Doctrine

La collecte des preuves numériques en droit belge après l'arrêt de la Cour constitutionnelle du 5 décembre 2018

Prolégomènes

1. La loi du 25 décembre 2016[1] a réformé de manière assez substantielle les méthodes de collecte des preuves numériques en droit de la procédure pénale belge. Jusqu'alors, les outils à disposition des autorités judiciaires étaient assez vieillots, voire obsolètes, puisqu'ils dataient de la loi du 28 novembre 2000 relative à la criminalité informatique[2], époque à laquelle il était quasi impossible d'anticiper l'avènement de la nouvelle ère dans laquelle nous vivons désormais, celle de la société de l'information. Que l'on se rappelle qu'en l'an 2000, on entendait encore crisser les modems lorsque l'on se connectait à internet, les smartphones n'étaient alors que des objets de science-fiction, le réseau 3 G n'en était qu'à ses balbutiements, les géants du net que sont devenus YouTube, Google, Facebook, Amazon… n'existaient pas (ou à peine), pas plus que les multiples applications qui facilitent désormais notre vie quotidienne, que l'on ne pouvait imaginer que les solutions de stockage allaient un jour se décliner sur le mode du *cloud computing* ni qu'il serait possible de s'envoyer des messages par des applications de messagerie chiffrée[3]…

2. Le législateur belge a donc voulu rattraper le temps perdu et tenter de mettre en place les fondements d'une « procédure pénale 2.0 »[4] à une époque où d'aucuns se projettent déjà dans le web 3.0 et ses promesses vertigineuses d'un monde dominé par les *blockchains*[5].

3. Notre contribution poursuivra un but bien moins ambitieux qui est de permettre de comprendre dans quelles conditions les autorités de poursuites peuvent

1 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, *M.B.*, 17 janvier 2017 (ci-après, « la loi du 25 décembre 2016 »).

2 Loi du 28 novembre 2000 relative à la criminalité informatique, *M.B.*, 3 février 2001.

3 WhatsApp, Viber, Messenger, Telegram, Signal…

4 V. Franssen et S. Tosza, « Vers plus de droits pour le justiciable sur internet ? Un nouveau cadre légal pour lutter contre la criminalité dans la société de l'information », *in Les droits des justiciables face à la justice pénale*, CUP, vol. 171, Limal, Anthemis, 2017, p. 207.

5 La *blockchain* est une technologie de stockage et de transmission d'informations, transparente, sécurisée et fonctionnant sans organe central de contrôle. Par extension, une *blockchain* constitue une base de données qui contient l'historique de tous les échanges effectués entre ses utilisateurs depuis sa création. Cette base de données est sécurisée et distribuée : elle est partagée par ses différents utilisateurs, sans intermédiaire, ce qui permet à chacun de vérifier la validité de la chaîne. Source : https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain.

collecter des preuves dites numériques, à quoi les nouvelles règles correspondent, ce qu'elles peuvent effectuer comme recherches relativement à ces preuves et dans quelle mesure elles peuvent contraindre les opérateurs de réseaux de communication et les fournisseurs de services de communications électroniques de prêter leur concours à l'exécution de devoirs judiciaires.

4. Nous analysons en premier lieu la saisie de données – ainsi que la mesure de conservation de celles-ci – (I), avant d'aborder la recherche informatique (II), pour terminer avec l'analyse de l'obligation de collaboration (III). Notre analyse intègre l'enseignement de l'arrêt rendu par la Cour constitutionnelle le 6 décembre 2018, par lequel la Cour, saisie sur recours en annulation de certaines dispositions de la loi du 25 décembre 2016, a fait partiellement droit à cette demande[6], ainsi que les nouvelles dispositions insérées par la loi du 5 mai 2019 en vue d'adapter les règles existantes à l'arrêt rendu[7].

I LA SAISIE ET LA MESURE DE CONSERVATION DE DONNÉES INFORMATIQUES

A La saisie de données informatiques

1 Remarques liminaires

5. Il importe de distinguer au préalable la saisie du *support* informatique (un ordinateur, un smartphone, un disque dur…) et la saisie de *données* informatiques intégrées dans un support. En effet, un ordinateur (le support) peut être saisi sans que les données qui y sont stockées ou auxquelles il permet d'avoir accès le soient, et inversement[8].

6. La saisie du support matériel est régie par le droit commun de la saisie des biens corporels aux articles 35 et suivants du Code d'instruction criminelle[9]. La saisie des données informatiques est quant à elle régie par l'article 39*bis*, §§ 1er, 5 à 8, du Code d'instruction criminelle. Les règles du droit commun s'y appliquent toutefois également de façon résiduaire.

7. La présente contribution étant limitée à la saisie des preuves numériques, nous examinerons seulement les règles relatives à la saisie des données informatiques, sans évoquer celles applicables à la saisie du support sur lequel celles-ci sont stockées. Puisque c'est d'actualités législatives dont il s'agit, nous nous concentrons par ailleurs sur les nouveautés récemment adoptées par le législateur

6 C.C., 6 décembre 2018, arrêt n° 174/2018, disponible sur http://www.const-court.be/fr/common/home.html.

7 Loi du 5 mai 2019 portant des dispositions diverses en matière pénale et en matière de cultes, et modifiant la loi du 28 mai 2002 relative à l'euthanasie et le Code pénal social, *M.B.*, 24 mai 2019.

8 Voy. *infra* à propos de cette question de l'articulation entre saisie du *support* et saisie des *données*.

9 V. Franssen et S. Tosza, *op. cit.*, p. 214.

belge en cette matière, tout en rappelant quelques principes généraux de la saisie de données. Nous renvoyons aux règles générales de la saisie pour le surplus[10].

8. La lecture intégrale de l'article 39*bis* du Code d'instruction criminelle peut faire naître une certaine confusion dans l'esprit d'un lecteur non averti. En effet, il traite simultanément de deux actes d'enquête distincts, à savoir la saisie des données informatiques, d'une part, et la recherche – non secrète – dans les systèmes informatiques, d'autre part, dont le régime juridique sera exposé *infra*. Les règles concernant ces deux actes d'enquête sont, certes, intimement liées. Toutefois, il eût été préférable, par souci de clarté, de définir, en deux dispositions séparées, les règles propres à chacun d'entre eux[11].

2 Bref rappel historique

9. La possibilité de saisir des données informatiques a été introduite en Belgique par la loi du 28 novembre 2000 relative à la criminalité informatique[12]. Avant cela, la saisie de données n'était pas possible sans que le support matériel abritant ces données soit également saisi. En effet, puisque la saisie de droit commun requiert en principe une dépossession, la copie de données n'était pas considérée comme une saisie. L'introduction par le législateur de la saisie de données informatiques a permis de remédier à cet écueil[13].

10. La procédure de saisie de données informatiques a été complétée suite à l'adoption de la loi du 25 décembre 2016[14], dont les nouveautés font majoritairement l'objet de la présente contribution.

3 Définitions

11. Les données informatiques constituent « *les représentations de l'information pouvant être stockées, traitées et transmises par le biais d'un système informatique* »[15].

---

10 F. Lugentz et D. Vandermeersch, *Saisie et confiscation en matière pénale*, Bruxelles, Bruylant, 2015, pp. 97-173 ; R. Verstraeten et L. Delbrouck, « Beslag in strafzaken », in *Strafrecht en strafvordering. Artikelsgewijze commentaar met overzicht van rechtspraak en rechtsleer*, Mechelen, Kluwer, 2015, pp. 129-197.

11 V. Franssen et S. Tosza, *op. cit.*, p. 214.

12 Loi du 28 novembre 2000 relative à la criminalité informatique, *M.B.*, 3 février 2001.

13 Projet de loi relatif à la criminalité informatique, *Doc. parl.*, Ch. repr., sess. ord., 1999-2000, n° 50-213/001, p. 20 : « *La saisie de données pertinentes pour l'instruction, stockées, traitées ou transmises par le biais d'un système informatique, peut s'effectuer intégralement conformément à la procédure traditionnelle dans la mesure où elle s'accompagne de la saisie du support matériel sur lequel elles se trouvent (par exemple l'ordinateur, des disques optiques, des disquettes…). Lorsque les autorités judiciaires veulent disposer uniquement des données et ne pas saisir le système informatique ou les autres supports, la situation juridique se présente différemment, principalement parce que la saisie requiert la soustraction de l'objet en question à celui qui le détient. Par conséquent, la copie de données ne peut pas être assimilée en tant que telle à la saisie d'objets matériels. La nouvelle disposition crée par conséquent une base juridique adéquate pour un nouveau moyen coercitif ayant les mêmes finalités que la saisie. Dans la mesure où aucune dérogation n'est prévue dans cette nouvelle disposition, il est logique que les règles en matière de saisie s'appliquent à la saisie de données* ».

14 Loi du 25 décembre 2016.

15 Projet de loi relatif à la criminalité informatique, *Doc. parl.*, Ch. repr., sess. ord., 1999-2000, n° 50-213/001, p. 12.

12. L'article 39*bis*, § 1er, du Code d'instruction criminelle définit la saisie de données comme étant (1) la possibilité de copier, (2) de rendre inaccessibles et (3) de retirer des données stockées dans un système informatique ou dans une partie de celui-ci. Le but d'une telle saisie est de permettre la conservation des données en vue de la procédure au fond, lors de laquelle elles pourront servir de preuves ou faire l'objet d'une confiscation[16].

13. L'article 39*bis*, § 6, du Code d'instruction criminelle est libellé comme suit : « *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* ».

14. S'agissant de l'articulation entre la saisie du support et/ou des données, certains auteurs qui se fondent sur la formulation du § 6 susmentionné soutiennent que la saisie du support informatique serait la règle, et la saisie des données informatiques, l'exception. La saisie des données informatiques ne pourrait donc avoir lieu que lorsque la saisie du support n'est pas souhaitable[17]. D'autres auteurs sont au contraire d'avis que le but de la saisie de données informatiques est d'éviter autant que possible de devoir saisir le support matériel[18].

15. Les travaux préparatoires de la loi du 25 décembre 2016 donnent comme exemple une enquête financière importante au cours de laquelle une saisie du système informatique serait envisagée ; dans un tel cas, elle peut toutefois « *causer des difficultés importantes de fonctionnement à la banque en question* »[19], de sorte qu'il vaut mieux privilégier la saisie des données. Il en ressort que le caractère « non souhaitable » de la saisie du support doit notamment s'apprécier au regard du préjudice encouru par le saisi. Pour rappel, une saisie doit en principe répondre

16 Au sujet de la confiscation potentielle de données informatiques, C. Meunier s'étonne que la loi du 28 novembre 2000 relative à la criminalité informatique n'étende pas aux données informatiques les articles 42 et suivants du Code pénal en matière de confiscation, qui ne visent pourtant que des « choses » matérielles. Il indique que « même s'il est vrai que la doctrine, en matière de vol, tend à étendre cette notion de "choses" aux données informatiques, on peut s'attendre à voir naître des controverses jurisprudentielles sur cette question ». Voy. C. Meunier, « La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère du numérique », *Rev. dr. pén. crim.*, 2001, p. 676. O. Klees, F. Roggen et D. Vandermeersch, « Les saisies en matière pénale et le référé pénal », in P. Chomé *et al.*, *Droit pénal et procédure pénale*, Malines, Kluwer, 2006, p. 40 ; Ch. Conings et S. Royer, « Verzamelen en vastleggen van digitaal bewijs in strafzaken », *Nullum Crimen*, 2017, pp. 311-338, spéc. p. 330.

17 Ch. Conings et S. Royer, *op. cit.*, p. 329.

18 F. Lugentz et D. Vandermeersch, *op. cit.*, p. 137 ; O. Klees, F. Roggen et D. Vandermeersch, *op. cit.*, p. 95 ; C. Meunier, « La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère du numérique », *Rev. dr. pén. crim.*, 2001, pp. 611-690, spéc. p. 672. Ce dernier auteur admet toutefois que si le juge décide de procéder à la saisie du support informatique, la motivation de son ordonnance ou de son réquisitoire doit idéalement mentionner les raisons pour lesquelles cette saisie est souhaitable. À défaut, l'auteur indique que la personne lésée par la mesure pourrait invoquer, dans le cadre d'un référé pénal, que la saisie des seules données aurait pu satisfaire aux nécessités de l'enquête.

19 Projet de loi relatif à l'amélioration des méthodes particulières de recherche et de certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications, *Doc. parl.*, Ch. repr., sess. ord., 2015-2016, n° 54-1966/001, p. 16.

au principe de proportionnalité selon lequel un lien doit exister entre ce qui est soumis à la saisie et l'infraction qui fait l'objet de l'enquête[20].

16. Or, en pratique, la saisie des données plutôt que du support est en effet, dans la plupart des cas, moins préjudiciable pour le saisi et davantage proportionnelle, pour autant que les données copiées soient liées à l'infraction faisant l'objet de l'enquête[21]. Il s'agit là, à notre estime, d'un argument déterminant pour considérer que la saisie du support devrait constituer non la règle, mais l'exception. Dans cette optique, la personne lésée par la mesure pourrait invoquer, dans le cadre d'un référé pénal, que la saisie des seules données aurait pu satisfaire aux nécessités de l'enquête[22].

4 Qui peut procéder à une saisie de données informatiques ?

17. Les règles relatives à l'autorité compétente pour saisir des données informatiques se trouvent à l'article 39*bis* du Code d'instruction criminelle et dans les règles générales concernant la saisie[23].

18. À l'origine, seul le juge d'instruction disposait du pouvoir de saisie dans le cadre d'une perquisition[24]. À présent, cette compétence pour saisir des données informatiques est également dévolue aux officiers de police judiciaire, au procureur du Roi[25].

19. Nous proposons d'examiner l'étendue des compétences de chacun d'entre eux dans les lignes qui suivent :

- Les officiers de police judiciaire (ou les inspecteurs sociaux[26])

  Divers fondements sont invoqués pour justifier la compétence des officiers de police judiciaire de saisir des données. Leur pouvoir de saisie est d'abord né d'une pratique courante chez ces derniers, qui ne voyaient pas d'inconvé-

20 Ch. Conings et S. Royer, *op. cit.*, p. 334.

21 En effet, si une quantité gigantesque de données est saisie de manière indifférenciée, la saisie des données se retrouve alors tout autant disproportionnée que celle du support dans lequel elles sont intégrées. Comme l'indiquent Ch. Conings et S. Royer, maintenant que la saisie des données est de plus en plus fréquente en vue d'une recherche informatique ultérieure, les autorités saisissent de plus grandes quantités de données, ce qui s'avère problématique. Voy. Ch. Conings et S. Royer, *op. cit.*, p. 334.

