Numéro du rôle : 6711
Arrêt n° 174/2018 du 6 décembre 2018

A R R Ê T

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.

Le Conseil des ministres, assisté et représenté par Me S. Depré, Me E. de Lophem et Me M. Chomé, avocats au barreau de Bruxelles, a introduit un mémoire, les parties requérantes ont introduit un mémoire en réponse et le Conseil des ministres a également introduit un mémoire en réplique.

Par ordonnance du 18 juillet 2018, la Cour, après avoir entendu les juges-rapporteurs P. Nihoul et E. Derycke, a décidé que l'affaire était en état, qu'aucune audience ne serait tenue, à moins qu'une partie n'ait demandé, dans le délai de sept jours suivant la réception de la notification de cette ordonnance, à être entendue, et qu'en l'absence d'une telle demande, les débats seraient clos le 19 septembre 2018 et l'affaire mise en délibéré.

À la suite de la demande des parties requérantes à être entendues, la Cour, par ordonnance du 25 septembre 2018, a fixé l'audience au 17 octobre 2018.

À l'audience publique du 17 octobre 2018 :

- ont comparu :

. Me A. Gruwez, avocat au barreau de Bruxelles, *loco* Me D. Ribant, pour l'ASBL « Ligue des Droits de l'Homme »;

. Me M. Chomé, qui comparaissait également *loco* Me S. Depré et Me E. de Lophem, pour le Conseil des ministres;

- les juges-rapporteurs P. Nihoul et E. Derycke ont fait rapport;

- les avocats précités ont été entendus;

- l'affaire a été mise en délibéré.

Les dispositions de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle relatives à la procédure et à l'emploi des langues ont été appliquées.

II. *En droit*

- *A* -

Quant à la recevabilité

A.1.1. L'ASBL « Ligue des droits de l'homme » et la VZW « Liga voor Mensenrechten », parties requérantes, estiment avoir intérêt, en vertu de leur but statutaire respectif, à solliciter l'annulation des dispositions 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), qui sont de nature à affecter négativement le droit à un procès équitable, le droit au respect de la vie privée, le principe d'égalité et le principe de légalité, dont elles se sont donné pour objet d'assurer la défense.

A.1.2. Le Conseil des ministres ne conteste pas la recevabilité du recours.

Quant au fond

En ce qui concerne le premier moyen

A.2. Les parties requérantes prennent un premier moyen de la violation, par l'article 2 de la loi du 25 décembre 2016, des articles 10, 11, 12, 14, 15, 16 et 22 de la Constitution, lus isolément ou en combinaison avec les articles 6, 7 et 8 de la Convention européenne des droits de l'homme, avec le droit à un procès équitable, avec les droits de la défense et avec le principe de légalité et de prévisibilité en matière pénale.

A.3.1. Par la première branche de ce moyen, les parties requérantes font valoir que la disposition qu'elles attaquent viole les articles 10, 11 et 22 de la Constitution, lus en combinaison avec les articles 6 et 8 de la Convention européenne des droits de l'homme. Elles exposent qu'à la différence des recherches secrètes dans un système informatique, qui ne peuvent être, en vertu de l'article 90*ter* du Code d'instruction criminelle, ordonnées que par un juge d'instruction, les recherches non secrètes dans un système informatique peuvent, en application de la disposition attaquée qui modifie l'article 39*bis* du même Code, soit être effectuées de manière autonome par la police, soit être ordonnées par le procureur du Roi ou par le juge d'instruction. Elles indiquent que la disposition attaquée permet au parquet, dans certaines hypothèses, d'ordonner la connexion avec les bases de données auxquelles l'appareil saisi est connecté sans intervention du juge d'instruction. Elles en concluent que le législateur a ainsi autorisé le ministère public à ordonner des devoirs touchant directement à la vie privée, alors que ces devoirs relevaient auparavant des compétences du juge d'instruction. Elles estiment que le caractère non secret des recherches concernées n'est pas pertinent pour justifier l'éviction du juge d'instruction en cette matière.

