleging, enkel worden toegelaten in het kader van een gerechtelijk onderzoek, waarbij de belanghebbenden beschikken over een georganiseerd recht om toegang tot het dossier en bijkomende onderzoekshandelingen te vragen en waarbij is voorzien in een toezicht door de kamer van inbeschuldigingstelling op de regelmatigheid van de procedure.

Door de huiszoeking, in de huidige stand van de regelgeving inzake de strafrechtspleging, onder het toepassingsgebied van het mini-onderzoek te brengen, zonder te voorzien in bijkomende waarborgen ter bescherming van de rechten van verdediging, doet de bestreden bepaling op discriminerende wijze afbreuk aan het recht op eerbiediging van het privéleven en aan het recht op de onschendbaarheid van de woning » (B.22.4).

B.15.5. Uit het voorgaande vloeit voort dat het verschil in behandeling tussen de personen die het voorwerp uitmaken van een maatregel van onderzoek met betrekking tot de netwerken die met hun informaticasysteem verbonden zijn, naargelang de zoeking al dan niet als geheim wordt beschouwd, in de zin van de bestreden bepaling, niet op een criterium berust dat relevant is ten aanzien van het principe volgens hetwelk de tijdens het strafonderzoek uitgevoerde onderzoeksmaatregelen die een schending inhouden van individuele rechten en vrijheden, in beginsel slechts kunnen worden verricht in het kader van een gerechtelijk onderzoek (artikel 28*bis*, § 3, eerste lid, van het Wetboek van strafvordering).

B.16.1. Daarenboven verantwoordt de omstandigheid dat indien de toegang tot de netwerken die verbonden zijn met het informaticasysteem wordt beveiligd met een sleutel of indien de gegevens op de netwerken of op een verbonden informaticasysteem gecodeerd of versleuteld zijn, de procureur des Konings enkel gebruik kan maken van valse sleutels of van technieken om te decoderen of te ontcijferen met de toestemming van de onderzoeksrechter, evenmin dat aan de inmenging in het recht op eerbiediging van het privéleven, die in dat geval niet minder is, niet dezelfde waarborgen verbonden zijn wanneer een dergelijke beveiliging niet is aangebracht.

B.16.2. Bovendien gaat in de bestreden bepaling de overdracht van de bevoegdheid van de onderzoeksrechter naar de procureur des Konings niet gepaard met extra waarborgen die bedoeld zijn om het privéleven en de rechten van de verdediging van de betrokken persoon daadwerkelijk te beschermen en die van dien aard zijn de afschaffing van het voorafgaand optreden van een onafhankelijke en onpartijdige rechter te compenseren (EHRM, 30 september 2014, *Prezhdarovi t. Bulgarije*, §§ 45 tot 47; 30 mei 2017, *Trabajo Rueda t. Spanje*, § 37). Dienaangaande blijkt uit de rechtspraak van het Europees Hof voor de Rechten van de Mens dat het bestaan van een daadwerkelijk rechtsmiddel afhangt van het adequate karakter ervan; daardoor moet het rechtsmiddel in kwestie samenhangen met de aangevoerde schending teneinde gepaste en gelijkwaardige waarborgen te verschaffen waardoor de in het geding zijnde rechten van het individu worden gevrijwaard. Daaruit volgt dat de nationale beroepsinstantie ertoe moet zijn gemachtigd ten gronde kennis te nemen van de op het Verdrag gebaseerde grief om te beslissen of de inmenging in de uitoefening van het recht van de betrokkene op de eerbiediging van zijn privéleven in overeenstemming was met artikel 8, lid 2 (EHRM, 1 april 2008, *Varga t. Roemenië*, §§ 72-73; 3 juli 2012, *Robathin t. Oostenrijk*, § 21; 30 september 2014, *Prezhdarovi t. Bulgarije*, § 47; 2 april 2015, *Vinci Construction en GTM Génie Civil et Services t. Frankrijk*, §§ 66-67).

B.16.3. Artikel 28*sexies* van het Wetboek van strafvordering is weliswaar van toepassing op het kopiëren, ontoegankelijk maken en verwijderen van in een informaticasysteem of een deel ervan opgeslagen gegevens. Die bepaling biedt eenieder die geschaad wordt door een opsporingshandeling met betrekking tot zijn goederen, de mogelijkheid de opheffing ervan te vragen aan de procureur des Konings, tegen wiens beslissing beroep kan worden ingesteld bij de kamer van inbeschuldigingstelling. Die procedure, die ook van toepassing is bij de onderzoeksrechter (artikel 61*quater*, § 1, van het Wetboek van strafvordering), is dus beperkt tot de mogelijkheid voor de betrokken persoon om de opheffing van de inbeslagneming, en bijgevolg de teruggave, te verkrijgen van het informaticamateriaal en van de gegevens die zijn verkregen door middel van een zoeking in een informaticasysteem. Zij belet echter niet de inmenging in het privéleven die heeft plaatsgehad en die niet wordt verholpen door de teruggave van het toestel en van de gegevens die erin zijn opgeslagen, hetgeen niet voldoet aan de in B.16.2 uitgedrukte vereisten van de rechtspraak van het Europees Hof voor de Rechten van de Mens.

B.16.4. Vanwege de ernst van de erdoor teweeggebrachte inmenging in het recht op eerbiediging van het privéleven, kan de maatregel die erin bestaat een zoeking in een informaticasysteem of een deel ervan die is aangevat in een informaticasysteem dat in beslag is genomen of dat door de procureur des Konings in beslag kan worden genomen, uit te breiden naar een informaticasysteem of een deel ervan dat zich op een andere plaats bevindt dan daar waar de zoeking wordt verricht, enkel worden toegelaten onder dezelfde voorwaarden als diegene die gelden in verband met de onderzoekshandelingen bedoeld in B.14.2.

B.17.1. Het eerste middel, in zijn eerste en vierde onderdeel, is in die mate gegrond.

Paragraaf 3 van artikel 39*bis* van het Wetboek van strafvordering, ingevoegd bij artikel 2 van de bestreden wet van 25 december 2016, dient te worden vernietigd. Om te vermijden dat een juridisch vacuüm ontstaat wat betreft de betrokken maatregel van zoeking, dient ook artikel 13 van de wet van 25 december 2016, dat onlosmakelijk verbonden is met de bestreden bepaling, te worden vernietigd in zoverre daarbij artikel 88*ter* van het Wetboek van strafvordering wordt opgeheven.

B.17.2. Teneinde de rechtsonzekerheid te vermijden die zou ontstaan in verband met de rechtsgeldigheid van de maatregelen van uitbreiding van zoekingen in informaticasystemen die worden verricht overeenkomstig de vernietigde bepaling, dienen de door die bepaling teweeggebrachte gevolgen te worden gehandhaafd tot de datum waarop dit arrest in het *Belgisch Staatsblad* wordt bekendgemaakt.

Wat het op de hoogte brengen van de verantwoordelijke van het informaticasysteem betreft

B.18.1. Het derde onderdeel van het eerste middel is afgeleid uit de schending van de artikelen 12 en 14 van de Grondwet, in samenhang gelezen met artikel 7 van het Europees Verdrag voor de rechten van de mens. Het beoogt het begrip « verantwoordelijke van het informaticasysteem », dat is opgenomen in paragraaf 7 van artikel 39*bis* van het Wetboek van strafvordering, ingevoerd bij artikel 2 van de bestreden wet van 25 december 2016. De verzoekende partijen verwijten de wetgever dat hij de inhoud van dat begrip niet heeft gepreciseerd, zodat de identiteit van de personen die van de zoeking of van de uitbreiding ervan op de hoogte moeten worden gebracht, vaag en onbepaald is.

B.18.2. In tegenstelling tot hetgeen de Ministerraad betoogt, leidt de omstandigheid dat in de wetgeving die voorafgaat aan de bestreden wet reeds werd verwezen naar de « verantwoordelijke van het informaticasysteem » niet tot de niet-ontvankelijkheid, wegens het niet-tijdig indienen van het beroep, van het derde onderdeel van het middel. Met de bestreden bepaling is de wetgever in die aangelegenheid immers opnieuw wetgevend opgetreden en heeft hij de aan de procureur des Konings en de onderzoeksrechter opgelegde verplichting om de « verantwoordelijke van het informaticasysteem » op de hoogte te brengen, bevestigd.

B.19.1. Artikel 12, tweede lid, van de Grondwet bepaalt :

« Niemand kan worden vervolgd dan in de gevallen die de wet bepaalt en in de vorm die zij voorschrijft ».

Artikel 14 van de Grondwet bepaalt :

« Geen straf kan worden ingevoerd of toegepast dan krachtens de wet ».

Artikel 7, lid 1, van het Europees Verdrag voor de rechten van de mens bepaalt :

« Niemand kan worden veroordeeld wegens een handelen of nalaten, dat geen strafbaar feit naar nationaal of internationaal recht uitmaakte ten tijde dat het handelen of nalaten geschiedde. Evenmin zal een zwaardere straf worden opgelegd dan die welke ten tijde van het begaan van het strafbare feit van toepassing was ».

B.19.2. In zoverre het het wettigheidsbeginsel in strafzaken waarborgt, heeft artikel 7, lid 1, van het Europees Verdrag voor de rechten van de mens een draagwijdte die analoog is aan de artikelen 12, tweede lid, en 14 van de Grondwet.

B.19.3. Uit die bepalingen vloeit voort dat de strafwet moet worden geformuleerd in bewoordingen op grond waarvan eenieder, op het ogenblik waarop hij een gedrag aanneemt, kan uitmaken of dat gedrag al dan niet strafbaar is en de mogelijkerwijs op te lopen straf kan kennen. De beginselen van wettigheid en voorspelbaarheid zijn van toepassing op de hele strafrechtspleging. De voormelde bepalingen willen aldus elk risico van willekeurig optreden vanwege de uitvoerende of de rechterlijke macht uitsluiten bij het vaststellen en toepassen van de straffen.

Het wettigheidsbeginsel in strafzaken gaat niet zover dat het de wetgever ertoe verplicht elk aspect van de strafbaarstelling, van de straf of van de strafrechtspleging zelf te regelen. Meer bepaald staat het niet eraan in de weg dat de wetgever aan de rechter of aan het openbaar ministerie een beoordelingsbevoegdheid toekent. Er dient immers rekening te worden gehouden met het algemene karakter van de wettelijke bepalingen, de uiteenlopende situaties waarop zij van toepassing zijn en de evolutie van de gedragingen die zij bestraffen.

B.19.4. Te dezen is niet de wettigheid van de strafbaarstelling of van de straf in het geding, maar die van de strafrechtspleging.

Een delegatie aan de uitvoerende macht is niet in strijd met dat beginsel voor zover de machtiging voldoende nauwkeurig is omschreven en betrekking heeft op de tenuitvoerlegging van maatregelen waarvan de essentiële elementen voorafgaandelijk door de wetgever zijn vastgesteld.

De vereiste van voorspelbaarheid van de strafrechtspleging waarborgt elke rechtsonderhorige dat tegen hem enkel een opsporingsonderzoek, een gerechtelijk onderzoek en een vervolging kunnen worden ingesteld volgens een procedure waarvan hij vóór de aanwending ervan kennis kan nemen.

B.20. Aangezien de bestreden bepaling de verplichting oplegt de « verantwoordelijke van het informaticasysteem » van de zoeking op de hoogte te brengen, is het aan die persoon dat zij de mogelijkheid biedt de nodige maatregelen te nemen voor het vrijwaren van zijn rechten, zodat dat begrip een essentieel element is van de strafrechtspleging inzake zoekingen in informaticasystemen.

B.21.1. In dat verband heeft de afdeling wetgeving van de Raad van State opgemerkt :

« Die bepaling geeft echter niet aan wat onder ' de verantwoordelijke van het informaticasysteem ' moet worden verstaan.

In de zin van de voormelde Aanbeveling nr. R(95)13 [van het Comité van de ministers van de Raad van Europa van 11 september 1995] geldt het begrip ' persoon die voor een computersysteem verantwoordelijk is ' voor alle personen die bij een opsporingsactie of een inbeslagneming formeel of werkelijk controle blijken uit te oefenen op het computersysteem waarop de opsporing betrekking heeft. Het kan gaan om de eigenaar van het systeem, om een operateur van dat systeem of zelfs om de bewaker (huurder of bewoner) van de lokalen waarin het computersysteem zich bevindt.

In de ontworpen bepaling dient bijgevolg uitdrukkelijk te worden bepaald welke personen moeten worden ingelicht.

Overigens kan de inbeslagneming van gegevens ook van belang zijn voor derden. Zo worden de Lid-Staten in de voormelde Aanbeveling nr. R(95)13 verzocht dit verstrekken van inlichtingen te regelen met oog voor de noden van het onderzoek.

Dat vereiste is van belang, aangezien eenieder die zich door een opsporingshandeling of een onderzoekshandeling met betrekking tot zijn goederen geschaad acht, krachtens de artikelen 28*sexies* en 61*quater* van het Wetboek van Strafvordering aan de procureur des Konings of aan de onderzoeksrechter de opheffing ervan kan vragen » (*Parl. St.*, Kamer, 2015-2016, DOC 54-1966/001, pp. 129-130).

B.21.2. In verband met die opmerking wordt in de memorie van toelichting vermeld :

« De Raad van State meent eveneens (en verwijst in dat opzicht naar advies nr. 28 029/2 van 31 mei 1999) dat deze ' verantwoordelijke van het informaticasysteem ' in de tekst van het voorontwerp zelf moet worden omschreven. De bedoeling van het op de hoogte brengen van de maatregel is evenwel duidelijk te stellen dat het niet gaat om een geheime maatregel (vergelijk met de huiszoekingsbevoegdheid). De terminologie in het voorontwerp behoudt in dat opzicht enige flexibiliteit aangaande de te contacteren persoon : het kan inderdaad niet in alle gevallen *a priori* eenduidig vastgesteld worden wie de reële of juridische controle heeft over het systeem (*Parl. St.*, Kamer, 1999-2000, nr. 0213/001, p. 21) » (*Parl. St.*, Kamer, 2015-2016, DOC 54-1966/001, p. 24).

B.22.1. Naast de vaststelling van het al dan niet geheime karakter van de onderzoeksmaatregel heeft de mededeling van de uitvoering van die maatregel ook tot gevolg de betrokken persoon of personen de mogelijkheid te bieden de procedurele rechten uit te oefenen die met name ten doel hebben de evenredigheid te controleren van de teweeggebrachte inmenging in het recht op eerbiediging van het privéleven van die persoon of personen.

B.22.2. Daaruit vloeit voort dat het begrip « verantwoordelijke van het informaticasysteem » in die zin moet worden begrepen dat het de persoon of de personen aanwijst die verantwoordelijk zijn voor de gegevens of de communicatie die zijn opgeslagen op het toestel dat in beslag is of kan worden genomen en voor de gegevens of de communicatie waarvan kennis kan worden genomen via de netwerken die worden beoogd door de uitbreiding van de in het voormelde toestel aangevatte zoeking, waarbij die persoon of die personen niet noodzakelijk de eigenaar of de houder van de betrokken toestellen zijn. Zoals is vermeld in B.15.2, is ook de verdachte bedoeld wiens gegevens het voorwerp uitmaken van de zoeking wanneer hij zelf niet de effectieve controle heeft over het desbetreffende informaticasysteem.

B.23. Onder voorbehoud dat het begrip « verantwoordelijke van het informaticasysteem » wordt geïnterpreteerd zoals in B.15.2 en B.22.2 is vermeld, is het eerste middel, in zijn derde onderdeel, niet gegrond.

Wat de informaticasystemen van de advocaten en de artsen betreft

B.24.1. Het vijfde onderdeel van het eerste middel is afgeleid uit de schending van de artikelen 10, 11 en 22 van de Grondwet, in samenhang gelezen met artikel 6 van het Europees Verdrag voor de rechten van de mens. De verzoekende partijen verwijten de wetgever dat hij, in artikel 39*bis* van het Wetboek van strafvordering, waarbij de niet-geheime zoekingen in een informaticasysteem worden geregeld, niet heeft voorzien in waarborgen die gelijkwaardig zijn met die welke zijn opgenomen in artikel 90*octies* van hetzelfde Wetboek en die de geheime zoekingen in een informaticasysteem betreffen.

B.24.2. Artikel 90*octies* van het Wetboek van strafvordering bepaalt :

« § 1. De maatregel kan alleen betrekking hebben op de lokalen aangewend voor beroepsdoeleinden, de woonplaats, de communicatiemiddelen of de informaticasystemen van een advocaat of een arts, indien deze er zelf van verdacht worden een van de strafbare feiten bedoeld in artikel 90*ter* te hebben gepleegd of eraan deelgenomen te hebben, of, indien precieze feiten doen vermoeden dat derden die ervan verdacht worden een van de strafbare feiten bedoeld in artikel 90*ter* te hebben gepleegd, gebruik maken van diens lokalen, woonplaats, communicatiemiddelen of informaticasystemen.

§ 2. De maatregel mag niet ten uitvoer worden gelegd zonder dat, naar gelang van het geval, de stafhouder of de vertegenwoordiger van de provinciale orde van geneesheren ervan op de hoogte werd gebracht.

Deze personen zijn tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.

§ 3. De onderzoeksrechter beoordeelt, na overleg met de stafhouder of de vertegenwoordiger van de provinciale orde van geneesheren, welke gedeelten van de in artikel 90*sexies*, § 3, bedoelde niet voor publiek toegankelijke communicatie of gegevens van een informaticasysteem, die hij van belang acht voor het onderzoek, onder het beroepsgeheim vallen en welke niet.

Enkel de gedeelten van de communicatie of gegevens bedoeld in het eerste lid die worden geacht niet onder het beroepsgeheim te vallen, worden overgeschreven of weergegeven en worden desgevallend vertaald. De onderzoeksrechter laat hiervan proces-verbaal opmaken. De bestanden bevattende deze communicatie of gegevens worden onder verzegelde omslag neergelegd ter griffie.

Alle overige communicatie of gegevens worden in een ander bestand onder afzonderlijke verzegelde omslag neergelegd ter griffie ».

B.24.3. Die bepaling is in het Wetboek van strafvordering ingevoerd bij artikel 22 van de bestreden wet. In verband daarmee wordt in de memorie van toelichting vermeld :

« De uitzondering voor advocaten en artsen werd ingegeven door de overweging dat deze beroepscategorieën bij uitstek het gevaar lopen om te worden geconfronteerd met verdachten, waarmee zij door hun beroepssituatie in een vertrouwelijke relatie verkeren die in het bijzonder beschermd moet worden. Dit is de klassieke beschermingsclausule zoals die ook voorkomt in gelijkaardige onderzoeksmaatregelen, zoals het inkijken van post (art. 88*sexies* van het Wetboek van strafvordering), een observatie met zicht in een woning (art. 56*bis* van het Wetboek van strafvordering) of een inkijkoperatie (art. 89*ter* van het Wetboek van strafvordering) » (*Parl. St.*, Kamer, 2015-2016, DOC 54-1966/001, pp. 72-73).