22 C. Meunier, *op. cit.*, p. 672.

23 Voy. l'article 39*bis*, § 1er, C. i. cr., qui indique que les règles relatives à la saisie s'appliquent à la saisie de données stockées dans un système informatique.

24 R. Declercq, « Hoofdstuk II. De gerechtelijke politie », *in Beginselen van strafrechtspleging*, Mechelen, Kluwer, 2014, p. 225.

25 Ch. Conings et S. Royer, *op. cit.*, pp. 332-333.

26 « Les inspecteurs sociaux revêtus de la qualité d'officier de police judiciaire pourront assister le ministère public au cours d'une enquête pénale visant à lutter contre la criminalité informatique ». Voy. Projet de loi relatif à l'amélioration des méthodes particulières de recherche et de certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications, *Doc. parl.*, Ch. repr., sess. ord., 2015-2016, n° 54-1966/001, p. 17.

nient à saisir des objets dans le cadre d'une audition ou d'une perquisition, par exemple[27]. Cette pratique fut validée par la Cour de cassation dans un arrêt du 19 février 2002 en ces termes :

« *Attendu que lorsque les officiers de police judiciaire effectuent une perquisition ou une visite domiciliaire régulière ils doivent saisir en application tant de l'ancienne version de l'article 35 du Code d'instruction criminelle que de la version actuelle, comme le formule cette nouvelle version, tout ce qui paraîtra constituer une des choses visées à l'article 42 du Code pénal et tout ce qui pourra servir à la manifestation de la vérité* »[28].

Les officiers de police judiciaire sont en outre compétents pour saisir des données informatiques sur pied de l'article 15 de la loi sur la fonction de police, qui prévoit que :

« *Dans l'exercice de leurs missions de police judiciaire, les services de police ont pour tâche : […] 3° de rechercher, de saisir et de mettre à la disposition de l'autorité compétente les objets dont la saisie est prescrite* »[29].

Enfin, en cas de flagrant délit, les officiers de police auxiliaires du procureur du Roi disposent également d'un pouvoir spécial de saisie (art. 49 et 52 C. i. cr.).

Le pouvoir de saisie des officiers de police judiciaire semble toutefois limité quant à sa portée. En effet, les travaux préparatoires de la loi du 25 décembre 2016 indiquent que les officiers de police judiciaire sont uniquement compétents pour copier des données, et non pour les bloquer ou les supprimer (voy. *infra*, points 28 et 29).

En outre, s'agissant des données susceptibles d'être couvertes par le secret professionnel des médecins et des avocats, les nouvelles dispositions de l'article 39*bis* du Code d'instruction criminelle nous paraissent exiger l'intervention du procureur du Roi[30]. Il est en effet prévu que ce dernier doit avertir le bâtonnier ou le représentant de l'ordre provincial des médecins des éléments qu'il estime relever du secret professionnel, qui ne peuvent dès lors être consignés dans un procès-verbal, et partant, faire l'objet d'une saisie[31].

27 Ch. Conings et S. Royer, *op. cit.*, p. 333.
28 Cass., 19 février 2002, R.G. P.00.1100.N, p. 16.
29 Loi du 5 août 1992 sur la fonction de police, *M.B.*, 22 décembre 1992.
30 Art. 39*bis*, § 9, al. 2, C. i. cr.
31 Si l'article 39*bis*, § 9, C. i. cr. impose l'intervention du procureur du Roi en cas de recherche effectuée sur le système informatique d'un avocat ou d'un médecin, il nous semble que cette procédure particulière doit être étendue à l'hypothèse où la recherche serait effectuée sur le système informatique d'un tiers, concernant une communication émanant d'un avocat ou d'un médecin (par ex., un sms reçu par un suspect de la part de son avocat). Une telle procédure est d'ailleurs prévue en cas de recherche secrète dans un système informatique, lorsque les données du système informatique (en ce compris celui d'une personne qui ne serait pas dépositaire du secret professionnel) sont couvertes par le secret professionnel. Le juge d'instruction est, dans ce cas, seul compétent pour évaluer les données qui relèvent du secret professionnel et celles qui n'en relèvent pas, après concertation avec le bâtonnier ou le représentant de l'ordre provincial des médecins. Voy. art. 90*sexies*, § 3, et 90*octies*, § 3, C. i. cr.

- Le procureur du Roi (ou l'auditeur du travail[32])

  Le procureur du Roi est habilité par l'article 39*bis* du Code d'instruction criminelle à saisir des données stockées dans un système informatique[33]. Il dispose en outre d'une compétence générale de saisie en vertu des articles 28*bis*, § 3[34], et 35 du Code d'instruction criminelle[35]. Il est également habilité par les articles 35 à 37 du Code d'instruction criminelle à pratiquer une saisie en cas de flagrant délit.

- Le juge d'instruction

  Enfin, le juge d'instruction est compétent durant l'instruction pour procéder à une saisie de données informatiques sur pied de l'article 89 du Code d'instruction criminelle. En cas de flagrant délit, c'est l'article 59 du Code d'instruction criminelle qui lui octroie la compétence de saisir.

5 Comment saisir des données informatiques ?

a) Quelles données peuvent être saisies ?

20. La saisie des données informatiques n'est possible que pour les mêmes finalités que celles prévues pour la saisie de droit commun[36]. Autrement dit, peuvent être saisies les données :

- qui sont utiles à la manifestation de la vérité ;
- qui peuvent faire l'objet d'une mesure de confiscation spéciale par le juge du fond (art. 42 et 43*quater* du Code pénal)[37].

b) Quelles sont les étapes de la saisie de données informatiques ?

21. Dans un ordre chronologique, la saisie comporte en principe d'abord la copie des données (voy. *infra*, point 22). Ensuite, elle comprend éventuellement le blocage (voy. point 25 ci-dessous) et le retrait (voy. point 26 ci-dessous) des

---

32 L'auditeur du travail a les mêmes pouvoirs que le procureur du Roi. Voy. Projet de loi relatif à l'amélioration des méthodes particulières de recherche et de certaines mesures d'enquête concernant internet, les communications électroniques et les télécommunications, *Doc. parl.*, Ch. repr., sess. ord., 2015-16, n° 54-1966/001, p. 17.

33 Projet de loi relatif à l'amélioration des méthodes particulières de recherche et de certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications, *Doc. parl.*, Ch. repr., sess. ord., 2015-2016, n° 54-1966/001, p. 12.

34 « *Sauf les exceptions prévues par la loi, les actes d'information ne peuvent comporter aucun acte de contrainte ni porter atteinte aux libertés et aux droits individuels. Ces actes peuvent toutefois comprendre la saisie des choses citées aux articles 35 et 35ter* ».

35 « *Le procureur du Roi se saisira de tout ce qui paraîtra constituer une des choses visées aux articles 42 et 43quater du Code pénal et de tout ce qui pourra servir à la manifestation de la vérité* ».

36 Art. 39*bis*, § 6, C. i. cr.

37 Voy. *supra*, note 14. O. Klees, F. Roggen et D. Vandermeersch, *op. cit.*, p. 40 ; Ch. Conings et S. Royer, *op. cit.*, p. 330.

données, ainsi qu'il en résulte, certes de façon très peu intelligible, du paragraphe 6 de l'article 39*bis* du Code d'instruction criminelle.

22. La **copie** des données est en principe un préalable obligatoire. Les données pertinentes sont ainsi copiées sur des supports de l'autorité, le SPF Justice. Quant aux « *supports dont disposent les personnes compétentes pour utiliser le système* », ceux-ci ne peuvent être employés que dans deux cas, à savoir en cas d'urgence ou en cas de problèmes techniques[38]. Ce dernier point mérite d'être quelque peu explicité afin de bien comprendre les termes de la loi.

23. Que vise-t-on par « *supports dont disposent les personnes compétentes pour utiliser le système informatique* » ? Comme l'indique C. Meunier[39], il s'agit des supports qui appartiennent aux utilisateurs habituels du système informatique et qui seraient disponibles sur le lieu de la saisie. L'article 39*bis*, § 6, du Code d'instruction criminelle permet ainsi aux autorités, uniquement en cas d'urgence (c'est-à-dire de risque de déperdition des données) ou de problèmes techniques, de réquisitionner du matériel nécessaire à la copie sur place si elles n'en disposent pas[40]. Il s'agit d'éviter de devoir interrompre ou abandonner la copie des données à cause d'un problème de matériel inapproprié[41].

24. À cette possibilité de réquisitionner du matériel adéquat s'ajoute celle, pour le procureur du roi, d'« *empêcher l'accès* » aux données dans le système informatique[42], si la copie des données n'est pas possible pour des raisons techniques (par exemple, lorsque le programme d'application est très complexe[43]), ou si le volume des données est tel qu'il est impossible de les copier en un court laps de temps. La doctrine fournit l'exemple d'une salle dans laquelle seraient stockées des centaines de serveurs informatiques contenant des données[44]. Les enquêteurs pourraient dans ce cas bloquer l'accès à cette salle et ainsi mettre virtuellement les données sous scellés[45]. Les données ne sont pas copiées, mais uniquement bloquées, en attendant de pouvoir matériellement les copier[46].

25. Le **blocage** des données est quant à lui facultatif dans la plupart des cas. Il est toutefois obligatoire lorsque deux conditions cumulatives sont remplies : (1) si

38 Art. 39*bis*, § 6, C. i. cr.
39 C. Meunier, *op. cit.*, p. 673.
40 « *En cas de refus des intéressés de fournir le matériel nécessaire à la copie, le magistrat – pourvu qu'il soit compétent à cet effet – peut requérir, sur la base de l'article 88quater nouveau, l'assistance technique d'une personne compétente, le cas échéant par la mise à disposition de matériel adéquat* ». Voy. C. Meunier, *op. cit.*, p. 674.
41 C. Meunier, *op. cit.*, pp. 673 et 674.
42 Art. 39bis, § 6, al. 3, C. i. cr.
43 Projet de loi relatif à la criminalité informatique, *Doc. parl.*, Ch. repr., sess. ord., 1999-2000, n° 50-213/001, p. 21.
44 J. Kerkhofs et P. Van Linthout, *Cybercrime*, Bruxelles, Politeia, 2013, pp. 172-173.
45 Projet de loi relatif à la criminalité informatique, *Doc. parl.*, Ch. repr., sess. ord., 1999-2000, n° 50-213/001, p. 21.
46 Ch. Conings et S. Royer, *op. cit.*, p. 332 ; P. Monville et M. Giacometti, « Les fournisseurs d'accès à internet, nouveaux gendarmes de la toile ? », *R.D.T.I.*, 2014, n° 68, p. 70.

les données forment l'objet de l'infraction et (2) si elles sont contraires à l'ordre public ou aux bonnes mœurs ou si elles constituent un danger pour l'intégrité des systèmes informatiques ou pour des données stockées[47].

26. Si le blocage des données est obligatoire, leur **retrait**, qui en est la conséquence logique, permettra finalement d'éviter que les données dommageables[48] ne se propagent. Le retrait n'est possible qu'après avoir préalablement pris copie des données (art. 39*bis*, § 6, alinéa 4, C. i. cr.), puisque l'idée est qu'à ce stade de la procédure, un retrait ne peut être définitif. En effet, seule une juridiction de fond peut décider d'un retrait ou d'une confiscation[49].

c) La saisie de données issues d'un système informatique verrouillé

27. Il n'est pas rare que le système informatique comportant les données à saisir soit verrouillé par un code ou par d'autres moyens, ou que les données soient chiffrées. L'article 39*bis*, § 5, du Code d'instruction criminelle précise que, dans un tel cas, le procureur du Roi et le juge d'instruction sont habilités à faire usage de « fausses clés »[50] ou de « dispositifs techniques » pour accéder au système informatique. En ce qui concerne l'officier de police judiciaire, la loi ne précise rien le concernant. Il semble donc que sans l'intervention du procureur du Roi ou du juge d'instruction, ce dernier ne soit pas habilité à entrer dans un système verrouillé ou chiffré en vue d'en saisir les données, à moins que le responsable du système informatique y consente[51]. Du reste, comme il le sera expliqué au chapitre suivant concernant la recherche dans un système informatique, lorsque les données saisies le sont dans le cadre d'une extension de recherche (voy. *infra*), seul le juge d'instruction peut faire usage des procédés susvisés pour accéder au système informatique[52].

d) En cas d'urgence…

28. La saisie de données est assortie d'une mesure d'urgence prévue par l'article 39*bis*, § 6, dernier alinéa, du Code d'instruction criminelle concernant certaines infractions limitativement énumérées, à savoir la menace de, et l'incitation à commettre une infraction terroriste (art. 137, § 3, 6°, et 140*bis* du Code pénal) et les infractions relatives à la pédopornographie (art. 383*bis* du Code pénal). Pour

47 Art. 39*bis*, § 6, al.4, C. i. cr.

48 Les travaux préparatoires font référence, par exemple, à des données relatives à la pornographie. Projet de loi relatif à l'amélioration des méthodes particulières de recherche et de certaines mesures d'enquête concernant internet, les communications électroniques et les télécommunications, *Doc. parl.*, Ch. repr., sess. ord., 2015-2016 n° 54-1966/001, p. 23.

49 Ch. Conings et S. Royer, *op. cit.*, p. 332.

50 À savoir « *tout moyen utilisé dans le but de contourner ou de craquer la sécurité d'un système informatique ou d'une partie de celui-ci afin d'obtenir l'accès – sous forme lisible – aux données contenues dans ce système* ». Projet de loi relatif à l'amélioration des méthodes particulières de recherche et de certaines mesures d'enquête concernant internet, les communications électroniques et les télécommunications, *Doc. parl.*, Ch. repr., sess. ord., 2015-2016, n° 54-1966/001, p. 22.

51 C. Forget, *op. cit.*, p. 37.

52 Art. 39*bis*, § 5, *in fine*, C. i. cr. ; C. Forget, *op. cit.*, p. 36.

de telles infractions, le procureur du Roi est habilité en cas d'extrême urgence à autoriser oralement l'officier de police judiciaire à rendre inaccessibles et supprimer des données. Il doit confirmer cette autorisation par écrit le plus rapidement possible.

29. Les travaux préparatoires indiquent que « *[c]ette nouvelle disposition permet de réagir rapidement, sans que le blocage de sites internet devienne une compétence autonome des services de police mêmes* »[53]. Un officier de police judiciaire n'est donc pas habilité à bloquer et à supprimer des données informatiques sans obtenir au minimum une autorisation orale du procureur du Roi[54].