Les parties requérantes exposent que les mécanismes de contrôle sont beaucoup moins stricts dans le cas d'une recherche non secrète que dans le cas d'une recherche secrète, alors que de telles recherches informatiques constituent une intrusion vaste et profonde dans la vie privée de chaque suspect et des autres personnes utilisant le même système informatique. Elles ajoutent que le caractère non secret résulte d'une obligation d'informer *a posteriori* le responsable du système informatique concerné, donc après que la recherche a eu lieu. Elles estiment que le critère de distinction, ainsi fondé sur le caractère secret ou non de la recherche, est arbitraire et subjectif et ne permet pas de justifier de manière raisonnable et objective la raison pour laquelle certains suspects faisant l'objet d'une recherche informatique considérée comme secrète bénéficient des fortes protections juridiques accompagnant une enquête judiciaire, alors que d'autres suspects ne bénéficient pas de la même protection. Elles considèrent qu'il en irait différemment si la recherche non secrète était obligatoirement autorisée par le responsable du système informatique visé avant qu'il y soit procédé.

A.3.2.1. Le Conseil des ministres rappelle que sous l'empire de l'ancien article 39*bis* du Code d'instruction criminelle, le procureur du Roi pouvait déjà procéder à la saisie de données informatiques à condition d'en informer le responsable du système informatique. Il expose que, même si cette disposition ne visait que la saisie, il était clair que le procureur pouvait explorer les données saisies. Il en déduit que la compétence du procureur du Roi lorsque la saisie et la recherche ne comportent pas de caractère secret n'est pas neuve et que la critique des parties requérantes est dans cette mesure tardive et donc irrecevable.

A.3.2.2. Le Conseil des ministres fait valoir qu'en réalité, les protections qui étaient prévues par l'ancienne législation, dans les articles 39*bis* et 88*ter* du Code d'instruction criminelle, n'ont pas été réduites mais, au contraire, renforcées par la loi attaquée. Il indique que les objectifs du législateur consistent en la nécessaire adaptation aux nouvelles technologies et en l'actualisation, la clarification et la simplification de l'arsenal législatif existant. De manière générale, il rappelle que le rôle du procureur du Roi dans la mise en œuvre des méthodes particulières de recherche a été consacré par la loi du 6 janvier 2003 concernant les méthodes particulières de recherche et quelques autres méthodes d'enquête et estime dès lors cohérent que le procureur exerce des compétences importantes en matière de recherche de données informatiques dans le cadre d'une information judiciaire.

Il souligne, d'une part, que le fait que le responsable du système informatique doit être informé dans les plus brefs délais constitue une garantie supplémentaire par rapport au droit antérieur et, d'autre part, que cette garantie constitue une dérogation au principe du secret de l'information, dans un souci de transparence. Il ajoute que l'information du responsable du système informatique lui permet de demander la levée de l'acte au procureur du Roi, avec possibilité de recours auprès de la Chambre des mises en accusation, conformément à l'article 28*sexies* du Code d'instruction criminelle, ce qu'une personne visée par une recherche secrète n'est pas en mesure de faire. Il en déduit qu'il existe effectivement un recours ouvert à la personne visée par la recherche non secrète. Enfin, il souligne que la distinction entre recherche secrète et recherche non secrète se substitue au critère auparavant utilisé, à savoir celui de la « transmission », dont il est apparu qu'il posait d'importantes difficultés au regard de l'évolution technologique.

A.3.2.3. Au sujet de l'extension de la recherche dans un système informatique, confiée à la compétence du procureur du Roi, le Conseil des ministres souligne que pour qu'elle soit légale, d'une part, l'extension doit être nécessaire à la manifestation de la vérité à l'égard de l'infraction qui fait l'objet de la recherche et, d'autre part, il doit être établi que d'autres mesures seraient disproportionnées ou qu'il y a un risque de perte d'éléments de preuve. Il ajoute que l'extension doit porter sur un système informatique que la personne est autorisée à utiliser et qu'elle ne peut être exercée sans intervention d'un juge d'instruction que si aucune fausse clé n'est nécessaire à sa réalisation. Il souligne enfin que les recherches ne peuvent être exercées par le procureur du Roi que dans un système informatique qui a été valablement saisi ou qui pouvait l'être. Il en conclut que l'extension de recherche exercée par le procureur du Roi est très fermement encadrée et comporte suffisamment de garanties. Il fait valoir que le législateur n'a fait que consacrer dans la loi la jurisprudence de la Cour de cassation et renvoie à cet égard à l'arrêt de cette Cour du 11 février 2015 (R.G. P.14.1739.F).

