La collecte des preuves informatiques en matière pénale

Forget, Catherine

Published in:
Pas de droit sans technologie

Publication date:
2015

Document Version
le PDF de l'éditeur

La collecte de preuves informatiques en matière pénale

Catherine Forget[1]
avocate
chercheuse au CRIDS (UNamur)

Introduction

Les nouvelles technologies permettent la transmission de données à une vitesse très rapide. Ces données sont autant d'éléments susceptibles d'intéresser les enquêteurs et de servir à titre de preuves. À cet égard, il est nécessaire aux services d'enquête de pouvoir prendre « la balle au bond » et de réagir vite, très vite. Or, le cadre légal actuel est relativement procédurier, il est parfois lent, très lent. L'intervention indispensable d'un juge d'instruction pour effectuer certaines mesures d'enquête, par exemple, peut ralentir la procédure entraînant la perte potentielle d'éléments utiles à l'enquête. Les autorités répressives seront donc tentées de favoriser des mesures d'investigation plus rapides et de passer outre un cadre légal considéré comme trop rigide à maints égards. Toutefois, ce cadre sert de rempart contre l'arbitraire et les risques d'abus de sorte qu'une certaine prudence s'impose.

Comme nous le verrons, différentes lois ont inséré dans notre Code d'instruction criminelle (ci-après C.I.cr.) des mesures d'investigation liées aux nouvelles technologies. Il s'agit notamment de la saisie de données informatiques, de la recherche et de l'extension de recherche informatique. Les controverses sont restées nombreuses et les acteurs compétents ne sont pas toujours évidents à identifier. En effet, comment le législateur aurait-il pu supposer l'évolution technologique actuelle et prévoir par anticipation un cadre légal clair ? De plus, les intermédiaires privés ont souvent une place privilégiée pour accéder au contenu de certaines informations. Ces derniers sont donc davantage sollicités en matière pénale qu'ils soient ou non enclins à participer à l'enquête. Leurs obligations s'étendent également en matière de surveillance, par exemple l'obligation de rétention impose aux acteurs privés de collecter des données de manière systématique et généralisée. Ces obligations soulèvent certaines questions tant pour le respect de nos droits fondamentaux que pour la responsabilisation des acteurs privés. Ensuite, les méthodes particulières

1. L'auteure tient à remercier Franck Dumortier pour son soutien et ses conseils éclairés.

de recherche n'échappent pas au monde informatique. L'observation et l'infiltration sur internet restent très peu connues malgré l'intérêt pour les enquêteurs de recourir à ces méthodes. Enfin, la mesure d'interception des (télé)communications amène certaines problématiques que nous exposerons dans le cadre de cette contribution.

Ainsi, nous verrons qu'en pratique la transposition des méthodes classiques en matière informatique ne coïncide pas toujours et fait l'objet de discussions. Analysons dès lors ces nouvelles méthodes, leur application, les enjeux et leurs controverses.

Section 1

La saisie de données informatiques et la recherche informatique

La saisie de données informatiques et la recherche informatique sont de nouvelles techniques d'enquêtes relatives aux systèmes informatiques. Certains aspects n'ont pas été prévus par le législateur pour différentes raisons, de sorte que des controverses subsistent.

A. *La saisie de données informatiques*

La saisie de données informatiques n'est pas définie par la loi. Les travaux préparatoires de la loi relative à la criminalité informatique[2], insérant la saisie de données informatiques dans le C.I.cr., soulignent le souhait du législateur de ne pas donner de définition aux termes utilisés « afin d'éviter que les concepts ne soient trop rapidement dépassés par l'évolution de la technologie de l'information »[3]. La saisie « classique » par contre, est définie par la jurisprudence. Selon la Cour de cassation, la saisie est « une mesure conservatoire par laquelle l'autorité compétente, selon la loi et à propos d'une infraction, soustrait une chose à la libre disposition de son propriétaire ou de son possesseur et, en vue de la manifestation de la vérité, de la confiscation, de la restitution ou de la sécurité des intérêts civils, et la place sous elle »[4]. La saisie de support informatique, par exemple un téléphone portable ou un ordinateur, est une saisie mobilière au sens de l'article 35 du C.I.cr.[5]. *A contrario*, la saisie des données stockées dans un système informatique au sens de l'article 39*bis* du C.I.cr. est une saisie de données « immatérielles », dont la mise en œuvre soulevait certaines difficultés avant l'intervention du législateur.

2. L. du 28 novembre 2000 relative à la criminalité informatique, *M.B.*, 3 février 2001.
3. Exposé des motifs, *Doc. parl.*, Ch. repr., n° 0213/001, p. 12.
4. Cass., 25 février 2003, *Pas.*, 2003, p. 412, www.cass.be.
5. Art. 35 C.I.cr.

La nécessité d'une modification législative se faisait d'autant plus ressentir qu'une recommandation du Conseil de l'Europe préconisait l'adoption par les États membres d'une législation spécifique aux systèmes informatiques en procédure pénale[6]. Dans la foulée, la loi du 28 novembre 2000 relative à la criminalité informatique[7] fut adoptée et inséra l'article 39*bis* dans le C.I.cr. Ce nouvel article répond également aux impératifs de l'article 8, § 2, de la Convention européenne des droits de l'homme selon lequel il ne peut y avoir d'ingérence dans la vie privée d'une personne que dans les cas prévus par la loi.

Pareillement à la saisie classique, la saisie de données informatiques s'effectue tant au stade de l'information[8] que de l'instruction[9]. Le procureur du Roi peut requérir la copie des données stockées, leur blocage et leur retrait. La personne responsable du système informatique dont les données sont saisies doit être informée *a posteriori* de la mise en œuvre de la mesure[10]. Enfin, l'autorité compétente peut disposer de tous les moyens techniques appropriés pour assurer la confidentialité et l'intégrité des données saisies[11].

À la différence de la saisie de données informatiques relevant de la compétence du procureur du Roi, la recherche informatique relève de la compétence du juge d'instruction. Or la notion de recherche informatique au sens de l'article 88*ter* du C.I.cr. se confond parfois avec la notion de saisie de données informatiques. Analysons dès lors la notion.

B. *La recherche informatique*

L'article 88*ter* du C.I.cr. ne définit pas la recherche informatique. Pour O. Leroux, il s'agit d'une « consultation de données stockées dans un système informatique »[12]. Sauf certaines exceptions[13], une recherche informatique relève de la compétence du juge d'instruction[14]. L'ordonnance émise par le juge d'instruction autorisant la recherche informatique doit être limitée dans le temps et viser un système informatique particulier. En pratique, cette restriction peut poser certaines difficultés. En effet, les

6. Recommandation n° R (95) 13 du comité des ministres du Conseil de l'Europe aux gouvernements des États membres, relative aux problèmes de procédure pénale liés à la technologie de l'information, www.coe.int.
7. L. du 28 novembre 2000 relative à la criminalité informatique, *M.B.*, 3 février 2001.
8. Art. 39*bis* C.I.cr.
9. Art. 89*bis* C.I.cr.
10. Art. 39*bis*, § 5, C.I.cr.
11. Art. 39*bis*, § 6, C.I.cr.
12. O. LEROUX, « Criminalité informatique », *in* X., *Postal Mémorialis. Lexique du droit pénal et des lois spéciales*, juillet 2014, C 362/46, p. 58.
13. O. KLEES, F. ROGGEN, D. VANDERMEERSCH, « Les saisies en matière pénale et référé pénal », *in Droit pénal et procédure pénale*, Waterloo, Kluwer, 2006, p. 67.
14. Art. 88*ter* C.I.cr.

systèmes informatiques sont souvent interconnectés de sorte qu'il n'est pas toujours évident pour le juge d'instruction de localiser un système informatique précis[15]. L'objectif du législateur était de limiter les espaces « perquisitionnés » et d'éviter une intrusion illimitée dans les systèmes informatiques[16]. Les travaux préparatoires de la loi relative à la cybercriminalité précisent que « lorsque les systèmes informatiques pour lesquels une recherche semble nécessaire sont dispersés en différents endroits, plusieurs mandat de perquisition ou de saisie doivent être délivrés »[17]. Pour laisser la possibilité au juge d'instruction d'étendre la recherche informatique, le législateur a donc prévu l'extension de recherche informatique[18]. Selon le paragraphe 1er de l'article 88*ter* du C.I.cr., cette extension doit respecter certaines conditions. Elle doit d'une part, être nécessaire à la manifestation de la vérité au regard de l'infraction visée dans l'ordonnance de recherche et d'autre part, soit l'exécution d'autres mesures serait disproportionnée soit il existe un risque de perdre certains éléments de preuve. En outre, l'ordonnance ne peut être étendue aux systèmes auxquels les parties n'ont pas accès[19].

Malgré l'intention du législateur de ne pas être « trop rapidement dépassé par l'évolution de la technologie de l'information »[20], en pratique, certaines situations n'ont tout simplement pas été pensées, débouchant dès lors sur certaines controverses.

C. *De nouvelles pratiques et leurs controverses*

Le législateur n'a pas réglementé toutes les modalités de la saisie de données informatiques et de la recherche informatique. Cette absence de réglementation claire et complète fait naître certaines controverses sur lesquelles il serait intéressant de s'attarder.