6 Varia

a) Droit à l'information du responsable du système informatique

30. Le ministère public ou le juge d'instruction, selon le cas, doit informer le responsable du système informatique dans les plus brefs délais de la saisie des données, « ***sauf*** *si son identité ou son adresse ne peuvent être raisonnablement retrouvées* ». Il doit ainsi « *communiquer un résumé des données qui ont été copiées, rendues inaccessibles ou retirées* »[55]. En pratique, cette obligation d'information pose toutefois question quant à son effectivité, dès lors que le critère prévu pour en justifier la dispense laisse une large marge d'appréciation aux enquêteurs[56].

b) Garanties d'intégrité et de confidentialité des données

31. Il appartient au ministère public, en vertu du l'article 39*bis*, § 8, du Code d'instruction criminelle de veiller à l'intégrité et à la confidentialité des données saisies. L'intégrité des données doit être garantie par le biais de leur conservation au greffe à l'aide de moyens appropriés[57]. Cette obligation se comprend aisément dès lors que les données saisies serviront ultérieurement de preuves devant la juridiction de fond. Dans cette optique, il importe qu'elles ne subissent aucune altération[58].

53 Projet de loi relatif à l'amélioration des méthodes particulières de recherche et de certaines mesures d'enquête concernant internet, les communications électroniques et les télécommunications, *Doc. parl.*, Ch. repr., sess. ord., 2015-2016, n° 54-1966/001, p. 23.
54 Ch. Conings et S. Royer, *op. cit.*, p. 333.
55 Art. 39*bis*, § 7. Cet article s'applique tant à la recherche qu'à la saisie des données.
56 Voy. également *infra*, point 39 concernant la recherche informatique non secrète.
57 Projet de loi relatif à l'amélioration des méthodes particulières de recherche et de certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications, *Doc. parl.*, Ch. repr., sess. ord., 2015-2016, n° 54-1966/001, p. 25.
58 Ch. Conings et S. Royer, *op. cit.*, p. 334.

B La mesure de conservation rapide des données informatiques

32. La loi du 25 décembre 2016 a ajouté un article 39*ter* dans le Code d'instruction criminelle afin de prévoir la possibilité, pour tout officier de police judiciaire, d'ordonner à une personne physique ou morale la conservation immédiate des données en sa possession ou sous son contrôle, pendant une période maximale de 90 jours, s'il existe une raison de croire que ces données sont susceptibles de perte ou de modification[59].

33. Cette mesure permet aux autorités « *de gagner un peu de temps avant de procéder à d'autres mesures d'enquête "visant à obtenir les données ou leur divulgation"* »[60]. Autrement dit, il s'agit d'une mesure provisoire qui donne la possibilité aux autorités d'accomplir d'autres actes d'enquête requérant des formalités supplémentaires, comme une saisie de données informatiques ou une perquisition[61].

34. La demande doit se faire par une décision écrite et motivée. En cas d'urgence, la conservation peut être ordonnée verbalement. Elle doit être confirmée dans les plus brefs délais par écrit. Bien que la conservation ne puisse excéder en principe 90 jours, ce délai peut être prolongé en réalité indéfiniment. La loi prévoit que la prolongation doit se faire par écrit[62].

35. L'article 39*quater*, § 1er, du Code d'instruction criminelle régit quant à lui les situations internationales et prévoit des dispositions analogues. Il s'adresse ainsi au ministère public qui souhaite solliciter la préservation de données se trouvant hors du territoire belge. L'article 39*quater*, § 2, du Code d'instruction criminelle vise enfin la situation d'autorités étrangères qui sollicitent[63] la conservation de données se trouvant sur le territoire national[64].

II La recherche dans un système informatique

A Introduction

36. Nous allons examiner, dans ce second chapitre, les pouvoirs dont disposent les autorités judiciaires lorsqu'elles souhaitent prendre connaissance de données stockées sur un support informatique, que l'on regroupe sous le vocable « générique de recherche informatique ».

---

59 Art. 39*ter*, C. i. cr. ; C. Forget, *op. cit.*, p. 27 ; V. Franssen et S. Tosza, *op. cit.*, pp. 224 et s.

60 V. Franssen et S. Tosza, *op. cit.*, p. 225.

61 C. Forget, « Les nouvelles méthodes d'enquête dans un contexte informatique : vers un encadrement (plus) strict ? », *R.D.T.I.*, 2017, pp. 25-52, spéc. p. 27 ; V. Franssen et S. Tosza, *op. cit.*, p. 225 ; Rapport explicatif de la Convention de Budapest sur la cybercriminalité, 23 novembre 2001, *Série des traités européens*, n° 185, points 149 à 169, spéc. point 156. et 163, disponible sur https://rm.coe.int/16800ccea4.

62 Art. 39*ter*, C. i. cr. ; V. Franssen et S. Tosza, *op. cit.*, pp. 227-228.

63 Dans le cadre d'une convention ou d'un autre instrument international liant la Belgique et cet État.

64 Pour une analyse plus détaillée de cette mesure de conservation des données informatiques, voy. V. Franssen et S. Tosza, *op. cit.*, pp. 224-234.

37. La nouvelle architecture mise en place par le législateur opère une distinction entre la recherche non secrète et la recherche secrète. La première est régie par les articles 39*ter* et *88ter* du Code d'instruction criminelle là où les articles 90*ter* et suivants réglementent la seconde.

38. Avant d'exposer, par le détail, la manière dont ces différentes recherches peuvent être exécutées, une première question doit être posée : comment peut-on distinguer l'une et l'autre de ces mesures et, surtout, à quel moment les autorités de poursuites peuvent-elles envisager d'y avoir recours ?

39. Il ressort des travaux parlementaires que « *la recherche non secrète sera effectuée en toute transparence, étant donné que le responsable du système analysé est informé de la recherche et qu'une synthèse des données copiées, rendues inaccessibles ou supprimées est communiquée* »[65]. À vrai dire, cette mise au point n'en est pas vraiment une, parce que, vu le libellé de l'article 39*ter* du Code d'instruction criminelle, il arrivera très régulièrement que la personne qui est visée par la mesure n'en soit pas informée, notamment si elle n'est pas considérée comme responsable du système informatique concerné[66], et qu'il est tout aussi rare qu'elle reçoive la moindre information concernant ce qui aura été consulté, rendu inaccessible ou supprimé, ces données étant par essence couvertes par le secret de l'instruction/information. L'on peut également douter de la pertinence de ce premier critère dans la mesure où le texte légal prévoit une dispense de cette obligation de notification si l'identité ou l'adresse du responsable du système informatique ne peut raisonnablement être trouvée, ce qui laisse une (large) marge d'appréciation aux enquêteurs[67].

40. La notion de responsable du système informatique est en outre relativement floue puisqu'elle ne s'identifie pas avec la personne dont les données sont exploitées : il peut s'agir de l'utilisateur du système, de la personne suspectée ou encore de l'opérateur[68].

41. La Cour constitutionnelle a toutefois effectué une mise au point à cet égard en précisant 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 »[69]. Dans la mesure où il y va de la protection des justiciables, la Cour constitutionnelle a par ailleurs très explicitement indi-

65 Rapport au nom de la Commission de la Justice, *Doc. parl.*, Ch. repr., sess. ord., 2015-2016, n° 54-1966/006, p. 64.

66 Il n'y a aucune obligation de mettre au courant l'utilisateur du système informatique (ou la personne) visé(e) par la recherche, voy. V. Franssen et S. Tosza, *op. cit.*, p. 212.

67 C. Forget, *op. cit.*, p. 30.

68 V. Franssen et S. Tosza, *op. cit.*, p. 223.

69 C.C., 6 décembre 2018, arrêt n° 174/2018, point B.22.2.

qué que le responsable du système informatique comprenait également le suspect dont les données ont fait l'objet de la recherche, même lorsqu'il n'exerce pas lui-même le contrôle effectif du système informatique concerné[70].

42. Une autre manière d'appréhender la différence entre ces deux catégories de recherche est de voir comment les travaux préparatoires définissent le caractère secret de la recherche : celui-ci dépend du but que les autorités policières et judiciaires poursuivent[71]. Si elles ont l'intention, par une intrusion et une surveillance en secret, de prendre connaissance de communications ou de données à l'insu des acteurs de ces communications ou à l'insu du propriétaire, du détenteur ou de l'utilisateur d'un système informatique[72], c'est l'article 90*ter* qui trouve à s'appliquer. Si ce but secret fait défaut, la recherche pourra être exécutée sur la base de l'article 39*ter* du Code d'instruction criminelle[73], voire de l'article 88*ter* du même Code lorsqu'elle est étendue à un système informatique distant. C'est donc l'intention d'agir en secret, d'effectuer une recherche à l'insu des personnes visées par la mesure qui constitue le critère déterminant. Les travaux parlementaires évoquent, à titre illustratif, la situation d'un téléphone portable trouvé dans une voiture, il pourra être exploité dans le cadre d'une recherche non secrète, l'objectif des enquêteurs n'étant pas d'effectuer une surveillance en secret[74].

43. L'on peut en conclure que la frontière entre l'une et l'autre de ces recherches est difficile à tracer malgré qu'elles représentent des ingérences considérables dans la vie privée et que les garanties procédurales qui les entourent sont radicalement différentes.

B La recherche non secrète dans un système informatique

1 La recherche locale (39bis, § 2, C. i. cr.)

44. La mesure d'enquête consistant à exécuter une recherche locale dans un système informatique a résisté au contrôle constitutionnel opéré par la Cour constitutionnelle, contrairement à l'extension de la recherche à des données distantes mais accessibles depuis le système informatique concerné[75].

45. Il n'en va par contre pas de même lorsque ce devoir d'enquête concerne les avocats et les médecins et précisément les systèmes informatiques qu'ils utilisent à titre professionnel, même si ladite recherche est portée à leur connaissance[76].

---

70 C.C., 6 décembre 2018, arrêt n° 174/2018, points B.15.2. et B.22.2.
71 *Ibidem*, p. 212.
72 Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord., 2015-2016, 54-1966/001, p. 54.
73 V. Franssen et S. Tosza, *op. cit.*, p. 213.
74 Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord., 2015-2016, 54-1966/001, p. 54.
75 Voy. *infra.*
76 S'il s'agit d'une recherche secrète, menée conformément à l'article 90*ter*, C. i. cr., l'article 90*octies* du même Code contient des garanties supplémentaires destinées à préserver, autant que possible, la relation de confiance qu'ils sont amenés à nouer avec les personnes qui se confient à eux.

La Cour a en effet estimé qu'il n'était pas justifié qu'ils ne bénéficient pas de la clause de protection du secret professionnel qui est par contre prévue lorsque la recherche informatique est menée de façon secrète, de la même manière qu'elle est prévue pour des mesures d'investigation similaires telles que l'ouverture du courrier[77], l'observation[78] ou le contrôle visuel discret[79, 80]. Ainsi, en ce qu'il ne prévoyait pas de dispositions spécifiques pour protéger le secret professionnel des avocats et des médecins, la Cour a annulé l'article 39*bis*[81].

46. À l'heure de clôturer la rédaction de la présente contribution, la loi du 5 mai 2019 portant des dispositions diverses en matière pénale vient juste d'être publiée au *Moniteur belge*[82]. Cette loi intègre l'enseignement de l'arrêt de la Cour constitutionnelle précité en insérant un paragraphe 9 à l'article 39*bis* du Code d'instruction criminelle : celui-ci prévoit désormais que la mesure d'enquête ne peut porter sur le système informatique d'un avocat ou d'un médecin que si celui-ci est lui-même soupçonné d'avoir commis une infraction ou d'y avoir participé, ou si des faits précis laissent présumer que des tiers soupçonnés d'avoir commis une infraction utilisent ce système informatique. La mesure ne peut être exécutée sans que le bâtonnier ou le représentant de l'ordre provincial des médecins en soit averti. Ceux-ci seront informés par le procureur du Roi des éléments qu'il estime relever du secret professionnel, et qui ne seront dès lors pas consignés au procès-verbal[83].

47. À notre estime, cette procédure justifiant l'avertissement donné au bâtonnier ou au représentant de l'ordre provincial des médecins devrait également s'appliquer aux données couvertes par le secret professionnel dont il aurait été pris connaissance à l'occasion de la recherche effectuée sur le système informatique d'un tiers (par ex. une communication électronique adressée par un avocat à son client, dont le système informatique fait l'objet de la recherche)[84].

48. Les modalités d'exécution de la recherche locale dans un système informatique supposent de distinguer selon que le système informatique a été ou non saisi.

a) La recherche dans un support informatique qui a été saisi

49. L'article 39*bis*, § 2, alinéa 1er, du Code d'instruction criminelle décrit la manière dont la recherche de données se trouvant dans un système informatique qui a été saisi peut être exécutée.

77 Conformément à l'art. 88*sexies*, C. i. cr.
78 Conformément à l'art. 56*bis*, C. i. cr.
79 Conformément à l'art. 89*ter*, C. i. cr.
80 C.C., 6 décembre 2018, arrêt n° 174/2018, points B.24.3 et B.25.
81 C.C., 6 décembre 2018, arrêt n° 174/2018, point B.27.
82 Loi du 5 mai 2019 portant des dispositions diverses en matière pénale et en matière de cultes, et modifiant la loi du 28 mai 2002 relative à l'euthanasie et le Code pénal social, *M.B.*, 24 mai 2019.
83 Art. 39*bis*, § 9, C. i. cr.
84 À l'instar de ce que prévoient les art. 90*sexies*, § 3 et 90*octies*, § 3, C. i. cr., concernant les données récoltées suite à l'exécution d'une recherche secrète dans un système informatique (d'un avocat, d'un médecin ou d'un tiers), lorsque celles-ci sont couvertes par le secret professionnel.

(1) Modalités de mise en œuvre de la recherche

50. S'agissant des conditions dans lesquelles cette recherche peut intervenir, elles peuvent être résumées comme suit :

- Ce devoir devra tout d'abord obligatoirement être posé par un officier de police judiciaire[85].

- Pour pouvoir effectuer une recherche, le support doit être préalablement saisi. Dans les faits, cette saisie s'opérera par la simple circonstance que l'officier de policier judiciaire s'emparera du support informatique convoité.

- Le support informatique ne doit pas être verrouillé ou son utilisateur doit avoir accepté de communiquer volontairement son code d'accès à l'enquêteur. S'il rencontre des difficultés à ce sujet, l'article 39*bis*, § 5, du Code d'instruction criminelle permet de forcer l'accès au système, sans le consentement de l'utilisateur :

  – Si l'accès au support informatique est conditionné par l'utilisation de codes d'accès (identifiant, code de saisie, mot de passe, touch ID, face ID...), l'officier de police judiciaire ne pourra effectuer la recherche et devra obtenir une autorisation préalable du procureur du Roi (art. 39*bis*, § 5, du Code d'instruction criminelle) qui pourra, le cas échéant, autoriser l'usage de fausses clés[86].