A.3.3. Les parties requérantes insistent sur le fait qu'en l'absence de garantie que les personnes affectées par une recherche dans leur système informatique en soient préalablement averties, la différence de traitement repose sur un critère arbitraire et subjectif. Elles ajoutent que s'il faut considérer qu'une recherche qui est portée à la connaissance de la personne concernée à n'importe quel moment est non secrète, en principe, toute recherche dans un système informatique est non secrète puisque même les recherches visées à l'article 90*ter* du Code sont à un certain moment, par exemple lors du règlement de la procédure, portées à la connaissance du suspect. Elles estiment que le Conseil des ministres, qui se limite à affirmer qu'en principe, la personne devrait être informée préalablement, ne fournit pas de réponse à cet argument.

Elles reconnaissent qu'avant l'adoption de la disposition attaquée, le procureur du Roi avait déjà la possibilité d'effectuer certaines recherches non secrètes dans un système informatique, mais elles soulignent qu'il s'agissait à ce moment d'actes beaucoup plus limités.

Elles estiment que les recours par la personne concernée à l'article 28*sexies*, cité par le Conseil des ministres, ne permettent pas de remédier à l'intrusion dans la vie privée causée par cette recherche, dès lors que cette disposition ne concerne que la levée de la saisie et n'est d'aucun secours dans l'hypothèse d'une recherche dans un système non saisi. Elles ajoutent que cette procédure prend deux à trois semaines et que, durant tout ce temps, les enquêteurs peuvent investiguer le système informatique.

A.3.4. Le Conseil des ministres estime que le moment auquel le responsable du système est informé est fondamental, étant donné que, dans le cadre d'une recherche non secrète, ce moment se situe plus tôt que dans le cadre d'une recherche secrète, ce qui lui offre une garantie supplémentaire puisqu'il peut se défendre le plus souvent avant que la recherche ait lieu, ou alors juste après qu'elle a eu lieu. Il ajoute qu'il n'est pas toujours possible de connaître le responsable du système visé avant de faire la recherche et qu'à suivre les parties requérantes, il ne serait pas possible, dans ces hypothèses, d'effectuer la recherche.

Il estime que les parties requérantes interprètent l'article 28*sexies* du Code d'instruction criminelle de manière trop restrictive et indique que, même en l'absence de saisie, le responsable du système informatique peut exercer la voie de recours prévue par cette disposition.

A.4.1. Par la deuxième branche de ce moyen, les parties requérantes font valoir que la disposition qu'elles attaquent viole les articles 10, 11 et 22 de la Constitution. Elles font valoir que la différence de régime juridique établie entre la recherche prévue par l'article 39*bis*, § 2, alinéa 1er, du Code d'instruction criminelle, qui est effectuée par un officier de police judiciaire, et celle qui doit être ordonnée par le procureur du Roi en application de l'alinéa 2 de la même disposition n'est pas justifiée. Elles exposent que dans le premier cas, la recherche est effectuée sur un objet saisi alors que dans le second cas, elle est effectuée sans saisir l'objet. Elles estiment qu'il n'y a pas de justification au fait que le procureur du Roi intervienne dans un cas et pas dans l'autre.

A.4.2. Le Conseil des ministres relève que la distinction attaquée vise à limiter la compétence de l'officier de police judiciaire en matière de recherche dans un système informatique à l'hypothèse dans laquelle le système informatique a été effectivement saisi. Il rappelle en outre que toutes les liaisons externes doivent être interrompues durant la recherche. Il estime que, contrairement à ce que soutiennent les parties requérantes, il n'est pas plus intrusif de procéder à une recherche sur un objet saisi plutôt qu'à l'endroit où le système informatique est placé habituellement, sans le saisir. Il estime pour sa part que, du point de vue des droits de la défense, il peut être considéré que la recherche dans un système informatique non saisi est plus intrusive que la recherche dans un système saisi, dès lors que, le système étant susceptible d'être altéré par son détenteur à la suite de la recherche, certaines mesures ultérieures, telles une contre-expertise, ne peuvent pas être réalisées. Il indique que c'est pour cette raison que l'officier de police judiciaire ne peut pas prendre d'initiative en pareille situation et que c'est le procureur du Roi qui doit ordonner ce type de recherches.