1. Une première controverse : l'exploitation des données stockées dans un système informatique légalement saisi

La saisie de données stockées dans un système informatique diffère selon le système informatique en cause. Si ce dernier est accessible au

15. O. LEROUX, « Criminalité informatique », *in* X., *Postal Mémorialis. Lexique du droit pénal et des lois spéciales, op. cit.*, C 362/47, p. 59.
16. *Doc. parl.*, Ch. repr., n° 50-213/1, p. 23. Voy. égal. F. DE VILLENFAGNE et S. DUSSOLIER, « La Belgique sort enfin ses armes contre la cybercriminalité : à propos de la loi du 28 novembre 2000 sur la criminalité informatique », *A. & M.*, 2001/1, pp. 60-81.
17. *Doc. parl.*, Ch. repr., n° 50-213/1, p. 22.
18. C. MEUNIER, « La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique », *Rev. dr. pén.*, 2001, p. 663.
19. Art. 88*ter*, § 2, C.I.cr.
20. Exposé des motifs, *Doc. parl.*, Ch. repr., n° 0213/001, p. 12.

public, les enquêteurs pourront exploiter les données contenues dans ce système au stade de l'information. Notons qu'un système informatique est accessible au public à la double condition d'être dans un lieu accessible au public et d'être, au sein du lieu, accessible au public. Par exemple, un café met à disposition des clients un ou des ordinateurs. Ces ordinateurs sont accessibles aux enquêteurs au même titre qu'ils sont accessibles au public. Par contre, le téléphone portable d'une personne se trouvant dans un café n'est pas accessible aux clients et n'est donc pas accessible aux enquêteurs. L'interprétation selon laquelle les enquêteurs peuvent, après s'être saisis d'un système informatique « non accessible au public » ou « privé », accéder et exploiter les données stockées ne fait pas l'unanimité. En effet, le paragraphe 1er de l'article 39*bis* du C.I.cr. ne nous éclaire pas beaucoup sur la question et stipule seulement « lorsque le procureur du Roi découvre dans un système informatique des données stockées ». Le législateur n'a donc pas précisé dans quelles situations le procureur du Roi pourrait découvrir des données stockées. Selon nous, le terme « lorsque » et la notion de « découverte » ne permettent pas d'en déduire la compétence du procureur du Roi d'exploiter les données stockées dans un système informatique légalement saisi.

a) *L'arrêt de la Cour de cassation du 11 février 2015 et l'extension du pouvoir des enquêteurs au stade de l'information*

La Cour de cassation trancha la controverse dans un arrêt du 11 février 2015. En l'espèce, un téléphone portable avait été saisi et consulté par les enquêteurs. Les parties en cause contestaient la compétence des enquêteurs d'exploiter les données saisies stockées dans un système informatique et invoquaient la nécessaire intervention du juge d'instruction, conformément à l'article 88*ter* du C.I.cr. La Cour considéra que « l'exploitation de la mémoire d'un téléphone portable, dont les messages qui y sont stockés sous la forme d'un SMS, est une mesure découlant de la saisie, laquelle peut être effectuée dans le cadre d'une information sans autres formalités que celles prévues pour cet acte d'enquête »[21]. Selon la Cour, consulter les données stockées dans un système informatique est une mesure pouvant se dérouler dans le cadre d'une saisie au sens de l'article 39*bis* du C.I.cr. Cet arrêt est étonnant à maints égards. Tout d'abord en autorisant les enquêteurs à exploiter les données stockées, la Cour fait œuvre du législateur puisqu'elle accorde une nouvelle compétence au procureur du Roi. Lors d'une saisie, ce dernier serait à présent habilité à consulter des données stockées dans un système informatique que l'accès à celui-ci soit public ou non. L'analyse de la Cour rejoint le point de vue déjà développé de J. de Codt selon lequel la consultation d'un téléphone

21. Cass., 11 février 2015, R.G. n° P.14.1739.F, www.cass.be.

portable saisi par les services de police, dont notamment la consultation du répertoire, des messages stockés et du journal d'appel, ne nécessite pas l'autorisation d'un juge d'instruction. Cependant, l'auteur précise: à condition toutefois pour les services de police de disposer du code d'accès[22]. Cette distinction, qu'aurait pu effectuer la Cour de cassation, aurait permis de distinguer l'intrusion «consentie» – la personne donne le mot de passe – de la «non consentie» et ainsi, réduire les pouvoirs des enquêteurs au stade de l'information.

Ensuite, la Cour restreint le champ d'application de la recherche informatique au sens de l'article 88*ter* du C.I.cr. Ce dernier doit être limité à «l'hypothèse de l'extension d'une recherche ordonnée par le juge d'instruction vers un système informatique ou une partie de celui-ci qui se trouve dans un autre lieu que celui où la recherche est effectuée». Ce faisant, la Cour de cassation fait fi de «recherche informatique» puisque l'article 88*ter* du C.I.cr. ne concernerait que la notion de «l'extension de recherche informatique».

Cette analyse avait déjà été exposée dans un jugement de la cour d'appel de Bruxelles du 19 décembre 2014[23]. En l'espèce, les services de polices avaient consulté les données informatiques d'un ordinateur saisi. Les parties appelantes invoquaient la violation de l'article 88*ter* du C.I.cr. En effet, les enquêteurs s'étaient introduits dans le système informatique pour consulter les données sans disposer de l'autorisation du juge d'instruction. La Cour considéra cependant que la mesure visée par l'article 88*ter* du C.I.cr., «celle de l'article 88*quater* du même Code et la compétence qu'elles réservent au seul juge d'instruction pour les mettre en œuvre, ne s'applique pas à la recherche menée directement dans un tel système informatique. Elles ne concernent en effet que l'hypothèse où cette recherche (est) étendue vers un système informatique (...)». Selon la cour d'appel, l'article 88*ter* du C.I.cr. vise l'extension de recherche informatique et non la simple recherche informatique.

Ces interprétations ont certes l'avantage de clôturer le débat sur le sens à donner à la «recherche informatique» de l'article 88*ter* du C.I.cr. qui ne viserait que l'extension de recherche informatique. Néanmoins, cette analyse limite les compétences exclusives du juge d'instruction et offre une nouvelle compétence au procureur du Roi. Ce dernier est désormais compétent pour ordonner une exploitation de données stockées dans un système, cette mesure découlant de la saisie. Or, un système informatique est un espace où des données potentiellement intimes sont conservées. Cet espace est un lieu où s'exerce notre vie privée protégée par l'article 8 de la Convention européenne des droits de l'homme. Conformément au C.I.cr., les actes portants atteintes aux droits et libertés doivent relever et

22. J. DE CODT, *Des nullités de l'instruction et du jugement*, Bruxelles, Larcier, 2006, p. 51.
23. Bruxelles (12e ch.), 19 décembre 2014, inédit.

relèvent de la compétence du juge d'instruction[24]. Cette interprétation de la Cour de cassation n'est donc pas anodine et potentiellement dangereuse pour le respect des droits fondamentaux des personnes concernées.

Notons par ailleurs que l'accès non autorisé à un système informatique, par des personnes extérieures au réseau ou à l'organisation, est sanctionné par l'article 550*bis* du Code pénal et qualifiée de *hacking* externe[25]. Les particuliers sont donc tenus de respecter le système informatique d'une personne et ne peuvent y accéder sans autorisation. En outre, à titre exemplatif, remarquons que si les enquêteurs peuvent saisir du courrier, son ouverture ne peut être effectuée sans l'autorisation d'un juge d'instruction[26]. De manière similaire, l'exploitation des données stockées dans un système informatique devrait, à notre sens, également relever de la compétence du juge d'instruction. Enfin, lors de l'adoption de l'article 39*bis* du C.I.cr., le législateur était guidé par la recommandation du Conseil de l'Europe relative aux problèmes de procédure pénale liés à la technologie de l'information[27]. Selon cette dernière, le droit des États membres devrait permettre de perquisitionner les systèmes informatiques dans «des conditions similaires à celles utilisées dans le cadre des pouvoirs traditionnels de perquisition et de saisie»[28]. Si le terme «perquisition» n'a pas été repris par le législateur dans un cadre informatique, la notion peut toutefois nous aiguiller dans la problématique en cause.

b) La perquisition et le système informatique non accessible au public: des garanties analogues?

L'intrusion dans un système informatique pour exploiter les données suppose une pénétration dans un espace informatisé. Cette intrusion pourrait s'analyser en une perquisition d'où découleraient certaines garanties protégeant les droits fondamentaux des personnes en cause. Reprenons dès lors les notions classiques de «perquisition» et de «domicile» afin de déterminer si la logique sous-jacente est défendable en matière informatique.