  – Si l'accès au support informatique est chiffré, l'officier de police judiciaire devra également s'en référer au procureur du Roi qui peut autoriser 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.

- Une fois qu'il est en possession du support informatique, l'officier devra couper les liaisons externes en activant par exemple le mode avion du téléphone[87].

---

85 Le statut d'officier de police judiciaire est nécessaire à l'accomplissement de certains actes de poursuite prévus par la loi, tels qu'une fouille judiciaire – qui se distingue d'une fouille de sécurité –, une perquisition, des écoutes téléphoniques, une arrestation en cas de flagrant délit, une identification d'un abonné auprès d'un service de télécommunication, la pénétration dans un lieu où des stupéfiants sont localisés, une observation ou une infiltration dans le cadre de la mise en œuvre de méthodes particulières de recherche. Certains de ces actes, spécialement ceux qui restreignent les libertés individuelles, ne peuvent être posés en principe que sur la base d'un mandat d'un juge d'instruction. Concrètement, tout fonctionnaire de police ayant un grade égal ou supérieur à celui d'un inspecteur principal a la qualité d'officier de police judiciaire (art. 138 de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux).

86 C'est-à-dire « tout moyen utilisé dans le but de contourner ou de craquer la sécurité d'un système informatique ou d'une partie de celui-ci afin d'obtenir l'accès sous frome lisible aux données contenues dans ce système », Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord., 2015-2016, 54-1966/001, p. 22.

87 C. Forget, *op. cit.*, p. 31.

- La recherche devra être limitée à l'examen des données sauvegardées sur l'appareil. La prise de connaissance porte sur les données qui sont stockées sur le support informatique, ce qui exclut donc de consulter les données qui sont accessibles *via* ce support informatique mais qui sont stockées ailleurs[88]. Des informations circulant via des applications telles WhatsApp, Facebook, Hotmail, Gmail ne seront donc pas directement accessibles à moins d'être stockées et accessibles « hors connexion »[89].

- La recherche en elle-même consistera à lire, inspecter ou examiner les données[90]. L'officier de police judiciaire pourra donc consulter toutes les données sauvegardées (courriels, textos, photos stockées, sms) sur l'appareil lui-même[91].

(2) Illustration

51. Afin d'illustrer le propos, l'on peut énoncer les situations suivantes auxquelles la recherche autorisée par l'article 39*bis*, § 2, du Code d'instruction criminelle s'appliquera :

- Un policier (officier de police judiciaire) surprend et interpelle en flagrant délit une personne soupçonnée de se livrer à la vente de produits stupéfiants. L'intéressé est en possession d'un smartphone que le policier saisit. Il pourra décider seul ou moyennant l'autorisation du procureur du Roi si le système est protégé par un mot de passe que la personne en cause refuse de communiquer, de procéder ou faire procéder à une recherche dans ce système informatique et à exploiter les données qui y sont stockées[92].

- Il en va de même concernant l'exploitation de données qui se trouvent sur un GPS ou un ordinateur (portable)[93].

(3) Appréciation

52. L'on peut tout d'abord se demander si l'efficacité de la recherche n'est pas compromise malgré les règles mises en place par le législateur. En effet, il n'existe quasiment plus aucun support informatique (que ce soit le plus simple téléphone portable, en passant par toute la gamme des smartphones jusqu'aux ordinateurs portables) qui ne se mette pas automatiquement en veille après l'écoulement d'un laps de temps assez bref, ce qui nécessite que son utilisateur s'identifie pour déverrouiller l'appareil et accéder aux fonctionnalités et/ou aux contenus de l'appareil. Dès lors, si l'utilisateur refuse de communiquer son identifiant et/ou code d'accès, l'officier de police judiciaire ne pourra prendre connaissance des données

88 Ch. Conings et S. Royer, *op. cit.*, p. 313.
89 Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord., 2015-2016, 54-1966/001, p. 17.
90 C. Forget, *op. cit.*, p. 31.
91 M.-A. Beernaert, H. D. Bosly et D. Vandermeersch, *Droit de la procédure pénale*, Bruxelles, la Charte, 2017, tome 1, p. 556.
92 M.-A. Beernaert, H. D. Bosly et D. Vandermeersch, *op. cit.*, p. 556.
93 V. Franssen et S. Stosza, *op. cit.*, p. 218.

stockées sur le support informatique, sur la seule base de l'article 39*bis*, § 2, du Code d'instruction criminelle. Le fait de recourir aux prérogatives découlant de l'article 39*bis*, § 5*bis*, du Code d'instruction criminelle (accès au système informatique moyennant fausse clé ou dispositif technique pour déchiffrer les données) justifiera bien souvent l'intervention d'unités spécialisées de la police (RCCU ou FCCU), qui devront déverrouiller l'accès au support informatique avant que le contenu puisse être examiné et encore uniquement en ce qui concerne les données déjà stockées sur celui-ci…

53. Une autre observation s'impose, à l'évidence : la procédure de recherche informatique prévue à l'article 39*bis*, § 2, du Code d'instruction criminelle n'offre que très peu de garanties au justiciable dont les données « stockées » vont pouvoir être examinées et exploitées dans le cadre d'une enquête pénale, et ce en dépit d'une ingérence importante dans le droit au respect de la vie privée[94].

54. La loi reste muette, par exemple, quant aux limites des pouvoirs accordés par l'article 39*bis*, § 2, du Code d'instruction criminelle à un officier de police judiciaire agissant de sa seule initiative et sans devoir en référer à une quelconque autorité judiciaire. Que penser d'un enquêteur qui, ayant saisi un smartphone, déciderait de prendre connaissance des données stockées sur ce support informatique et qui, après avoir activé le mode avion, interromprait la recherche, reconnecterait l'appareil laissant entrer de nouveaux messages ou de nouvelles données dans l'appareil, dont il prendrait connaissance une fois les connexions externes à nouveau désactivées ? Si certains semblent penser qu'une telle pratique serait envisageable[95], nous estimons qu'il s'agirait d'un moyen de contourner l'obligation de passer par un juge d'instruction pour effectuer une recherche informatique secrète…

55. L'on peut encore s'interroger sur le bien-fondé même de l'octroi de compétences tellement étendues à un officier de police judiciaire. En effet, à partir du moment où les liaisons externes d'un support informatique ont été désactivées, le risque de disparition, de suppression ou d'altération de données stockées par un suspect ou un tiers n'est plus envisageable et, dès lors, rien ne semble justifier l'absence d'intervention d'un juge d'instruction ou, à tout le moins, d'un procureur du Roi[96]...

56. Qu'à cela ne tienne, la Cour constitutionnelle a, dans son arrêt du 6 décembre 2018, validé la recherche informatique effectuée par un officier de police judiciaire dans un système informatique qui a été saisi, en estimant que celle-ci constituait seulement un accessoire de la saisie dudit système[97]. À l'instar de l'exploitation de documents ou de livres régulièrement saisis, rien ne s'oppose en

94 C. Forget, *op. cit.*, p. 31.
95 Ch. Conings et S. Royer, *op. cit.*, p. 313.
96 C. Forget, *op. cit.*, p. 32.
97 C.C., 6 décembre 2018, arrêt n° 174/2018, point B.8.6.

effet à ce qu'un officier de police judiciaire effectue une recherche dans les données stockées dans la mémoire d'un système informatique régulièrement saisi, comme il pourrait prendre connaissance du contenu d'un livre ou de documents saisis[98].

57. Selon la Cour, la loi prévoit déjà suffisamment de garanties juridictionnelles concernant la mesure de saisie du système informatique de sorte que l'ingérence dans le droit au respect de la vie privée qui résulte de la recherche dans le système informatique saisi est justifiée au regard des articles 22 de la Constitution et 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales[99].

b) Recherche dans un support informatique qui n'a pas été saisi

58. L'article 39*bis*, § 2, alinéa 2, du Code d'instruction criminelle permet au procureur du Roi (ou au juge d'instruction) d'ordonner une recherche informatique dans un système informatique qui n'est pas saisi mais qui pourrait l'être[100].

59. La situation procédurale prise en considération est celle où il est possible d'un point de vue juridique de saisir le système informatique en question, mais où cela n'est pas considéré opportun ou nécessaire pour certaines raisons[101]. À titre d'exemple, les travaux préparatoires évoquent la recherche dans les ordinateurs d'un cybercafé : si la police constate qu'un suspect a utilisé les services d'un cybercafé, le procureur du Roi peut autoriser une recherche dans les ordinateurs concernés sans que ceux-ci soient préalablement saisis s'il souhaite savoir quels sites ont été consultés par une personne faisant l'objet d'une enquête pour participation à un groupe terroriste[102]. Comme déjà indiqué à l'occasion de l'examen des dispositions relatives à la saisie, il en irait de même d'une recherche dans le système informatique d'une banque, dans la mesure où la saisie du système informatique pourrait causer des difficultés importantes de fonctionnement[103].

60. Concernant les modalités de mise en œuvre de cette mesure, l'on retiendra que :

- Le texte de la loi ne précise pas si l'autorisation du ministère public peut être donnée oralement[104].

- Les mêmes restrictions s'imposent quant à l'obligation de désactiver au préalable toute liaison externe du système informatique examiné.

98 C.C., 6 décembre 2018, arrêt n° 174/2018, point B.8.6 et B.8.7.
99 C.C., 6 décembre 2018, arrêt n° 174/2018, point B.8.7.
100 V. Franssen et S. Stosza, *op. cit.*, p. 218.
101 M.-A. Beernaert, H. D. Bosly et D. Vandermeersch, *Droit de la procédure pénale*, Bruxelles, la Charte, 2017, tome 1, p. 557.
102 Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord., 2015-2016, 54-1966/001, p. 16.
103 *Ibidem*.
104 C. Forget, *op. cit.*, p. 31.

- Le procureur dispose des mêmes prérogatives que celles analysées ci-dessus pour déverrouiller un système informatique, sans le consentement de l'utilisateur.

61. Au final, le système de recherche informatique « locale » mis en place par le législateur apparaît comme peu satisfaisant non seulement parce qu'il institutionnalise une ingérence dans les droits fondamentaux du justiciable[105] en n'offrant à ce dernier aucune garantie (sérieuse), mais en outre parce qu'il peut conduire à des aberrations puisque, par exemple, un officier de police judiciaire qui trouve un système informatique pendant une fouille et veut prendre connaissance de son contenu sur place a besoin d'une autorisation du procureur du Roi alors que ce n'est pas le cas s'il décide de saisir et d'emmener avec lui le support informatique[106]…

62. La Cour constitutionnelle n'y voit à nouveau pas de difficulté, en assimilant cette situation où le procureur du Roi autorise une recherche dans un système informatique non saisi pour des raisons d'opportunité pratique, mais qui pourrait l'être, à une recherche dans des documents préalable à la saisie de ceux-ci[107].

63. La Cour prend appui ici, non pas directement sur les recours et les garanties qui encadrent une saisie puisque le système informatique n'est pas saisi, mais bien sur une disposition équivalente qui encadre la copie des données. En effet, l'article 39*bis*, § 1er, du Code d'instruction criminelle précise que les règles relatives aux saisies s'appliquent, notamment à la copie des données qui résulterait de la recherche dans le système informatique non saisi.

64. Dès lors, non seulement l'on se trouve dans une situation où les conditions légales permettant la saisie du système informatique sont rencontrées[108] mais, en outre, la personne concernée bénéficiera, par l'intermédiaire de la disposition précitée, des recours et garanties relatifs aux saisies[109].

65. Dès lors, l'ingérence dans le droit au respect de la vie privée qui résulte d'une recherche informatique dans un système non saisi est justifiée au regard des exigences des articles 22 de la Constitution et 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales[110].

66. Ce raisonnement nous paraît légèrement critiquable dans la mesure où les garanties et recours sur lesquels la Cour constitutionnelle s'appuie ne trouvent à s'appliquer que si des données sont copiées. Dans le cas contraire, la recherche informatique dans un système non saisi qui ne débouche sur aucune copie des

105 *Ibidem.*
106 Ch. Conings et S. Royer, *op. cit.*, p. 314.
107 C.C., 6 décembre 2018, arrêt n° 174/2018, point B.9.3.
108 Puisqu'il est explicitement prévu que le système informatique pourrait être saisi.
109 C.C., 6 décembre 2018, arrêt n° 174/2018, point B.9.2.
110 C.C., 6 décembre 2018, arrêt n° 174/2018, point B.9.5.

données, malgré l'atteinte au droit au respect de la vie privée qu'elle induit, ne comporte aucune garantie de sorte qu'on peut se demander s'il était effectivement justifié de confier une telle compétence au procureur du Roi et non au juge d'instruction…

67. Amenée à se prononcer également sous l'angle de l'égalité de traitement, la Cour constitutionnelle reproduit la même incohérence, en se référant aux garanties et aux recours applicables aux saisies qui s'appliquent, selon elle, tant concernant la recherche informatique dans un système saisi (intervention d'un officier de police judiciaire) que dans un système informatique qui ne l'est pas (intervention du procureur du Roi). À l'égard de cette dernière recherche, en effet, la Cour se réfère à nouveau au fait que les recours et garanties prévus pour la saisie sont applicables aux copies des données identifiées suite à la recherche effectuée dans le système informatique non saisi[111]. À nouveau, la Cour fait abstraction de l'hypothèse où la recherche informatique dans un système non saisi ne mène à aucune copie de données de sorte qu'aucun recours ou garantie ne s'applique à la personne concernée, qui pourra toutefois compter (pour autant que cela soit réellement une garantie) sur l'intervention du procureur du Roi.

2 L'extension de la recherche informatique (art. 39bis, § 3, et 88ter du Code d'instruction criminelle)

a) Le régime introduit par la loi du 25 décembre 2016

68. La loi du 25 décembre 2016 a introduit, à l'article 39*bis*, § 3, du Code d'instruction criminelle, la possibilité d'ordonner une extension de la recherche effectuée au départ d'un système informatique saisi ou pouvant être saisi.