B.25. Het beroepsgeheim waartoe de advocaten en de artsen zijn gehouden, strekt niet ertoe hun enig voorrecht toe te kennen, maar heeft hoofdzakelijk tot doel het fundamentele recht op eerbiediging van het privéleven te beschermen van diegene die hen in vertrouwen neemt, soms over iets strikt persoonlijks. De vertrouwelijke informatie die wordt toevertrouwd aan een advocaat bij de uitoefening van zijn beroep en wegens die hoedanigheid, geniet bovendien ook, in bepaalde gevallen, de bescherming die voor de rechtzoekende voortvloeit uit de waarborgen die zijn neergelegd in artikel 6 van het Europees Verdrag voor de rechten van de mens, aangezien de aan de advocaat opgelegde regel van het beroepsgeheim een fundamenteel element is van de rechten van de verdediging van de rechtzoekende die hem in vertrouwen neemt.

B.26.1. Het is niet verantwoord dat enkel in de clausule van bescherming van het beroepsgeheim van de advocaten en de artsen wordt voorzien wanneer de zoeking in een informaticasysteem dat zij beroepsmatig gebruiken, in het geheim wordt uitgevoerd en niet wanneer zij hun ter kennis wordt gebracht. De inmenging in het recht op eerbiediging van het privéleven van de personen die aan hen informatie hebben toevertrouwd die door hun beroepsgeheim is gedekt, gebeurt immers op dezelfde wijze, ongeacht of de zoeking al dan niet buiten het medeweten van de betrokken advocaat of arts wordt uitgevoerd.

B.26.2. Het is, zoals de Ministerraad betoogt, juist dat wanneer de zoeking in een informaticasysteem gebeurt in het kader van een huiszoeking, de bepalingen met betrekking tot de huiszoekingen in de beroepslokalen van advocaten of artsen van toepassing zijn en het mogelijk maken het beroepsgeheim te waarborgen. De niet-geheime mogelijkheden tot zoeking waarin is voorzien bij artikel 39*bis* van het Wetboek van strafvordering gaan echter verder dan dat precieze geval en die zoekingen kunnen worden uitgevoerd buiten het geval van de huiszoeking in beroepslokalen.

B.27. Het eerste middel, in zijn vijfde onderdeel, is gegrond. Artikel 39*bis* van het Wetboek van strafvordering, ingevoerd bij artikel 2 van de bestreden wet, dient te worden vernietigd, in zoverre daarin niet in een specifieke bepaling is voorzien teneinde het beroepsgeheim van de artsen en de advocaten te beschermen.

Teneinde de rechtszekerheid met betrekking tot de zoekingen verricht in informaticasystemen die aan artsen of advocaten toebehoren, te waarborgen, moeten de gevolgen van de vernietigde bepaling worden gehandhaafd zoals in het dictum is aangegeven.

Ten aanzien van het tweede middel

Wat de bestreden bepaling betreft

B.28.1. Het tweede middel heeft betrekking op artikel 7 van de wet van 25 december 2016, waarbij in het Wetboek van strafvordering een artikel 46*sexies* wordt ingevoegd dat bepaalt :

« § 1. Bij het opsporen van de misdaden en wanbedrijven, wanneer het onderzoek zulks vereist en de overige middelen van onderzoek niet lijken te volstaan om de waarheid aan de dag te brengen, kan de procureur des Konings de politiediensten bedoeld in het tweede lid machtigen om op het internet, desgevallend onder een fictieve identiteit, contact te onderhouden met een of meerdere personen waarvan er ernstige aanwijzingen zijn dat zij strafbare feiten die een correctionele hoofdgevangenisstraf van een jaar of een zwaardere straf tot gevolg kunnen hebben, plegen of zouden plegen.

De Koning bepaalt de voorwaarden, onder meer voor wat de opleiding betreft, en de nadere regels voor de aanwijzing van de politiediensten die bevoegd zijn om de maatregel, bedoeld in dit artikel, ten uitvoer te leggen.

In uitzonderlijke omstandigheden en mits uitdrukkelijke machtiging van de procureur des Konings, kan de ambtenaar van de in het tweede lid bedoelde politiediensten bij een welbepaalde operatie kortstondig een beroep doen op de deskundigheid van een persoon die niet tot de politiediensten behoort, indien dit strikt noodzakelijk voorkomt voor het welslagen van zijn opdracht. De machtiging en de identiteit van deze persoon worden bewaard in het in paragraaf 3, zevende lid, bedoelde dossier.

Dit artikel is niet van toepassing op de persoonlijke interactie op het internet van politieambtenaren, bij de uitvoering van hun opdrachten van gerechtelijke politie, met een of meerdere personen, die enkel een gerichte verificatie of een arrestatie tot direct doel heeft, en dit zonder gebruik te maken van een geloofwaardige fictieve identiteit.

§ 2. De maatregel bedoeld in § 1 wordt door de procureur des Konings bevolen met een voorafgaandelijke en met redenen omklede schriftelijke machtiging. Deze machtiging is geldig voor een termijn van drie maanden, onverminderd hernieuwing.

In spoedeisende gevallen kan de machtiging mondeling worden verstrekt. De machtiging moet zo spoedig mogelijk worden bevestigd in de vorm bepaald in het eerste lid.

§ 3. Blijven vrij van straf de politieambtenaren die, in het kader van hun opdracht en met het oog op het welslagen ervan of ter verzekering van hun eigen veiligheid of deze van andere bij de maatregel betrokken personen, strikt noodzakelijke strafbare feiten plegen, mits uitdrukkelijk akkoord van de procureur des Konings.

Die strafbare feiten mogen niet ernstiger zijn dan die waarvoor de maatregel wordt aangewend en moeten noodzakelijkerwijze evenredig zijn met het nagestreefde doel.

Het eerste en het tweede lid zijn eveneens van toepassing op de personen die aan de uitvoering van deze opdracht noodzakelijke en rechtstreekse hulp of bijstand hebben verleend en op de personen, bedoeld in § 1, derde lid.

Blijft vrij van straf de magistraat die, met inachtneming van dit Wetboek, machtiging verleent aan een politieambtenaar en aan de persoon bedoeld in het derde lid tot het plegen van strafbare feiten in het kader van de uitvoering van de maatregel.

De politieambtenaren melden schriftelijk en vóór de uitvoering van de maatregel aan de procureur des Konings, de misdrijven die zij of de personen bedoeld in het derde lid, voornemens zijn te plegen.

Indien deze voorafgaande kennisgeving niet kon gebeuren, stellen de politieambtenaren de procureur des Konings onverwijld in kennis van de misdrijven die zij of de personen bedoeld in het derde lid, hebben gepleegd en bevestigen dit nadien schriftelijk.

De procureur des Konings vermeldt in een afzonderlijke en schriftelijke beslissing de misdrijven die door de politiediensten en de personen bedoeld in het derde lid in het kader van deze door hem bevolen maatregel kunnen worden gepleegd. Deze beslissing wordt in een afzonderlijk en vertrouwelijk dossier bewaard. Hij heeft als enige toegang tot dit dossier, onverminderd het in artikel 56*bis*, respectievelijk de artikelen 235*ter*, § 3, en 235*quater*, § 3, bedoelde inzagerecht van de onderzoeksrechter en de kamer van inbeschuldigingstelling. De inhoud van dit dossier valt onder het beroepsgeheim.

§ 4. De met het onderzoek belaste officier van gerechtelijke politie stelt proces-verbaal op van de verschillende fasen in de uitvoering van deze maatregel, met inbegrip van de relevante contacten. Deze processen-verbaal worden uiterlijk na het beëindigen van de maatregel bij het dossier gevoegd.

De contacten bedoeld in paragraaf 1 worden met de passende technische middelen geregistreerd en uiterlijk na het beëindigen van de maatregel bij het dossier gevoegd of ter griffie, al dan niet in digitale vorm, neergelegd.

§ 5. De procureur des Konings staat in voor de tenuitvoerlegging van de machtigingen tot de maatregel bedoeld in § 1, eerste lid, die zijn verleend door de onderzoeksrechter in het kader van een gerechtelijk onderzoek overeenkomstig artikel 56*bis*.

De procureur des Konings vermeldt op dat ogenblik in een afzonderlijke en schriftelijke beslissing de misdrijven die door de politiediensten en de personen bedoeld [in] § 3, derde lid, in het kader van de door de onderzoeksrechter bevolen maatregel kunnen worden gepleegd. Deze beslissing wordt in het dossier bedoeld in § 3, zevende lid, bewaard ».

B.28.2. In de memorie van toelichting met betrekking tot die bepaling wordt vermeld :

« Dit artikel voert de mogelijkheid in over te gaan tot een infiltratie op internet of een interactie op internet die niet enkel een gerichte verificatie of een arrestatie tot doel heeft.

Aangezien de infiltratie op internet een minder verregaand karakter heeft dan de ' klassieke ' infiltratie, en aangezien de verschillende contacten gedurende de uitvoering van deze maatregel worden geregistreerd, is een soepeler regime gerechtvaardigd » (*Parl. St.*, Kamer, 2015-2016, DOC 54-1966/001, p. 36).

Wat betreft het verschil in regeling met de infiltratie in de reële wereld

B.29.1. Het eerste onderdeel van het tweede middel is afgeleid uit de schending van de artikelen 10 en 11 van de Grondwet. De verzoekende partijen zijn van mening dat het criterium van het virtuele of reële karakter van de infiltratiemaatregel het niet mogelijk maakt te verantwoorden, enerzijds, dat de procureur des Konings, in het kader van een infiltratie op internet, geen maatregelen kan nemen ter vrijwaring van de veiligheid en de fysieke, psychische en morele integriteit van de infiltrant en, anderzijds, dat de controle op de tenuitvoerlegging van de methode waarin is voorzien bij de artikelen 235*ter* en 235*quater* van het Wetboek van strafvordering, niet van toepassing is op de infiltratie op internet.

B.29.2. Aangezien de verzoekende partijen belang hebben bij de vernietiging van de bestreden bepaling, is er, in tegenstelling tot hetgeen de Ministerraad betoogt, geen reden om zich vragen te stellen over hun belang bij het eerste onderdeel van dat middel.

De veiligheid van de « cyberinfiltranten »

B.30.1. In paragraaf 2, derde lid, van artikel 47*octies* van het Wetboek van strafvordering, dat de infiltratie in de reële wereld betreft, wordt gepreciseerd dat de procureur des Konings, indien daartoe grond bestaat, tevens toelating kan verlenen om de noodzakelijke maatregelen te nemen ter vrijwaring van de veiligheid en de fysieke, psychische en morele integriteit van de infiltrant.

B.30.2. In antwoord op een opmerking van de Raad van State op dat punt, wordt in de memorie van toelichting gepreciseerd :

« De Raad van State vraagt zich in punt 25 van het advies ook af waarom de procureur des Konings, in tegenstelling tot wat het geval is voor de klassieke infiltratie, geen maatregelen kan nemen ter vrijwaring van de veiligheid en de fysieke, psychische en morele integriteit van de cyberinfiltrant (zie artikel 47*octies*, § 2 laatste lid). De regering acht dit overbodig bij een infiltratie die enkel via internet verloopt. Er is vooreerst geen enkel fysiek contact met mogelijke verdachten. Bovendien spreekt het voor zich dat de cyber-infiltranten voortdurend zullen worden opgevolgd. Voor het garanderen van hun psychologische en morele integriteit is geen wettelijke basis vereist » (*Parl. St.*, Kamer, 2015-2016, DOC 54-1966/001, p. 42).

B.30.3. De infiltratie die alleen op internet gebeurt, houdt, voor de fysieke veiligheid van de infiltrant, niet dezelfde risico's in als een infiltratie in de reële wereld. De wetgever kon bijgevolg redelijkerwijs van oordeel zijn dat het niet noodzakelijk is te voorzien in dezelfde mogelijkheden om maatregelen te nemen ter vrijwaring van de fysieke veiligheid van de infiltrant die enkel in de virtuele wereld handelt. Het bestreden verschil in behandeling berust bijgevolg, in dat opzicht, op een relevant criterium.

B.30.4. Bovendien verbiedt de bepaling niet dat binnen de betrokken politiediensten maatregelen voor psychologische nazorg en ondersteuning worden aangewend die aangepast zijn aan de situatie van de personen die infiltraties op internet verrichten, zodat de bestreden bepaling voor de cyberinfiltranten geen onevenredige gevolgen heeft wat hun psychische en morele veiligheid betreft.

De controle door de kamer van inbeschuldigingstelling

B.31.1. Bij artikel 235*ter* van het Wetboek van strafvordering is de kamer van inbeschuldigingstelling belast met de controle over de toepassing van, onder meer, de infiltraties verricht in de reële wereld. Krachtens dezelfde bepaling controleert de kamer van inbeschuldigingstelling de toepassing van de infiltraties op internet enkel indien daarbij een vertrouwelijk dossier werd aangelegd.

Wanneer een machtiging wordt verleend voor een infiltratie in de reële wereld, moet steeds een vertrouwelijk dossier worden aangelegd. Het omvat de machtiging tot infiltratie, de beslissingen tot wijziging, uitbreiding of verlenging, alsook de door de officier van gerechtelijke politie opgestelde verslagen over elke fase van de uitvoering van de infiltraties die hij leidt. In het geval van een infiltratie op internet, daarentegen, moet een vertrouwelijk dossier enkel worden aangelegd in twee gevallen : wanneer de infiltrant een beroep doet op de deskundigheid van een persoon die niet tot de politiediensten behoort en wanneer de procureur des Konings machtiging verleent voor het plegen van een strafbaar feit.

B.31.2. Het aanleggen van het vertrouwelijk dossier vloeit voort uit de noodzaak om, in sommige strafprocessen, de anonimiteit van de getuigen te beschermen of het geheim te bewaren over aangewende onderzoeksmethoden, belangen die moeten worden afgewogen tegen de rechten van de verdediging van de beklaagde, die in beginsel impliceren dat die met kennis van zaken elk tegen hem in aanmerking genomen bewijsmiddel kan betwisten. Het optreden van de kamer van inbeschuldigingstelling krachtens de artikelen 235*ter* en 235*quater* van het Wetboek van strafvordering beoogt specifiek het vertrouwelijk dossier en vormt de waarborg dat een onafhankelijke en onpartijdige rechter een controle uitoefent op de regelmatigheid van de aanwending van de bijzondere opsporingsmethoden en van de bewijzen die zij hebben kunnen opleveren wanneer de voormelde belangen verantwoorden dat de beschuldigde geen toegang heeft tot het volledige strafdossier.

B.31.3. In tegenstelling tot hetgeen in de reële wereld het geval is, worden krachtens paragraaf 4, tweede lid, van de bestreden bepaling alle in het kader van de infiltratie op internet gelegde contacten geregistreerd en bij het dossier gevoegd of ter griffie neergelegd. Personen die worden vervolgd op basis van bewijzen die werden verzameld tijdens een infiltratie op internet hebben dus toegang tot de volledige toepassing van de infiltratie. Zij zijn in staat de aanwending van die methode en de uitvoeringsmodaliteiten ervan te betwisten en zij kunnen het onderzoeksgerecht of het vonnisgerecht verzoeken de regelmatigheid ervan te controleren. Het is dus in dat geval niet vereist dat een vertrouwelijk dossier wordt aangelegd en dat daarop door de kamer van inbeschuldigingstelling een specifieke controle wordt uitgeoefend. Het verschil in behandeling berust, ook in dat opzicht, op een relevant criterium.

B.31.4. Het tweede middel, in zijn eerste onderdeel, is niet gegrond.

Wat betreft de nadere regels voor de aanwijzing van de politiediensten die bevoegd zijn om een infiltratie op internet uit te voeren

B.32.1. Het tweede onderdeel van het tweede middel is afgeleid uit de schending van de artikelen 12 en 14 van de Grondwet, in samenhang gelezen met artikel 6 van het Europees Verdrag voor de rechten van de mens, en beoogt paragraaf 1, tweede lid, van het bestreden artikel 7. De verzoekende partijen verwijten de wetgever dat hij, met schending van het wettigheidsbeginsel in strafzaken, aan de Koning de bevoegdheid heeft gedelegeerd om de nadere regels te bepalen voor de aanwijzing van de politiediensten die bevoegd zijn om de maatregel van infiltratie op internet ten uitvoer te leggen.

B.32.2. In de memorie van toelichting wordt in verband met die delegatie vermeld :

« Wat betreft de politiediensten die de nieuwe maatregel zullen kunnen uitvoeren, is het niet noodzakelijk om een even strikte regeling te hebben als de thans bestaande regeling voor de infiltratie. Die laatste is voorbehouden voor de leden van de speciale eenheden van de federale politie (DSU). Dat is verantwoord op grond van het gevaar dat de maatregel inhoudt, ook en vooral voor de infiltrerende politieambtenaar. Die beperking is niet verantwoord voor de maatregel die uitsluitend op internet plaatsvindt. Dat betekent evenwel niet dat om het even welke onderzoeker kan worden belast met de uitvoering van een dergelijke interactie of infiltratie. Enkel de specifiek aangewezen politiediensten zullen de maatregel kunnen uitvoeren. In het voorontwerp werd deze aanwijzing gedelegeerd aan de minister van Justitie. De Raad van State merkt op dat een dergelijke delegatie niet toegestaan is en dat de bevoegde politiediensten in de wet zouden moeten worden opgenomen. De regering wijst er op dat een delegatie aan de minister van Justitie reeds bestaat in het raam van de toepassing van bijzondere opsporingsmethoden (art. 47*ter*, § 1, tweede lid Sv.) en dat het niet aan de wetgever toekomt om een gedetailleerde regeling uit te werken. Er zal immers worden voorzien in een specifieke opleiding voor de beoogde politiediensten met het oog op zowel de bescherming van de persoonlijke levenssfeer van de beoogde personen als het verzekeren van het goede verloop van de onderzoeken. Om die reden opteert de regering ervoor om de voorwaarden, onder meer wat betreft de opleiding, en modaliteiten van de aanwijzing van de bevoegde politiediensten door de Koning te laten bepalen » (*Parl. St.*, Kamer, 2015-2016, DOC 54-1966/001, p. 40).

B.33.1. Door aan de wetgevende macht de bevoegdheid te verlenen, enerzijds, om te bepalen in welke gevallen en in welke vorm strafvervolging mogelijk is en, anderzijds, om een wet aan te nemen krachtens welke een straf kan worden bepaald en toegepast, waarborgen de artikelen 12, tweede lid, en 14 van de Grondwet aan elke rechtsonderhorige dat geen enkele gedraging strafbaar zal worden gesteld, geen enkele straf zal worden opgelegd en geen strafrechtspleging zal worden gevoerd dan krachtens regels aangenomen door een democratisch verkozen beraadslagende vergadering.