24. Art. 28*ter*, § 1, C.I.cr. et art. 56, § 1er, al. 5, C.I.cr.
25. À cet égard voy. O. LEROUX, «Criminalité informatique», *in Les infractions contre les biens*, Bruxelles, Larcier, 2008, pp. 365-453.
26. Art. 46*ter* C.I.cr. et 88*sexies* C.I.cr.
27. Recommandation nº R (95) 13 du comité des ministres du Conseil de l'Europe aux gouvernements des États membres, relative aux problèmes de procédure pénale liés à la technologie de l'information, www.coe.int.
28. Annexe à la recommandation nº R (95) 13 du comité des ministres du Conseil de l'Europe aux gouvernements des États membres, relative aux problèmes de procédure pénale liés à la technologie de l'information, p. 2.

i) LA PROTECTION DU DOMICILE PRIVÉ ET LA PERQUISITION

La protection du domicile privé est un droit garanti par les articles 15 de la Constitution et 8 de la Convention européenne des droits de l'homme. La notion de domicile est une notion autonome analysée *in concreto*. La Cour de Strasbourg prône une interprétation souple de la notion[29], considérant qu'elle relève du bien-être personnel et du droit à la sécurité des personnes[30]. Cette dernière définit le domicile comme «tout endroit utilisé comme logement, résidence ou lieu d'activité par une personne physique ou morale, au sein duquel un individu a le sentiment d'être dans l'intimité, en sécurité contre l'immixtion de personnes contre sa volonté, indépendamment de la durée et de l'intensité d'utilisation»[31]. La protection du domicile suppose donc la protection de «l'intimité» des «lieux» où s'exerce la vie privée. Une perquisition est une mesure dérogatoire aux articles 15 de la Constitution et 8 de la Convention européenne des droits de l'homme garantissant l'inviolabilité du domicile privé. Cette mesure implique la pénétration physique d'une autorité au sein d'un lieu appartenant à la sphère privée d'une personne[32]. Elle requiert en principe l'intervention du juge d'instruction[33]. Cette obligation connaît toutefois certaines exceptions strictement circonscrites par la loi[34]. En dehors de ces cas dérogatoires, seul un juge d'instruction est compétent pour ordonner

29. J.-F. RENUCCI, *Traité de droit européen des droits de l'homme*, Paris, L.G.D.J., 2012, p. 319.
30. Cour eur. D.H., *Gillow c. Royaume-Uni*, 24 novembre 1986, § 55.
31. Cour eur. D.H., *Niemietz c. la République fédérale d'Allemagne*, 16 décembre 1992, *Rev. trim. dr. h.*, 1993, p. 467 et *J.T.*, 1994, p. 65, note E. JAKHIAN et P. LAMBERT, «Les perquisitions dans les cabinets d'avocats»; Cour eur. D.H., *Société Colas Est et autres c. France*, 16 avril 2002, § 41; Cour eur. D.H., *Van Rossem cl Belgique*, 9 décembre 2004. Notons qu'une interprétation similaire à celle de la Cour européenne des droits de l'homme est retenue par la Cour constitutionnelle. La Cour de cassation a opté de manière constante pour une définition plus restrictive de la notion mais étant donné que les dispositions de la Convention priment sur celles de la Constitution, nous rejoignons L. Kennes lorsqu'il écrit qu'«il est donc évident que toute personne bénéficie de la protection de l'article 8 de la Convention, telle qu'interprétée par la Cour européenne des droits de l'Homme». Voy. L. KENNES, *Manuel de la preuve en matière pénale*, Waterloo, Kluwer, 2009, p. 24.
32. L. KENNES, *La preuve en matière pénale*, coll. Pratiques du droit, Bruxelles, Kluwer, 2005, vol. II, pp. 281-299.
33. M. FRANCHIMONT, A. JACOBS et A. MASSET, «§ 8. – Les perquisitions (art. 87 et 88 C.I.C.)», *in Manuel de procédure pénale*, Bruxelles, Larcier, 2012, pp. 515-531.
34. Voy. l'article 1er de la loi du 7 juin 1969 fixant le temps pendant lequel il ne peut être procédé à des perquisitions ou visites domiciliaires et l'article 27 de la loi sur la fonction de police du 5 août 1992. Ainsi, dans certaines situations exceptionnelles par exemple en cas d'appel venant des lieux, en cas d'urgence, ou de flagrant délit, les autorités de police et le procureur du Roi peuvent s'introduire dans un domicile privé sans disposer de mandat de perquisition. En outre, les lieux accessibles au public ne sont pas protégés au même titre qu'un domicile privé. Ils sont accessibles aux enquêteurs de la même manière qu'ils le sont pour le public. Voy. égal.: M. BEYS, *Quels droits face à la police?*, Couleur livres – J&D Éditions, 2014, pp. 233-264.

une mesure de perquisition, sous réserve de déléguer la mise en exécution à des fonctionnaires de police en vertu de l'article 89*bis* du C.I.cr.

ii) QUELLES GARANTIES POUR L'INTRUSION DANS UN SYSTÈME INFORMATIQUE?

Ni les travaux préparatoires, ni le Code d'instruction criminelle ne précisent expressément si l'intrusion dans un système informatique va de pair avec le respect de certaines garanties. Or, un système informatique est un espace où sont stockées des données relevant potentiellement de la sphère intime d'une personne, de sa vie privée. Les travaux préparatoires de la loi du 28 novembre 2000 relative à la criminalité informatique[35] le caractérisent comme «tout système permettant le stockage, le traitement ou la transmission de données»[36]. Il s'agit notamment d'un téléphone portable, d'une carte à puce, d'un ordinateur ainsi que leurs composants et leurs réseaux[37]. Vu l'utilisation actuelle des systèmes informatiques – agenda, données professionnelles, courriers, portefeuille électronique, ... – il s'agit d'un lieu d'activité «au sein duquel un individu a le sentiment d'être dans l'intimité, en sécurité contre l'immixtion de personnes contre sa volonté, indépendamment de la durée et de l'intensité d'utilisation»[38]. Cette interprétation crée le parallèle entre le système informatique et le domicile. De plus, la directive 2002/58/CE dite directive «vie privée et communications électroniques» précise que les informations stockées dans un «terminal» relèvent de la vie privée d'une personne au sens de l'article 8 de la Convention européenne des droits de l'homme[39].

Nous rejoignons l'analyse de certains auteurs[40] selon laquelle toute intrusion dans un système informatique par les autorités est, sous réserve de certains cas prévus par la loi, une mesure de perquisition. Une recom-

35. L. du 28 novembre 2000 relative à la criminalité informatique, *M.B.*, 3 février 2001.
36. *Doc. parl.*, Ch. repr., n° 50-213/1, p. 3. À titre informatif, le Conseil de l'Europe définit le système informatique comme «un dispositif composé de matériel et de logiciels, conçus pour le traitement automatisé des données numériques. Il peut comprendre des moyens d'acquisition, de restitution et de stockage des données. Il peut être isolé ou connecté à d'autres dispositifs similaires au sein d'un réseau». Voy. rapport explicatif de la recommandation R(89) 9 du Conseil de l'Europe, éd. du Conseil de l'Europe, Strasbourg, 1990, § 23.
37. Exposé des motifs, *Doc. parl.*, Ch. repr., n° 0213/001, p. 12.
38. Cour eur. D.H., *Niemietz c. la République fédérale d'Allemagne*, 16 décembre 1992, *Rev. trim. D.H.*, 1993, p. 467 et *J.T.*, 1994, p. 65, note E. JAKHIAN et P. LAMBERT, «Les perquisitions dans les cabinets d'avocats».
39. Considérant 24 de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, http://eur-lex.europa.eu/.
40. C. MEUNIER, «La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique», *Rev. dr. pén.*, 2001/7-8, pp. 663-664; T. INCALZA, «Strafonderzoek in het digitale tijdperk: zoeking en inbeslagneming», *Jura Falc.*, 2010-2011/2, pp. 329-383; B. LOSDYCK, «Les saisies et perquisitions

mandation du Conseil de l'Europe relative à la cybercriminalité appuie cette analyse. Selon celle-ci: «L'emploi du mot classique 'perquisitionner' traduit l'idée de l'exercice par l'État d'un pouvoir coercitif et montre que le pouvoir visé dans cet article est analogue à la perquisition classique. 'Perquisitionner' veut dire rechercher, lire, inspecter ou examiner des données, et inclut aussi les notions de recherche de données et d'examen de données»[41]. De plus, la convention sur la cybercriminalité récemment ratifiée par la Belgique[42], impose aux États membres d'adopter des «mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à accéder d'une façon similaire à un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées»[43]. La convention de Budapest évoque donc la perquisition lorsqu'il y a intrusion dans un système informatique. Enfin, au moment de l'adoption de la loi relative à la cybercriminalité, la Commission vie privée (C.V.P.) donnait un avis où elle exposait la recherche informatique et l'extension de la «perquisition» à d'autres systèmes informatiques[44]. Il s'agissait donc selon la C.V.P. de perquisition et d'extension de la perquisition, la saisie ne permettant pas, *a priori*, d'accéder au système. L'ensemble de ces éléments nous permet de raisonnablement considérer que l'intrusion dans un système informatique suppose une perquisition. Par conséquent, accéder à un système informatique implique, selon nous, le respect de certaines garanties visant à préserver l'inviolabilité du système visé. L'inverse reviendrait à laisser un pouvoir important aux enquêteurs surtout eu égard à l'ampleur des données susceptibles d'être stockées dans un système informatique.

2. Une seconde controverse: Le blocage de site internet et l'obligation de collaboration des tiers

Le Code d'instruction criminelle ne précise pas si le blocage d'un site internet peut intervenir au stade de l'information. Il ne précise pas non plus quels sont les acteurs susceptibles de devoir intervenir. L'arrêt *Pirate Bay*[45] est intéressant à deux égards. Premièrement, il pose la question du

de matériel informatique: les «garde-fous» entourant leur mise en œuvre», *R.D.T.I.*, 2013/3, n° 52.