(1) Champ d'application et autorité compétente

69. Le champ d'application de cette mesure est extrêmement large puisqu'il couvre toute situation où les enquêteurs entendent accéder aux données de réseaux sociaux qui ne sont pas présentes sur le support informatique au moment de la saisie ou prendre connaissance de courriels/textos qui auraient été réceptionnés après la saisie. L'extension de la recherche vise ainsi des situations où un smartphone a été saisi et où il apparaît nécessaire d'avoir accès au compte Hotmail, Facebook ou Dropbox auquel le smartphone est connecté[112]. L'on peut également penser à la situation où l'on souhaite pouvoir prendre connaissance du contenu d'un site internet ou d'une banque de données non accessible à partir de l'appareil d'un des utilisateurs réguliers de ce site ou de cette banque de données[113].

111 C.C., 6 décembre 2018, arrêt n° 174/2018, points B.10.1. et B.10.2.
112 Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord., 2015-2016, n° 54-1966/001, p. 18.
113 M.-A. Beernaert, H. D. Bosly et D. Vandermeersch, *op. cit.*, p. 556.

70. Le nouvel article 39*bis* permettait au procureur du Roi d'ordonner une telle extension, à condition toutefois que ne soit pas nécessaire l'usage de fausse clé ou de technique de décryptage, auquel cas seul un juge d'instruction était compétent pour étendre la recherche informatique.

71. Il s'agissait là d'une nouveauté introduite par la loi du 25 décembre 2016, dans la mesure où, auparavant, l'article 88*ter* du Code d'instruction criminelle – qui a néanmoins été réintroduit par la loi du 5 mai 2019[114] – imposait l'intervention du juge d'instruction pour ordonner une telle extension de la recherche informatique[115].

72. Ce transfert de compétences du magistrat instructeur au procureur du Roi était toutefois justifié par le fait qu'il s'agissait d'une recherche non secrète, sans approche ou exploitation secrète des éléments de la vie privée de la personne concernée, de sorte que l'intervention du procureur du Roi avait été jugée suffisante par le législateur[116].

(2) Modalités de mise en œuvre

73. Comme auparavant[117], le législateur soumettait à trois conditions le recours à ce qui s'apparente à une véritable perquisition virtuelle[118] :

- La mesure doit être nécessaire pour la manifestation de la vérité à l'égard de l'infraction qui fait l'objet de la recherche.
- D'autres mesures seraient disproportionnées, ou 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.

74. En réalité, très peu de restrictions à la possibilité d'ordonner une recherche en réseau étaient prévues sur la base de l'article 39*bis*, § 3, du Code d'instruction criminelle :

- La recherche informatique pouvait uniquement être étendue à d'autres systèmes informatiques accessibles pour l'utilisateur habituel à partir du support où la recherche informatique avait commencé. Cette connexion technique avec les systèmes informatiques auxquels la recherche pouvait être étendue

114 Art. 11 de la loi du 5 mai 2019 portant des dispositions diverses en matière pénale et en matière de cultes, et modifiant la loi du 28 mai 2002 relative à l'euthanasie et le Code pénal social, *M.B.*, 24 mai 2019.
115 Art. 88*ter*, C. i. cr., tel qu'en vigueur avant son abrogation par la loi du 25 décembre 2016.
116 Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord., 2015-2016, n° 54-1966/001, p. 18.
117 Voy. art. 88*ter*, §§ 1er et 2, C. i. cr., tel qu'en vigueur avant son abrogation par la loi du 25 décembre 2016.
118 *Ibidem*, p. 557 ; V. Franssen et S. Stosza, *op. cit.*, p. 220.

devait représenter un lien permanent et stable[119]. La recherche ne pouvait donc s'étendre à n'importe quel système informatique qui serait techniquement accessible à partir du support initial[120].

- Cette compétence extrêmement large du procureur du Roi ne pouvait être exercée que si l'accès aux données distantes n'était pas protégé et/ou qu'elles n'étaient pas sécurisées. La seule véritable limite aux pouvoirs conférés au ministère public était liée à cette seule circonstance : s'il fallait utiliser une fausse clé ou des techniques de décryptage ou de hacking pour effectuer cette extension de la recherche, l'intervention du juge d'instruction était requise (art. 39*bis*, § 5, du Code d'instruction criminelle), éventuellement via la mini-instruction[121].

  Pour illustrer le propos, l'on peut reprendre un exemple cité lors des travaux parlementaires[122] : un smartphone saisi est protégé par un code d'accès. Le policier qui désirait prendre connaissance de son contenu devait obtenir l'autorisation préalable du procureur du Roi pour forcer son accès. Une fois entré dans le smartphone, le policier pouvait accéder à des applications qui se situaient dans le cloud de l'utilisateur (par exemple Dropbox) si ce compte était immédiatement accessible. En revanche, si l'accès à ces applications nécessitait un code d'accès complémentaire et spécifique, il devait obtenir une décision du juge d'instruction.

(3) Appréciation

75. Pour mesurer la portée des compétences qui avaient ainsi été confiées au ministère public, l'on peut prendre l'exemple suivant : un smartphone est saisi dans le cadre d'une information. L'enquêteur souhaite avoir accès aux données distantes stockées dans le cloud. Sur simple autorisation orale du procureur du Roi, il pouvait accéder aux comptes Facebook, Hotmail, aux informations stockées sur des espaces de stockage dématérialisés (Dropbox, Google Drive…) à partir du moment où le mot de passe de ces applications/services avait été retenu automatiquement par le smartphone. Vu le nombre d'utilisateurs qui, par facilité, recourent à cette modalité d'accès pour leurs connexions à distance, la mesure exécutée sur la base de l'article 39*bis*, § 3, du Code d'instruction criminelle présentait un caractère hautement intrusif.

76. La variable d'ajustement qui justifiait l'intervention obligatoire d'un juge d'instruction et des garanties qui accompagnent son intervention était alors tributaire de la simple possibilité qu'un système retienne un mot de passe. Le Conseil d'État s'en était ému, à juste titre[123].

119 V. Franssen et S. Stosza, *op. cit.*, p. 221 ; Ch. Conings et S. Royer, *op. cit.*, p. 315.
120 V. Franssen et S. Stosza, *op. cit.*, p. 221.
121 M.-A. Beernaert, H. D. Bosly et D. Vandermeersch, *op. cit.*, p. 558 ; Ch. Conings et S. Royer, *op. cit.*, p. 315.
122 Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord., n° 54-1966/001, pp. 19-20.
123 C. Forget, *op. cit.*, p. 33.

(4) Varia

77. Comme le prévoyait déjà l'article 88*ter* du Code d'instruction criminelle[124], l'article 39*bis*, § 3, permettait de collecter des preuves éventuellement situées à l'étranger, et ce sans devoir passer par les lourdeurs d'une commission rogatoire.

78. La loi prévoyait en effet que, lorsqu'il s'avérait que ces données ne se trouvaient pas sur le territoire du Royaume, elles pouvaient seulement être copiées. Dans ce cas, le procureur du Roi devait communiquer sans délai cette information au Service public fédéral Justice, qui en informait les autorités compétentes de l'État concerné, à tout le moins si celui-ci pouvait raisonnablement être déterminé[125].

79. Les frontières du principe de territorialité qui fonde en principe l'intervention des autorités judiciaires belges s'en trouvaient clairement élargies…

b) L'arrêt de la Cour constitutionnelle : retour à la situation antérieure de l'article 88*ter*, C. i. cr.

80. D'aucuns se sont inquiétés[126] de l'étendue des pouvoirs coercitifs et intrusifs accordés au ministère public lorsqu'il s'agissait d'étendre la recherche informatique à d'autres systèmes, et de la faiblesse des garanties prévues par le législateur face à un tel niveau d'intrusion dans la vie privée[127].

81. Contrairement à la recherche informatique « locale », cette nouvelle méthode d'enquête n'a toutefois pas résisté à la censure de la Cour constitutionnelle.

82. La Cour constitutionnelle fait état, à cet égard, du développement considérable des réseaux accessibles au départ des systèmes informatiques et de leur utilisation intensive par l'immense majorité des citoyens, que ce soit pour y stocker des documents et des données relevant de leur vie privée, en ce compris ce qu'elle a de plus intime, ou pour communiquer entre eux. Elle estime qu'une mesure d'investigation qui permet d'accéder à l'ensemble de ces données et communications sur les réseaux connectés à un système informatique appartenant à un individu constitue une ingérence dans son droit au respect de la vie privée comparable à celles causées par une perquisition dans un domicile privé ou par une interception de ses communications téléphoniques ou de son courrier postal[128].

83. En disant cela, la Cour constitutionnelle laissait peu de doute sur sa conclusion puisque les trois mesures auxquelles elle compare l'extension d'une recherche informatique relèvent toutes trois de la compétence du juge d'instruction[129]. Les

124 Art. 88*ter*, § 3, al. 2, C. i. cr., tel qu'en vigueur avant son abrogation par la loi du 25 décembre 2016.
125 M.-A. Beernaert, H. D. Bosly et D. Vandermeersch, *op. cit.*, p. 559.
126 V. Franssen et S. Stosza, *op. cit.*, p. 221.
127 C. Forget, *op. cit.*, p. 33.
128 C.C., 6 décembre 2018, arrêt n° 174/2018, point B.14.1.
129 Art. 87 ; 88 ; 88*sexies* et 90*ter*, C. i. cr. Voy. C.C., 6 décembre 2018, arrêt n° 174/2018, point B.14.2.

critères mis en avant par le législateur pour justifier l'intervention du procureur du Roi au détriment du juge d'instruction dont la mission est encadrée par son indépendance et son impartialité ne constituaient pas, à ce titre, une justification raisonnable, selon le point de vue de la Cour constitutionnelle.

84. Ainsi, le fait que la recherche étendue exécutée sur décision du procureur du Roi présente un caractère non secret n'était pas suffisamment pertinent, puisque certains devoirs relevant de la compétence du juge d'instruction, telle une perquisition dans un domicile – à l'égard de laquelle la Cour a déjà eu l'occasion de rappeler qu'elle ne pouvait être autorisée que dans le cadre d'une instruction[130] –, ne présentent pas forcément un caractère secret[131].

85. La Cour constitutionnelle poursuit son raisonnement en précisant que l'information donnée au responsable du système informatique et, le cas échéant, au suspect[132] – ce qui rend la recherche informatique et son extension non secrète – n'est donnée qu'après que la mesure ait pris fin. Cette mesure comporte dès lors une ingérence importante dans le droit au respect de la vie privée de la personne concernée, qui n'y aura, en outre, pas consenti[133].

86. Dès lors, la justification de la différence de traitement entre les personnes soumises à une recherche portant sur les réseaux connectés à leur système informatique, selon que la recherche est considérée comme secrète ou non, n'est pas parue suffisante à la Cour pour permettre l'intervention du procureur du Roi à la place du juge d'instruction. Il n'y avait dès lors pas lieu de se détacher du principe selon lequel une mesure d'investigation portant autant atteinte aux droits et libertés individuels qu'une recherche informatique étendue aux systèmes connectés ne peut être accomplie que dans le cadre d'une instruction[134].

87. La Cour estime en outre que le second critère de répartition des compétences entre procureur du Roi et juge d'instruction, soit le fait que l'accès aux réseaux connectés au système informatique soit protégé par un mot de passe ou que les données distantes soient codées ou cryptées, ne justifiait pas non plus que l'ingérence dans le droit au respect de la vie privée, qui n'est pas moindre lorsque de telles protections n'ont pas été installées, ne soit pas entourée des mêmes garanties[135].

88. Vu la gravité de l'ingérence dans le droit au respect de la vie privée provoquée par l'extension d'une recherche dans un système informatique, seule l'inter-

130 C.C., 21 décembre 2017, arrêt n° 148/2017.
131 C.C., 6 décembre 2018, arrêt n° 174/2018, point B.15 .4.
132 C.C., 6 décembre 2018, arrêt n° 174/2018, point B.15.2.
133 C.C., 6 décembre 2018, arrêt n° 174/2018, point B.15.3.
134 C.C., 6 décembre 2018, arrêt n° 174/2018, point B.15.5.
135 C.C., 6 décembre 2018, arrêt n° 174/2018, point B.16.1.

vention préalable d'un juge indépendant et impartial présente les garanties suffisantes pour justifier une telle ingérence[136].

89. La Cour constitutionnelle a ainsi annulé l'article 39*bis*, § 3, du Code d'instruction criminelle, et est dès lors revenue au système antérieur de l'article 88*ter* du Code d'instruction criminelle[137], qui prescrivait l'intervention du juge d'instruction pour étendre une recherche informatique vers les systèmes ou parties de systèmes connectés au système informatique faisant l'objet de la recherche locale.

90. Suite à l'adoption de la loi du 5 mai 2019, l'article 88*ter* a été remplacé en vue d'y intégrer quelques adaptations purement formelles[138]. Le régime antérieur est ainsi à nouveau pleinement en vigueur : seul le juge d'instruction peut ordonner une extension de la recherche dans un système informatique.

91. Ainsi que l'article 39*bis*, § 3, le prévoyait, cette recherche ne sera permise qu'aux conditions suivantes[139] :

- l'extension est nécessaire pour la manifestation de la vérité à l'égard de l'infraction qui fait l'objet de la recherche ;
- d'autres mesures seraient disproportionnées, ou il existe un risque que, sans cette extension, des éléments de preuve soient perdus ;
- l'extension ne peut excéder les systèmes informatiques ou les parties de tels systèmes auxquels les personnes autorisées à utiliser le système informatique faisant l'objet de la saisie ont accès.

92. Le cas échéant, le juge d'instruction pourra également recueillir des preuves à l'étranger en copiant celles-ci, à condition d'en avertir l'autorité compétente par l'intermédiaire du ministère public et du ministre de la Justice, à tout le moins, si celle-ci peut raisonnablement être identifiée[140].

93. Il est également prévu – et c'est une nouveauté prévue par la loi du 5 mai 2019 – que le juge d'instruction ordonne verbalement, en cas d'urgence, l'extension de la recherche, à condition de confirmer cet ordre par écrit, dans les meilleurs délais, avec mention des motifs de l'extrême urgence[141].

---

136 C.C., 6 décembre 2018, arrêt n° 174/2018, point B.16.4.

137 Afin d'éviter de créer un vide juridique concernant la mesure d'extension de la recherche dans un système informatique, la Cour constitutionnelle a également annulé l'article 13 de la loi du 25 décembre 2016, indissociablement lié à l'article 39*bis*, § 3, du Code d'instruction criminelle, lequel abrogeait en effet l'article 88*ter* dudit Code.

138 Art. 88*ter*, C. i. cr., tel qu'inséré par l'art. 11 de la loi du 5 mai 2019 portant des dispositions diverses en matière pénale et en matière de cultes, et modifiant la loi du 28 mai 2002 relative à l'euthanasie et le Code pénal social, *M.B.*, 24 mai 2019.