B.33.2. Het wettigheidsbeginsel in strafzaken gaat niet zover dat het de wetgever ertoe verplicht elk aspect van de strafrechtspleging zelf te regelen. Een delegatie aan de uitvoerende macht is niet in strijd met dat beginsel voor zover de machtiging voldoende nauwkeurig is omschreven en betrekking heeft op de tenuitvoerlegging van maatregelen waarvan de essentiële elementen voorafgaandelijk door de wetgever zijn vastgesteld.

B.34.1. Te dezen kan worden aanvaard dat de wetgever ervan is uitgegaan dat het noodzakelijk is de Koning ertoe te machtigen de politiediensten aan te wijzen die bevoegd zijn om infiltraties op internet te verrichten. In een aangelegenheid die voortdurend in ontwikkeling is, zoals internet, is het immers aangewezen dat een zekere flexibiliteit de overheden de mogelijkheid biedt regelmatig de inhoud aan te passen van de opleiding die de politiemensen de mogelijkheid biedt de maatregel van infiltratie op internet toe te passen, hetgeen ook veronderstelt de aanwijzing van de gemachtigde politieofficieren te kunnen aanpassen naar gelang van de beschikbare en door de leden van de betrokken diensten gevolgde opleidingen.

Daarenboven bepaalt artikel 46*sexies* van het Wetboek van strafvordering de voorwaarden waaronder de infiltratie op internet kan worden bevolen. Bij de bestreden bepaling heeft de wetgever de Koning ertoe gemachtigd bepalingen aan te nemen die betrekking hebben op maatregelen waarvan hij dus zelf de essentiële elementen heeft vastgelegd.

B.34.2. Het tweede middel, in zijn tweede onderdeel, is niet gegrond.

Wat betreft de uitsluiting van het begrip « infiltratie » uit bepaalde gerichte maatregelen

B.35.1. Het derde onderdeel van het tweede middel is afgeleid uit de schending van de artikelen 12 en 14 van de Grondwet en beoogt paragraaf 1, vierde lid, van artikel 46*sexies* van het Wetboek van strafvordering. De verzoekende partijen verwijten de wetgever dat hij, met schending van het wettigheidsbeginsel in strafzaken, heeft nagelaten te bepalen welke op het internet verrichte onderzoekshandelingen niet het voorwerp moeten uitmaken van een machtiging vanwege de procureur des Konings en dus door de politiemensen op eigen initiatief kunnen worden gesteld. Zij zijn van mening dat de uitdrukking « interactie [...] die enkel een gerichte verificatie of een arrestatie tot direct doel heeft » de officieren van gerechtelijke politie de mogelijkheid biedt de strikte voorwaarden van de infiltratie op internet te omzeilen of te schenden.

B.35.2. De vereiste van voorspelbaarheid van de strafrechtspleging, opgenomen in artikel 12, tweede lid, van de Grondwet, waarborgt elke rechtsonderhorige dat tegen hem enkel een opsporingsonderzoek, een gerechtelijk onderzoek en een vervolging kunnen worden ingesteld volgens een procedure waarvan hij vóór de aanwending ervan kennis kan nemen.

B.36. In de memorie van toelichting met betrekking tot de bestreden bepaling wordt vermeld :

« Die verduidelijking strekt ertoe te voorkomen dat een situatie wordt gecreëerd waarin de slagvaardigheid van de politiediensten wordt beperkt ten opzichte van wat thans bestaat, zowel op internet als in de fysieke wereld » (*Parl. St.*, Kamer, 2015-2016, DOC 54-1966/001, p. 38).

De volgende voorbeelden worden vervolgens aangehaald : een contact om een afspraak te maken teneinde een goed te zien dat te koop wordt aangeboden via een « zoekertje » dat in een krant is gepubliceerd of op een tweedehandsverkoopsite is geplaatst, een korte interactie met een persoon die een bericht op internet heeft geplaatst om te bepalen of het gaat om een ernstig geradicaliseerde persoon dan wel om een flauwe grappenmaker, het afspreken van een plaats om een persoon fysiek te ontmoeten teneinde hem te kunnen arresteren. In de tekst wordt gepreciseerd dat de politieambtenaar in die gevallen zijn hoedanigheid niet vermeldt, maar dat hij evenmin een valse identiteit gebruikt en dat dat soort van interactie « enkel betrekking [heeft] op een specifiek en zeer beperkt aspect » (*ibid.*, p. 39).

B.37.1. Uit de tekst van de bestreden bepaling, verduidelijkt door de in de voormelde memorie van toelichting vermelde preciseringen, blijkt voldoende dat de infiltratie op internet die enkel kan worden aangewend mits de procureur des Konings machtiging daartoe verleent, bestaat in het « onderhouden » van contacten met een of meer verdachten, onder dekking van een fictieve identiteit. Insgelijks wordt in artikel 47*octies* van het Wetboek van strafvordering, dat de infiltratie in de reële wereld betreft, die infiltratie gedefinieerd als het « onder een fictieve identiteit, duurzaam contact onderhouden » met een of meer verdachten. Infiltratie, in die beide vormen, veronderstelt dus, enerzijds, het construeren van een geloofwaardige fictieve identiteit voor de infiltrant en, anderzijds, een interactie van een bepaalde duur met een of meer personen die ervan verdacht worden strafbare feiten van een zekere ernst te plegen of te kunnen plegen. De doelgerichte contacten teneinde een afspraak te maken of een gerichte verificatie te doen, die de gerechtelijke politie de mogelijkheid bieden haar opdrachten te vervullen overeenkomstig artikel 15 van de wet van 5 augustus 1992 op het politieambt, beantwoorden niet aan die definitie en dienen dus niet voorafgaandelijk door de procureur des Konings te zijn toegestaan.

B.37.2. Het tweede middel, in zijn derde onderdeel, is niet gegrond.

Om die redenen,

het Hof

1. vernietigt

- artikel 39*bis*, § 3, van het Wetboek van strafvordering, ingevoegd bij artikel 2 van de wet van 25 december 2016 « houdende diverse wijzigingen van het Wetboek van strafvordering en het Strafwetboek, met het oog op de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet en elektronische en telecommunicaties en tot oprichting van een gegevensbank stemafdrukken »;

- artikel 13 van de voormelde wet van 25 december 2016;

- artikel 39*bis* van het Wetboek van strafvordering, ingevoegd bij artikel 2 van de voormelde wet van 25 december 2016, in zoverre daarbij niet wordt voorzien in een specifieke bepaling teneinde het beroepsgeheim van de artsen en de advocaten te beschermen;

2. handhaaft de door de vernietigde bepalingen teweeggebrachte gevolgen tot de datum waarop dit arrest in het *Belgisch Staatsblad* wordt bekendgemaakt;

3. onder voorbehoud van de in B.15.2 en B.22.2 vermelde interpretaties, verwerpt het beroep voor het overige.

Aldus gewezen in het Frans, het Nederlands en het Duits, overeenkomstig artikel 65 van de bijzondere wet van 6 januari 1989 op het Grondwettelijk Hof, op 6 december 2018.

De griffier, De voorzitter,

F. Meersschaut F. Daoût

VERFASSUNGSGERICHTSHOF

[2019/200144]

Auszug aus dem Entscheid Nr. 174/2018 vom 6. Dezember 2018

Geschäftsverzeichnisnummer 6711

In Sachen: Klage auf Nichtigerklärung der Artikel 2 und 7 des Gesetzes vom 25. Dezember 2016 « zur Festlegung verschiedener Abänderungen des Strafprozessgesetzbuches und des Strafgesetzbuches im Hinblick auf die Verbesserung der besonderen Ermittlungsmethoden und bestimmter Ermittlungsmaßnahmen in Sachen Internet, elektronische Nachrichten und Telekommunikation und zur Schaffung einer Datenbank der Stimmabdrücke », erhoben von der VoG « Ligue des Droits de l'Homme » und der VoG « Liga voor Mensenrechten ».

Der Verfassungsgerichtshof,

zusammengesetzt aus den Präsidenten F. Daoût und A. Alen, den Richtern L. Lavrysen, J.-P. Snappe, J.-P. Moerman, E. Derycke, T. Merckx-Van Goey, P. Nihoul, T. Giet, R. Leysen, J. Moerman und M. Pâques, unter Assistenz des Kanzlers F. Meersschaut, unter dem Vorsitz des Präsidenten F. Daoût,

erlässt nach Beratung folgenden Entscheid:

I. *Gegenstand der Klage und Verfahren*

Mit einer Klageschrift, die dem Gerichtshof mit am 17. Juli 2017 bei der Post aufgegebenem Einschreibebrief zugesandt wurde und am 19. Juli 2017 in der Kanzlei eingegangen ist, erhoben Klage auf Nichtigerklärung der Artikel 2 und 7 des Gesetzes vom 25. Dezember 2016 « zur Festlegung verschiedener Abänderungen des Strafprozessgesetzbuches und des Strafgesetzbuches im Hinblick auf die Verbesserung der besonderen Ermittlungsmethoden und bestimmter Ermittlungsmaßnahmen in Sachen Internet, elektronische Nachrichten und Telekommunikation und zur Schaffung einer Datenbank der Stimmabdrücke » ″ (veröffentlicht im *Belgischen Staatsblatt* vom 17. Januar 2017): die VoG « Ligue des Droits de l'Homme » und die VoG « Liga voor Mensenrechten », unterstützt und vertreten durch RA D. Ribant und RÄin C. Forget, in Brüssel zugelassen, und durch RA J. Heymans, in Gent zugelassen, und RA J. Vander Velpen, in Antwerpen zugelassen.

(...)

II. *Rechtliche Würdigung*

(...)

In Bezug auf den Gegenstand der Klage

B.1.1. Die Klage bezieht sich auf die Artikel 2 und 7 des Gesetzes vom 25. Dezember 2016 « zur Festlegung verschiedener Abänderungen des Strafprozessgesetzbuches und des Strafgesetzbuches im Hinblick auf die Verbesserung der besonderen Ermittlungsmethoden und bestimmter Ermittlungsmaßnahmen in Sachen Internet, elektronische Nachrichten und Telekommunikation und zur Schaffung einer Datenbank der Stimmabdrücke » (nachstehend: Gesetz vom 25. Dezember 2016).

B.1.2. Mit diesem Gesetz soll eine Reihe von Änderungen des Strafprozessgesetzbuches bezüglich der strafrechtlichen Ermittlung und Untersuchung vorgenommen werden, insbesondere bei der Anwendung von besonderen Ermittlungsmethoden und bestimmten anderen Untersuchungsmethoden für die Suche im Internet und in elektronischen Nachrichten. Die durch das angefochtene Gesetz abgeänderten Bestimmungen wurden durch verschiedene Gesetze in das Strafprozessgesetzbuch eingeführt und « seit dem Jahr 2000 nicht mehr abgeändert oder angepasst », was « in der Welt der sich rasch entwickelnden Informationstechnologie eine Ewigkeit » darstellt (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-1966/001, S. 5). Mit dem angefochtenen Gesetz wollte der Gesetzgeber daher « einen für die Suche in einem Datenverarbeitungssystem und die Überwachung sowie die Kenntnisnahme von elektronischen Nachrichten geeigneteren Rechtsrahmen » schaffen (ebd., S. 7).

B.1.3. Der erste Klagegrund, der fünf Teile umfasst, richtet sich gegen Artikel 2 dieses Gesetzes, der die Suche in einem Datenverarbeitungssystem betrifft. Der zweite Klagegrund, der drei Teile enthält, richtet sich gegen Artikel 7 dieses Gesetzes, der die Infiltrierung im Internet betrifft.

In Bezug auf den ersten Klagegrund

Was die angefochtene Bestimmung betrifft

B.2. Durch Artikel 2 des Gesetzes vom 25. Dezember 2016 wird Artikel 39*bis* des Strafprozessgesetzbuches wie folgt abgeändert:

1. In Paragraph 1 - der bestimmte: « Unbeschadet der spezifischen Bestimmungen des vorliegenden Artikels sind die Regeln des vorliegenden Gesetzbuches mit Bezug auf die Beschlagnahme einschließlich des Artikels 28*sexies* auf Maßnahmen anwendbar, die darin bestehen, in einem Datenverarbeitungssystem gespeicherte Daten zu kopieren, unzugänglich zu machen und zu entfernen » - werden zwischen den Wörtern « in einem Datenverarbeitungssystem » und den Wörtern « gespeicherte Daten » die Wörter « oder einem Teil davon » eingefügt.

2. Die Paragraphen 2 bis 6 werden durch folgende Bestimmungen ersetzt:

« § 2. Die Suche in einem Datenverarbeitungssystem oder einem Teil davon, das beschlagnahmt worden ist, kann von einem Gerichtspolizeioffizier beschlossen werden.

Unbeschadet des Absatzes 1 kann der Prokurator des Königs eine Suche in einem Datenverarbeitungssystem oder einem Teil davon, das von ihm beschlagnahmt werden kann, anordnen.

Die in den Absätzen 1 und 2 erwähnten Suchen können sich nur auf Daten erstrecken, die im Datenverarbeitungssystem gespeichert sind, das entweder beschlagnahmt worden ist oder beschlagnahmt werden kann. Zu diesem Zweck wird vor Beginn der Suche jede externe Verbindung dieses Datenverarbeitungssystems verhindert.

§ 3. Der Prokurator des Königs kann die auf der Grundlage von § 2 begonnene Suche in einem Datenverarbeitungssystem oder einem Teil davon auf ein Datenverarbeitungssystem oder einen Teil davon ausweiten, das sich an einem anderen Ort als dem, wo die Suche durchgeführt wird, befindet:

- wenn diese Ausweitung für die Wahrheitsfindung mit Bezug auf die Straftat, die Gegenstand der Suche ist, notwendig ist und

- wenn andere Maßnahmen unverhältnismäßig wären oder wenn das Risiko besteht, dass ohne diese Ausweitung Beweismaterial verloren geht.

Die Ausweitung der Suche in einem Datenverarbeitungssystem darf nicht über die Datenverarbeitungssysteme oder Teile von solchen Systemen hinausgehen, zu denen die Personen, die berechtigt sind, das untersuchte Datenverarbeitungssystem zu benutzen, insbesondere Zugang haben.

Was die durch die Ausweitung der Suche in einem Datenverarbeitungssystem gesammelten Daten betrifft, die denselben Zwecken dienen wie die der Beschlagnahme, sind die in § 6 vorgesehenen Regeln anwendbar.

Wenn sich herausstellt, dass diese Daten sich nicht auf dem Staatsgebiet des Königreichs befinden, dürfen sie nur kopiert werden. In diesem Fall teilt der Prokurator des Königs dies unverzüglich dem Föderalen Öffentlichen Dienst Justiz mit, der die zuständigen Behörden des betreffenden Staates darüber informiert, wenn dieser richtigerweise bestimmt werden kann.

In Fällen äußerster Dringlichkeit kann der Prokurator des Königs die Ausweitung der in Absatz 1 erwähnten Suche mündlich anordnen. Diese Anordnung wird schnellstmöglich unter Angabe der Gründe für die äußerste Dringlichkeit schriftlich bestätigt.

§ 4. Nur der Untersuchungsrichter kann eine andere Suche in einem Datenverarbeitungssystem oder einem Teil davon als die in den Paragraphen 2 und 3 erwähnten Suchen anordnen:

- wenn diese Suche für die Wahrheitsfindung mit Bezug auf die Straftat, die Gegenstand der Suche ist, notwendig ist und

- wenn andere Maßnahmen unverhältnismäßig wären oder wenn das Risiko besteht, dass ohne diese Suche Beweismaterial verloren geht.

In Fällen äußerster Dringlichkeit kann der Untersuchungsrichter die Ausweitung der in Absatz 1 erwähnten Suche mündlich anordnen. Diese Anordnung wird schnellstmöglich unter Angabe der Gründe für die äußerste Dringlichkeit schriftlich bestätigt.

§ 5. Um die in vorliegendem Artikel erwähnten Maßnahmen zu ermöglichen, kann der Prokurator des Königs oder der Untersuchungsrichter anordnen, jederzeit auch ohne die Zustimmung des Eigentümers oder des Inhabers seiner Rechte oder des Nutzers:

- jegliche Sicherung der betreffenden Datenverarbeitungssysteme gegebenenfalls mit Hilfe von technischen Mitteln, falschen Signalen, falschen Schlüsseln oder falschen Eigenschaften zeitweilig aufzuheben,

- technische Vorrichtungen in die betreffenden Datenverarbeitungssysteme zu installieren im Hinblick auf die Entschlüsselung und die Dekodierung der durch dieses Datenverarbeitungssystem gespeicherten, verarbeiteten oder übermittelten Daten.

Jedoch kann nur der Untersuchungsrichter diese zeitweilige Aufhebung der Sicherung oder diese Installierung technischer Vorrichtungen anordnen, wenn dies insbesondere für die Anwendung von § 3 notwendig ist.

§ 6. Wenn in den betreffenden Datenverarbeitungssystemen gespeicherte Daten entdeckt werden, die für dieselben Zwecke nützlich sind wie die der Beschlagnahme, jedoch die Beschlagnahme des Datenträgers nicht wünschenswert ist, werden diese Daten sowie diejenigen, die notwendig sind, um sie zu verstehen, auf Datenträger kopiert, die der Behörde gehören. Im Dringlichkeitsfall oder aus technischen Gründen können Datenträger verwendet werden, die Personen, die berechtigt sind, das Datenverarbeitungssystem zu benutzen, zur Verfügung stehen.

Außerdem werden geeignete technische Mittel verwendet, um den Zugang zu diesen Daten im Datenverarbeitungssystem sowie zu den Kopien dieser Daten, die Personen, die berechtigt sind, das Datenverarbeitungssystem zu benutzen, zur Verfügung stehen, zu verhindern und ihre Unversehrtheit zu gewährleisten.

Wenn die in Absatz 1 vorgesehene Maßnahme aus technischen Gründen oder wegen des Umfangs der Daten nicht möglich ist, verwendet der Prokurator des Königs die geeigneten technischen Mittel, um den Zugang zu diesen Daten im Datenverarbeitungssystem sowie zu den Kopien dieser Daten, die Personen, die berechtigt sind, das Datenverarbeitungssystem zu benutzen, zur Verfügung stehen, zu verhindern und ihre Unversehrtheit zu gewährleisten.

Wenn die Daten den Gegenstand der Straftat bilden oder aus der Straftat hervorgegangen sind und wenn sie gegen die öffentliche Ordnung oder die Sittlichkeit verstoßen oder eine Gefahr für die Unversehrtheit der Datenverarbeitungssysteme oder für durch solche Systeme gespeicherte, verarbeitete oder übermittelte Daten darstellen, verwendet der Prokurator des Königs alle geeigneten technischen Mittel, um diese Daten unzugänglich zu machen oder um sie zu entfernen, nachdem er sie kopiert hat.