A.4.3. Les parties requérantes estiment que la réponse du Conseil des ministres ignore le problème principal qu'elles dénoncent, à savoir que la décision de saisir ou non le système informatique ne repose pas sur un critère objectif mais dépend uniquement de la volonté de l'officier de police judiciaire, qui peut décider seul de la saisie d'un système informatique, tel un portable ou un ordinateur, lors d'une perquisition ou d'une fouille, laquelle peut, de plus, avoir lieu sans aucune autorisation préalable d'un magistrat. Elles en déduisent que la recherche dans les informations privées qui se trouvent sur les ordinateurs et portables dépend uniquement de la décision d'un officier de police judiciaire et que la loi attaquée introduit un critère pour distinguer le régime de l'autorisation du procureur du Roi de celui de l'initiative de l'officier de police judiciaire qui ne dépend que de l'appréciation de ce dernier.

A.4.4. Le Conseil des ministres estime que la critique des parties requérantes ne vise pas la loi attaquée mais bien les textes qui régissent les missions de police judiciaire. Il rappelle que, lors de l'examen du contenu du matériel saisi, toutes les liaisons extérieures sont coupées, de sorte que cette analyse ne diffère pas de celle d'un document physique.

A.5.1. Par la troisième branche de ce moyen, les parties requérantes font valoir que la disposition qu'elles attaquent viole les articles 12 et 14 de la Constitution, lus en combinaison avec l'article 7 de la Convention

européenne des droits de l'homme. Elles déclarent que la loi attaquée ne précise pas le contenu normatif du concept de « responsable du système informatique » qui doit être informé de la recherche dans le système ou de son extension, de sorte que l'identité des personnes qui doivent être informées de la recherche reste floue. Elles font également grief à la disposition attaquée de ne pas imposer aux enquêteurs de cibler préalablement les parties du système concerné, de sorte qu'ils pourraient consulter un système informatique sans but précis et mener une pêche à l'information dans l'espoir de trouver la preuve d'une infraction. Elles reprochent encore à la disposition attaquée de sembler limiter l'obligation d'information à une seule personne, le « responsable », alors qu'en réalité, une grande variété de personnes peuvent être responsables d'un système informatique déterminé.

A.5.2. Le Conseil des ministres souligne d'abord que la notion de « responsable du système informatique » n'est pas neuve, de sorte qu'en ce qu'elle vise cette notion, cette branche du moyen est tardive et donc irrecevable. Pour le surplus, il indique que le choix de cette notion a été dicté par la souplesse qu'elle permet et estime que, de manière générale, la nécessité de permettre au dispositif législatif d'être en phase avec la rapidité d'adaptation caractérisant les milieux criminels peut justifier le choix de notions volontairement moins précises. Enfin, il considère que la communication au responsable du système est de nature à renforcer la protection des droits du justiciable plutôt qu'à la mettre en péril et qu'il est dès lors souhaitable que la notion retenue n'empêche pas cette protection par une rigueur excessive.

A.5.3. Les parties requérantes estiment que la réponse du Conseil des ministres ignore l'ampleur de la réforme. Elles font valoir que la réforme compense, par l'obligation d'informer le responsable du système, la forte diminution des garanties judiciaires dont étaient auparavant entourées les recherches dans un système informatique. Elles estiment qu'à défaut de définition claire de ce concept, cette protection est illusoire.