139 Art. 88*ter*, al. 1er et 2, C. i. cr.

140 Art. 88*ter*, al. 3, C. i. cr.

141 Art. 88*ter*, al. 5, C. i. cr.

3 Autres recherches informatiques : compétence du magistrat instructeur

94. Le législateur a enfin introduit une catégorie résiduelle de recherche informatique[142] : l'article 39*bis*, § 4, du Code d'instruction criminelle prévoit en effet que 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.

95. Toute autre recherche non secrète dans un système informatique que celles examinées ci-dessus ne peut donc être ordonnée que par un juge d'instruction.

96. Il s'agira surtout de la recherche dans un système informatique à distance, c'est-à-dire la situation où la recherche ne s'effectue pas à partir d'un support physique en présence des enquêteurs, mais à partir de leurs propres ordinateurs[143]. L'on pense à des situations où les autorités judiciaires souhaiteraient procéder à une recherche sur un compte Gmail ou Yahoo d'un suspect, sans le saisir, ou à une situation où elles n'ont pas pu saisir un support matériel à partir duquel le suspect a pris accès à ce compte[144].

97. Pour le surplus, le régime juridique est calqué sur celui de l'extension de recherche informatique relevant de la compétence du procureur du Roi : les conditions de nécessité et de proportionnalité s'appliquent de la même manière ainsi que la possibilité d'une autorisation orale en cas d'extrême urgence[145].

C La recherche secrète dans un système informatique

1 Présentation et définitions

98. L'article 90*ter*, § 1er, alinéa 1er, du Code d'instruction criminelle permet « *au juge d'instruction, dans un but secret, d'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* ».

99. Ce faisant, le législateur a choisi de fusionner en une seule et même mesure la recherche secrète dans un système informatique et l'interception de télécommunications, et ce dans l'optique d'adapter la procédure pénale aux évolutions technologiques qui rendent impossible la distinction entre, d'une part, la recherche dans un système informatique et, d'autre part, l'interception de communications[146].

142 Ch. Conings et S. Royer, *op. cit.*, p. 315.
143 V. Franssen et S. Stosza, *op. cit.*, p. 222.
144 V. Franssen et S. Stosza, *op. cit.*, p. 222 ; Ch. Conings et S. Royer, *op. cit.*, p. 315.
145 V. Franssen et S. Stosza, *op. cit.*, p. 222.
146 *Ibidem*.

100. Quelques précisions de langage s'imposent tout d'abord :

- Le législateur a pris le soin de préciser que le terme « communication » recouvre tout énoncé, oral ou non oral, fait directement ou à distance et, notamment, les déclarations et conversations directes ou téléphoniques, de même que toutes les formes modernes de la télématique. Pour ce qui est des communications électroniques, la notion vise tout contenu de communications électroniques, peu importe qu'il s'agisse de signes, messages écrits, dessins, photos, sons, vidéos[147]… C'est donc le contenu de la communication qui importe, qu'elle soit orale ou écrite, analogique ou numérique[148].

- La loi a remplacé le critère traditionnel de la communication « en cours de transmission » par la phrase « quel que soit leur stade de transmission ». Le critère traditionnel se révélait particulièrement difficile à appliquer aux nouvelles formes de communication. Il est en effet malaisé de déterminer quand une communication – et particulièrement une communication électronique – est délivrée, soit en raison de la durée extrêmement courte de la transmission, soit parce que la durée de la transmission peut varier selon le type de logiciel utilisé[149].

- Le terme non accessible s'entend dès lors que les communications ont lieu dans la sphère privée et ne sont pas destinées à être entendues par tout un chacun, peu importe le lieu où les propos ou les messages sont émis ou entendus[150]. En ce qui concerne les communications électroniques, le même critère est d'application : selon que les données sont accessibles ou non à tous, la communication aura un caractère privé ou non. Ainsi, les communications via Skype, WhatsApp, Facebook, Messenger sur une page dont l'accès est réservé à certaines personnes ont un caractère privé contrairement aux données auxquelles n'importe quel internaute peut avoir accès via un moteur de recherche[151].

- Le terme « explorer » se rapporte aux systèmes informatiques et a la même signification que l'exécution d'une recherche dans un système informatique[152].

- Le terme « enregistrer » porte tant sur les communications non accessibles au public (enregistrements sonores dans le cadre d'écoutes téléphoniques) que sur l'enregistrement ou la copie de données d'un système informatique (copie d'images ou de documents d'un ordinateur sur une clé USB)[153].

147 M.-A. Beernaert, H. D. Bosly et D. Vandermeersch, *op. cit.*, p. 793.
148 V. Franssen et S. Stosza, *op. cit.*, p. 222.
149 *Ibidem*, p. 223.
150 M.-A. Beernaert, H. D. Bosly et D. Vandermeersch, *op. cit.*, p. 793.
151 *Ibidem*, p. 794.
152 Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord., n° 54-1966/001, p. 53.
153 Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord., n° 54-1966/001, pp. 53-54.

- Le caractère secret de la mesure renvoie au fait que le juge d'instruction a l'intention, par une intrusion et une surveillance en secret, de prendre connaissance de communications ou de données à l'insu des acteurs de ces communications, ou à l'insu du propriétaire, du détenteur ou de l'utilisateur du système informatique[154]. Si la prise de connaissance, l'exploration ou l'enregistrement des communications non accessibles au public ou des données informatiques ont lieu de façon non secrète, les règles édictées à l'article 39*bis* du Code d'instruction criminelle trouveront à s'appliquer[155].

2 Qui peut ordonner la recherche ? Formalités

101. La recherche secrète dans un système informatique est de la compétence exclusive du juge d'instruction, laquelle ne peut par ailleurs pas être ordonnée dans le cadre d'une mini-instruction[156], sauf cas particulier du flagrant délit. L'article 90*ter*, § 5, du Code d'instruction criminelle prévoit alors la possibilité pour le procureur du Roi d'ordonner pareille mesure[157].

102. Lors de la mise en œuvre d'un tel dispositif, le juge d'instruction peut requérir le concours « en temps réel » des opérateurs et fournisseurs de communications électroniques, ainsi que nous le verrons plus loin.

103. Sur le plan formel, le juge d'instruction doit rendre une ordonnance motivée qui doit contenir un certain nombre de mentions, même si ces mentions ne sont plus prévues à peine de nullité.

104. La durée de validité de la mesure est en principe d'un mois à dater de la première autorisation[158], renouvelable sans que la durée totale de l'interception puisse dépasser 6 mois[159], sauf en cas de retard dû à sa préparation technique[160].

3 Modalités de mise en œuvre de la mesure

105. Pour le surplus, la loi fixe des balises très peu contraignantes à la possibilité pour le juge d'instruction de s'ingérer dans une communication privée :

154 Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord., n° 54-1966/001, p. 54.
155 M.-A. Beernaert, H. D. Bosly et D. Vandermeersch, *op. cit.*, p. 795.
156 Art. 28*septies*, C. i. cr. ; Ch. Conings et S. Royer, *op. cit.*, p. 318.
157 En cas de flagrant délit et tant que la situation de flagrant délit perdure, le procureur du Roi peut ordonner la mesure visée au § 1er de l'art. 90*ter pour* les infractions visées aux articles 137, 347*bis*, 434 ou 470 du Code pénal. En outre, en cas de flagrant délit, le procureur du Roi peut ordonner la mesure visée au § 1er pour les infractions visées à l'article 137 du Code pénal, à l'exception de l'infraction visée à l'article 137, § 3, 6°, du même Code, dans les septante-deux heures qui suivent la découverte de cette infraction.
158 Art. 90*quater*, § 1, 4°, C. i. cr.
159 Art. 90*quinquies*, al. 1er, C. i. cr.
160 C. Forget, *op. cit.*, p. 50.

– En ce qui concerne les personnes visées : la recherche secrète n'est autorisée qu'à l'égard des personnes soupçonnées sur la base d'indices précis d'avoir commis une des infractions visées par la loi, soit à l'égard de moyens de communication ou de systèmes informatiques régulièrement utilisés par un suspect. Cependant, peuvent également faire l'objet d'une telle recherche, les lieux présumés fréquentés par un suspect, de même que les personnes présumées, sur la base de faits précis, être en communication régulière avec celui-ci[161]. Une mesure de recherche pourra donc être effectuée aux lieux de résidence habituels d'un suspect sans violer les règles de l'inviolabilité du domicile, notamment pour le placement de l'appareillage technique en vue de l'exécution de la mesure[162]. Une telle mesure peut en outre être envisagée au parloir d'une prison[163].

  Si l'on combine ce champ d'application *ratione personae* et *ratione loci* extrêmement large aux autres prérogatives dont dispose un magistrat instructeur, le résultat a de quoi laisser pantois... Un juge d'instruction pourrait ainsi parfaitement ordonner par une mesure de contrôle visuel discret, la pénétration dans un domicile, dans un lieu privé ou dans un système informatique à l'insu de son propriétaire ou utilisateur en vue de réaliser une mesure de recherche par le placement d'un matériel technique adéquat, et ce tant de jour que de nuit[164]. Il pourrait ainsi faire placer, à l'insu de l'utilisateur d'un système informatique, des logiciels espions pour décrypter et décoder les données stockées, traitées ou transmises par ce système[165].

  La seule limitation concerne les locaux utilisés à des fins professionnelles, la résidence, les moyens de communication ou les systèmes informatiques d'un avocat ou d'un médecin : la mesure ne peut être ordonnée sans que le bâtonnier ou le représentant de l'ordre provincial des médecins en soit averti, tandis que le juge d'instruction évaluera, après concertation avec ceux-ci, quelles parties des communications ou des données, qu'il estime pertinentes pour son instruction, relèvent du secret professionnel et celles qui n'en relèvent pas. Seules celles-ci seront transcrites ou reproduites[166].

– Le juge d'instruction doit constater l'existence d'indices sérieux de la commission d'une des infractions énumérées limitativement par la loi[167]. Il s'agit là du respect d'un principe de proportionnalité. Il ne s'agit cependant que d'une garantie de façade tant la liste des infractions pour lesquelles est autorisé le recours à une mesure de recherche secrète est longue et ne cesse de s'allonger.

161 Art. 90*ter*, § 1er, alinéa 4, C. i. cr.
162 M.-A. Beernaert, H. D. Bosly et D. Vandermeersch, *op. cit.*, p. 799.
163 *Ibidem.*
164 *Ibidem*, p. 800.
165 *Ibidem.*
166 Art. 90*sexies*, § 3, et 90*octies*, C. i. cr.
167 Art. 90*ter*, § 2, C. i. cr.

– Une troisième limitation apparaît tout aussi inopérante puisqu'elle subordonne la mesure à la recherche de données qui peuvent servir à la manifestation de la vérité[168]. Bref, cela revient à uniquement interdire les recherches exploratoires dans des systèmes informatiques[169].
– Enfin, la mesure de recherche ne peut en principe être ordonnée que si d'autres moyens d'investigation ne suffisent pas à la manifestation de la vérité[170], soit le respect d'un principe de subsidiarité. En théorie, la recherche ne pourra être ordonnée que si les autres moyens d'enquête[171] ne permettent pas d'obtenir le même résultat. En pratique, cette exigence n'implique pas que ces autres moyens d'enquête usuels aient été effectivement utilisés[172]. La garantie prévue par la loi fait donc long feu puisque la mesure peut être prise dès que le juge d'instruction estime que les autres moyens d'investigation ne suffisent pas à la manifestation de la vérité mais qu'il est quasi impossible de démontrer que le juge aurait dû recourir à d'autres moyens d'investigation pouvant aboutir au même résultat[173].

4 Mesures d'accompagnement

106. Le juge d'instruction peut, par ailleurs, ordonner des mesures d'accompagnement : il sera parfois nécessaire, pour un système informatique ultra-protégé, de se rendre dans le domicile de l'utilisateur afin d'installer un dispositif technique pour contourner la protection mise en place et éventuellement d'intercepter sur place les données.

107. L'article 90*ter*, § 1er, alinéa 3, du Code d'instruction criminelle prévoit ainsi que le juge d'instruction peut, et ce à l'insu et sans le consentement de l'occupant, du propriétaire ou de son ayant droit, ou de l'utilisateur, ordonner, à tout moment :

- la pénétration dans un domicile, un lieu privé ou un système informatique ;
- 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.

168 Art. 90*ter*, § 1er, al. 4, C. i. cr.
169 Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord., 2015-2016, n° 54-1966/001, p. 58.
170 Art. 90*ter*, § 1er, al. 2, C. i. cr.
171 Perquisition, repérage de télécommunications, surveillances, recherches informatiques non secrètes…
172 M.-A. Beernaert, H. D. Bosly et D. Vandermeersch, *op. cit.*, p. 808.
173 *Ibidem.*

108. Les champs du possible semblent définitivement infinis puisqu'en application de la disposition examinée, des enquêteurs peuvent être autorisés à placer un logiciel espion sur l'ordinateur d'une personne en vue d'exploiter le contenu du disque dur ou à intercepter une conversation et d'en prendre copie[174], mais encore à surveiller un ordinateur et à intercepter l'ensemble des données informatiques, par exemple les entrées clavier, les mots de passe, voire à intercepter les échanges de flux de données circulant via l'appareil et par internet[175]. Il va sans dire que la mesure ordonnée par le juge d'instruction peut donc s'avérer particulièrement intrusive pour la vie privée des personnes concernées.

5 Recherche secrète versus contrôle visuel discret dans des systèmes informatiques

109. L'article 89*ter*, alinéa 1er, du Code d'instruction criminelle prévoit que seul un juge d'instruction peut autoriser un service de police à s'introduire dans un système informatique et à l'explorer, à l'insu du propriétaire, du détenteur ou de l'utilisateur, sans leur consentement.

110. Il s'agit d'une mesure ressortissant de la compétence exclusive du juge d'instruction, qui ne pourra être ordonnée – sauf cas d'urgence – que sur la base d'une décision écrite et motivée[176]. Les principes de proportionnalité et de subsidiarité devront également être respectés.

111. Dans le respect des objectifs assignés dans le cadre d'une opération classique de contrôle visuel discret[177], cette mesure ordonnée dans un système informatique devrait permettre de s'assurer de la présence de fichiers numériques falsifiés[178], d'un compte email qui aurait servi à commettre une infraction[179] ou de bitcoins qui représenteraient des avantages patrimoniaux tirés d'une infraction[180].

112. La distinction avec la recherche informatique secrète réside principalement dans la finalité de cette mesure : il s'agirait, selon les travaux parlementaires, d'un « *instrument orienté qui permet une intrusion graduelle dans la vie privée et la prise de prélèvements qui, le cas échéant, peuvent justifier une mesure encore plus intrusive* »[181].