Er kann jedoch, außer in dem in Absatz 4 vorgesehenen Fall, die spätere Verwendung der Gesamtheit oder eines Teils dieser Daten erlauben, wenn dies keine Gefahr für die Ausübung der Strafverfolgung darstellt.

In Fällen äußerster Dringlichkeit und wenn es sich offensichtlich um eine in den Artikeln 137 § 3 Nr. 6, 140*bis* oder 383*bis* § 1 des Strafgesetzbuches erwähnte Straftat handelt, kann der Prokurator des Königs mündlich anordnen, dass alle geeigneten Mittel verwendet werden, um die Daten, die den Gegenstand der Straftat bilden oder aus der Straftat hervorgegangen sind und die gegen die öffentliche Ordnung oder die Sittlichkeit verstoßen, unzugänglich zu machen. Diese Anordnung wird schnellstmöglich unter Angabe der Gründe für die äußerste Dringlichkeit schriftlich bestätigt.

3. Der Artikel wird um die folgendermaßen lautenden Paragraphen 7 und 8 ergänzt:

« § 7. Der Prokurator des Königs oder der Untersuchungsrichter informiert den Verantwortlichen des Datenverarbeitungssystems schnellstmöglich über die Suche im Datenverarbeitungssystem oder ihre Ausweitung, außer wenn seine Identität oder seine Adresse begründeterweise nicht herausgefunden werden können. Er übermittelt ihm gegebenenfalls eine Zusammenfassung der Daten, die kopiert, unzugänglich gemacht oder entfernt worden sind.

§ 8. Der Prokurator des Königs verwendet die geeigneten technischen Mittel, um die Unversehrtheit und die Vertraulichkeit dieser Daten zu gewährleisten.

Es werden geeignete technische Mittel für ihre Aufbewahrung bei der Kanzlei verwendet.

Dieselbe Regel gilt, wenn Daten, die in einem Datenverarbeitungssystem gespeichert oder verarbeitet sind oder in ein Datenverarbeitungssystem übermittelt werden, zusammen mit ihrem Datenträger gemäß den vorhergehenden Artikeln beschlagnahmt werden ».

B.3.1. Der so abgeänderte Artikel 39*bis* des Strafprozessgesetzbuches betrifft die sogenannten « nicht geheimen » Suchen in einem Datenverarbeitungssystem. Denn gemäß seinem Paragraphen 7 muss der Verantwortliche des Datenverarbeitungssystems « schnellstmöglich » über die Suche in dem System und gegebenenfalls die Ausweitung der Suche auf ein Datenverarbeitungssystem, das sich an einem anderen Ort befindet, informiert werden.

Laut der Begründung des Gesetzes vom 28. November 2000 über die Computerkriminalität, durch das der ursprüngliche Artikel 39*bis* in das Strafprozessgesetzbuch eingeführt wurde, ist unter « Datenverarbeitungssystem » « ein System, mit dem Daten gespeichert, verarbeitet oder übermittelt werden können, » zu verstehen (*Parl. Dok.*, Kammer, 1999-2000, DOC 50-0213/001 und 50-0214/001, S. 12).

B.3.2. Grundsätzlich kann eine Suche in einem Datenverarbeitungssystem oder einem Teil davon nur von einem Untersuchungsrichter angeordnet werden, wenn diese Suche für die Wahrheitsfindung mit Bezug auf die Straftat, die Gegenstand der Suche ist, notwendig ist und wenn andere Maßnahmen unverhältnismäßig wären oder wenn das Risiko besteht, dass ohne diese Suche Beweismaterial verloren geht (§ 4). Das Gleiche gilt für die Ausweitung der Suche auf ein Datenverarbeitungssystem, auf das von dem System zugegriffen werden kann, das Gegenstand der anfänglichen Suche war.

B.3.3. Die angefochtene Bestimmung sieht mehrere Ausnahmen von der grundsätzlichen Zuständigkeit des Untersuchungsrichters in Bezug auf nicht geheime Suchen vor.

Zum einen kann die Suche in den in einem Datenverarbeitungssystem oder einem Teil davon gespeicherten Daten, das Gegenstand einer Beschlagnahme ist, von einem Gerichtspolizeioffizier veranlasst werden, unter der Voraussetzung, dass es für den Zugriff auf die Daten nicht notwendig ist, eine Sicherung aufzuheben oder die Daten zu entschlüsseln oder zu dekodieren. Falls es für den Zugriff auf die gespeicherten Daten notwendig ist, eine Sicherung aufzuheben oder sie zu entschlüsseln oder zu dekodieren, muss der Gerichtspolizeioffizier zu diesem Zweck die Erlaubnis des Prokurators des Königs einholen.

Zweitens kann der Prokurator des Königs eine Suche in den in einem Datenverarbeitungssystem oder einem Teil davon gespeicherten Daten anordnen, das nicht Gegenstand einer Beschlagnahme war, das aber von ihm beschlagnahmt werden könnte. In diesem Fall kann er ebenfalls die Aufhebung der etwaigen Sicherung oder die Entschlüsselung oder Dekodierung der Daten anordnen.

Drittens kann die Ausweitung der Suche, die in einem beschlagnahmten Datenverarbeitungssystem oder in einem System, das beschlagnahmt werden könnte, begonnen wurde, auf Daten in einem anderen Datenverarbeitungssystem, auf das über eine Verbindung aus dem System, in dem die Suche begonnen wurde, zugegriffen werden kann, vom Prokurator des Königs angeordnet werden. Wenn jedoch der Zugang zu den Daten in diesem anderen Datenverarbeitungssystem gesichert ist, muss der Prokurator des Königs die Genehmigung des Untersuchungsrichters einholen, um die Sicherung aufzuheben oder eine technische Vorrichtung zu installieren, die es ihm ermöglicht, sie zu entschlüsseln oder zu dekodieren.

B.3.4. Die geheimen Suchen, auf die sich Artikel 90*ter* des Strafprozessgesetzbuches bezieht, dürfen nur von einem Untersuchungsrichter in Ausnahmefällen angeordnet werden, wenn die Untersuchung es erfordert, wenn schwerwiegende Indizien dafür bestehen, dass dies eine in diesem Artikel aufgeführte Straftat betrifft, und wenn die anderen Untersuchungsmittel nicht ausreichen, um die Wahrheit herauszufinden.

In Bezug auf das Recht auf Achtung des Privatlebens

B.4.1. Der Gerichtshof prüft zunächst den ersten, zweiten und vierten Teil des ersten Klagegrunds, die aus einer Verletzung des Rechts auf Achtung vor dem Privatleben, das durch Artikel 22 der Verfassung und Artikel 8 der Europäischen Menschenrechtskonvention gewährleistet wird, sowie hinsichtlich des ersten und zweiten Teils aus einer Verletzung des Grundsatzes der Gleichheit und Nichtdiskriminierung, der durch die Artikel 10 und 11 der Verfassung gewährleistet wird, abgeleitet sind.

B.4.2. Die klagenden Parteien bemängeln an Artikel 39*bis* des Strafprozessgesetzbuches, der durch die angefochtene Bestimmung eingeführt wurde, dass er Einmischungen in das Recht auf Achtung des Privatlebens durch die Gerichtspolizeioffiziere oder die Magistrate der Staatsanwaltschaft ohne Kontrolle durch einen unabhängigen und unparteiischen Richter erlaube. Sie sind der Auffassung, dass die in Artikel 39*bis* erwähnten Suchen in einem Datenverarbeitungssystem zu einer vergleichbaren Verletzung des Privatlebens führen wie die Verletzung, die durch eine Haussuchung verursacht wird, die jedoch nur durch einen Untersuchungsrichter genehmigt werden darf (vierter Teil des Klagegrunds). Sie vertreten auch die Auffassung, dass der Behandlungsunterschied zwischen den in Artikel 90*ter* desselben Gesetzbuches erwähnten geheimen Suchen, die stets von einem Untersuchungsrichter genehmigt werden müssen, und den nicht geheimen Suchen, auf die sich die angefochtene Bestimmung bezieht und die nicht von einem Untersuchungsrichter genehmigt werden müssen, auf einem Kriterium beruht, das weder objektiv noch sachdienlich ist (erster Teil des Klagegrunds). Zudem sind sie der Meinung, dass der Behandlungsunterschied zwischen den Suchen in einem beschlagnahmten Datenverarbeitungssystem, die von einem Gerichtspolizeioffizier beschlossen werden können, und den Suchen in einem nicht beschlagnahmten Datenverarbeitungssystem, das aber beschlagnahmt werden kann, die nur durch den Prokurator des Königs beschlossen werden können, auch auf einem Kriterium beruht, das weder objektiv noch sachdienlich ist (zweiter Teil des Klagegrunds).

B.5. Im Gegensatz zu dem, was der Ministerrat ausführt, zieht der Umstand, dass die Rechtsvorschriften vor dem angefochtenen Gesetz bereits in gewissem Maße die Zuständigkeit des Prokurators des Königs vorsahen, um die Beschlagnahme von Datenverarbeitungssystemen und die Suchen in diesen Systemen anzuordnen, nicht die Unzulässigkeit wegen verspäteten Einreichens des ersten Teils des Klagegrunds nach sich. Mit der angefochtenen Bestimmung hat der Gesetzgeber nämlich erneut Gesetzesbestimmungen auf diesem Gebiet erlassen und hat die Zuständigkeit des Prokurators des Königs bestätigt und ausgeweitet.

B.6.1. Artikel 22 der Verfassung bestimmt:

« Jeder hat ein Recht auf Achtung vor seinem Privat- und Familienleben, außer in den Fällen und unter den Bedingungen, die durch Gesetz festgelegt sind.

Das Gesetz, das Dekret oder die in Artikel 134 erwähnte Regel gewährleistet den Schutz dieses Rechtes ».

Artikel 8 der Europäischen Menschenrechtskonvention bestimmt:

« (1) Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs.

(2) Der Eingriff einer öffentlichen Behörde in die Ausübung dieses Rechts ist nur statthaft, insoweit dieser Eingriff gesetzlich vorgesehen ist und eine Maßnahme darstellt, die in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist ».

B.6.2. Der Verfassungsgeber hat eine möglichst weitgehende Übereinstimmung zwischen Artikel 22 der Verfassung und Artikel 8 der vorerwähnten europäischen Konvention angestrebt (*Parl. Dok.*, Kammer, 1992-1993, Nr. 997/5, S. 2).

Die Tragweite dieses Artikels 8 entspricht derjenigen der vorgenannten Verfassungsbestimmung, sodass die durch die beiden Bestimmungen gewährleisteten Garantien eine untrennbare Einheit bilden.

B.6.3 Diese Bestimmungen erfordern es, dass jede behördliche Einmischung in das Recht auf Achtung des Privatlebens in einer ausreichend präzisen Gesetzesbestimmung festgelegt ist, einer zwingenden gesellschaftlichen Notwendigkeit entspricht und im Verhältnis zu dem darin angestrebten rechtmäßigen Ziel steht.

B.7.1. Wie die Gesetzgebungsabteilung des Staatsrats in ihrer Stellungnahme zum Vorentwurf des Gesetzes, das zu dem angefochtenen Gesetz geworden ist, unterstreicht, kann die Suche in einem Datenverarbeitungssystem einen erheblichen Eingriff in das Recht auf Achtung des Privatlebens darstellen (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-1966/001, S. 126).

B.7.2. Der Europäische Gerichtshof für Menschenrechte hat ebenfalls bereits mehrmals geurteilt, dass « das Durchsuchen und die Beschlagnahme elektronischer Daten einen Eingriff in das Recht auf Achtung des ' Privatlebens ' und der ' Korrespondenz '; im Sinne von [Art. 8 EMRK] » darstellen und dass « ein solcher Eingriff [...] Art. 8 [verletzt], es sei denn, er ist ' gesetzlich vorgesehen ' und verfolgt ein legitimes Ziel oder mehrere legitime Ziele im Sinne von Abs. 2 und ist ferner in einer demokratischen Gesellschaft zu deren Erreichung notwendig » (EuGHMR, 2. April 2015, *Vinci Construction und GTM Génie Civil et Services gegen Frankreich*, §§ 63-64).

Vor diesem Hintergrund untersucht der Gerichtshof, « ob das innerstaatliche Recht und die innerstaatliche Praxis angemessene und ausreichende Garantien gegen Missbrauch und Willkür bieten ». Zu diesen Garantien gehört « eine vorhandene wirksame Kontrolle von Maßnahmen, die gegen Artikel 8 der Konvention verstoßen » (ebd., §§ 66-67).

B.7.3. In Anbetracht des Ausmaßes des Eingriffs in das Recht auf Achtung des Privatlebens, den die Suche in einem Datenverarbeitungssystem verursachen kann, muss ihre Anwendung der Kontrolle durch einen unabhängigen und unparteiischen Richter unterliegen.

In Bezug auf die Suche in einem Datenverarbeitungssystem, das Gegenstand einer Beschlagnahme ist

B.8.1. Die angefochtene Bestimmung ermöglicht in ihrem Paragraphen 2 Absatz 1, dass ein Gerichtspolizeioffizier die Durchführung einer Suche in einem Datenverarbeitungssystem beschließt, das Gegenstand einer Beschlagnahme ist. Die Suche darf sich nur auf die in dem beschlagnahmten Gerät gespeicherten Daten erstrecken, denn vor Beginn der Suche muss dieses daran gehindert werden, eine Verbindung zu externen Systemen herzustellen. Wenn die Suche die zeitweilige Aufhebung einer Sicherung oder die Entschlüsselung oder Dekodierung der Daten erfordert, muss der Gerichtspolizeioffizier zu diesem Zweck außerdem die Erlaubnis des Prokurators des Königs einholen (§ 5 Absatz 1).

B.8.2. Aus der Begründung geht hervor, dass mit der angefochtenen Bestimmung das Ziel verfolgt wird, in dem Gesetz die Rechtsprechung des Kassationshofs hinsichtlich der Suche in einem beschlagnahmten System zu bestätigen:

« Dans son arrêt du 11 février 2015 (AR P.14 1739.F), la Cour de cassation a en effet indiqué que le droit actuel permet déjà à l'officier de police judiciaire de prendre connaissance des données d'un GSM qui a été saisi. Bien entendu, l'exploitation de ces données se déroule toujours dans les limites de l'enquête pénale et sous le contrôle du magistrat en charge de celle-ci » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1966/001, p. 15).

B.8.3. In seinem vorerwähnten Entscheid vom 11. Februar 2015 hat der Kassationshof geurteilt:

« L'exploitation de la mémoire d'un téléphone portable, dont les messages qui y sont stockés sous forme de *sms*, est une mesure découlant de la saisie, laquelle peut être effectuée dans le cadre d'une information sans autres formalités que celles prévues pour cet acte d'enquête » (Cass., 11 février 2015, P.14.1739.F).

B.8.4. Die Beschlagnahme ist eine Untersuchungshandlung, die in den Fällen und unter den Bedingungen vorgenommen werden kann, die gemäß den Bestimmungen des Strafprozessgesetzbuches vorgesehen sind, insbesondere im Fall einer Entdeckung auf frischer Tat oder im Laufe einer ordnungsgemäß vom Untersuchungsrichter angeordneten Haussuchung. Sie kann sich auf alles beziehen, was dazu gedient zu haben oder dazu bestimmt gewesen zu sein scheint, eine Straftat zu begehen, was durch sie hervorgebracht worden zu sein scheint, und auf alles, was der Wahrheitsfindung dienlich sein kann (Art. 35 ff. des Strafprozessgesetzbuches).

B.8.5. Jeder, der glaubt, dass ihm durch die Beschlagnahme Schaden zugefügt worden ist, kann je nach Fall beim Prokurator des Königs (Artikel 28*sexies* § 1 des Strafprozessgesetzbuches) oder beim Untersuchungsrichter (Artikel 61*quater* § 1 desselben Gesetzbuches) Aufhebung davon beantragen. Im Fall einer Abweisung kann die Anklagekammer von der geschädigten Person mit der Sache befasst werden.

B.8.6. Die Suche in den Daten, die im Speicher des beschlagnahmten Geräts gespeichert sind, ist eine Ergänzung der Beschlagnahme selbst, ebenso wie die Kenntnisnahme des Inhalts von Büchern, Aufzeichnungen oder Dokumenten auf beschlagnahmten physischen Trägern durch den Gerichtspolizeioffizier. Da das beschlagnahmte Gerät, das Gegenstand der Suche ist, keine Verbindung zu anderen Systemen hat, sodass der Polizeioffizier, der die Suche durchführt, nur Zugang zu dem Inhalt hat, den der Eigentümer oder Besitzer des Geräts dort aufgezeichnet oder gespeichert hat, unterscheidet sich die Suche nicht von der Auswertung des Inhalts von Dokumenten, die Gegenstand einer Beschlagnahme sind, durch die Ermittler.

B.8.7. Aus dem Vorstehenden ergibt sich, dass die Suche in einem Datenverarbeitungssystem, das ordnungsgemäß beschlagnahmt wurde, ebenso wie die Auswertung von ordnungsgemäß beschlagnahmten Dokumenten, mit ausreichenden rechtlichen Garantien versehen ist, mit denen sichergestellt werden kann, dass der Eingriff in das Recht auf Achtung des Privatlebens, der durch diese Untersuchungshandlung verursacht wird, im Hinblick auf die Anforderungen von Artikel 22 der Verfassung und 8 der Europäischen Menschenrechtskonvention gerechtfertigt ist.

B.8.8. Die Prüfung anhand der Artikel 10 und 11 der Verfassung führt nicht zu einer anderen Schlussfolgerung, was die Suchen in einem beschlagnahmten Datenverarbeitungssystem betrifft. Der erste und vierte Teil des ersten Klagegrunds ist unbegründet, insofern er sich gegen die Suchen in einem ordnungsgemäß beschlagnahmten Datenverarbeitungssystem richtet.

In Bezug auf die Suche in einem Datenverarbeitungssystem, das Gegenstand einer Beschlagnahme sein kann

B.9.1. Die angefochtene Bestimmung ermöglicht es in ihrem Paragraph 2 Absatz 2 dem Prokurator des Königs, eine Suche in einem Datenverarbeitungssystem zu beschließen, das nicht beschlagnahmt wurde, aber « für das alle gesetzlichen Bedingungen einer Beschlagnahme erfüllt sind » (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-1966/001, S. 16). Die Suche darf sich nur auf die in dem betreffenden Gerät gespeicherten Daten beziehen, denn dieses muss vorher daran gehindert werden, eine Verbindung zu externen Systemen herzustellen. Wenn die Suche die zeitweilige Aufhebung einer Sicherung oder die Entschlüsselung oder Dekodierung der Daten erfordert, muss der Gerichtspolizeioffizier zu diesem Zweck außerdem auch die Erlaubnis des Prokurators des Königs einholen (§ 5 Absatz 1).