41. Rapport explicatif de la recommandation R(89) 9 du Conseil de l'Europe, éd. du Conseil de l'Europe, Strasbourg, 1990, § 191.
42. L. du 3 août 2012 portant assentiment à la convention sur la cybercriminalité, faite à Budapest le 23 novembre 2001, *M.B.*, 21 novembre 2012.
43. Art. 19 de la convention de Budapest sur la cybercriminalité, Conseil de l'Europe, 23 novembre 2001.
44. Avis n° 33/1999 du 13 décembre 1999 relatif aux projets de loi relatifs à la criminalité informatique, Commission Vie privée, disponible sur http://www.privacycommission.be/sites/privacycommission/files/documents/avis_33_1999_0.pdf.
45. Cass. (2e ch., sect. nl.), 22 octobre 2013, R.G. n° P.13.0550.N, www.cass.be.

cadre légal applicable pour requérir le blocage de sites internet. Deuxièmement, il met en avant la problématique relative à l'obligation de collaboration des tiers dans le cadre d'une saisie. Examinons dès lors cet arrêt.

a) *Une première problématique: le blocage de site internet, une mesure applicable dans le cadre d'une saisie?*

L'article 39*bis* du C.I.cr. habilite le procureur du Roi à prendre des mesures dans le cadre d'une saisie, par exemple saisir le support informatique où sont stockées les données fait l'objet de la mesure. L'article 89*bis* du C.I.cr. confère les mêmes compétences au juge d'instruction. Si la saisie du support informatique entraîne des conséquences disproportionnées, par exemple empêche le fonctionnement du système informatique d'une entreprise[46], le procureur du Roi peut requérir la simple copie des données stockées sur un support vers un autre support[47]. Si la copie des données est impossible pour des questions techniques ou pratiques, les données peuvent être bloquées[48]. Il s'agit alors d'une «mise sous scellés» des données[49] effectuée dans l'attente d'une copie ultérieure[50]. Enfin, les données peuvent être retirées du système si elles sont contraires à l'ordre public et aux bonnes mœurs ou si elles risquent d'endommager le système informatique s'il s'agit par exemple d'un virus informatique[51].

Des controverses subsistent quant aux dispositions légales applicables pour ordonner le blocage d'un site internet[52] et notamment si la mesure peut intervenir dans le cadre d'une saisie de données informatiques[53].

La Cour de cassation trancha la controverse dans un arrêt du 22 octobre 2013[54]. La Cour dit pour droit que le blocage d'un site internet peut intervenir dans le cadre d'une saisie. En l'espèce, une ordonnance du juge d'instruction prise sur la base des articles 39*bis* du C.I.cr. et 89 du C.I.cr. imposait aux opérateurs et fournisseurs d'internet de rendre inaccessible l'accès au contenu des sites liés à l'adresse IP du nom de domaine «thepiratebay.org». Le blocage visait donc d'une part, à faire cesser des actes susceptibles de constituer une infraction et d'autre part, à protéger des intérêts civils. Les demandeurs en cassation contestaient la validité

46. *Doc. parl.*, Ch. repr., n° 50-213/1, p. 21.
47. Art. 39*bis* C.I.cr.
48. Art. 39*bis*, § 4, C.I.cr.
49. O. KLEES, F. ROGGEN et D. VANDERMEERSCH, *op. cit.*, p. 71.
50. F. ROGGEN, «L'extension des moyens d'investigation et des mesures de contrainte en procédure pénale», *R.G.C.F.*, 2003/5, p. 113.
51. *Doc. parl.*, Ch. repr., n° 50-213/1, pp. 20-21.
52. D. DECKMYN et N. VANHECKE, «Geen juridische basis om websites te blokkeren», *De standaard*, 23 mai 2013, http://www.standaard.be/cnt/dmf20130522_090.
53. P. MONVILLE et M. GIACOMETTI, «Les fournisseurs d'accès à internet, nouveaux gendarmes de la toile?», *R.D.T.I.*, 2014/2, n° 55, pp. 68-76.
54. Cass. (2e ch., sect. nl.), 22 octobre 2013, R.G. n° P.13.0550.N.

de l'ordonnance basée sur les dispositions légales relatives à la saisie de données informatiques puisque selon ces derniers, l'ordonnance ne rencontrait pas les mêmes finalités visées par la saisie.

En effet, le paragraphe 2 de l'article 39*bis* du C.I.cr. prévoit la saisie du support et/ou la copie des données stockées. Le paragraphe 4 dudit article ajoute que, si la copie est impossible, le procureur du Roi peut empêcher l'accès aux données dans le but de mettre « sous scellées » les données. Dans le cadre du paragraphe 3 de l'article précité, les données peuvent être rendues indisponibles soit parce qu'elles serviront à titre de preuve, l'original doit donc rester intact, soit parce qu'elles portent atteinte à l'ordre public, aux bonnes mœurs, ou qu'elles représentent un danger. Le procureur du Roi pourra interdire l'accès aux données si elles « forment l'objet de l'infraction ou ont été produites par l'infraction *et* si elles sont contraires à l'ordre public ou aux bonnes mœurs ou constituent un danger pour l'intégrité »[55] Les finalités de la saisie sont donc très précises. Le C.I.cr. distingue l'empêchement d'accès aux données de l'interdiction d'accès aux données. Dans le premier cas, les données subsistent dans le système informatique et sont conservées à titre de preuve[56]. Dans le second cas, les données sont retirées afin d'éviter la propagation de données susceptibles de porter atteinte à l'ordre public, aux bonnes mœurs ou parce qu'elles représentent un danger[57]. Or en l'espèce, il ne s'agissait pas d'éviter la propagation d'un danger ou d'une infraction susceptible de porter atteinte à l'ordre public. Il ne s'agissait pas non plus d'une mesure visant à conserver les données à titre de preuve. Il s'agissait tout au plus de faire cesser une potentielle infraction ou de protéger des intérêts civils. Ce faisant, la Cour a étendu les modalités de la saisie de données informatiques à une finalité non visée expressément par le C.I.cr.[58]. Or, une saisie est une mesure d'enquête susceptible d'être effectuée au stade de l'information. Par conséquent, l'arrêt en cause autorise le procureur du Roi à bloquer un site internet, mesure susceptible de porter atteinte à la liberté d'expression d'une personne garantie par l'article 10 de la Convention européenne des droits de l'homme. Une telle disposition devrait prévoir certaines garanties pour éviter les abus et le risque d'arbitraire[59]. Pour ces raisons, il serait, selon nous, judicieux et conforme à la *ratio legis* de l'article 39*bis* du C.I.cr. de laisser cette compétence au juge d'instruction.

55. Art. 39*bis*, § 3, C.I.cr. C'est nous qui soulignons.
56. C. MEUNIER, *op. cit.*, p. 674.
57. *Ibid.*, p. 675.
58. R. SCHOEFS, « Changement de méthode dans la lutte contre The Pirate Bay: la saisie de données autorisée », *T. Strafr.*, 2014/2, pp. 131-142 (note sous Cass., 22 octobre 2013, R.G. nos P.13.0550.N et P.13.0551.N).
59. Q. VAN ENIS, « Les mesures de filtrage et de blocage de contenus sur l'internet: un mal (vraiment) nécessaire dans une société démocratique? Quelques réflexions autour de la liberté d'expression », *Rev. trim. dr. h.*, 96, pp. 879 et s.

Compétence qu'il pourrait exercer sur la base de l'article 88*quater* du C.I.cr. que nous examinerons *infra*.

b) *Une seconde problématique: à qui s'adresse l'obligation de collaboration dans le cadre d'une saisie?*

Dans l'arrêt *Pirate Bay*[60], l'ordonnance du juge d'instruction prise sur la base des articles 39*bis* du C.I.cr. et 89 du C.I.cr. imposait aux opérateurs et fournisseurs d'internet de rendre inaccessible l'accès au contenu des sites liés à l'adresse IP du nom de domaine « thepiratebay.org ». Les demandeurs en cassation contestaient l'obligation de collaboration qui leur était imposée dans le cadre d'une saisie. En effet, sur la base de l'ordonnance, ces derniers étaient obligés d'effectuer un procédé technique « *reverse IP domain check* » pour déterminer les noms de domaines renvoyant au serveur associé au nom de domaine « thepiratebay.org ».