---

174 Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord., 2015-2016, n° 54-1966/001, p. 57.
175 C. Forget, *op. cit.*, p. 50.
176 Art. 89*ter juncto* art. 46*quinquies*, § 1er, al. 1er, C. i. cr.
177 Art. 46*quinquies*, § 2, al. 1er, C. i. cr. : « *La pénétration du lieu privé visé au paragraphe 1er, et l'ouverture des objets fermés se trouvant sur ce lieu, peut uniquement avoir lieu aux fins : 1) d'inspecter ce lieu et de s'assurer de la présence éventuelle de choses qui forment l'objet d'une infraction, qui ont servi ou qui sont destinées à en commettre une ou qui ont été produites par une infraction, des avantages patrimoniaux tirés directement de l'infraction, des biens et valeurs qui leur ont été substitués et des revenus de ces avantages investis ; 2) de réunir les preuves de la présence des choses visées au 1°* ».
178 Ch. Conings et S. Royer, *op. cit.*, p. 317.
179 *Ibidem.*
180 *Ibidem.*
181 Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord., 2015-2016, n° 54-1966/001, p. 52.

113. Le contrôle visuel discret permet la recherche de preuves d'infractions ainsi que, le cas échéant, la prise d'échantillons, tandis que la recherche informatique permet de collecter des moyens de preuve[182]. D'un côté, les enquêteurs peuvent vérifier si des preuves existent dans un système informatique, mais non les emporter, à l'exception de certains échantillons[183], de l'autre, la recherche secrète permet de collecter, utiliser et copier les données interceptées et/ou enregistrées dans un système informatique qui ont été découvertes[184].

114. La limite entre l'une et l'autre de ces mesures apparaît néanmoins difficile à tracer en pratique[185].

III L'obligation de collaboration

115. Afin de renforcer l'efficacité de la récolte de preuves numériques, le législateur a pris le soin de permettre aux autorités judiciaires de solliciter, si besoin, le concours technique de tiers à l'enquête pénale, et précisément des opérateurs de réseaux de communications électroniques, ainsi que des fournisseurs de services relatifs à ces réseaux.

A Une obligation de coopération relativement large

116. La coopération des opérateurs de réseaux de communications électroniques et de fournisseurs de services relatifs à ces réseaux peut être requise par les autorités judiciaires à l'occasion de l'exécution de trois mesures d'enquête :

- la recherche secrète dans un système informatique telle que visée à l'article 90*ter* du Code d'instruction criminelle[186] ;
- la mesure d'enquête visée à l'article 46*bis* du même Code, soit l'identification d'un abonné ou d'un utilisateur habituel d'un service de communications électroniques, ainsi que pour l'identification du moyen ou des services de communications électroniques qu'il utilise[187] ;
- le repérage de communications électroniques ou la localisation de l'origine ou de la destination de communications électroniques, prévus à l'article 88*bis* du Code d'instruction criminelle[188].

117. Il est également possible que les opérateurs ou fournisseurs de services, s'ils ne sont pas directement visés, doivent collaborer à la conservation des don-

182 V. Franssen et S. Stosza, *op. cit.*, p. 236.
183 Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord., 2015-2016, n° 54-1966/001, p. 51.
184 C. Forget, *op. cit.*, p. 45.
185 C. Forget, *op. cit.*, p. 46 ; V. Franssen et S. Stosza, *op. cit.*, p. 236 ; Ch. Conings et S. Royer, *op. cit.*, p. 317.
186 Art. 90*quater*, § 2, C. i. cr.
187 Art. 46*bis*, § 1er, al. 2, C. i. cr.
188 Art. 88*bis*, § 1er, al. 2, C. i. cr.

nées qui sont en leur possession ou sous leur contrôle, sur la base de l'article 39*ter* du Code d'instruction criminelle, lorsque celles-ci sont particulièrement susceptibles de perte ou de modification[189]. Les opérateurs de réseaux et les fournisseurs de services pourraient également, bien que cette obligation de coopération soit également plus large[190], être tenus de collaborer à la mesure d'enquête visée à l'article 88*quater* du Code d'instruction criminelle, et dès lors de fournir des informations sur le fonctionnement d'un système informatique faisant l'objet d'une recherche secrète ou non, ou sur la manière d'y accéder ou d'accéder aux données qui sont stockées, traitées ou transmises par un tel système, particulièrement lorsque celles-ci sont protégées ou cryptées[191].

118. L'obligation de collaboration des fournisseurs de services dans le cadre de la collecte de preuves numériques n'est pas neuve[192]. Elle a toutefois été précisée[193] et étendue avec l'adoption de la loi du 25 décembre 2016[194], tandis que les sanctions pénales ont parfois été renforcées[195].

119. En effet, l'opérateur ou le fournisseur de services concerné qui ne prête pas son concours à l'enquête ou ne le prête pas en temps réel ou au moment précisé dans la réquisition, encourt une amende[196] qui peut s'élever jusqu'à une somme

189 L'art. 39*ter*, C. i. cr. vise, en effet, « les personnes physiques ou morales » qui posséderaient ou auraient le contrôle de données susceptibles de perte ou de modification.

190 Elle vise en effet les importateurs ou détaillants d'ordinateurs, les fournisseurs de service, les opérateurs, les ingénieurs d'entreprise qui auraient mis en place une configuration informatique, les spécialistes de la sécurité… Voy. J. Keustermans, F. Mols, et T. de Maere, « Informaticacriminaliteit », *Strafrecht en strafvordering. Artikelsgewijze commentaar met overzicht van rechtspraak en rechtsleer*, Mechelen, Kluwer, 2010, pp. 65-103, spéc. p. 100.

191 L'art. 88*quater*, § 1er, al. 1er, C. i. cr. précise que l'obligation de coopérer s'impose à quiconque dont le juge d'instruction présume qu'il a une connaissance particulière du système informatique qui fait l'objet de la recherche ou de son extension visée à l'article 39*bis*, § 3, ou des services qui permettent de protéger ou de crypter des données qui sont stockées, traitées ou transmises par un système informatique. Une obligation identique existe à l'art. 90*quater*, § 4, C. i. cr.

192 Voy. not. art. 46*bis*, 88*bis*, § 1er, al. 1er et § 2, C. i. cr. et *90quater*, § 2, C. i. cr., tels qu'en vigueur avant leur révision par 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, *M.B.*, 17 janvier 2017 (ci-après la loi « Noël »), lesquels prévoyaient déjà une obligation de coopération pour les opérateur de réseau de télécommunication ou pour les fournisseurs d'un service de télécommunications.

193 Notamment concernant la définition des fournisseurs de services de communications électroniques. Voy. *infra.*

194 L'obligation de collaborer à la conservation des données, prévues à l'art. 39*ter* C. i. cr., bien qu'elle ne vise pas uniquement les fournisseurs de services, a été insérée par l'art. 3 de la loi Noël.

195 Voy. par ex. art. 90*quater*, § 2, al. 3, C. i. cr., tel qu'inséré par l'art. 7 de la loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées, *M.B.*, 22 septembre 1998 qui visait une amende de 26 à 10.000 francs, contre 26 à 20.000 € actuellement. Voy. aussi l'art. 88*quater*, § 3, C. i. cr., tel qu'inséré par l'art. 8 de la loi du 28 novembre 2000 relative à la criminalité informatique (*M.B.*, 3 février 2001), qui prévoyait un emprisonnement de 6 mois à un an et une amende de 26 à 20.000 € ou une de ces peines seulement, contre un emprisonnement de 6 mois à trois ans actuellement, et toujours une amende de 26 à 20.000 €.

196 La personne qui refuse de coopérer à une demande de conservation de données peut toutefois être punie d'un emprisonnement de 6 mois à un an, outre une amende de 26 à 20.000 €. Voy. art. 39*ter*, § 3, al. 2, C. i. cr. Celui qui refuse de fournir la collaboration visée par l'art. 88*quater* ou à l'art. 90*quater*, § 4, C. i. cr., ou qui fait obstacle à la recherche ou à son extension dans le système

de 20.000 €[197] à multiplier en application de la loi sur les décimes additionnels, laquelle peut dès lors actuellement atteindre un montant de 160.000 €[198].

120. La collaboration avec les opérateurs téléphoniques et les fournisseurs de services est assurée au travers d'une cellule de coordination « Justice » instituée au sein des opérateurs et fournisseurs de services[199]. Celle-ci est censée être disponible en continu, 24 heures sur 24 et sept jours sur sept. Elle est composée de membres[200] qui doivent avoir fait l'objet d'un avis de sécurité positif lequel doit être renouvelé tous les cinq ans[201].

121. Cette cellule, dont les membres sont les seuls à pouvoir effectuer les tâches par lesquelles ils prêtent l'assistance demandée par les autorités judiciaires afin de protéger au maximum la confidentialité des recherches et la vie privée des personnes[202], reçoit les demandes de coopération via le magistrat instructeur ou via une unité de police spécialisée, le système central d'interception technique du NTSU-CTIF[203], par qui transitent également ensuite les données ainsi collectées[204].

---

informatique, est puni d'un emprisonnement de six mois à un an (90*quater*, § 4) ou trois ans (88*quater) et* d'une amende de vingt-six euros à vingt mille euros ou d'une de ces peines seulement, sauf si cette collaboration pouvait empêcher la commission d'un crime ou d'un délit ou en limiter les effets, auquel cas les peines sont un emprisonnement de un à cinq ans et une amende de cinq cents euros à cinquante mille euros. Voy. art. 88*quater*, § 3, C. i. cr.

197 Les art. 46*bis*, § 2, al. 4 et 88*bis*, § 4, al. 3, C. i. cr. visent une amende de 26 à 10.000 €. L'art. 90*quater*, § 2, al. 3, C. i. cr. vise quant à lui une amende de 26 à 20.000 €.

198 L'article 1er de la loi du 5 mars 1952 relative aux décimes additionnels sur les amendes pénales prévoit, en effet, que le montant des amendes pénales est majoré de 70 décimes pour les faits commis à partir du 1er janvier 2017, *M.B.*, 3 avril 1952.

199 Mise en place par l'art. 2 de l'A.R. du 9 janvier 2003 déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques, *M.B.*, 10 février 2003.

200 Voy. exposé introductif du représentant de la « Belgian Internet Service Providers Association », Projet de loi relatif à l'amélioration des méthodes particulières de recherche et de certaines mesures d'enquête concernant internet, les communications électroniques et les télécommunications, Rapport fait au nom de la Commission de la Justice, *Doc. parl.*, Ch. repr., sess. ord., 2015-2016, n° 54-1966/006, p. 46.

201 Conformément à l'art. 22*quinquies* de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, *M.B.*, 7 mai 1999. Voy. art. 2, § 3, de l'A.R. du 9 janvier 2003 déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques, *M.B.*, 10 février 2003.

202 Voy. Central Technical Interception Facility, *Obligations de collaboration des opérateurs de réseau et fournisseurs de services de communications électroniques*, 17 mai 2017, p. 12, disponible sur https://www.ibpt.be/public/files/fr/22376/Brochure_Informative_Obligations_Collaboration_Autorites_Judiciaires.pdf, consulté le 8 novembre 2018.

203 National Technical & Tactical Support Unit – Central Technical Interception Facility ; qui constitue le service de police désigné à cette fin par le Roi.

204 Art. 5, al. 2, de l'A.R. du 9 janvier 2003 déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques, *M.B.*, 10 février 2003.

B Les destinataires de l'obligation : les opérateurs de réseaux et les fournisseurs de services au sens large

122. La définition des fournisseurs de services à qui s'impose l'obligation de coopérer a été adaptée par la loi du 25 décembre 2016[205], pour viser désormais, non seulement les opérateurs de réseaux et les fournisseurs d'un service de télécommunications électroniques[206], mais également toute personne – physique ou morale – qui met à disposition ou offre, sur le territoire belge, un service consistant à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques[207].

123. Cette définition correspond à celle donnée par la Cour de cassation dans l'un des arrêts « Yahoo », et précisément celui rendu le 18 janvier 2011[208].

124. La Cour précise alors en effet que l'obligation de concours[209] ne se limite pas aux opérateurs d'un réseau de communications électroniques ou aux fournisseurs d'un service de communications électroniques qui sont aussi opérateurs au sens de la loi du 13 juin 2005 relative aux communications électroniques ou qui ne dispensent leurs services de communications électroniques qu'au moyen de leur propre infrastructure. Elle s'impose également, à « *celui qui fournit un service consistant entièrement ou principalement dans la transmission de signaux par la voie des réseaux de communications électroniques* ». Dès lors, « *la personne qui fournit un service consistant à autoriser ses clients à obtenir ou recevoir ou diffuser des informations, au moyen d'un réseau électronique peut aussi être un fournisseur d'un service de communications électroniques* »[210].

---

205 Cette adaptation vise toutes les dispositions du Code d'instruction criminelle qui utilisaient la notion de « fournisseurs de services », soit les art. 46*bis*, 88*bis*, 90*quater*, et 464/13 et 464/25, qui concernent les mesures d'enquête visées aux art. 46*bis* et 88*bis* mais dans le cadre d'une enquête pénale d'exécution.

206 Le terme télécommunication vise toute transmission, émission, ou réception de signes, de signaux, d'écrits, d'images, de sons ou de données de toute nature, par fil, radio-électricité, signalisation optique ou un autre système électromagnétique, les communications par GSM, mobilophone, télex, télécopieur ou la transmission électronique de données par ordinateur ou sur réseau informatique. Voy. projet de loi modifiant la loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communication et de télécommunications privées, *Doc. parl.*, Ch. repr., sess. ord., 1996-1997, n° 1075/1, p. 4. Par souci de clarté, le législateur a précisé que rentrait dans cette nouvelle définition le fournisseur d'un service de communications électroniques. Voy. projet de loi relatif à l'amélioration des méthodes particulières de recherche et de certaines mesures d'enquête concernant internet, les communications électroniques et les télécommunications, *Doc. parl.*, Ch. repr., sess. ord., 2015-2016, n° 54-1966/001, p. 32.