A.6.1. Par la quatrième branche de ce moyen, les parties requérantes font valoir que la disposition qu'elles attaquent viole l'article 22 de la Constitution, lu en combinaison avec l'article 8 de la Convention européenne des droits de l'homme. Elles font valoir que la loi attaquée s'inscrit dans une tendance lourde qui opère un glissement des prérogatives du juge d'instruction au profit du parquet et des forces de police, alors que la mission légale de ces derniers est de viser à la recherche et à la répression des infractions et de leurs auteurs. Elles estiment que toute intrusion par les autorités dans un système informatique doit être entourée des mêmes garanties qu'une mesure de perquisition. Elles indiquent que selon la directive 2002/58/CE, dite « directive vie privée et communications électroniques », un système informatique entre dans le champ d'application de l'article 8 de la Convention européenne des droits de l'homme. Elles estiment que ceci est d'autant plus interpellant que le législateur n'a prévu aucune protection spécifique pour les personnes soumises au secret professionnel ou au secret des sources. Elles considèrent en outre que la disposition attaquée est totalement disproportionnée, dès lors que la recherche dans un système informatique constitue une ingérence particulièrement importante dans la vie la plus privée des personnes concernées, qu'un système informatique peut être utilisé par d'autres personnes que celle qui est soupçonnée et que la disposition attaquée permet que toutes les données qui se trouvent sur le système soient exploitées, indépendamment de leur pertinence pour la recherche de la vérité.

A.6.2. Le Conseil des ministres renvoie à sa réponse au même moyen, en sa première branche. Il souligne par ailleurs que, de manière générale, les parties requérantes n'explicitent pas concrètement ce qui serait disproportionné dans la loi attaquée. Il rappelle que le rôle du procureur du Roi dans la mise en œuvre des méthodes particulières de recherche a été établi par la loi du 6 janvier 2003 concernant les méthodes particulières de recherche et quelques autres méthodes d'enquête. Il précise que les recherches organisées par la loi attaquée sont réactives et en déduit que dans le cadre de la loi attaquée, le procureur du Roi et l'officier de police judiciaire disposent de moins de marge de manœuvre que dans le cadre d'autres méthodes particulières de recherche. Il indique que la problématique de l'usage mixte du système informatique se présente de la même manière en matière d'ouverture du courrier ou d'écoutes téléphoniques et qu'il n'est pas possible d'isoler la personne soupçonnée d'infraction de tout contact avec des tiers. Il répète que des garanties entourent la recherche informatique, que la recherche doit se limiter scrupuleusement à ce qui est enregistré sur l'appareil et que les personnes intéressées disposent de recours en cas d'abus.

A.6.3. Les parties requérantes font valoir que, selon la Recommandation n° R(95)13 du Comité des ministres aux États membres relative aux problèmes de procédure pénale liés à la technologie de l'information et la Convention du Conseil de l'Europe sur la cybercriminalité du 23 novembre 2001, dans le cas d'une intrusion dans un système effectuée par les autorités en vue de saisir des données, la procédure applicable dans le contexte numérique devrait s'aligner sur celle qui est prévue dans le cadre des pouvoirs traditionnels d'une perquisition. Elles ajoutent qu'une recherche dans un système informatique n'est pas une méthode particulière de recherche. Elles renvoient également à la jurisprudence de la Cour européenne des droits de l'homme qui considère que la règle doit être celle du mandat judiciaire ou de l'autorisation préalable conférée par un organe indépendant.

A.7.1. Par la cinquième branche de ce moyen, les parties requérantes font valoir que la disposition qu'elles attaquent viole les articles 10, 11 et 22 de la Constitution, lus en combinaison avec l'article 6 de la Convention européenne des droits de l'homme. Elles reprochent à l'article 39*bis* du Code d'instruction criminelle, tel qu'il a été modifié par la disposition attaquée, de ne prévoir aucune protection spécifique afin de garantir le secret professionnel des avocats ou des médecins dont le système informatique fait l'objet de la recherche. Elles indiquent qu'en revanche, l'article 90*ter* du Code d'instruction criminelle prévoit une telle protection spécifique. Elles estiment que la différence de traitement établie par la comparaison de ces deux dispositions manque de toute justification. Elles ajoutent que l'obligation du procureur du Roi d'informer *a posteriori* le responsable du système informatique n'offre aucune protection contre l'intrusion dans la vie privée et aucune garantie de préservation du secret professionnel pesant sur les données récoltées.