Les demandeurs invoquaient l'article 21 de la loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information[61]. En effet, l'article précité réfère *in fine* directement à l'article 39*bis* du C.I.cr. et précise: « Aussi longtemps que le procureur du Roi n'a pris aucune décision concernant le copiage, l'inaccessibilité et le retrait des documents stockés dans un système informatique, le prestataire peut uniquement prendre des mesures visant à empêcher l'accès aux informations ». Ainsi, le temps nécessaire au procureur du Roi de prendre des dispositions, par exemple requérir un mandat de perquisition pour saisir les données, le prestataire *peut* empêcher l'accès aux données. Ce dernier n'a pas l'obligation de prendre des mesures. En outre, l'article 20 de la loi du 11 mars 2003 prescrit une obligation de dénonciation envers les hébergeurs[62], cet article ne concerne pas les fournisseurs d'accès à internet. La Cour ne retient pas cet argument et, se basant sur le paragraphe 4 de l'article 39*bis* du C.I.cr., elle « n'exclut pas que cet ordre soit adressé à des tiers » obli-

60. Cass., 22 octobre 2013, R.G. nº P.13.0550.N.
61. Depuis lors, les dispositions de la loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information sont reprises dans le Code de droit économique. Voy. L. du 15 décembre 2013, *M.B.*, 14 janvier 2014, p. 1524.
62. Les hébergeurs peuvent voir leur responsabilité engagée s'ils ont une connaissance effective de l'activité ou de l'information illicite sans avoir réagi promptement pour retirer ou bloquer l'accès à ces informations. Voy. R. HARDOUIN, « La connaissance de l'illicéité par les hébergeurs ou quand être notifié ne signifie pas nécessairement devoir retirer », *R.D.T.I.*, 2012/2, nº 47, pp. 5-19. La notion d'hébergeur est sujette à différentes interprétations à cet égard voy. not. E. MONTERO, « Les responsabilités liées au web 2.0 », *R.D.T.I.*, 2008/3, nº 32, pp. 363-388 et H. JACQUEMIN, « Qui peut obtenir les informations permettant de rechercher et de poursuivre les auteurs d'infractions commises sur les réseaux? », *R.D.T.I.*, 2012/2, nº 47, pp. 74-81; Voy. E. RICBOURG-ATTAL, « Section II. – Les juges face aux nouveaux intermédiaires de services », *in La responsabilité civile des acteurs de l'internet*, Bruxelles, Larcier, 2014, pp. 247-295.

geant dès lors ces derniers à collaborer. Or, cette obligation de collaboration en l'espèce était particulièrement large, l'ordonnance n'était pas limitée dans le temps et visait beaucoup de noms de domaines différents. Par conséquent, les tiers visés par l'ordonnance se sont trouvés contraints de surveiller de manière générale les noms de domaines en cause. Ce faisant, la Cour de cassation a étendu le rôle de tiers dans le cadre d'une saisie. Soulignons que de manière générale, les intermédiaires privés sont de plus en plus demandés par les enquêteurs en matière informatique.

Section 2

Le rôle des intermédiaires privés dans la collecte de preuves

Le rôle des intermédiaires privés dans la collecte de preuves en matière pénale tend à s'accentuer. En effet, certaines données informatiques ne sont accessibles qu'aux acteurs privés de sorte que les enquêteurs les sollicitent davantage. De plus, des moyens de connexion anonyme tels TOR[63] ou VPN[64] ou et les techniques de chiffrement des données sont autant d'éléments susceptibles d'échapper aux enquêteurs. Le législateur a donc organisé différents devoir de collaboration à l'égard des acteurs privés susceptibles de faciliter l'accès aux données utiles à l'enquête.

A. *L'obligation de collaboration*

L'article 88*quater* du C.I.cr. prévoit une obligation de collaboration à l'égard des personnes présumées disposer d'une connaissance particulière du système en cause. Il s'agit, par exemple, des personnes gérant les services permettant de protéger ou de crypter les données stockées dans un système informatique. Celles-ci doivent fournir des informations aux enquêteurs à leur demande. Le paragraphe 2 du même article habilite le juge d'instruction à enjoindre en cas de nécessité les personnes appropriées à agir directement dans le système informatique. Celles-ci peuvent devoir le mettre en fonctionnement, copier les données, les rendre inaccessibles ou encore les retirer. Les travaux préparatoires de la loi relative à la criminalité informatique indiquent que par « personnes appropriées », il y a lieu d'entendre « des importateurs, distributeurs d'ordinateur, fournisseurs de services, opérateurs, ingénieurs d'entreprise ayant élaboré une configuration informatique spécifique, spécialistes de la sécurité... »[65]. Il revient en dernier ressort au juge de déterminer *in specie* les personnes

63. Voy. https://www.torproject.org/.
64. Le 'Virtual Private Network' est un système permettant de créer un lien direct entre des ordinateurs distants. Voy., par exemple, https://help.riseup.net/fr/vpn.
65. *Doc. parl.*, Ch. repr., n° 50-213/1, p. 27.

susceptibles de devoir collaborer. On précisera encore que la mesure ne peut porter atteinte au principe de protection contre l'auto-incrimination, au droit au silence et aux règles de droit commun relatives aux personnes tenues au secret[66]. Selon nous, une mesure visant à bloquer un site internet pourrait intervenir dans le cadre de l'article 88*quater* du C.I.cr., *a contrario* de l'enseignement tiré de l'arrêt de la Cour de cassation exposé *supra*[67]. Ce blocage s'effectuera dès lors sous le contrôle d'un juge d'instruction. Ce dernier ayant la possibilité de mettre en balance les enjeux en cause et de préserver le risque d'atteinte disproportionné à la liberté d'expression garanti par l'article 10 de la Convention européenne des droits de l'homme.

B. *Les réquisitions informatiques*

L'article 46*bis* du C.I.cr. permet au procureur du Roi de requérir le concours d'opérateur de réseau de communications électroniques pour obtenir certaines données d'identification[68]. Les notions « d'opérateur » et de « données d'identification » ne sont toutefois pas aussi limpides qu'elles n'y paraissent. Ainsi, les données susceptibles d'être demandées au stade de l'information dans le cadre d'une réquisition informatique sont, par exemple, l'identité de l'abonné d'une ligne téléphonique, d'une adresse de courrier électronique, d'une connexion internet, d'une adresse IP[69]. La réquisition informatique ne doit pas être confondue avec le repérage nécessitant l'autorisation d'un juge d'instruction[70]. La différence entre la notion de repérage au sens de l'article 88*bis* du C.I.cr. et d'identification au sens de l'article 46*bis* du C.I.cr. est parfois ténue. Pour distinguer le champ d'application des articles précités, P. Van Linthout différencie les données statiques des données dynamiques[71]. Les données statiques sont les données isolées dans le temps, par exemple l'identification d'un code 'IMEI' d'un téléphone[72], de l'adresse 'MAC' d'un ordinateur[73], de l'utilisateur d'une adresse électronique, d'une adresse IP... L'article 46*bis*

66. *Doc. parl.*, Ch. repr., n° 50-213/1, p. 28.
67. Cass. (2e ch., sect. nl.), 22 octobre 2013, R.G. n° P.13.0550.N., www.cass.be.
68. En effet, la loi du 23 janvier 2007 a étendu l'application de l'article 46*bis* C.I.cr. des simples « télécommunications » aux « communications électroniques ». Voy. L. du 23 janvier 2007 modifiant l'article 46*bis* du Code d'instruction criminelle, *M.B.*, 14 mars 2007.
69. J. KERKHOFS et P. VAN LINTHOUT, « L'article 46*bis* du Code d'instruction criminelle et l'obligation de motivation : *de minimis non curat praetor* ? », *T. Strafr.*, 2011/6, pp. 426-431.
70. Art. 88*bis* C.I.cr.
71. J. KERKHOFS et P. VAN LINTHOUT, *op. cit.*, p. 428.
72. International Mobile Equipment Identity. L'IMEI est un numéro permettant d'identifier de manière unique les terminaux d'un téléphone mobile. Toute personne peut l'obtenir en composant le code : « *#06# » sur le clavier de son téléphone portable.
73. L'adresse MAC est un identifiant stocké dans une carte réseau ou une interface réseau stockée dans l'ordinateur. Elle permet de se connecter au routeur d'un réseau.

du C.I.cr. se limite, selon cet auteur, à un croisement de données statiques. Les données dynamiques, par contre, sont les données enregistrées ou localisées en temps réel, par exemple le signal émis par un téléphone portable.

Par ailleurs, l'article 46*bis* du C.I.cr.[74] impose aux « fournisseurs de services » et « opérateurs de réseaux » de transférer les données nécessaires à l'enquête sur la base d'un réquisitoire du procureur du Roi[75]. L'absence de qualification claire d'« opérateurs ou de fournisseurs de service » au sens de l'article 46*bis* du C.I.cr. pose certains problèmes en pratique puisque certaines sociétés refusent de collaborer. Ainsi, la société américaine '*Yahoo !*' contestait un réquisitoire du procureur du Roi lui imposant de communiquer certaines données. L'affaire fut portée devant les cours et tribunaux. En première instance[76], le tribunal qualifie la société de « fournisseur de communications électroniques » au sens de l'article 46*bis* du Code d'instruction criminelle l'obligeant dès lors à collaborer dans les limites de cet article. En appel, la cour réforma le jugement[77]. Selon cette dernière, les notions d'« opérateurs de réseaux de communications électroniques » et de « fournisseurs d'un service de communications électroniques » doivent être interprétées à la lumière de la loi du 30 juin 2005 relative aux communications électroniques[78]. En effet, même si le principe de l'autonomie du droit pénal laisse la possibilité au juge de s'affranchir du sens donné par certaines lois, il n'empêche pas qu'il puisse s'en inspirer[79]. L'affaire ne s'arrêta pas là. Saisie d'un pourvoi en cassation, la Cour considéra que la notion de « fournisseur d'un service de communication électronique » ne se limite pas à l'interprétation donnée par la loi du 30 juin 2005 mais s'étend à tout service de communications électroniques. Selon la Cour, il s'agit d'une part, de celui qui offre un service permettant la transmission de signaux par la voie des réseaux de communications électroniques et d'autre part, du service offrant la possibilité de recevoir ou diffuser des informations aux moyens d'un réseau électronique[80]. Ce faisant, la Cour étend le champ d'application de l'article 46*bis* du C.I.cr. à tout type de services de communications électroniques. Cette interprétation extrêmement large de la notion de « fournisseur d'un service de communication électronique » laisse un pouvoir d'appréciation important au juge du fond à qui il appartiendra de considérer si l'entreprise considérée entre en ligne de compte[81]. Or, cette mesure peut être prise dans le cadre d'une enquête proactive[82] au stade de l'information. Il conviendrait donc de disposer d'un cadre légal clair afin d'éviter tout risque d'abus et d'étendre de manière trop importante les acteurs susceptibles de devoir collaborer.