207 Art. 90*quater*, § 2, C. i. cr.

208 Cass., 18 janvier 2011, R.G. P.10.1347.N.

209 En l'espèce, celle visée par l'art. 46*bis*, C. i. cr.

210 En l'espèce soumise à la Cour de cassation, les juges d'appel avaient relevé que Yahoo procure seulement une application software permettant d'envoyer et de recevoir des messages à n'importe quel endroit au moyen d'une adresse mail Yahoo, sans intervenir dans le transfert de données à partir de la Belgique jusqu'à son site portail, soit en tant qu'opérateur d'un réseau, soit en tant que fournisseur d'un service de communications, vu que, pour ses services de courriels, elle fait usage de l'infrastructure existante (le réseau) et des services de communication existants développés et gérés sur le plan mondial par des opérateurs de réseaux et des fournisseurs de services de communications électroniques devant être distingués de Yahoo. Ce dernier ne pouvait dès lors, selon le point de vue de la cour d'appel – cassé par la Cour de cassation – être considéré comme un fournisseur de services au sens de l'article 46*bis* du C. i. cr.

125. La définition des tiers à l'enquête pénale susceptibles d'y apporter un concours technique brasse désormais large : on peut penser à Yahoo, Google, Skype, Microsoft… qui, utilisant les réseaux existants, offrent des services de communications électroniques accessibles en Belgique, tout comme c'est également le cas de Facebook, Twitter, WhatsApp et Instagram qui entrent désormais sans aucune difficulté dans la définition légale[211].

126. Une décision intéressante a été rendue par la cour d'appel d'Anvers le 15 novembre 2017 à l'égard de la société luxembourgeoise « Skype »[212] : la Cour estime que cette entreprise participe effectivement à la vie économique en Belgique, qu'elle possède ou non un siège social ou un siège d'exploitation en Belgique. Skype fournit en effet des moyens techniques – un logiciel gratuit – à des utilisateurs qui peuvent ainsi communiquer entre eux par le biais d'un réseau électronique (internet) et échanger des données une fois qu'ils se sont inscrits sur Skype et que leurs données ont été vérifiées. Elle offre également des services payants à des utilisateurs belges et leur adresse aussi une publicité ciblée. Le fait que ces annonces soient placées par la société-mère Microsoft n'y change rien. Skype est donc un fournisseur d'un service de télécommunication au sens du Code d'instruction criminelle, à l'égard duquel s'impose une obligation de coopérer aux enquêtes pénales belges.

127. Le législateur n'a prévu aucune dérogation à l'obligation de collaboration qui s'impose à tous les opérateurs et fournisseurs de services, même si ceux-ci ne disposent pas des possibilités techniques afin de transmettre aux autorités belges les données sollicitées.

128. Dans l'arrêt précité, la cour d'appel d'Anvers a estimé, à l'égard de l'entreprise Skype qui invoquait l'impossibilité matérielle de prêter son concours à l'enquête en raison du chiffrement des données depuis l'émetteur jusqu'au destinataire, qui était le seul à pouvoir déchiffrer ces données, que celle-ci aurait dû prendre les mesures techniques et organisationnelles appropriées afin de pouvoir se conformer à l'obligation de collaboration imposée par la législation belge[213].

C Une collaboration « en temps réel » ou au moment déterminé dans la réquisition

129. L'obligation de coopération prévue par les articles 46*bis*, 88*bis* et 90*quater*, qui concerne exclusivement les opérateurs de réseaux et les fournisseurs de services, doit s'effectuer en temps réel ou, le cas échéant, au moment précisé dans la

211 Projet de loi relatif à l'amélioration des méthodes particulières de recherche et de certaines mesures d'enquête concernant internet, les communications électroniques et les télécommunications, *Doc. parl.*, Ch. repr., sess. ord., 2015-2016, n° 54-1966/001, pp. 32-33.

212 Anvers, 15 novembre 2017, *N.J.W.*, 2018, p. 78 et note S. Royer.

213 Anvers, 15 novembre 2017, *N.J.W.*, 2018, p. 78 et note S. Royer. ; voy. aussi C. Forget, *op. cit.*, pp. 25-52, spéc. pp. 51-52.

réquisition. Il n'est donc plus question pour un opérateur ou un fournisseur de postposer, de manière consciente ou non, sa collaboration technique à l'enquête pénale sous prétexte que cela ne constituerait pas un refus de collaboration qui était autrefois seul sanctionné pénalement[214]. Une telle attitude – tout autant susceptible de compromettre l'enquête – équivaut désormais à un refus et peut également donner lieu à des poursuites pénales[215].

130. Le temps réel dont il est question ne signifie pas que la coopération doit être prêtée immédiatement[216]. Il s'agit en effet du temps qui est nécessaire à l'exécution de la prestation sollicitée, selon les règles de l'art, sans interruption et en mettant en œuvre les moyens et le personnel adéquats[217]. Si la demande de collaboration adressée à l'opérateur ou au fournisseur de services vise un moment précis, celui-ci doit nécessairement être ultérieur au temps réel[218].

D Une appréciation souple du principe de territorialité ?

131. Lorsqu'il a redéfini le fournisseur de services de communications électroniques soumis à l'obligation de coopération, le législateur a précisé que celle-ci s'imposait dès lors que de tels services étaient mis à disposition ou offerts sur le territoire belge, afin d'établir un lien de rattachement territorial qui n'était pas précisé antérieurement[219].

132. Dans l'affaire ayant mené à cette évolution législative[220], Yahoo avait en effet estimé ne pas pouvoir être soumis à cette obligation de collaboration résultant du droit belge[221], dans la mesure où, étant localisée sur le territoire des États-Unis, seul le droit américain (en l'espèce, l'*Electronic Communications Privacy Act*) avait force obligatoire à son égard. Dès lors, les autorités en charge de l'enquête

214 Voy art. 90*quater*, § 2, al. 3, tel qu'en vigueur avant sa révision par la loi « Noël » du 25 décembre 2016.

215 Projet de loi relatif à l'amélioration des méthodes particulières de recherche et de certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications, *Doc. parl.*, Ch. repr., sess. ord., 2015-2016, n° 54-1966/001, p. 34.

216 Voy. à ce sujet, Avis du Conseil d'État n° 59.199/3 du 9 mai 2016 relatif à l'avant-projet de loi 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, et la précision apportée par le législateur à ce sujet, *Doc. parl.*, Ch. repr., sess. ord., 2015-2016, n° 54-1966/001, pp. 34, 118.

217 Art. 1er, 3°, de l'A.R. du 9 janvier 2003 déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques, *M.B.*, 10 février 2003.

218 Projet de loi relatif à l'amélioration des méthodes particulières de recherche et de certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications, *Doc. parl.*, Ch. repr., sess. ord., 2015-2016, n° 54-1966/001, p. 34.

219 Voy. art. 90*quater*, § 2, al. 1er, tel qu'en vigueur avant sa révision par la loi « Noël » du 25 décembre 2016.

220 Cass., 18 janvier 2011, R.G. P.10.1347.N.

221 En l'espèce, il s'agissait de fournir l'adresse IP d'un utilisateur suite à une fraude en ligne au cours de laquelle une adresse email Yahoo avait été utilisée, sur la base de l'article 46*bis* du Code d'instruction criminelle.

auraient dû passer par une commission rogatoire internationale adressée à leurs homologues américains[222]. Cette argumentation avait été balayée par la Cour de cassation qui avait pris en considération le fait que Yahoo était actif sur le territoire belge.

133. Étant désormais légalement prévu, le critère de localisation retenu par le législateur pour imposer aux fournisseurs de services l'obligation de coopérer aux enquêtes pénales belges ne devrait plus susciter de difficultés pour ces sociétés localisées à l'étranger, à l'égard desquelles les autorités belges pourront directement s'adresser[223].

134. Les fournisseurs de services sont en effet soumis à la loi pénale belge dès qu'ils exercent leurs activités sur le territoire du Royaume, peu importe où sont stockées les données numériques auxquelles les autorités belges cherchent à avoir accès. Il n'est par ailleurs pas nécessaire que la personne concernée par les données que l'on cherche à recueillir – qu'elle soit ou non soupçonnée dans le cadre de l'enquête – se trouve sur le territoire belge au moment où une demande de collaboration est adressée au fournisseur de services.

135. La législation belge est relativement avant-gardiste à cet égard. Elle engendre une appréciation souple du principe de territorialité dans la mesure où peuvent être poursuivis en Belgique des opérateurs et fournisseurs de services dont le siège social est localisé ailleurs qu'en Belgique, qui détiendraient des données stockées sur le territoire d'un autre État, simplement parce qu'ils sont actifs en Belgique et qu'ils ne prêtent pas leur collaboration à une enquête belge[224]. Le délit de refus d'un fournisseur de services de communiquer les données sollicitées est en effet commis à l'endroit où les données demandées doivent être transmises mais ne l'ont pas été, soit en Belgique si la demande provient des autorités judiciaires belges[225].

136. Elle permet par ailleurs aux enquêteurs belges de s'adresser à ces fournisseurs de services étrangers sans devoir passer par une demande de commission rogatoire internationale. S'agissant des demandes de conservation des données, il est d'ailleurs explicitement précisé que la possibilité de demander à une autorité compétente étrangère d'ordonner ou d'imposer la conservation des données informatiques vaut « sans préjudice des possibilités de collaboration directe avec des opérateurs de réseaux de communication électroniques et des fournisseurs de services de communications électroniques étrangers »[226].

---

222 Pour un résumé de cette affaire, voy. O. Leroux, « Criminalité informatique », *Postal Memorialis*, décembre 2014, pp. 967, spéc. pp. 52-53.

223 Art. 90*quater*, § 2, al. 1er.

224 Sur cette question de la territorialité dans le cadre de la récolte de preuves numériques, voy. Ch. Conings, « De lokalisatie van opsporing in een virtuele omgeving – Wie zoekt waar in cyberspace », *Nullum Crimen*, 2014, pp. 1-25.

225 Anvers, 15 novembre 2017, *N.J.W.*, 2018, p. 78 et note S. Royer.

226 Art. 39*quater*, § 1er, al. 1er, C. i. cr.

137. Le lien de rattachement développé par le législateur belge correspond toutefois à celui qu'a choisi d'adopter la Commission européenne, dans la proposition de règlement qu'elle a récemment déposée pour assurer une possibilité de collaboration directe entre les autorités judiciaires et les fournisseurs de services. Cette nouvelle réglementation européenne permettra en effet, sans qu'il n'y ait encore la moindre hésitation à cet égard, aux autorités d'enquête d'un État membre de s'adresser directement à un fournisseur de services proposant des services sur le territoire de l'Union[227], sans l'intervention des autorités de l'État où est établi ou représenté le fournisseur de services[228].

Conclusions

138. La récolte de preuves numériques paraît désormais assurée plus efficacement en droit belge. Vu la mine d'informations qu'elles représentent dans le cadre des enquêtes pénales, on comprend le souci du législateur d'avoir souhaité adapter les techniques d'enquête à la mutation technologique qu'induit le basculement vers une société de l'information.

139. Avec les nouvelles dispositions introduites par la loi du 25 décembre 2016, la récolte de données numériques ne devrait plus poser de difficultés à l'avenir, que les autorités agissent dans le cadre d'une recherche secrète ou non, qu'elles aient ou non saisi lesdites données, qu'elles aient ou non accès aux systèmes informatiques et aux lieux dans lesquels ces données sont stockées, et que ces données soient localisées sur le territoire belge ou ailleurs…

140. Les autorités judiciaires belges peuvent également compter sur une collaboration efficace des opérateurs de réseaux de communications électroniques et de fournisseurs de tels services de communications qui, au mépris du droit à la protection des données de leurs utilisateurs, seront tenus de répondre aux demandes des autorités judiciaires belges, sous peine d'être poursuivis et sanctionnés pénalement pour défaut de collaboration.

141. Efficacité ne rime toutefois que rarement avec respect des droits fondamentaux, dont la protection de la vie privée et le respect de la confidentialité des communications – qu'elles soient électroniques ou non. La Cour constitutionnelle l'a rappelé dans son arrêt du 6 décembre 2018.

---

227 Art. 3, § 1er, de la proposition de règlement du Parlement européen et du Conseil relative aux injonctions européennes de production et de conservation des preuves électroniques en matière pénale, Strasbourg, 17 avril 2018, COM (2018) 225 final, p. 17. C'est-à-dire que le fournisseur permet à des personnes morales ou physiques d'utiliser lesdits services dans un ou plusieurs États membres, sans toutefois que la simple possibilité d'accès à ces services ne soit une condition suffisante pour l'application du règlement. Voy. la page 17 de la proposition.

228 Voy. Proposition de règlement du Parlement européen et du Conseil relative aux injonctions européennes de production et de conservation des preuves électroniques en matière pénale, Strasbourg, 17 avril 2018, COM (2018) 225 final, p. 14.

142. Le législateur ne s'était en effet pas préoccupé outre mesure du déséquilibre qu'il créait entre, d'une part, la nécessaire modernisation des méthodes d'investigation et, d'autre part, l'absence de protection du justiciable face au caractère intrusif desdites méthodes d'enquête. On en veut pour preuve que, lors des travaux parlementaires[229], l'article 32 du Titre préliminaire du Code de procédure pénale a été mentionné en tant que garantie en cas de violation de droits fondamentaux. Le recours à cette disposition qui, pour rappel, autorise l'utilisation de preuves illicites sauf dans trois cas précis : si la nullité est stipulée par la loi, si l'omission a fait perdre à la preuve sa fiabilité ou si l'usage de la preuve compromet l'équité du procès[230], semble totalement inadéquat[231]. La Cour constitutionnelle a néanmoins réaffirmé le caractère fondamental du droit à la protection de la vie privée qui se trouvait sérieusement affecté par ces nouvelles mesures d'enquête et a confirmé que les garanties prévues n'étaient pas suffisantes pour justifier l'ingérence dans la vie privée des individus. L'extension de la recherche informatique décidée par le procureur du Roi n'y a pas résisté, et la mise en œuvre de recherches dans les systèmes informatiques utilisés par les médecins et les avocats non plus.

143. La loi du 5 mai 2019 a rééquilibré les dispositions légales applicables en intégrant l'enseignement de la Cour constitutionnelle. De là à dire que l'exécution de ces mesures d'enquête ne souffre plus d'aucune critique eu égard au respect de la vie privée des individus, il y a un pas que nous ne franchirons pas…

Pierre Monville,
Avocat (Iuxta Legal),
Assistant ULiège

Mona Giacometti,
Avocat (Iuxta Legal),
Assistante & Doctorante (UCLouvain – CRID&P)

Lorraine Grisard,
Avocat (Iuxta Legal),
Assistante ULiège

229 Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord., 2015-2016, n° 54-1966/001, p. 61.
230 M.-A. Beernaert, H. D. Bosly et D. Vandermeersch, *op. cit.*, tome 2, p. 1203.
231 C. Forget, *op. cit.*, p. 52.