B.9.2. In dem Fall, dass das Datenverarbeitungssystem, das Gegenstand der Untersuchung ist, vom Prokurator des Königs beschlagnahmt werden könnte, sind alle gesetzlichen Bedingungen, unter denen die Beschlagnahme beschlossen werden kann, erfüllt. Außerdem sind aufgrund von Artikel 39*bis* Paragraph 1 des Strafprozessgesetzbuches die Regeln mit Bezug auf die Beschlagnahme auf Maßnahmen anwendbar, die darin bestehen, in einem Datenverarbeitungssystem oder einem Teil davon gespeicherte Daten zu kopieren, unzugänglich zu machen und zu entfernen. Das Kopieren von Daten, die eine Suche in einem Datenverarbeitungssystem ergeben hat, das aus Gründen der praktischen Zweckmäßigkeit nicht beschlagnahmt wurde, das aber gemäß den gesetzlichen Bedingungen für die Beschlagnahme hätte beschlagnahmt werden können, wird also hinsichtlich der Rechtsmittel und Garantien, die der betreffenden Person geboten sind, selbst als eine Beschlagnahme angesehen.

B.9.3. Da das Gerät, in dem die Suche durchgeführt wird, keine Verbindung zu anderen Systemen hat, sodass der Polizeioffizier, der die Suche durchführt, nur Zugang zu dem Inhalt hat, den der Eigentümer oder Besitzer des Geräts dort aufgezeichnet oder gespeichert hat, unterscheidet sich die Suche außerdem nicht von einer Suche in Dokumenten vor einer Beschlagnahme.

B.9.4. Daraus ergibt sich, das die Person, der durch die Beschlagnahme der Daten in einem nicht beschlagnahmten Datenverarbeitungssystem Schaden zugefügt wird, über dieselben Rechtsmittel und Garantien verfügt wie eine von einer nach den Rechtsvorschriften durchgeführten Haussuchung oder Durchsuchung betroffene Person.

B.9.5. Aus dem Vorstehenden ergibt sich, dass die Suche in einem Datenverarbeitungssystem, das nicht beschlagnahmt wurde, aber hätte beschlagnahmt werden können, mit ausreichenden rechtlichen Garantien versehen ist, mit denen sichergestellt werden kann, dass der Eingriff in das Recht auf Achtung des Privatlebens, der durch diese Untersuchungshandlung verursacht wird, im Hinblick auf die Anforderungen von Artikel 22 der Verfassung und 8 der Europäischen Menschenrechtskonvention gerechtfertigt ist.

B.9.6. Die Prüfung anhand der Artikel 10 und 11 der Verfassung führt nicht zu einer anderen Schlussfolgerung, was die Suchen in einem Datenverarbeitungssystem betrifft, das nicht beschlagnahmt wurde, aber hätte beschlagnahmt werden können. Der erste und vierte Teil des ersten Klagegrunds ist unbegründet, insofern er sich gegen die Suchen in einem Datenverarbeitungssystem richtet, das ordnungsgemäß beschlagnahmt werden kann.

In Bezug auf den Behandlungsunterschied zwischen der Suche in einem beschlagnahmten Datenverarbeitungssystem und der Suche in einem Datenverarbeitungssystem, das beschlagnahmt werden kann

B.10.1. Da die Möglichkeit des Gerichtspolizeioffiziers, die Durchführung einer Suche in einem beschlagnahmten Datenverarbeitungssystem selbst zu beschließen, durch die in B.8.1 ff. dargelegten Gründe gerechtfertigt ist, ist der Behandlungsunterschied, der sich daraus ergibt, dass die Suche durch den Prokurator des Königs in einem Datenverarbeitungssystem, das nicht beschlagnahmt ist, aber beschlagnahmt werden könnte, nur durch diesen beschlossen werden kann, durch dieselben Gründe gerechtfertigt.

B.10.2. Der zweite Teil des ersten Klagegrunds ist unbegründet.

In Bezug auf die Ausweitung der Suche

B.11.1. Der durch die angefochtene Bestimmung eingeführte Artikel 39*bis* § 3 des Strafprozessgesetzbuches ermöglicht es dem Prokurator des Königs zu beschließen, eine Suche, die in einem Datenverarbeitungssystem begonnen wurde, das beschlagnahmt wurde oder beschlagnahmt werden kann, auf ein Datenverarbeitungssystem oder einen Teil davon auszuweiten, das sich an einem anderen Ort als dem, wo die Suche durchgeführt wird, befindet und auf das über eine Verbindung zugegriffen werden kann. Ist jedoch der Zugriff auf die Daten gesichert, kann nur der Untersuchungsrichter die Aufhebung der Sicherung oder die Entschlüsselung oder Dekodierung der Daten genehmigen (§ 5 Absatz 2).

B.11.2. Die Ausweitung der Suche ermöglicht es den Ermittlern, nicht nur auf sämtliche aufgezeichneten oder gespeicherten Daten auf dem Gerät, das Ausgangspunkt der Suche ist, Zugriff zu haben, sondern auch auf alle in den Datenverarbeitungssystemen gespeicherten Dokumente, auf die durch eine Verbindung über dieses Gerät zugegriffen werden kann, sowie auf die gesamte Kommunikation, die sein Nutzer mit Dritten unterhalten hat, einschließlich der neu erhaltenen oder versandten Nachrichten, von denen der Nutzer noch keine Kenntnis genommen hat.

B.12.1. Vor dem Inkrafttreten der angefochtenen Bestimmung befand sich die Bestimmung zu Suchen in den Netzen, die durch Artikel 3 des Gesetzes vom 28. November 2000 über die Computerkriminalität eingefügt wurde, in Artikel 88*ter* des Strafprozessgesetzbuches. Dieser Artikel wurde durch Artikel 13 des angefochtenen Gesetzes aufgehoben.

B.12.2. In der Begründung des Gesetzes vom 28. November 2000 ist zu diesem Artikel 88*ter* angegeben:

« Une mesure coercitive traditionnelle, telle que la perquisition, est restrictive en ce sens que, par définition, elle ne peut être effectuée que sur le lieu pour lequel elle a été ordonnée. Ce qui caractérise les systèmes informatiques - qu'il s'agisse de systèmes importants dans des sociétés ou d'ordinateurs portables - c'est qu'ils sont de plus en plus connectés en réseaux.

Dans le contexte actuel, lorsque les systèmes informatiques pour lesquels une recherche semble nécessaire sont dispersés en divers endroits, plusieurs mandats de perquisition ou de saisie doivent être délivrés. Pareille approche suscite bien évidemment des problèmes : on court non seulement le risque de voir des éléments de preuve disparaître si l'intervention n'est pas simultanée mais en outre dans de nombreux cas, il ne sera pas possible *a priori* de déterminer les endroits où doivent s'effectuer les recherches, les fichiers pertinents ou même la localisation géographique des ordinateurs.

Pour pallier ces problèmes, le nouvel article fixe les conditions qui permettent l'extension de la recherche dans un système informatique vers des systèmes situés ailleurs. Il doit s'agir de systèmes liés entre eux.

La mesure doit avant tout être nécessaire à la manifestation de la vérité et il faut en outre qu'il y ait un risque de perdre les éléments de preuve ou que la prise d'autres mesures (par exemple plusieurs mandats de perquisition) soit disproportionnée. Il appartient au juge d'instruction d'apprécier raisonnablement ces considérations. En raison du caractère exceptionnel de l'extension de la recherche dans un système informatique, notamment en raison de ses éventuels effets extra-territoriaux, une telle recherche ne pourra être étendue que si elle apparaît nécessaire dans le cadre d'une affaire pénale concrète dont le juge est saisi » (*Doc. parl.*, 1999-2000, DOC 50-0213/001 et 50-0214/001, pp. 22-23).

B.13.1. Seit dem Inkrafttreten der angefochtenen Bestimmung erfordert die Ausweitung einer in einem Datenverarbeitungssystem begonnenen Suche auf Netze, die mit ihm verbunden sind, nicht mehr die Befassung und Genehmigung des Untersuchungsrichters. Der Prokurator des Königs ist dafür zuständig, diese Ausweitung der Suche anzuordnen, sofern der Zugang zu den Netzen nicht gesichert ist.

B.13.2. In der Begründung des angefochtenen Gesetzes ist hierzu angegeben:

« L'extension de la recherche dans un système informatique peut désormais être ordonnée par le procureur du Roi ou l'auditeur du travail.

Cette extension vise par exemple les situations où un smartphone a été saisi et où il apparaît nécessaire d'avoir accès au compte Hotmail, Facebook ou Dropbox auquel ce smartphone est connecté. Comme indiqué précédemment, le droit actuel permet seulement à l'autorité qui a décidé la saisie de l'appareil de faire une recherche dans l'appareil lui-même, pas dans les données auxquelles cet appareil est connecté dans le cloud par exemple.

Même si l'intervention du juge d'instruction inclut une garantie essentielle en matière d'intrusion dans la vie privée, la modification de loi est justifiée parce que l'article 39*bis* se limite aux recherches non secrètes. Comme il a été dit, l'article 39*bis* est utilisé de manière réactive à la suite du fait que l'on a pu s'emparer légalement d'un système informatique. Il n'y a en aucun cas d'approche ou d'exploitation secrète d'éléments de la vie privée des personnes. Dans ces circonstances, le contrôle du magistrat du parquet offre une garantie suffisante.

En revanche, la pénétration en secret dans un système informatique et sa mise sous surveillance restent soumises à l'intervention du juge d'instruction, conformément aux articles 90*ter* et suivants ou à l'article 89*ter* du Code d'instruction criminelle.

Par ailleurs, le transfert de cette mesure (c'est-à-dire l'extension de la recherche) de l'article 88*ter* vers l'article 39*bis* et donc du juge d'instruction vers le procureur du Roi se justifie par le fait que, avec le développement des nouvelles technologies, la distinction entre ce qui se trouve sur l'appareil et ce qui se trouve dans le cloud devient en partie artificielle.

Toutefois, cette modification doit être lue en combinaison avec le nouveau paragraphe 5 qui concerne l'utilisation de ' fausses clés ' etc. pour accéder aux données. Le dernier alinéa du paragraphe 5 prévoit que seul le juge d'instruction peut ordonner l'usage de ' fausses clés ' dans le cadre de l'application spécifique du § 3 » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1966/001, pp. 18-19).

B.14.1. Angesichts der bedeutenden Entwicklung der von Datenverarbeitungssystemen aus zugänglichen Netze und ihrer intensiven Nutzung durch die überwiegende Mehrheit der Bürger, sowohl um dort Dokumente und Daten zu speichern, die zu ihrem Privatleben gehören, einschließlich sehr persönlicher Dinge, als auch um miteinander zu kommunizieren, kann zum gegenwärtigen Zeitpunkt davon ausgegangen werden, dass eine Untersuchungsmaßnahme, die es ermöglicht, auf sämtliche Daten und Nachrichten zuzugreifen, die sich in den Netzen befinden, die mit einem Datenverarbeitungssystem verbunden sind, das einer Einzelperson gehört, einen Eingriff in ihr Recht auf Achtung des Privatleben darstellt, der mindestens vergleichbar mit den Eingriffen ist, die einerseits durch eine Durchsuchung in einem Haus oder an einem privaten Ort und andererseits durch ein Abhören ihrer Telefongespräche oder ein Abfangen ihrer Post verursacht werden.

B.14.2. Aufgrund der Artikel 87 und 88 des Strafprozessgesetzbuches ist für Haussuchungen der Untersuchungsrichter zuständig. Nach Artikel 88*sexies* desselben Gesetzbuches darf außer in Fällen der Entdeckung auf frischer Tat nur der Untersuchungsrichter Kenntnis vom Inhalt der Post nehmen, die einem Postbetreiber anvertraut und vom Prokurator des Königs in Anwendung von Artikel 46*ter* desselben Gesetzbuches abgefangen und beschlagnahmt wurde. Nach Artikel 90*ter* desselben Gesetzbuches kann der Untersuchungsrichter im Rahmen seiner Zuständigkeit, « der Öffentlichkeit nicht zugängliche Nachrichten oder Daten eines Datenverarbeitungssystems oder eines Teils davon anhand technischer Mittel [...] abfangen, von ihnen Kenntnis nehmen, sie durchsuchen und aufzeichnen oder die Suche in einem Datenverarbeitungssystem oder einem Teil davon ausweiten ».

B.14.3. Wie der Staatsrat in der Stellungnahme, die er zu der angefochtenen Bestimmung abgegeben hat, bemerkt hat, « ist der Untersuchungsrichter ein unabhängiger Magistrat, der eine objektive Untersuchung sowohl im belastenden als auch entlastenden Sinne führt, während die Staatsanwaltschaft eine am Strafprozess beteiligte Partei ist » (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-1966/001, S. 127).

B.14.4. Die Ermittlungshandlungen dürfen grundsätzlich nicht die individuellen Rechte und Freiheiten beeinträchtigen, sodass die Untersuchungsmaßnahmen, die im Laufe der strafrechtlichen Ermittlung durchgeführt werden und eine solche Beeinträchtigung mit sich bringen, nur im Rahmen einer gerichtlichen Untersuchung durchgeführt werden können. Zumindest dürfen die Handlungen, auf die sich Artikel 28*septies* des Strafprozessgesetzbuches bezieht, der die sogenannte « Mini-Untersuchung » regelt, nur mit der Genehmigung und unter der Kontrolle eines Untersuchungsrichters durchgeführt werden, auch wenn in der Sache keine gerichtliche Untersuchung eingeleitet wird.

B.14.5. Die Ermittlung ist gekennzeichnet durch ihre ausgesprochen geheime und nicht kontradiktorische Beschaffenheit, wobei die Betroffenen über weniger Garantie zum Schutz der Rechte der Verteidigung verfügen als während der gerichtlichen Untersuchung.

Zwar haben die direkt Betroffenen bereits während der Ermittlung das Recht, Zugang zur Strafakte zu beantragen (Artikel 21*bis* des Strafprozessgesetzbuches). Im Unterschied zur gerichtlichen Untersuchung (Artikel 61*ter* des Strafprozessgesetzbuches) ist dieses Recht auf Zugang zur Akte für die Ermittlung jedoch nicht verfahrensrechtlich geregelt, sodass die Staatsanwaltschaft - in Ermangelung von gesetzlich festgelegten Ablehnungsgründen - den Antrag auf Zugang zu einer Akte ohne weiteres ablehnen kann und kein Rechtsmittel gegen eine Verweigerungsentscheidung oder das Ausbleiben einer Entscheidung besteht. In seinem Entscheid Nr. 6/2017 vom 25. Januar 2017 hat der Gerichtshof geurteilt, dass dieses Fehlen eines Rechtsmittels gegen die Verweigerung oder das Fehlen einer Entscheidung der Staatsanwaltschaft in Bezug auf einen von einem Beschuldigten verfassten Antrag auf Zugang zu einer Akte in der Ermittlung gegen die Artikel 10 und 11 der Verfassung verstößt. Da diese Verfassungswidrigkeit ausreichend präzise und vollständig formuliert ist, damit Artikel 21*bis* des Strafprozessgesetzbuches unter Einhaltung der Referenznormen, auf deren Grundlage der Gerichtshof seine Kontrolle ausübt, angewandt werden kann, hat der Gerichtshof auch geurteilt, dass es in Erwartung des Auftretens des Gesetzgebers dem Richter obliegt, dem Verstoß gegen diese Normen ein Ende zu setzen, indem er Artikel 61*ter* des Strafprozessgesetzbuches sinngemäß anwendet.

Ferner verfügen die Betroffenen während der Ermittlung nicht über ein formales Recht, eine bestimmte Ermittlungshandlung zu beantragen, während das Recht, zusätzliche gerichtliche Untersuchungshandlungen zu beantragen, wohl dem Beschuldigten und der Zivilpartei während der gerichtlichen Untersuchung zuerkannt wird (Artikel 61*quinquies* des Strafprozessgesetzbuches). Die Betroffenen können zwar immer einen informellen Antrag an die Staatsanwaltschaft richten, doch diese ist keineswegs verpflichtet, auf einen solchen Antrag einzugehen, und die Parteien besitzen keinerlei Rechtsmittel gegen eine Verweigerungsentscheidung oder das Fehlen einer Entscheidung.

Schließlich gibt es während der Ermittlung keine Kontrolle von Amts wegen über die Regelmäßigkeit des Verfahrens durch einen unabhängigen und unparteilichen Richter, der die Akte von etwaigen Nichtigkeiten bereinigen kann, während eine solche Kontrolle wohl während der gerichtlichen Untersuchung besteht (Artikel 235*bis* des Strafprozessgesetzbuches).

B.14.6. Aus dem Vorstehenden ergibt sich, dass diese Ermittlungsmaßnahme, insofern die angefochtene Bestimmung es ermöglicht, dass die Ausweitung der Suche, die in einem beschlagnahmten Gerät oder einem Gerät, das beschlagnahmt werden könnte, begonnen wurde, auf ein Datenverarbeitungssystem, das sich an einem anderen Ort als das Gerät selbst befindet oder mit dem das Gerät verbunden ist, vom Prokurator des Königs ohne Beteiligung eines Untersuchungsrichters angeordnet wird, mit weniger Garantien für den Rechtsunterworfenen versehen ist, dessen Datenverarbeitungssystem Gegenstand der Untersuchungsmaßnahme ist, als die Haussuchung, die Öffnung der Post, das Abfangen von elektronischen Nachrichten und das Abhören von Telefongesprächen und die geheime Suche in einem Datenverarbeitungssystem.

B.15.1. Dieser Behandlungsunterschied wurde durch den Gesetzgeber mit dem nicht geheimen Charakter der Untersuchung gerechtfertigt:

« Même si l'intervention du juge d'instruction inclut une garantie essentielle en matière d'intrusion dans la vie privée, la modification de la loi est justifiée parce que l'article 39*bis* se limite aux recherches non secrètes. Comme il a été dit, l'article 39*bis* est utilisé de manière réactive à la suite du fait que l'on a pu s'emparer légalement d'un système informatique. Il n'y a en aucun cas d'approche ou d'exploitation secrète d'éléments de la vie privée des personnes. Dans ces circonstances, le contrôle du magistrat du parquet offre une garantie suffisante.

En revanche, la pénétration en secret dans un système informatique et sa mise sous surveillance restent soumises à l'intervention du juge d'instruction, conformément aux articles 90*ter* et suivants ou à l'article 89*ter* du Code d'instruction criminelle.

Par ailleurs, le transfert de cette mesure (c'est-à-dire l'extension de la recherche) de l'article 88*ter* vers l'article 39*bis* et donc du juge d'instruction vers le procureur du Roi se justifie par le fait que, avec le développement des nouvelles technologies, la distinction entre ce qui se trouve sur l'appareil et ce qui se trouve dans le cloud devient en partie artificielle » (*Doc. parl.*, 2015-2016, DOC 54-1966/001, p. 19).

B.15.2. Der in B.14.6 dargelegte Behandlungsunterschied beruht somit auf dem Kriterium des geheimen oder nicht geheimen Charakters der in den Netzen durchgeführten Suche, mit denen das beschlagnahmte Gerät oder das Gerät, das beschlagnahmt werden könnte, verbunden ist.