74. L'article 46*bis* C.I.cr. est introduit par la loi du 10 juin 1998 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 communications et de télécommunications privées, *M.B.*, 24 janvier 1995.
75. De même, remarquons que les fonctionnaires sont soumis à une obligation de dénonciation en cas de connaissance de crime ou de délit conformément à l'article 29 C.I.cr. Les personnes ayant connaissance d'un attentat soit contre la sûreté publique soit contre la vie ou la propriété d'un individu doivent également informer le procureur du Roi conformément à l'article 30 C.I.cr.
76. Corr. Termonde, 2 mars 2009, *T. Strafr.*, 2009, p. 116, et le reflet de E. DE BUSSER, *Juristenkrant*, 2009, p. 3. Notons que la société contestait la compétence des autorités judiciaires belges, celle-ci n'ayant pas de siège d'exploitation en Belgique. Les autorités devaient, selon Yahoo !, passer par le biais d'une commission rogatoire internationale. Le juge du tribunal de première instance considéra que la société est soumise à la législation belge puisqu'elle a des activités commerciales en Belgique.
77. Gand, 30 juin 2010, *T. Strafr.*, 2011, p. 132 et le reflet de P. VAN LINTHOUT, *Juristenkrant*, 2010, liv. 216, p. 4.
78. L. du 13 juin 2005 relative aux communications électroniques, *M.B.*, 20 juin 2005.
79. Fr. KUTY, « Chapitre IV – L'autonomie du droit pénal », *in Principes généraux du droit pénal belge – Tome I*, Bruxelles, Larcier, 2009, pp. 115-137.

C. *Le repérage*

Le repérage est une mesure d'enquête par laquelle le juge d'instruction requiert des opérateurs de télécommunications d'isoler certaines données d'appel, par exemple d'isoler les différents numéros de téléphones composés par un téléphone. Cette mesure doit être limitée dans le temps, deux mois maximum à dater de l'ordonnance et peut être renouvelée[83]. En principe, les télécommunications visées dans l'ordonnance de repérage doivent concerner une période postérieure. Dans certains cas, l'ordonnance peut comprendre des opérations émises par le passé, la motivation se limite alors à un simple réquisitoire destiné à l'opérateur ou au fournisseur de télécommunications[84].

Notons qu'une certaine jurisprudence[85] considérait que la localisation d'un téléphone portable effectuée par la détection du signal émis par l'appareil ne nécessite pas l'autorisation d'un juge d'instruction. Il s'agit selon cette jurisprudence d'une simple recherche technique effectuée par l'Institut belge des services postaux et de télécommunications et non d'un repérage. Dans un arrêt du 24 mai 2011, la Cour de cassation clôt la

80. Cass., 18 janvier 2011, www.cass.be. Notons que l'affaire a ensuite été renvoyée vers la cour d'appel puis la Cour de Cassation et enfin la cour d'appel, celles-ci étant appelées à se prononcer sur la régularité du réquisitoire du procureur du Roi. Voy. O. LEROUX, « Criminalité informatique », *in* X., *Postal Mémorialis. Lexique du droit pénal et des lois spéciales, op. cit.*, C 362/01-C 362/55 (58 p.), p. 65.
81. L. KERZMANN, « L'affaire Yahoo ! ou à qui s'adresse l'obligation de collaboration instaurée par l'article 46*bis* du Code d'instruction criminelle ? », *R.D.T.I.*, 2011/3, n° 44, pp. 116-123.
82. Art. 46*bis*, § 1er, al. 2, C.I.cr.
83. Art. 88*bis* C.I.cr.
84. J. DE CODT, *Des nullités de l'instruction et du jugement*, Bruxelles, Larcier, 2006, pp. 45-46.
85. Cass., 10 novembre 2009, R.G. n° P.09.1584.F, *Pas.*, 2009, www.cass.be.

controverse et souligne que « la localisation par la détection du seul signal émis par l'appareil en fonctionnement et sans qu'une télécommunication soit émise ou reçue pendant le repérage, est régie par la loi et impose au juge d'instruction de la requérir par ordonnance motivée. »[86]. Cette jurisprudence n'a plus été remise en cause par les cours et tribunaux[87].

D. *La rétention de données*

L'article 126 de la loi du 13 juin 2005 relative aux communications électroniques[88] prévoit une obligation de rétention de données envers les fournisseurs de services de téléphonie fixe et mobile, les fournisseurs d'accès à internet, les fournisseurs de réseaux publics de communications électroniques et de courrier électroniques ou téléphonie par internet. Ceux-ci doivent conserver les données de trafic, de localisation, d'identification des utilisateurs finaux, d'identification des services de communications électroniques utilisés et les données d'identification de l'équipement terminal présumé avoir été utilisé. Il s'agit donc des données traitées et générées dans le cadre de la fourniture de services de communication, c'est-à-dire toutes nos données générées par nos communications électroniques (liste de contacts, date, heure des échanges des communications électroniques, sites internet consultés...), à l'exception du contenu des messages envoyés[89].

L'obligation de rétention de données est introduite par la loi du 30 juillet 2013 portant modification des articles 2, 126 et 145 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 90*decies* du C.I.cr.[90]. Cette loi est complétée par l'arrêté royal du 19 septembre 2013 portant exécution de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques[91] et l'arrêté royal du 9 janvier 2003 déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques[92].

86. Cass., 24 mai 2011, R.G. n° P.11.0909.N, *Pas.*, 2011, www.cass.be.
87. A. LINERS, K. VANDERHEIDEN et M. LANGOUCHE, « Le signal émis par un téléphone mobile et permettant sa géolocalisation tombe-t-il sous le champ d'application de l'article 88*bis* C.I.cr.? », *Vigiles 2013*, liv. 1-2, pp. 62-63.
88. L. du 13 juin 2005 relative aux communications électroniques, *M.B.*, 20 juin 2005.
89. Pour une explication détaillée des données en cause voy. http://stopdataretention.be/files/dataretention-decree_fr.pdf.
90. L. 30 juillet 2013 « portant modification des articles 2, 126 et 145 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 90*decies* du Code d'instruction criminelle », *M.B.*, 23 août 2013. Ci-après, « loi rétention de données ».
91. A.R. du 19 septembre 2013 portant exécution de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques, *M.B.*, 8 octobre 2013.
92. A.R. du 31 janvier 2013 remplaçant l'annexe reprise à l'arrêté royal du 9 janvier 2003 déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques, *M.B.*, 4 mars 2013.

Ces dispositions légales assurent la transposition de la directive 2006/24/CE[93], directive déclarée invalide dans un arrêt du 8 avril 2014 par la Cour de justice de l'Union européenne[94]. Ce texte, né dans un contexte de lutte contre la criminalité grave et le terrorisme[95], a dès le départ provoqué une réticence certaine de la part de nombreux acteurs notamment du groupe de travail « Article 29 »[96], d'eurodéputés[97]et de sociétés de téléphonie et fournisseurs d'accès à internet[98]. Après son adoption, le texte n'a cessé de faire des vagues vu les enjeux de la rétention de données pour le respect des droits fondamentaux[99]. En 2010, Peter Hustinx, le contrôleur européen de la protection des données, émet de vives critiques vis-à-vis des objectifs de la directive et de leurs applications[100]. En 2014, la Cour de justice de l'Union européenne fut saisie de questions préjudicielles. Celles-ci remettaient eu cause l'adéquation de la directive 2006/24 à la Charte des droits fondamentaux de l'Union européenne et en particulier aux articles 7 et 8 de la Charte consacrant respectivement le droit au respect de la vie privée et le droit à la protection des données à caractère personnel[101]. Elle invalida la directive au motif qu'elle « comporte une ingérence dans ces droits fondamentaux d'une vaste ampleur

93. Directive 2006/24/CE sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications.
94. C.J.U.E. (gde ch.), 8 avril 2014, *Digital Rights Ireland Ltd & Michael Seitlinger e.a.*, aff. jtes C-293/12 et C-594/12.
95. Conseil européen, Déclaration sur la lutte contre le terrorisme, Bruxelles, le 25 mars 2004, p. 1.
96. À l'heure de l'adoption de la directive, le groupe de travail « article 29 » met en garde l'Union européenne et souligne que « La décision de conserver les données de communication aux fins de la répression des infractions graves est sans précédent et elle fera date. Elle empiète sur la vie quotidienne de chacun et menace les valeurs et les libertés fondamentales érigées en principes et chères au cœur de tous les citoyens européens. », p. 2, avis 3/2006 du groupe article 29 du 25 mars 2006, disponible sur http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp119_fr.pdf.
97. Rapport du 28 novembre 2005 sur la proposition de directive du Parlement européen et du Conseil sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public, et modifiant la directive 2002/58/CE (COM(2005)0438 – C6-0293/2005 – 2005/0182(COD).
98. Rapport de la commission au Conseil et au Parlement européen, Rapport d'évaluation concernant la directive sur la conservation des données, (directive 2006/24/CE), Bruxelles, le 18 avril 2011, p. 30.
99. Voy. le rapport de l'A.S.B.L. internationale European Digital Rights, http://www.edri.org/files/shadow_drd_report_110417.pdf; voy. égal. la déclaration du 7 juin 2011 déposée par diverses associations considérant que la surveillance de masse est inacceptable disponible sur http://www.liguedh.be/images/PDF/documentation/divers/directive_dataretention_joint_position_07-06-2011.pdf.
100. Voy. Discours prononcé par Peter Hustinx lors de la conférence « Taking on the Data Retention directive », 3 décembre 2010, disponible sur https://secure.edps.europa.eu/EDPSWEB/edps/lang/fr/EDPS/Publications/SpeechArticle/SA2010.
101. C.J.U.E. (gde ch.), 8 avril 2014, *Digital Rights Ireland Ltd & Michael Seitlinger e.a.*, aff. jtes C-293/12 et C-594/12.

et d'une gravité particulière dans l'ordre juridique de l'Union sans qu'une telle ingérence ne soit précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au strict nécessaire »[102]. En effet, la directive rétention de données s'appliquait de manière générale sans aucune différenciation ou limitation selon les personnes. Elle ne prévoyait pas de distinction par exemple liée au secret professionnel des avocats ou aux données sensibles des médecins susceptibles d'être traitées.