A.7.2. Le Conseil des ministres souligne d'abord que cette critique des parties requérantes ne vise pas une nouveauté introduite dans le Code d'instruction criminelle, mais bien une disposition ancienne de ce Code, de sorte qu'elle est tardive et, partant, irrecevable. En ordre subsidiaire, il indique qu'il existe une différence fondamentale entre l'article 39*bis* du Code d'instruction criminelle et l'article 90*ter* du même Code, en ce que le premier vise les recherches non secrètes dans un système informatique alors que le second vise les recherches secrètes. Il estime que, dans le cas d'une recherche non secrète, la protection du secret professionnel est déjà assurée lors de la saisie du système. Il expose que puisque l'exploration du matériel saisi n'est que la conséquence logique de la saisie, le tri entre ce qui est couvert par le secret professionnel et ce qui n'est pas couvert a déjà été fait au moment de la saisie et ne doit plus l'être au moment de l'exploration du système. Il en conclut que le secret professionnel est effectivement protégé.

A.7.3. Les parties requérantes font valoir que la disposition attaquée vise de nombreuses situations qui ne bénéficient pas de la protection vantée par le Conseil des ministres. Elles citent en exemple la fouille d'un avocat et la saisie de son portable en indiquant que dans ce cas, il n'y a aucune protection du secret professionnel de l'avocat. Elles estiment que cela est d'autant plus inquiétant qu'une telle saisie peut avoir lieu sur la base d'une décision autonome d'un officier de police judiciaire, sans aucun contrôle judiciaire. Elles ajoutent que l'on peut se demander dans quelle mesure le bâtonnier peut empêcher ou contrôler la recherche effectuée dans un système informatique qui pourrait être saisi mais qui ne l'est pas.

A.7.4. Le Conseil des ministres rappelle que la protection du secret professionnel n'est pas limitée au cas de la perquisition, de sorte que les documents couverts par ce secret ne pourraient pas figurer dans le dossier pénal qui serait ouvert. Il en déduit que la chambre des mises en accusation pourrait être saisie par l'avocat ou par le médecin concerné sur la base de l'article 61*quater* du Code d'instruction criminelle, que la chambre des mises en accusation pourrait prononcer l'irrecevabilité des poursuites sur la base de l'article 235 du Code d'instruction criminelle et que le juge du fond doit écarter les pièces couvertes par le secret professionnel.

En ce qui concerne le second moyen

A.8. Les parties requérantes prennent un second moyen de la violation, par l'article 7 de la loi attaquée, des articles 10, 11, 12, 14, 15, 16 et 22 de la Constitution, lus isolément ou en combinaison avec les articles 6, 7 et 8 de la Convention européenne des droits de l'homme, avec le droit à un procès équitable, avec les droits de la défense et avec le principe de légalité et de prévisibilité en matière pénale.

A.9.1. Par la première branche de ce moyen, les parties requérantes font valoir que la disposition qu'elles attaquent viole les articles 10 et 11 de la Constitution, dès lors que le régime juridique qu'elle crée spécifiquement pour l'infiltration sur internet est différent du régime de l'infiltration traditionnelle prévu par l'article 47*octies* du Code d'instruction criminelle. Elles estiment que l'affirmation du législateur, selon laquelle l'infiltration sur internet aurait un caractère moins intrusif que l'infiltration classique, ne permet pas de justifier la différence de traitement entre les personnes impliquées ou affectées par une infiltration sur internet et celles qui le sont par une infiltration classique. Elles ajoutent qu'il n'y a aucune justification au fait que les contrôles sur les méthodes particulières de recherche prévus par les articles 235*ter* et 235*quater* du Code d'instruction criminelle ne s'appliquent pas de la même manière à l'infiltration sur internet. Elles soulignent qu'aujourd'hui, il y a déjà des méthodes particulières de recherche utilisées dans un contexte virtuel et que ces méthodes sont toujours soumises au contrôle de la chambre des mises en accusation. Elles citent en exemple à cet égard les observations systématiques dans les forums publics.