Der nicht geheime Charakter des Eingriffs in das Recht auf Achtung des Privatlebens der von der Maßnahme betroffenen Person ist durch die Pflicht gewährleistet, die dem Prokurator des Königs durch Paragraph 7 der angefochtenen Bestimmung auferlegt wird, den Verantwortlichen des Datenverarbeitungssystems, das Gegenstand der Untersuchung ist, « schnellstmöglich » zu informieren.

Da die Pflicht, den Verantwortlichen des Datenverarbeitungssystems der Suche zu informieren, dazu benutzt wird, den geheimen und den nicht geheimen Charakter einer Untersuchung voneinander zu unterscheiden und dies im Hinblick auf den Schutz der Rechtsunterworfenen erfolgt, ist davon auszugehen, dass die Mitteilung an den Verantwortlichen des Datenverarbeitungssystem auch den Verdächtigen betrifft, dessen in dem System gespeicherte Daten Gegenstand dieser Suche sind, wenn der Verdächtige nicht die tatsächliche Kontrolle über das fragliche Datenverarbeitungssystem hat.

B.15.3. Der Umstand, dass der Eingriff in das Recht auf Achtung des Privatlebens einer Person ohne deren Wissen vorgenommen wird, macht ihn noch schwerwiegender, was bedeutet, dass er mit den höchsten Garantien versehen sein muss und infolgedessen nur im Rahmen einer strafrechtlichen gerichtlichen Untersuchung durchgeführt werden darf (EuGHMR, 4. Dezember 2015, *Zakharov gegen Russland*, §§ 233, 249 und 259; 12. Januar 2016, *Szabó und Vissy gegen Ungarn*, § 77; 30. Mai 2017, *Trabajo Rueda gegen Spanien*, § 33). Der Umstand, dass dieselbe Untersuchungsmaßnahme der betroffenen Person mitgeteilt wurde, gegebenenfalls nachdem sie beendet wurde, beinhaltet jedoch ebenfalls einen erheblichen Eingriff in das Recht auf Achtung des Privatlebens dieser Person. Dass sie darüber informiert wurde, bedeutet nämlich nicht, dass sie dem zugestimmt hätte.

B.15.4. Durch das vorherige Eingreifen eines unabhängigen und unparteiischen Richters kann gewährleistet werden, dass der Eingriff in das Recht auf Achtung des Privatlebens im Verhältnis zu den Anforderungen von Artikel 22 der Verfassung und von Artikel 8 der Europäischen Menschenrechtskonvention steht.

Daher hat der Gerichtshof mit seinem Entscheid Nr. 202/2004 vom 21. Dezember 2004 geurteilt, dass die Observation mit technischen Mitteln mit dem Zweck, Einblick in eine Wohnung zu erlangen und für die diskrete Sichtkontrolle eines privaten Ortes, Maßnahmen sind, die hinsichtlich der Schwere des Eingriffs in das Recht auf Achtung vor dem Privatleben mit einer Haussuchung sowie mit Abhörungen und mit Aufzeichnungen von privaten Kommunikationen und Telekommunikationen verglichen werden können und nur unter den gleichen Bedingungen, das heißt im Rahmen einer gerichtlichen Untersuchung, genehmigt werden können.

Durch seinen Entscheid Nr. 178/2015 vom 17. Dezember 2015 hat der Gerichtshof zur Ausweitung der Suche in einem Datenverarbeitungssystem geurteilt:

« Die Ausweitung der Suche in einem Datenverarbeitungssystem unterliegt der vorherigen Genehmigung durch den Strafvollstreckungsrichter, der prüfen muss, ob die Erfordernisse bezüglich der Rechtmäßigkeit, der Verhältnismäßigkeit und der Subsidiarität erfüllt sind, und der insbesondere darüber wachen muss, dass die Grundrechte der Betreffenden nicht auf unverhältnismäßige Weise verletzt werden.

Um eine tatsächliche gerichtliche Kontrolle zu gewährleisten, muss der SVE-Magistrat, wenn er eine Genehmigung bei dem Strafvollstreckungsrichter beantragt, auch die Reichweite der Ausweitung der Suche in einem Datenverarbeitungssystem angeben, um zu verhindern, dass die Verletzung des Privatlebens potenziell unbegrenzt und folglich unverhältnismäßig ist (EuGHMR, 9. Dezember 2004, *Van Rossem* gegen Belgien, § 45), und damit eine Kontrolle darüber durch den Strafvollstreckungsrichter möglich ist. Eine andere Auslegung der angefochtenen Bestimmungen wäre nicht mit dem Recht auf Achtung des Privatlebens und der Wohnung vereinbar » (B.48.4).

Durch seinen Entscheid Nr. 148/2017 vom 21. Dezember 2017 hat der Gerichtshof zur Haussuchung einer Wohnung, die im Übrigen nicht unbedingt einen geheimen Charakter hat, geurteilt:

« Wegen der Schwere der dadurch verursachten Einmischung in das Recht auf Achtung des Privatlebens und die Unverletzlichkeit der Wohnung kann die Haussuchung bei dem heutigen Stand der Regelung bezüglich des Strafverfahrens nur erlaubt werden im Rahmen einer gerichtlichen Untersuchung, wobei die Betroffenen über ein organisiertes Recht verfügen, Zugang zur Akte und zusätzliche Untersuchungshandlungen zu beantragen, und wobei eine Aufsicht durch die Anklagekammer über die Regelmäßigkeit des Verfahrens vorgesehen ist.

Indem die Haussuchung, beim heutigen Stand der Regelung bezüglich des Strafverfahrens, in den Anwendungsbereich der Mini-Untersuchung aufgenommen wird, ohne zusätzliche Garantien zum Schutz der Rechte der Verteidigung vorzusehen, verletzt die angefochtene Bestimmung auf diskriminierende Weise das Recht auf Achtung des Privatlebens und das Recht auf die Unverletzlichkeit der Wohnung » (B.22.4).

B.15.5. Aus dem Vorstehenden ergibt sich, dass der Behandlungsunterschied zwischen den Personen, die Gegenstand einer Untersuchungsmaßnahme in den mit ihrem Datenverarbeitungssystem verbundenen Netzen sind, je nachdem, ob die Suche im Sinne der angefochtenen Bestimmung als geheim oder nicht geheim angesehen wird, nicht auf einem sachdienlichen Kriterium hinsichtlich des Grundsatzes beruht, dass im Laufe der strafrechtlichen Ermittlung durchgeführte Untersuchungsmaßnahmen, die eine Beeinträchtigung der individuellen Rechte und Freiheiten mit sich bringen, grundsätzlich nur im Rahmen einer gerichtlichen Untersuchung durchgeführt werden können (Artikel 28*bis* § 3 Absatz 1 des Strafprozessgesetzbuches).

B.16.1. Außerdem rechtfertigt der Umstand, dass der Prokurator des Königs, wenn der Zugriff auf die mit dem Datenverarbeitungssystem verbundenen Netze durch einen Schlüssel gesichert ist oder wenn die Daten in den Netzen oder in einem verbundenen Datenverarbeitungssystem kodiert oder verschlüsselt sind, nur mit Genehmigung des Untersuchungsrichters von falschen Schlüsseln oder Dekodierungs- oder Entschlüsselungstechniken Gebrauch machen kann, es auch nicht, dass der Eingriff in das Recht auf Achtung des Privatlebens, der in diesem Fall nicht geringer ist, nicht mit denselben Garantien versehen ist, wenn solche Sicherungen nicht installiert worden sind.

B.16.2. Zudem wurde die Übertragung der Zuständigkeit des Untersuchungsrichters auf den Prokurator des Königs durch die angefochtene Bestimmung nicht mit zusätzlichen Garantien versehen, die dazu bestimmt sind, das Privatleben und die Verteidigungsrechte der betroffenen Person wirksam zu schützen, und die geeignet sind, die Abschaffung des vorherigen Eingreifens eines unabhängigen und unparteiischen Richters auszugleichen (EuGHMR, 30. September 2014, *Prezhdarovi gegen Bulgarien*, §§ 45 bis 47; 30. Mai 2017, *Trabajo Rueda gegen Spanien*, § 37). In dieser Hinsicht geht aus der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte hervor, dass das Vorhandensein einer wirksamen Beschwerde davon abhängt, ob sie angemessen ist; der fragliche Rechtsbehelf muss daher in Bezug zu der geltend gemachten Verletzung stehen, um geeignete und gleichwertige Garantien zu bieten, die die fraglichen Rechte des Einzelnen gewährleisten. Daraus folgt, dass die nationale Beschwerdeinstanz befugt sein muss, im Wesentlichen über die auf die Konvention gestützte Beschwerde zu befinden, um zu entscheiden, ob der Eingriff in das Recht des Betroffenen auf Achtung seines Privatlebens mit Artikel 8 Absatz 2 im Einklang stand (EuGHMR, 1. April 2008, *Varga gegen Rumänien*, §§ 72-73; 3. Juli 2012, *Robathin gegen Österreich*, § 21; 30. September 2014, *Prezhdarovi gegen Bulgarien*, § 47; 2. April 2015, *Vinci Construction und GTM Génie Civil et Services gegen Frankreich*, §§ 66-67).

B.16.3. Artikel 28*sexies* des Strafprozessgesetzbuches ist zwar auf Maßnahmen anwendbar, die darin bestehen, in einem Datenverarbeitungssystem oder einem Teil davon gespeicherte Daten zu kopieren, unzugänglich zu machen und zu entfernen. Diese Bestimmung ermöglicht es jedem, dem durch eine Ermittlungshandlung in Bezug auf seine Güter Schaden zugefügt worden ist, beim Prokurator des Königs Aufhebung davon zu beantragen, gegen dessen Entscheidung bei der Anklagekammer Rechtsbehelf eingelegt werden kann. Dieses Verfahren, das ebenfalls vor dem Untersuchungsrichter anwendbar ist (Artikel 61*quater* § 1 des Strafprozessgesetzbuches), beschränkt sich also auf die Möglichkeit der betreffenden Person, die Aufhebung der Beschlagnahme und somit die Rückgabe der IT-Geräte und der Daten zu erreichen, die mit einer Suche in einem Datenverarbeitungssystem erlangt wurden. Sie verhindert aber nicht den Eingriff in das Privatleben, der stattgefunden hat und der durch die Rückgabe des Geräts und der darauf gespeicherten Daten nicht beseitigt wird, was nicht den in B.16.2 aufgeführten Anforderungen der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte entspricht.

B.16.4. Aufgrund der Schwere des Eingriffs in das Recht auf Achtung des Privatlebens, den sie mit sich bringt, kann die Maßnahme, die darin besteht, eine Suche in einem Datenverarbeitungssystem oder einem Teil davon, die in einem Datenverarbeitungssystem begonnen wurde, das beschlagnahmt wurde oder das vom Prokurator des Königs beschlagnahmt werden kann, auf ein Datenverarbeitungssystem oder einen Teil davon auszuweiten, das sich an einem anderen Ort als dem, wo die Suche durchgeführt wird, befindet, nur unter den gleichen Bedingungen wie denen, die für die in B.14.2 erwähnten Untersuchungshandlungen gelten, genehmigt werden.

B.17.1. Der erste und vierte Teil des ersten Klagegrunds ist in diesem Maße begründet.

Artikel 39*bis* Paragraph 3 des Strafprozessgesetzbuches, der durch Artikel 2 des angefochtenen Gesetzes vom 25. Dezember 2016 eingefügt wurde, ist für nichtig zu erklären. Um ein Rechtsvakuum hinsichtlich der betreffenden Suchmaßnahme zu vermeiden, ist auch Artikel 13 des Gesetzes vom 25. Dezember 2016, der untrennbar mit der angefochtenen Bestimmung verbunden ist, insofern er Artikel 88*ter* des Strafprozessgesetzbuches aufhebt, für nichtig zu erklären.

B.17.2. Um die Rechtsunsicherheit zu vermeiden, die bezüglich der Gültigkeit von Maßnahmen zur Ausweitung der Suchen in Datenverarbeitungssystemen, die gemäß der für nichtig erklärten Bestimmung durchgeführt wurden, entstehen würde, sind die Folgen dieser Bestimmung bis zum Datum der Veröffentlichung des vorliegenden Entscheids im *Belgischen Staatsblatt* aufrechtzuerhalten.

In Bezug auf die Information des Verantwortlichen des Datenverarbeitungssystems

B.18.1. Der dritte Teil des ersten Klagegrunds ist aus einer Verletzung der Artikel 12 und 14 der Verfassung in Verbindung mit Artikel 7 der Europäischen Menschenrechtskonvention abgeleitet. Er richtet sich gegen den Begriff des « Verantwortlichen des Datenverarbeitungssystems », der in Artikel 39*bis* Paragraph 7 des Strafprozessgesetzbuches enthalten ist, der durch Artikel 2 des angefochtenen Gesetzes vom 25. Dezember 2016 eingeführt wurde. Die klagenden Parteien werfen dem Gesetzgeber vor, den Inhalt dieses Begriffs nicht näher bestimmt zu haben, sodass die Identität der Personen, die über die Suche oder ihre Ausweitung informiert werden müssen, nicht eindeutig definiert und unklar sei.

B.18.2. Im Gegensatz zu dem, was der Ministerrat ausführt, führt der Umstand, dass die Rechtsvorschriften vor dem angefochtenen Gesetz bereits auf den « Verantwortlichen des Datenverarbeitungssystems » Bezug nahmen, nicht zur Unzulässigkeit wegen verspäteten Einreichens des dritten Teils des Klagegrunds. Durch die angefochtene Bestimmung hat der Gesetzgeber nämlich erneut Gesetzesbestimmungen auf diesem Gebiet erlassen und hat die dem Prokurator des Königs und dem Untersuchungsrichter auferlegte Pflicht, den « Verantwortlichen des Datenverarbeitungssystems » zu informieren, bestätigt.

B.19.1. Artikel 12 Absatz 2 der Verfassung bestimmt:

« Niemand darf verfolgt werden, es sei denn in den durch Gesetz bestimmten Fällen und in der dort vorgeschriebenen Form ».

Artikel 14 der Verfassung bestimmt:

« Eine Strafe darf nur aufgrund des Gesetzes eingeführt oder angewandt werden ».

Artikel 7 Absatz 1 der Europäischen Menschenrechtskonvention bestimmt:

« Niemand kann wegen einer Handlung oder Unterlassung verurteilt werden, die zur Zeit ihrer Begehung nach inländischem oder internationalem Recht nicht strafbar war. Ebenso darf keine höhere Strafe als die im Zeitpunkt der Begehung der strafbaren Handlung angedrohte Strafe verhängt werden ».

B.19.2. Insofern er das Legalitätsprinzip in Strafsachen gewährleistet, hat Artikel 7 Absatz 1 der Europäischen Menschenrechtskonvention eine ähnliche Tragweite wie die Artikel 12 Absatz 2 und 14 der Verfassung.

B.19.3. Aus den vorerwähnten Bestimmungen geht hervor, dass das Strafgesetz so formuliert werden muss, dass jeder zu dem Zeitpunkt, wo er ein Verhalten annimmt, wissen kann, ob dieses Verhalten strafbar ist oder nicht, und die gegebenenfalls die drohende Strafe kennen kann. Das Legalitätsprinzip und der Grundsatz der Vorhersehbarkeit gelten für das gesamte Strafverfahren. Somit soll durch die vorerwähnten Bestimmungen jegliche Gefahr eines willkürlichen Eingreifens der ausführenden oder der rechtsprechenden Gewalt bei der Festlegung und Anwendung der Strafen ausgeschlossen werden.

Das Legalitätsprinzip in Strafsachen reicht nicht so weit, dass der Gesetzgeber verpflichtet wäre, selbst jeden Aspekt der Unterstrafestellung, der Strafe oder des Strafverfahrens zu regeln. Es verhindert es insbesondere nicht, dass der Gesetzgeber dem Richter oder der Staatsanwaltschaft eine Ermessensbefugnis gewährt. Die allgemeine Beschaffenheit der Gesetzesbestimmungen, die Verschiedenartigkeit der Situationen, auf die sie Anwendung finden, und die Entwicklung der durch sie geahndeten Verhaltensweisen müssen nämlich berücksichtigt werden.

B.19.4. Im vorliegenden Fall wird nicht die Legalität der Unterstrafestellung oder der Strafe, sondern diejenige des Strafverfahrens in Frage gestellt.

Eine Ermächtigung der ausführenden Gewalt verletzt nicht dieses Prinzip, insofern die Ermächtigung ausreichend genau beschrieben ist und sich auf die Ausführung von Maßnahmen bezieht, deren wesentliche Elemente vorher durch den Dekretgeber festgelegt wurden.

Das Erfordernis der Vorhersehbarkeit des Strafverfahrens garantiert jedem Rechtsunterworfenen, dass er nur Gegenstand einer Ermittlung, einer gerichtlichen Untersuchung oder einer Verfolgung gemäß einem Verfahren sein kann, von dem er vor dessen Anwendung Kenntnis nehmen kann.

B.20. Da die angefochtene Bestimmung vorschreibt, den « Verantwortlichen des Datenverarbeitungssystems » über die Suche zu informieren, ermöglicht sie es dieser Person, die notwendigen Vorkehrungen zur Wahrung ihrer Rechte zu treffen, sodass dieser Begriff ein wesentliches Element des Strafverfahrens auf dem Gebiet von Suchen in den Datenverarbeitungssystemen ist.

B.21.1. Diesbezüglich hat die Gesetzgebungsabteilung des Staatsrates bemerkt:

« Mais la disposition ne donne pas une définition de ce qu'il faut entendre par ' le responsable du système informatique '.

Au sens de la recommandation n° R(95)13 [du Comité des ministres du Conseil de l'Europe du 11 septembre 1995], la notion englobe toutes les personnes qui, lors de la perquisition ou de la saisie, paraissent disposer formellement ou réellement du contrôle sur le système informatique, objet de la perquisition. Il peut s'agir du propriétaire du système, d'un opérateur de ce système ou même du gardien (locataire ou occupant) des locaux abritant le système informatique.

La disposition en projet doit, en conséquence, définir expressément les personnes concernées par l'information.

Par ailleurs, la saisie de données peut également concerner des tierces personnes. C'est ainsi que la recommandation n° R(95)13, précitée, invite les Etats membres à organiser ce type d'information et ce dans le respect des impératifs de l'enquête.

Cette exigence est importante car, en vertu des articles 28*sexies* et 61*quater* du Code d'instruction criminelle, toute personne qui s'estime lésée par un acte d'information ou par un acte d'instruction relatif à ses biens peut en demander la levée soit au procureur du Roi, soit au juge d'instruction » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1966/001, pp. 129-130).