Même si cette invalidation n'entraîne pas l'invalidation de la loi transposant la directive précitée dans l'ordre juridique belge, il est permis de tirer quelques enseignements relatifs à la constitutionnalité de la disposition. Tout d'abord, la rétention de données s'applique également de manière générale, sans distinction entre les personnes concernées. Ensuite, la loi belge a un objectif plus large que la directive transposée. Elle étend son champ d'application à la lutte contre les crimes et les délits visés aux articles 46*bis* et 88*bis* du C.I.cr. La directive 2006/24/CE ne visait que la lutte contre la criminalité grave. Un objectif aussi large met en doute le caractère « strictement nécessaire » de la mesure, caractère pourtant obligatoire en cas d'ingérence dans les droits fondamentaux[103]. Par ailleurs, la loi en cause n'impose pas de conserver les données sur un territoire donné. Celles-ci pourraient donc être conservées à l'étranger. Enfin, la durée de conservation est de 12 mois en principe. Pour certaines données, le délai peut dépasser 18 mois voire 24 mois lors de circonstances exceptionnelles, notamment « lorsque la sécurité publique, la santé publique, l'ordre public ou la défense du Royaume l'exigent »[104]. Ce délai peut être étendu sur la base d'un arrêté royal, laissant donc un pouvoir d'appréciation important au Roi.

En tout état de cause, il est permis de se demander si la loi « rétention de données » n'étend pas la notion d'enquête proactive tout en déplaçant subtilement la tâche vers des acteurs privés. En effet, la rétention de données vise à lutter contre les crimes et les délits. S'appliquant de manière systématique et généralisée, elle laisse supposer qu'il existe dans le chef de chacun de nous la suspicion raisonnable que des infractions seront commises mais ne sont pas encore connues. Outre l'obligation de

102. Pt 65 de l'arrêt. Pour une analyse de cet arrêt voy. I. CHATELIER et M. V. PEREZ ASINARI, « Arrêt "Digital Rights Ireland" : invalidité de la directive sur la conservation des données de trafic », *J.D.E.*, n° 210, 2014, p. 251 ; M.-L. BASILIEN-GAINCHE, « Une prohibition européenne claire de la surveillance électronique de masse », *La Revue des droits de l'homme* [En ligne], Actualités Droits-Libertés, mis en ligne le 14 mai 2014, consulté le 3 octobre 2014. URL : http://revdh.revues.org/746.

103. C. DE GEEST et R. JESPERS, « Dataretentie : buitensporig en onevenredig ! », *Mondiaal Nieuws*, 18 mars 2015, http://www.mo.be/opinie/dataretentie-buitensporig-en-onevenredig.

104. Art. 5, § 4, de la loi « rétention de données ».

rétention incombant à des acteurs privés et non à des autorités judiciaires, le principe de la rétention rappelle l'enquête proactive caractérisée par l'anticipation de l'action judiciaire par les services de police[105]. Or, selon l'article 28*bis*, § 2, du C.I.cr., l'enquête proactive est limitée à la lutte contre les infractions graves, *a contrario* de la rétention de données où l'objectif est beaucoup plus large puisque cette dernière s'étend à la lutte contre tout crime et délit.

De plus, le législateur aurait pu se limiter à imposer un système de préservation de données dans l'esprit insufflé par la convention de Budapest[106]. La '*data preservation*' s'effectue *a posteriori*, les opérateurs doivent geler les données suite à une injonction judiciaire[107]. *A contrario*, la '*data retention*' suppose une conservation de données *a priori*, les opérateurs retiennent les données de manière généralisée et systématique. Le caractère *a priori* de la mesure permet, certes, de collecter des données potentiellement utiles pour une enquête qui, sans la rétention automatique, pourraient être perdues. Elle implique cependant une ingérence sans précédent dans les droits fondamentaux. Outre le choix politique d'adopter une telle mesure, l'ingérence doit juridiquement être contrôlée à la lumière du principe de proportionnalité.

Contrôle strict que devra effectuer la Cour constitutionnelle puisqu'à l'heure actuelle, un recours en annulation qui a été plaidé le 18 mars 2015 est toujours pendant[108].

105. B. RENARD, « La mise en œuvre et le suivi de l'enquête de recherche proactive : étude qualitative des facteurs influençant le processus de décision », *Rev. dr. pén.*, 2003, liv. 2, pp. 133-167.

106. Convention de Budapest sur la cybercriminalité, Conseil de l'Europe, 23 novembre 2001.

107. Voy. Centre for strategy and Evaluation Services, Evidence of Potential Impacts of Options for Revising the Data Retention directive : Current approaches to data preservation in the EU and in third countries, novembre 2010, disponible sur http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/data-retention/docs/drd_task_2_report_final_en.pdf.

108. Recours devant la Cour constitutionnelle en annulation de l'article 5 de la loi du 30 juillet 2013 « portant modification des articles 2, 126 et 145 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 90*decies* du Code d'instruction criminelle » (publiée au *M.B.*, 23 août 2013) par l'Ordre des barreaux francophones et germanophone et par l'A.S.B.L. « Liga voor Mensenrechten » et l'A.S.B.L. « Ligue des Droits de l'Homme », aff. jtes (numéros de rôle 5856 et 5859), *M.B.*, 2 avril 2014, p. 28570.

5

Section 3

Les méthodes particulières de recherche et les nouvelles technologies

La loi du 6 janvier 2003 concernant les méthodes particulières de recherche et quelques autres méthodes d'enquête[109] ne donne pas de définition des méthodes particulières de recherche (ci-après M.P.R.). Selon l'article 47*ter*, § 1er, du C.I.cr., il s'agit au sens strict des méthodes d'observation, d'infiltration et de recours aux indicateurs. Elles sont particulières dans le sens où elles sont susceptibles de porter atteinte aux libertés et droits fondamentaux[110]. À la différence des autres méthodes d'enquêtes, par exemple l'interception des communications, les enquêteurs établissent un dossier confidentiel où sont glissées certaines pièces du dossier[111]. Les travaux préparatoires de la loi précitée précisent qu'elles ont pour finalité la découverte des infractions et de leurs auteurs[112]. La plupart peuvent être mises en œuvre dans un cadre proactif, l'enquêteur doit néanmoins disposer d'indices sérieux de la commission d'une infraction déjà commise mais non encore connue ou en passe d'être commise[113]. Ce dernier sera, par ailleurs, strictement soumis au principe de l'interdiction de la provocation au risque d'entraîner l'irrecevabilité des poursuites[114]. Enfin, le choix de recourir aux M.P.R. doit s'effectuer à la lumière des principes de proportionnalité et de subsidiarité[115]. Dans le cadre de cette contribution, nous limiterons notre analyse à deux méthodes particulières de recherche à savoir l'infiltration et l'observation dans un contexte informatique.

A. *L'infiltration dans un contexte informatique*

L'infiltration est «le fait, pour un fonctionnaire de police, appelé infiltrant, d'entretenir, sous une identité fictive, des relations durables avec une ou plusieurs personnes concernant lesquelles il existe des indices sérieux qu'elles commettent ou commettraient des infractions dans le cadre d'une organisation criminelle visée à l'article 324*bis* du Code pénal ou des crimes ou des délits visés à l'article 90*ter*, §§ 2 à 4»[116]. L'infiltrant établi nécessairement sous une identité fictive un contact durable avec

109. L. du 6 janvier 2003, *M.B.*, 12 mai 2003.
110. *Doc. parl.*, Ch. repr., nº 50-1688/001, p. 132.
111. *Ibid.*, p. 132.
112. *Ibid.*, p. 8.
113. D. CHICHOYAN et A. JACOBS, *Les méthodes particulières de recherche*, Postal Memorialis, 2009, M105/7.
114. Art. 30 du Titre préliminaire du Code de procédure pénale.
115. D. CHICHOYAN et A. JACOBS, *op. cit.*, M105/10.
116. Art. 47*octies* C.I.cr.

l'infiltré, ce contact pouvant néanmoins être occasionnel[117]. Le cadre dans lequel s'inscrit une mesure d'infiltration est en principe réactif[118]. En effet, l'article 47*octies* du C.I.cr. précise la nécessité de disposer «d'indices sérieux qu'elles commettent ou commettraient des infractions. Elle pourrait toutefois à certaines conditions s'inscrire dans un cadre proactif[119].