A.9.2. Le Conseil des ministres estime que les parties requérantes n'ont pas intérêt à contester la différence de traitement dénoncée, dès lors que les mesures citées sont prises en vue de la protection des cyberinfiltrants et qu'elles ne sont pas des cyberinfiltrants. Au surplus, il estime que la différence de traitement est justifiée. Il considère par ailleurs que, dans l'hypothèse de l'ouverture d'un dossier confidentiel à l'occasion de l'application de l'article 46*sexies* du Code d'instruction criminelle, la différence de traitement est inexistante. Il estime que la différence de traitement dans le cas dans lequel il n'y a pas d'ouverture d'un dossier confidentiel est justifiée par l'objectif d'éviter d'alourdir le travail de la chambre des mises en accusation dans des cas où cela n'est pas indispensable, puisque l'infiltration sur internet a un caractère moins intrusif que l'infiltration classique. Il indique que toutes les actions de l'infiltration sur internet et tous les contacts noués à cette occasion sont consignés dans des procès-verbaux qui font partie du dossier répressif et peuvent donc être consultés par les parties et contrôlés par le juge du fond, ce qui constitue des garanties en termes de droits de la défense qui n'existent pas pour les infiltrations dans le monde physique.

A.9.3. Les parties requérantes considèrent qu'au vu de leurs statuts, elles ont intérêt à demander l'annulation de la disposition attaquée qui organise pour l'infiltration virtuelle un régime plus souple et donc moins contrôlé que l'infiltration dans le monde physique. Pour le surplus, elles font valoir que la disposition attaquée crée bien une différence de traitement pour laquelle il n'existe aucune justification.

A.10.1. Par la deuxième branche de ce moyen, les parties requérantes font valoir que la disposition qu'elles attaquent viole les articles 12 et 14 de la Constitution, lus en combinaison avec l'article 6 de la Convention européenne des droits de l'homme. Elles estiment que les modifications que la disposition attaquée apporte à l'article 46*sexies*, § 1er, alinéa 2, du Code d'instruction criminelle, violent le principe de légalité en matière pénale, en ce qu'elles prévoient que le Roi détermine les modalités de désignation des services de police habilités à exécuter la mesure d'enquête envisagée par cet article. Elles renvoient sur ce point à l'avis de la section de législation du Conseil d'État.

A.10.2. Le Conseil des ministres observe que la critique des parties requérantes porte sur un point qui n'est pas susceptible de porter atteinte aux principes cités ou aux droits de la défense des personnes visées par les mesures d'enquête puisque l'article 46*sexies* du Code d'instruction criminelle prévoit en toute hypothèse qu'un dossier est constitué et qu'il est, sauf certaines exceptions très spécifiques, accessible à la personne concernée. Il estime que le fait que ce soit le Roi qui désigne les services de police compétents n'a aucune incidence sur ce principe.

A.11.1. Par la troisième branche de ce moyen, les parties requérantes font valoir que la disposition qu'elles attaquent viole les articles 12 et 14 de la Constitution. Elles font grief au nouvel article 46*sexies*, § 1er, alinéa 4, du Code d'instruction criminelle de prévoir une clause d'exclusion pour permettre aux forces de police de « patrouiller » sur internet sans devoir se soumettre au prescrit de l'article 46*sexies*, c'est-à-dire sans avoir obtenu l'autorisation du procureur du Roi, dès lors que l'objectif n'a pour finalité directe qu'une vérification ciblée ou une arrestation. Elles estiment que cette exclusion prête à confusion et que la formulation de la loi laisse la porte ouverte à des opérations de pêche à l'information permettant aux policiers de détourner ou de méconnaître les conditions strictes d'une infiltration sur internet.

A.11.2. Le Conseil des ministres estime que la disposition en cause est claire. L'alinéa 4, du § 1er de cette disposition vise le cas d'un contact spécifique, bref dans le temps, sans identité fictive. Il fait valoir que si le législateur n'avait pas prévu cette disposition, les enquêteurs auraient eu moins de marge de manœuvre sur internet que dans le monde physique.

- *B* -

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, n° 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 n° 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 n° 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 n° 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 n° 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 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 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 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.*, 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