B.21.2. In der Begründung ist zu dieser Bemerkung angegeben:

« Le Conseil d'Etat estime également (et renvoie à cet égard à l'avis n° 28 029/2 du 31 mai 1999) que le texte de l'avant-projet de loi doit lui-même contenir une définition du ' responsable du système informatique '. Le but de la communication de la mesure est toutefois d'établir clairement qu'il ne s'agit pas d'une mesure secrète (cf. la compétence de perquisitionner). La terminologie de l'avant-projet comporte dans cette optique une certaine souplesse pour ce qui est de la personne à contacter : en effet, il n'est pas possible de déterminer *a priori* pour tous les cas et de manière univoque qui exerce le contrôle réel ou juridique sur le système (*Doc. parl.*, Chambre, 1999-2000, n° 0213/001, p. 21) » (*Doc. parl.*, 2015-2016, DOC 54-1966/001, p. 24).

B.22.1. Über die Feststellung des geheimen oder nicht geheimen Charakters der Untersuchungsmaßnahme hinaus hat die Mitteilung der Durchführung dieser Maßnahme außerdem zur Folge, dass es der betroffenen Person oder den betroffenen Personen möglich ist, die Verfahrensrechte wahrzunehmen, die insbesondere dazu dienen, die Verhältnismäßigkeit der in das Recht auf Achtung des Privatlebens dieser Person oder Personen verursachten Einmischung zu kontrollieren.

B.22.2. Daraus ergibt sich, dass der Begriff des « Verantwortlichen des Datenverarbeitungssystems » als Bezeichnung der Person oder Personen verstanden werden muss, die für die Daten oder Nachrichten, die auf dem beschlagnahmten Gerät oder dem Gerät, das beschlagnahmt werden kann, gespeichert sind, und für die Daten und Nachrichten, von denen über die Netze Kenntnis genommen werden kann, die von der Ausweitung der in dem vorerwähnten Gerät begonnenen Suche betroffen sind, verantwortlich sind, wobei diese Person oder Personen nicht zwangsläufig die Eigentümer oder Besitzer der betreffenden Geräte sind. Wie in B.15.2 erwähnt, bezieht sich dieser Begriff ebenfalls auf den Verdächtigen, dessen Daten Gegenstand der Suche sind, wenn er nicht selbst die tatsächliche Kontrolle über das fragliche Datenverarbeitungssystems ausübt.

B.23. Vorbehaltlich der Auslegung des Begriffs des « Verantwortlichen des Datenverarbeitungssystems » wie in B.15.2 und B.22.2 angegeben, ist der dritte Teil des ersten Klagegrunds unbegründet.

In Bezug auf Datenverarbeitungssysteme von Rechtsanwälten und Ärzten

B.24.1. Der fünfte Teil des ersten Klagegrunds ist aus einer Verletzung der Artikel 10, 11 und 22 der Verfassung in Verbindung mit Artikel 6 der Europäischen Menschenrechtskonvention abgeleitet. Die klagenden Parteien werfen dem Gesetzgeber vor, in Artikel 39*bis* des Strafprozessgesetzbuches, der die nicht geheimen Suchen in einem Datenverarbeitungssystem regelt, keine gleichwertigen Garantien wie die, die in Artikel 90*octies* desselben Gesetzbuches festgelegt sind und die die geheimen Suchen in einem Datenverarbeitungssystem betreffen, vorgesehen zu haben.

B.24.2. Artikel 90*octies* des Strafprozessgesetzbuches bestimmt:

« § 1. Die Maßnahme darf sich nur dann auf zu Berufszwecken benutzte Räumlichkeiten, den Wohnort, Kommunikationsmittel oder Datenverarbeitungssysteme eines Rechtsanwalts oder Arztes beziehen, wenn dieser selber verdächtigt wird, eine der in Artikel 90*ter* erwähnten Straftaten begangen zu haben oder daran beteiligt gewesen zu sein, oder wenn genaue Tatsachen vermuten lassen, dass Dritte, die verdächtigt werden, eine der in Artikel 90*ter* erwähnten Straftaten begangen zu haben, seine Räumlichkeiten, seinen Wohnort, seine Kommunikationsmittel oder seine Datenverarbeitungssysteme benutzen.

§ 2. Die Maßnahme darf nicht durchgeführt werden, ohne dass - je nach Fall - der Präsident der Rechtsanwaltskammer oder der Vertreter der provinzialen Ärztekammer davon in Kenntnis gesetzt worden ist.

Diese Personen unterliegen der Schweigepflicht. Jegliche Verletzung der Schweigepflicht wird gemäß Artikel 458 des Strafgesetzbuches geahndet.

§ 3. Der Untersuchungsrichter beurteilt nach Konzertierung mit dem Präsidenten der Rechtsanwaltskammer oder dem Vertreter der provinzialen Ärztekammer, welche Teile der in Artikel 90*sexies* § 3 erwähnten der Öffentlichkeit nicht zugänglichen Nachrichten oder Daten eines Datenverarbeitungssystems, die er für die Untersuchung als relevant erachtet, unter das Berufsgeheimnis fallen und welche nicht.

Nur die Teile der Nachrichten oder Daten, die in Absatz 1 erwähnt sind und nicht unter das Berufsgeheimnis fallen, werden niedergeschrieben oder wiedergegeben und gegebenenfalls übersetzt. Der Untersuchungsrichter lässt davon ein Protokoll erstellen. Die Dateien mit diesen Nachrichten oder Daten werden unter versiegeltem Umschlag bei der Kanzlei hinterlegt.

Alle anderen Nachrichten oder Daten werden in einer anderen Datei unter getrenntem, versiegeltem Umschlag bei der Kanzlei hinterlegt ».

B.24.3. Diese Bestimmung wurde durch Artikel 22 des angefochtenen Gesetzes in das Strafprozessgesetzbuch aufgenommen. In der Begründung ist hierzu angegeben:

« L'exception pour les avocats et les médecins était dictée par la considération que ces catégories professionnelles sont par excellence exposées au risque d'être confrontées à des suspects avec qui, en raison de leur situation professionnelle, elles entretiennent une relation de confiance qui doit tout particulièrement être préservée. Il s'agit de la clause de protection classique telle qu'elle apparaît également dans des mesures d'investigation similaires comme l'ouverture de courrier (article 88*sexies* du Code d'instruction criminelle), une observation afin d'avoir une vue dans un domicile (article 56*bis* du Code d'instruction criminelle) ou un contrôle visuel discret (article 89*ter* du Code d'instruction criminelle) » (*Doc. parl.*, 2015-2016, DOC 54-1966/001, pp. 72-73).

B.25. Das Berufsgeheimnis, an das Rechtsanwälte und Ärzte gebunden sind, dient nicht dazu, ihnen irgendein Vorrecht zu gewähren, sondern bezweckt hauptsächlich, das Grundrecht auf Achtung des Privatlebens derjenigen, die sie in bisweilen sehr persönlichen Dingen ins Vertrauen ziehen, zu schützen. Zudem genießen die vertraulichen Informationen, die einem Rechtsanwalt bei der Ausübung seines Berufes und wegen dieser Eigenschaft anvertraut werden, in bestimmten Fällen auch den Schutz, der sich für den Rechtsuchenden aus den Garantien ergibt, die in Artikel 6 der Europäischen Menschenrechtskonvention festgelegt sind, da die dem Rechtsanwalt auferlegte Regel des Berufsgeheimnisses ein fundamentales Element der Rechte der Verteidigung des Rechtsuchenden, der ihn ins Vertrauen zieht, ist.

B.26.1. Es ist nicht gerechtfertigt, dass die Bestimmung zur Wahrung des Berufsgeheimnisses von Rechtsanwälten und Ärzten nur vorgesehen ist, wenn die Suche in einem von ihnen zu Berufszwecken genutzten Datenverarbeitungssystem geheim durchgeführt wird, und nicht, wenn sie ihnen mitgeteilt wird. Der Eingriff in das Recht auf Achtung des Privatlebens von Personen, die ihnen unter das Berufsgeheimnis fallende Informationen anvertraut haben, erfolgt nämlich in der gleichen Weise, unabhängig davon, ob die Suche ohne Wissen des betroffenen Rechtsanwalts oder Arztes durchgeführt wird oder nicht.

B.26.2. Es ist richtig - wie es der Ministerrat ausführt -, dass, wenn die Suche in einem Datenverarbeitungssystem im Rahmen einer Haussuchung stattfindet, die Bestimmungen zu Haussuchungen in den beruflichen Räumlichkeiten von Rechtsanwälten oder Ärzten anwendbar sind und es ermöglichen, das Berufsgeheimnis zu gewährleisten. Die Möglichkeiten der nicht geheimen Suche, die durch Artikel 39*bis* des Strafprozessgesetzbuches vorgesehen sind, gehen jedoch über diesen konkreten Fall hinaus und können nicht nur im Fall der Haussuchung in beruflichen Räumlichkeiten angewandt werden.

B.27. Der fünfte Teil des ersten Klagegrunds ist begründet. Artikel 39*bis* des Strafprozessgesetzbuches, der durch Artikel 2 des angefochtenen Gesetzes eingeführt wurde, ist für nichtig zu erklären, insofern er keine besondere Bestimmung im Hinblick auf die Wahrung des Berufsgeheimnisses von Ärzten und Rechtsanwälten vorsieht.

Um die Rechtssicherheit in Bezug auf durchgeführte Suchen in Datenverarbeitungssystemen, die Ärzten oder Rechtsanwälten gehören, zu gewährleisten, müssen die Folgen der für nichtig erklärten Bestimmung, wie im Tenor angegeben, aufrechterhalten werden.

In Bezug auf den zweiten Klagegrund

Was die angefochtene Bestimmung betrifft

B.28.1. Der zweite Klagegrund bezieht sich auf Artikel 7 des Gesetzes vom 25. Dezember 2016, durch den in das Strafprozessgesetzbuch ein Artikel 46*sexies* eingeführt wird, der bestimmt:

« Art. 46*sexies*. § 1. Bei der Ermittlung von Verbrechen und Vergehen kann der Prokurator des Königs, wenn die Untersuchung dies erfordert und wenn die anderen Untersuchungsmittel nicht auszureichen scheinen, um die Wahrheit herauszufinden, die in Absatz 2 erwähnten Polizeidienste dazu ermächtigen, im Internet gegebenenfalls unter einer fiktiven Identität Kontakt zu einer oder mehreren Personen zu unterhalten, bei denen es schwerwiegende Indizien dafür gibt, dass sie Straftaten begehen oder begehen könnten, die eine Hauptkorrektionalgefängnisstrafe von einem Jahr oder eine schwerere Strafe zur Folge haben können.

Der König bestimmt die Bedingungen, auch für die Ausbildung, und die Modalitäten zur Bestimmung der Polizeidienste, die ermächtigt sind, die in vorliegendem Artikel erwähnte Maßnahme durchzuführen.

Unter außergewöhnlichen Umständen und mit der ausdrücklichen Erlaubnis des Prokurators des Königs kann der Beamte der in Absatz 2 erwähnten Polizeidienste im Rahmen eines bestimmten Einsatzes kurzzeitig auf die Fachkompetenz einer Person zurückgreifen, die nicht den Polizeidiensten angehört, wenn dies für das Gelingen seines Auftrags als absolut notwendig erscheint. Die Erlaubnis und die Identität dieser Person werden in der in § 3 Absatz 7 erwähnten Akte aufbewahrt.

Vorliegender Artikel findet keine Anwendung auf die persönliche Interaktion von Polizeibeamten bei der Ausführung ihrer gerichtspolizeilichen Aufträge mit einer oder mehreren Personen im Internet, die nur eine gezielte Überprüfung oder eine Festnahme zum unmittelbaren Zweck hat, und zwar ohne Verwendung einer glaubwürdigen fiktiven Identität.

§ 2. Die in § 1 erwähnte Maßnahme wird vom Prokurator des Königs durch eine vorherige schriftliche und mit Gründen versehene Erlaubnis angeordnet. Diese Erlaubnis gilt für einen Zeitraum von drei Monaten, unbeschadet einer Erneuerung.

Im Dringlichkeitsfall kann die Erlaubnis mündlich erteilt werden. Sie muss so schnell wie möglich in der in Absatz 1 vorgesehenen Form bestätigt werden.

§ 3. Straffrei bleiben Polizeibeamte, die im Rahmen ihres Auftrags und im Hinblick auf dessen Gelingen oder zur Gewährleistung ihrer eigenen Sicherheit oder der anderer von der Maßnahme betroffenen Personen absolut notwendige Straftaten mit ausdrücklicher Zustimmung des Prokurators des Königs begehen.

Diese Straftaten dürfen nicht schwerwiegender sein als die Straftaten, für die die Maßnahme angewandt wird, und müssen notwendigerweise im Verhältnis zum angestrebten Ziel stehen.

Die Absätze 1 und 2 sind ebenfalls auf die Personen anwendbar, die direkte zur Durchführung dieses Auftrags notwendige Hilfe oder Unterstützung geleistet haben, sowie auf die in § 1 Absatz 3 erwähnten Personen.

Straffrei bleibt auch der Magistrat, der unter Einhaltung des vorliegenden Gesetzbuches einen Polizeibeamten und die in Absatz 3 erwähnten Personen dazu ermächtigt, im Rahmen der Durchführung der Maßnahme Straftaten zu begehen.

Die Polizeibeamten teilen dem Prokurator des Königs die Straftaten, die sie selbst oder die in Absatz 3 erwähnten Personen zu begehen beabsichtigen, vor Durchführung der Maßnahme schriftlich mit.

Wenn diese Notifizierung nicht vorab hat erfolgen können, informieren die Polizeibeamten den Prokurator des Königs unverzüglich über die Straftaten, die sie selbst oder die in Absatz 3 erwähnten Personen begangen haben, und bestätigen dies anschließend schriftlich.

Der Prokurator des Königs vermerkt in einer getrennten schriftlichen Entscheidung die Straftaten, die von den Polizeidiensten und den in Absatz 3 erwähnten Personen im Rahmen der von ihm angeordneten Maßnahme begangen werden dürfen. Diese Entscheidung wird in einer getrennten und vertraulichen Akte aufbewahrt. Er hat als Einziger Zugang zu dieser Akte, unbeschadet des in Artikel 56*bis* beziehungsweise in den Artikeln 235*ter* § 3 und 235*quater* § 3 erwähnten Rechts auf Einsichtnahme des Untersuchungsrichters und der Anklagekammer. Der Inhalt dieser Akte fällt unter das Berufsgeheimnis.

§ 4. Der mit der Ermittlung beauftragte Gerichtspolizeioffizier erstellt ein Protokoll über die verschiedenen Phasen der Durchführung dieser Maßnahme, einschließlich der relevanten Kontakte. Diese Protokolle werden der Akte spätestens nach Beendigung der Maßnahme beigefügt.

Die in § 1 erwähnten Kontakte werden mit den geeigneten technischen Mitteln registriert und spätestens nach Beendigung der Maßnahme der Akte beigefügt oder in elektronischer oder nicht elektronischer Form bei der Kanzlei hinterlegt.

§ 5. Der Prokurator des Königs ist mit der Ausführung der Genehmigungen in Bezug auf die in § 1 Absatz 1 erwähnte Maßnahme, die im Rahmen einer gerichtlichen Untersuchung gemäß Artikel 56*bis* vom Untersuchungsrichter erteilt wurden, beauftragt.

Der Prokurator des Königs vermerkt zu diesem Zeitpunkt in einer getrennten schriftlichen Entscheidung die Straftaten, die von den Polizeidiensten und den in § 3 Absatz 3 erwähnten Personen im Rahmen der vom Untersuchungsrichter angeordneten Maßnahme begangen werden dürfen. Diese Entscheidung wird in der in § 3 Absatz 7 erwähnten Akte aufbewahrt ".

B.28.2. In der Begründung zu dieser Bestimmung heißt es:

« Cet article introduit la possibilité de procéder à une infiltration ou à une interaction sur Internet qui ne vise pas uniquement une vérification ciblée ou une arrestation.

Étant donné que l'infiltration sur Internet a un caractère moins intrusif que l'infiltration ' classique ' et que les différents contacts durant l'exécution de cette mesure sont enregistrés, un régime plus souple est justifié » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1966/001, p. 36).

Was den Unterschied der Regelung gegenüber der Infiltrierung in der realen Welt betrifft

B.29.1. Der erste Teil des zweiten Klagegrunds ist abgeleitet aus einer Verletzung der Artikel 10 und 11 der Verfassung. Die klagenden Parteien sind der Auffassung, dass das aus dem virtuellen oder realen Charakter der Infiltrierungsmaßnahme hergeleitete Kriterium nicht rechtfertigen kann, dass einerseits der Prokurator des Königs im Rahmen einer Infiltrierung im Internet keine Maßnahmen zur Gewährleistung der Sicherheit sowie der körperlichen, geistigen und moralischen Unversehrtheit des Infiltranten ergreifen kann, und dass andererseits die Kontrolle über die Anwendung der Methode, die in den Artikeln 235*ter* und 235*quater* des Strafprozessgesetzbuches vorgesehen ist, nicht auf die Infiltrierung im Internet anwendbar ist.

B.29.2. Da die klagenden Parteien ein Interesse an der Nichtigerklärung der angefochtenen Bestimmung haben, ist die Frage nach ihrem Interesse am ersten Teil dieses Klagegrunds entgegen den Ausführungen des Ministerrats nicht zu stellen.

Die Sicherheit der « Cyberinfiltranten »

B.30.1. In Artikel 47*octies* des Strafprozessgesetzbuches, der sich auf die Infiltrierung in der realen Welt bezieht, ist in Paragraph 2 Absatz 3 präzisiert, dass der Prokurator des Königs, wenn dies gerechtfertigt ist, die Genehmigung zur Ergreifung der notwendigen Maßnahmen zur Gewährleistung der Sicherheit sowie der körperlichen, geistigen und moralischen Unversehrtheit des Infiltranten erteilt.

B.30.2. In Beantwortung einer Bemerkung des Staatsrates zu diesem Punkt ist in der Begründung erläutert:

« Le Conseil d'Etat se demande aussi, au point 25 de l'avis, pourquoi le procureur du Roi, contrairement à ce qui est le cas pour l'infiltration classique, ne peut pas prendre des mesures en vue de garantir la sécurité, ainsi que l'intégrité physique, psychique et morale du cyberinfiltrant (voir l'article 47*octies*, § 2, dernier alinéa, du Code d'instruction criminelle). Le gouvernement estime que ceci est superflu lorsqu'une infiltration est réalisée uniquement via Internet. Il n'y a tout d'abord pas de contact physique avec d'éventuels suspects. En outre, il va de soi que les cyberinfiltrants continueront de faire l'objet d'un suivi. Aucune base légale n'est requise pour garantir leur intégrité psychique et morale » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1966/001, p. 42).

B.30.3. Die allein im Internet durchgeführte Infiltrierung weist nicht die gleichen Gefahren für die körperliche Sicherheit des Infiltranten auf wie eine Infiltrierung in der realen Welt. Der Gesetzgeber konnte daher vernünftigerweise den Standpunkt vertreten, dass es nicht notwendig ist, die gleichen Möglichkeiten zur Ergreifung von Maßnahmen zur Gewährleistung der körperlichen Sicherheit des Infiltranten, der nur in der virtuellen Welt handelt, vorzusehen. Der beanstandete Behandlungsunterschied beruht somit in diesem Zusammenhang auf einem sachdienlichen Kriterium.

B.30.4. Zudem untersagt die Bestimmung nicht die Anwendung von Maßnahmen zur Begleitung und psychologischen Unterstützung innerhalb der betroffenen Polizeidienste, die für die Situation der Personen geeignet sind, die die Infiltrierungen im Internet durchführen, sodass die angefochtenen Bestimmung keine unverhältnismäßigen Folgen für die Cyberinfiltranten hinsichtlich ihrer geistigen und moralischen Sicherheit hat.

Die Kontrolle durch die Anklagekammer

B.31.1. Durch Artikel 235*ter* des Strafprozessgesetzbuches wird die Anklagekammer beauftragt, unter anderem die Anwendung der Infiltrierungen in der realen Welt zu kontrollieren. Aufgrund derselben Bestimmung kontrolliert die Anklagekammer die Anwendung der Infiltrierungen im Internet nur, wenn in diesem Rahmen eine vertrauliche Akte angelegt worden ist.

Eine vertrauliche Akte muss bei der Genehmigung einer Infiltrierung in der realen Welt immer angelegt werden. Sie enthält die Genehmigung zur Infiltrierung, die Entscheidungen zur Änderung, Ergänzung oder Verlängerung sowie die Berichte, die vom Gerichtspolizeioffizier über jede Phase der Durchführung der Infiltrierungen erstellt werden, die er leitet. Hingegen muss bei einer Infiltrierung im Internet eine vertrauliche Akte nur in zwei Fällen angelegt werden: wenn der Infiltrant auf die Fachkompetenz einer nicht den Polizeidiensten angehörenden Person zurückgreift und wenn der Prokurator des Königs die Begehung einer Straftat genehmigt.

B.31.2. Die Erstellung der vertraulichen Akte rührt aus der Notwendigkeit her, in bestimmten Strafprozessen die Anonymität von Zeugen zu wahren oder die eingesetzten Ermittlungsmethoden geheim zu halten; diese Interessen und die Verteidigungsrechte des Angeklagten, die grundsätzlich beinhalten, dass dieser jedes gegen ihn verwandte Beweismittel in Kenntnis des Sachverhalts anfechten kann, müssen gegeneinander abgewogen werden. Die Beteiligung der Anklagekammer aufgrund der Artikel 235*ter* und 235*quater* des Strafprozessgesetzbuches bezieht sich besonders auf die vertrauliche Akte und stellt die Garantie dafür dar, dass ein unabhängiger und unparteiischer Richter eine Kontrolle über die Ordnungsmäßigkeit der Anwendung von besonderen Ermittlungsmethoden und der Beweise, die mit ihnen erlangt wurden, ausübt, wenn die vorerwähnten Interessen es rechtfertigen, dass der Angeklagte keinen Zugang zu der gesamten Strafakte hat.

B.31.3. Im Gegensatz zu dem, was in der realen Welt der Fall ist, werden aufgrund von Paragraph 4 Absatz 2 der angefochtenen Bestimmung alle Kontakte im Rahmen der Infiltrierung im Internet registriert und der Akte beigefügt oder bei der Kanzlei hinterlegt. Personen, die auf der Grundlage von Beweisen verfolgt werden, die im Laufe einer Infiltrierung im Internet gewonnen wurden, haben also Zugang zu der gesamten Durchführung der Infiltrierung. Sie sind in der Lage, den Einsatz dieser Methode und ihre Ausführungsmodalitäten anzufechten und sie können das Untersuchungsgericht oder das erkennende Gericht auffordern, deren Ordnungsmäßigkeit zu kontrollieren. Es ist also in diesem Fall nicht notwendig, dass eine vertrauliche Akte angelegt und dass eine besondere Kontrolle über sie durch die Anklagekammer ausgeübt wird. Der Behandlungsunterschied beruht in diesem Zusammenhang ebenfalls auf einem sachdienlichen Kriterium.

B.31.4. Der erste Teil des zweiten Klagegrunds ist unbegründet.

Was die Modalitäten zur Bestimmung der Polizeidienste betrifft, die ermächtigt sind, eine Infiltrierung im Internet durchzuführen

B.32.1. Der zweite Teil des zweiten Klagegrunds ist aus einer Verletzung der Artikel 12 und 14 der Verfassung in Verbindung mit Artikel 6 der Europäischen Menschenrechtskonvention abgeleitet und richtet sich gegen Paragraph 1 Absatz 2 des angefochtenen Artikels 7. Die klagenden Parteien werfen dem Gesetzgeber vor, dem König unter Verstoß gegen das Legalitätsprinzip in Strafsachen die Befugnis erteilt zu haben, die Modalitäten zur Bestimmung der Polizeidienste festzulegen, die ermächtigt sind, die Infiltrierungsmaßnahme im Internet durchzuführen.

B.32.2. In der Begründung ist zu dieser Ermächtigung angegeben:

« S'agissant des services de police qui vont pouvoir réaliser la nouvelle mesure, il n'est pas nécessaire d'avoir un régime aussi strict que pour l'infiltration telle qu'elle existe actuellement. Cette dernière est réservée aux membres des unités spéciales de la police fédérale (DSU). Cela est justifié par la dangerosité de la mesure, y compris et surtout pour l'agent infiltrant. Cette limitation n'est pas justifiée pour la mesure se déroulant uniquement sur Internet. Cela ne signifie toutefois pas que tout enquêteur pourra se voir charger d'exécuter une telle interaction ou infiltration. Seuls les services de police spécifiquement désignés pourront exécuter la mesure. Une formation spécifique sera prévue tant pour protéger la vie privée des personnes visées que pour assurer le bon déroulement des enquêtes. Dans l'avant-projet, cette désignation était déléguée au ministre de la Justice. Le Conseil d'Etat observe qu'une telle délégation n'est pas autorisée et que les services de police compétents devraient être repris dans la loi. Le gouvernement fait remarquer qu'une telle délégation au ministre de la Justice existe déjà dans le cadre de l'application des méthodes particulières de recherche (art. 47*ter*, § 1er, alinéa 2, CIC) et qu'il n'appartient pas au législateur d'élaborer un règlement détaillé. Une formation spécifique sera en effet prévue pour les services de police visés, en vue aussi bien de la protection de la vie privée des personnes visées que de l'assurance du bon déroulement des enquêtes. Pour ces raisons, le gouvernement prend l'option de faire déterminer les conditions, y compris pour ce qui concerne la formation, et modalités de la désignation des services de police compétents par le Roi » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1966/001, p. 40).

B.33.1. Indem die Artikel 12 Absatz 2 und 14 der Verfassung der gesetzgebenden Gewalt die Zuständigkeit verleihen, einerseits festzulegen, in welchen Fällen und in welcher Form eine Strafverfolgung möglich ist, und andererseits ein Gesetz anzunehmen, aufgrund dessen eine Strafe festgelegt und angewandt werden kann, gewährleisten sie jedem Rechtsuchenden, dass ein Verhalten nur strafbar gemacht werden und eine Strafe nur auferlegt werden kann auf der Grundlage von Regeln, die durch eine demokratisch gewählte beratende Versammlung angenommen wurden.

B.33.2. Das Legalitätsprinzip in Strafsachen geht nicht soweit, dass es den Gesetzgeber verpflichtet, jeden Aspekt des Strafverfahrens selbst zu regeln. Eine Ermächtigung der ausführenden Gewalt verletzt nicht dieses Prinzip, insofern die Ermächtigung ausreichend genau beschrieben ist und sich auf die Ausführung von Maßnahmen bezieht, deren wesentliche Elemente vorher durch den Gesetzgeber festgelegt wurden.

B.34.1. Im vorliegenden Fall kann angenommen werden, dass der Gesetzgeber der Auffassung war, es sei notwendig, den König zu ermächtigen, die für die Durchführung von Infiltrierungen im Internet zuständigen Polizeidienste zu bestimmen. In einem sich fortwährend weiterentwickelnden Bereich wie dem Internet ist es in der Tat angezeigt, dass eine gewisse Flexibilität es den Behörden ermöglicht, den Inhalt der Ausbildung, mit der die Polizisten die Infiltrierungsmaßnahme im Internet durchführen können, regelmäßig anzupassen, was ebenfalls voraussetzt, die Bestimmung der ermächtigten Polizeioffiziere entsprechend der Ausbildungen, über die die Mitglieder der betroffenen Dienste verfügen und die sie absolviert haben, anpassen zu können.

Außerdem legt Artikel 46*sexies* des Strafprozessgesetzbuches die Bedingungen fest, unter denen die Infiltrierung im Internet angeordnet werden kann. Der Gesetzgeber hat durch die angefochtene Bestimmung den König ermächtigt, Bestimmungen zu erlassen, die sich auf Maßnahmen beziehen, deren wesentliche Elemente er also selbst festgelegt hat.

B.34.2. Der zweite Teil des zweiten Klagegrunds ist unbegründet.

Was den Ausschluss von bestimmten zielgerichteten Maßnahme aus dem Begriff der Infiltrierung betrifft

B.35.1. Der dritte Teil des zweiten Klagegrunds ist aus einer Verletzung der Artikel 12 und 14 der Verfassung abgeleitet und richtet sich gegen Artikel 46*sexies* Paragraph 1 Absatz 4 des Strafprozessgesetzbuches. Die klagenden Parteien werfen dem Gesetzgeber vor, dass er es unter Verstoß gegen das Legalitätsprinzip in Strafsachen unterlassen hat, zu definieren, welche im Internet durchgeführten Ermittlungshandlungen nicht vom Prokurator des Königs erlaubt werden müssen und somit auf Initiative der Polizisten vorgenommen werden können. Sie sind der Auffassung, dass es der Ausdruck « Interaktion, die nur eine gezielte Überprüfung oder eine Festnahme zum unmittelbaren Zweck hat, » den Gerichtspolizeioffizieren ermöglicht, die strengen Bedingungen für die Infiltrierung im Internet zu umgehen oder zu missachten.

B.35.2. Das in Artikel 12 Absatz 2 der Verfassung festgelegte Erfordernis der Vorhersehbarkeit des Strafverfahrens garantiert jedem Rechtsunterworfenen, dass er nur Gegenstand einer Ermittlung, einer gerichtlichen Untersuchung oder einer Verfolgung gemäß einem Verfahren sein kann, von dem er vor dessen Anwendung Kenntnis nehmen kann.

B.36. In der Begründung zu der angefochtenen Bestimmung ist angegeben:

« Cette précision vise à éviter de créer une situation où les services de police voient leur capacité d'action sur Internet réduite par rapport à ce qui existe actuellement que ce soit sur Internet ou dans le monde physique » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1966/001, p. 38).

Die folgenden Beispiele werden anschließend genannt: ein Kontakt für die Vereinbarung eines Treffens, um einen Gegenstand anzusehen, der über eine « Kleinanzeige » zum Verkauf angeboten wurde, die in einer Zeitung veröffentlicht oder auf einer Internetseite für den Verkauf von Gebrauchtartikeln platziert wurde; eine kurze Interaktion mit einer Person, die eine Nachricht im Internet gepostet hat, um festzustellen, ob es sich um eine ernsthaft radikalisierte Person oder einen unbedeutenden Witzbold handelt; die Festlegung eines Treffpunkts mit einer Person, um sie festzunehmen zu können. In dem Text wird erläutert, dass in diesen Fällen der Polizist seine Stellung nicht erwähnt, aber auch keine falsche Identität benutzt, und dass diese Art der Interaktion « sich nur auf einen spezifischen und sehr beschränkten Aspekt bezieht » (ebd., S. 39).

B.37.1. Aus dem Text der angefochtenen Bestimmung, der durch die Präzisierungen in der vorerwähnten Begründung erläutert wird, ist ausreichend ersichtlich, dass die Infiltrierung im Internet, die nur mit der Genehmigung des Prokurators des Königs durchgeführt werden kann, in der « Unterhaltung » von Kontakten mit einem oder mehreren Verdächtigen unter Vorspiegelung einer fiktiven Identität besteht. Ebenso definiert Artikel 47*octies* des Strafprozessgesetzbuches, der sich auf die Infiltrierung in der realen Welt bezieht, diese als den « unter einer fiktiven Identität unterhaltenen dauerhaften Kontakt » zu einem oder mehreren Verdächtigen. Die Infiltrierung in diesen beiden Formen setzt also einerseits die Entwicklung einer glaubwürdigen fiktiven Identität für den Infiltranten und andererseits eine Interaktion von einer gewissen Dauer mit einer oder mehreren Personen voraus, die im Verdacht

stehen, Straftaten einer bestimmten Schwere zu begehen oder begehen zu können. Punktuelle Kontakte, um ein Treffen zu vereinbaren oder eine gezielte Überprüfung vorzunehmen, die es der Gerichtspolizei ermöglichen, gemäß Artikel 15 des Gesetzes vom 5. August 1992 über das Polizeiamt ihre Aufgaben zu erfüllen, fallen nicht unter diese Definition und müssen daher nicht vorher vom Prokurator des Königs genehmigt werden.

B.37.2. Der dritte Teil des zweiten Klagegrunds ist unbegründet.

Aus diesen Gründen:

Der Gerichtshof

1. erklärt für nichtig:

- Artikel 39*bis* § 3 des Strafprozessgesetzbuches, eingefügt durch Artikel 2 des Gesetzes vom 25. Dezember 2016 « zur Festlegung verschiedener Abänderungen des Strafprozessgesetzbuches und des Strafgesetzbuches im Hinblick auf die Verbesserung der besonderen Ermittlungsmethoden und bestimmter Ermittlungsmaßnahmen in Sachen Internet, elektronische Nachrichten und Telekommunikation und zur Schaffung einer Datenbank der Stimmabdrücke »;

- Artikel 13 des vorerwähnten Gesetzes vom 25. Dezember 2016;

- Artikel 39*bis* des Strafprozessgesetzbuches, eingefügt durch Artikel 2 des vorerwähnten Gesetzes vom 25. Dezember 2016, insofern er keine besondere Bestimmung im Hinblick auf die Wahrung des Berufsgeheimnisses von Ärzten und Rechtsanwälten vorsieht;

2. erhält die Folgen der für nichtig erklärten Bestimmungen bis zum Datum der Veröffentlichung des vorliegenden Entscheids im *Belgischen Staatsblatt* aufrecht;

3. weist die Klage, vorbehaltlich der in B.15.2 und B.22.2 erwähnten Auslegungen, im Übrigen zurück.

Erlassen in französischer, niederländischer und deutscher Sprache, gemäß Artikel 65 des Sondergesetzes vom 6. Januar 1989 über den Verfassungsgerichtshof, am 6. Dezember 2018.

Der Kanzler — Der Präsident

F. Meersschaut — F. Daoût

GRONDWETTELIJK HOF

[2019/200079]

Uittreksel uit arrest nr. 178/2018 van 6 december 2018

Rolnummer 6814

In zake : het beroep tot vernietiging van artikel 5 van de wet van 19 november 2017 tot wijziging van diverse bepalingen betreffende de bevordering van de militairen, ingesteld door Stéphane Deham.

Het Grondwettelijk Hof,

samengesteld uit de voorzitters A. Alen en F. Daoût, en de rechters T. Merckx-Van Goey, P. Nihoul, T. Giet, J. Moerman en M. Pâques, bijgestaan door de griffier F. Meersschaut, onder voorzitterschap van voorzitter A. Alen,

wijst na beraad het volgende arrest :

I. *Onderwerp van het beroep en rechtspleging*

Bij verzoekschrift dat aan het Hof is toegezonden bij op 10 januari 2018 ter post aangetekende brief en ter griffie is ingekomen op 12 januari 2018, heeft Stéphane Deham, bijgestaan en vertegenwoordigd door Mr. P. Vande Casteele, advocaat bij de balie te Antwerpen, beroep tot vernietiging ingesteld van artikel 5 van de wet van 19 november 2017 tot wijziging van diverse bepalingen betreffende de bevordering van de militairen (bekendgemaakt in het *Belgisch Staatsblad* van 28 november 2017).

Bij hetzelfde verzoekschrift vorderde de verzoekende partij eveneens de schorsing van dezelfde wetsbepaling. Bij het arrest nr. 65/2018 van 31 mei 2018, bekendgemaakt in het *Belgisch Staatsblad* van 9 november 2018, heeft het Hof de vordering tot schorsing verworpen.

(...)

II. *In rechte*

(...)

Ten aanzien van de bestreden bepaling en haar context

B.1. De wet van 19 november 2017 tot wijziging van diverse bepalingen betreffende de bevordering van de militairen (hierna : wet van 19 november 2017) strekt ertoe een aantal wijzigingen aan te brengen in het statuut van de militairen, in het bijzonder wat hun bevordering betreft.

B.2.1. De voorwaarden om te kunnen worden bevorderd in de graad van hoofdofficier of opperofficier zijn inhoudelijk en procedureel van aard.

Artikel 139/1 van de wet van 28 februari 2007 tot vaststelling van het statuut van de militairen en kandidaat-militairen van het actief kader van de Krijgsmacht (hierna : wet van 28 februari 2007), vóór de wijziging ervan bij artikel 2 van de wet van 19 november 2017, bepaalde :

« Geen officier kan in een graad van hoofdofficier of opperofficier worden benoemd indien hij wegens zijn leeftijd niet gedurende ten minste drie jaar in zijn nieuwe graad kan dienen.

Geen officier kan in de graad van majoor benoemd worden indien hij :

1° de vervolmakingscursussen bedoeld in artikel 111, eerste lid, 1° en 2°, niet met succes gevolgd heeft;

2° niet geslaagd is in een test betreffende de kennis van een door de Koning te bepalen taal, die niet het Frans of het Nederlands is;

3° niet geslaagd is voor de beroepsproeven waarvoor de Koning de regels inzake deelneming, de programma's en de wijze van inrichting bepaalt ».

Daarnaast bepaalt artikel 6, § 1, van het koninklijk besluit van 7 april 1959 betreffende de stand en de bevordering van de beroepsofficieren dat de « chef defensie » voor elk bevorderingscomité en in volgorde van hun anciënniteit in de laatste graad, de lijst opstelt van alle officieren wier kandidatuur aan het comité wordt voorgelegd. Verder bepaalt artikel 6, § 2, eerste en tweede lid, van hetzelfde koninklijk besluit :

« Een kandidaat wordt voor de eerste maal op een lijst ingeschreven indien hij, op de voorziene benoemingsdatum, voldoet aan de bij artikel 21 voor zijn graad vastgestelde anciënniteitsvoorwaarden.

Zolang hij blijft voldoen aan de bevorderingsvoorwaarden, wordt elke kandidaat op zeven opeenvolgende lijsten ingeschreven ».