En matière informatique, l'enquêteur peut créer une identité fictive et l'utiliser pour collecter certaines informations. La mesure suppose dès lors la commission de deux infractions à savoir le faux informatique[120] et le port public de faux nom[121]. Ces dernières ne pourront être commises sans l'autorisation du procureur du Roi[122]. Par ailleurs, l'enquêteur ne doit pas forcément utiliser une fausse identité pour rassembler les données en ligne utiles à l'enquête. Toutefois, sans l'utilisation d'une identité fictive, il ne s'agira pas d'une infiltration. L'agent compétent devra, selon nous, mentionner sa qualité dès le moment où il établit un contact avec la personne visée, au risque de manquer à son devoir de loyauté[123]. De plus, l'utilisation d'un pseudonyme est très proche de la création d'une identité fictive, la limite est en tout cas ténue. En effet, l'infiltration peut être accompagnée d'autres techniques prévues par l'arrêté royal du 19 avril 2003[124]. En l'occurrence, l'utilisation d'un surnom attractif sur un '*chat*' rappelle la pseudo-vente, par exemple. Cette technique autorise les enquêteurs à se présenter ou être présentés comme vendeurs potentiels de services ou de biens[125]. Or, les services de police affirment leur souhait de pouvoir enquêter rapidement et efficacement sur les réseaux sociaux mais trouvent la procédure actuelle trop lourde[126]. Un cadre légal clair serait donc souhaitable afin d'éviter tout risque d'abus. Enfin, une mesure d'infiltration doit avoir un caractère durable. Cette caractéristique s'interprète également *in concreto* et dépendra de l'intensité de la relation entre les deux personnes[127]. La durée de l'infiltration est limitée, elle ne

117. D. CHICHOYAN et A. JACOBS, *op. cit.*, M105/31.
118. M. SALMON, J.-P. BUYLE, E. CORNU, B. DEJEMEPPE, B. DESCHUYTENEER, B. DOCQUIR, M. GIACOMETTI, B. LEMAL, T. LEONARD, P. MONVILLE et E. PLASSCHAERT, «6 – Réseaux sociaux, anonymat et faux profils: vrais problèmes en droit pénal et de la procédure pénale», *in Les réseaux sociaux et le droit*, Bruxelles, Larcier, 2014, pp. 202-204.
119. M. SALMON, J.-P. BUYLE, E. CORNU, B. DEJEMEPPE, B. DESCHUYTENEER, B. DOCQUIR, M. GIACOMETTI, B. LEMAL, T. LEONARD, P. MONVILLE et E. PLASSCHAERT, *op. cit.*, p. 204.
120. Art. 210 C. pén.
121. Art. 231 C. pén.
122. Art. 47*octies*, § 4, C.I.cr.
123. Art. 28*bis* C.I.cr.
124. A.R. 9 avril 2003, *M.B.*, 12 mai 2003.
125. Art. 4 de l'A.R. du 9 avril 2003, *M.B.*, 12 mai 2003.
126. K. CLERIX, «Politie wil met fictieve identiteit op Facebook infiltreren», *M.O.*, 14 mars 2014, http://www.mo.be/nieuws/politie-wil-met-fictieve-identiteit-op-facebook-infiltreren.
127. D. CHICHOYAN et A. JACOBS, *op. cit.*, M105/31.

peut dépasser trois mois renouvelables[128]. Cette limitation dans le temps peut poser certains problèmes d'application pratique, par exemple si l'enquêteur laisse son profil inactif et le réutilise après une certaine période, il dépassera rapidement le délai légal prescrit[129].

Sur les réseaux sociaux par exemple, les enquêteurs pourraient utiliser un pseudonyme pour intégrer un groupe lié à un intérêt particulier et se présenter comme susceptibles de proposer des services. Il n'y aura pas infiltration au sens de l'article 47*octies* du C.I.cr. s'il n'y a pas utilisation d'une « identité fictive ». La mesure rappelle néammoins les caractéristiques d'autres techniques pouvant accompagner l'infiltration à savoir par exemple, la pseudo vente. Par conséquent, selon nous, l'utilisation d'un pseudonyme est très proche de l'infiltration de sorte qu'il conviendrait de lui attacher les mêmes garanties afin d'éviter un recours trop rapide à ces techniques d'enquêtes et sans lui accorder les précautions nécessaires.

B. *L'observation sur internet*

L'article 47*sexies*, § 1er, du C.I.cr. définit l'observation par « une observation de plus de cinq jours consécutifs ou de plus de cinq jours non consécutifs répartis sur une période d'un mois, une observation dans le cadre de laquelle des moyens techniques sont utilisés, une observation revêtant un caractère international ou une observation exécutée par des unités spécialisées de la police fédérale». L'observation en tant que méthode particulière de recherche se définit donc par sa durée, par l'utilisation de moyens techniques ou par son étendue internationale. Elle se distingue de l'observation « non-systématique » qui relève de la compétence générale des services de police. Cette dernière s'exerce, par exemple à des occasions déterminées lorsqu'un policier « en civil » épie des personnes organisant une manifestation sans autorisation[130].

Selon nous, l'observation effectuée sur internet est nécessairement une observation systématique puisqu'elle est effectuée avec un moyen technique, en l'occurrence internet[131]. Dès lors, un enquêteur consultant

128. Art. 47*octies*, § 3, 5°, C.I.cr.
129. MM. SALMON, J.-P. BUYLE, E. CORNU, B. DEJEMEPPE, B. DESCHUYTENEER, B. DOCQUIR, M. GIACOMETTI, B. LEMAL, T. LEONARD, P. MONVILLE et E. PLASSCHAERT, *op. cit.*, pp. 202 et s.
130. *Doc. parl.*, Ch. repr., n° 20/1688/001, p. 30; voy. égal. M. BEYS, *Quels droits face à la police ?*, Couleur livres – J&D Éditions, 2014, pp. 323 et s.
131. L'article 47*sexies*, § 1er, du C.I.cr. définit le moyen technique par une « configuration de composants qui détecte des signaux, les transmet, active leur enregistrement et enregistre les signaux, à l'exception des moyens techniques utilisés en vue de l'exécution d'une mesure visée à l'article 90*ter*. » Les moyens techniques utilisés sont, par exemple le 'GPS' ou la caméra. Par contre, l'utilisation d'une caméra thermique ou d'un appareil photo ne rentrent pas dans le champ d'application de l'article 47*sexies* du C.I.cr. Dans le cas où ces derniers ont une vue dans un domicile ou une habitation privée, elle sera alors qualifiée de contrôle visuel discret au sens de l'article 89*ter* du C.I.cr. Notons que la

des forums, même de manière occasionnelle, effectue une observation. Dans le cas où internet ne peut être considéré comme un moyen technique, d'autres méthodes techniques sont concevables, par exemple l'utilisation du 'troyen' placé sur l'ordinateur d'une personne[132]. L'« espion » sera implanté dans le système informatique d'une personne en vue soit d'exploiter le contenu d'un disque dur, soit d'intercepter le contenu de conversations en cours de transmission. La mesure d'observation au sens strict sera très vite rattrapée par d'autres mesures d'enquête. Dans le premier cas, l'enquêteur effectuera une recherche informatique ou une extension de recherche informatique nécessitant l'intervention du juge d'instruction[133]. Dans le second cas, il interceptera des données en cours de transmission au sens de l'article 90*ter* et suivants du C.I.cr. Par conséquent, la méthode particulière de recherche d'observation sur internet chevauche nécessairement d'autres méthodes d'enquête de sorte que l'on peut douter de son application effective.

Section 4
L'interception des communications électroniques

L'interception de communications privées des articles 90*ter* et suivants du C.I.cr. s'appliquent en matière de communications électroniques. En effet, les travaux préparatoires de la loi du 30 juin 1994[134] précisent que la notion de télécommunication en procédure pénale se calque sur la définition donnée par l'article 68, 4° de la loi « Belgacom » du 21 mars 1991[135], à savoir « toute transmission, émission ou réception de signes, de signaux, d'écrits, d'images, de sons ou de données de toute nature, par fil, radioélectricité, signalisation optique ou autre système électro-

surveillance par GPS suscite certaines controverses. Pour une analyse de droit comparé, voy. E. VERGES, « La géolocalisation : une preuve pénale licite au regard de l'article 8 de la Convention européenne des droits de l'homme ? Analyse comparée des positions adoptées par la Cour de cassation et la Cour européenne des droits de l'homme (Cass. crim. 22 novembre 2011 ; Cour eur. D.H., 2 septembre 2010, n° 35623/05, *Uzun cl Allemagne*) », *R.D.L.F.*, 2012, chron. n° 04. À propos de l'utilisation des caméras et de la législation afférente voy. F. DUMORTIER, *Caméras de surveillance : la cohabitation légale reste houleuse : à propos du champ d'application de la loi du 21 mars 2007 et de sa coexistence avec d'autres normes réglant les caméras de surveillance*, Bruxelles, Politeia, 2009.
132. Le troyen ou cheval de Troie est un logiciel malveillant qui s'apparente à un logiciel légitime.
133. Art. 88*ter* C.I.cr.
134. L. 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.*, 24 janvier 1995, p. 1542.
135. L. du 21 mars 1991 portant réforme de certaines entreprises publiques économiques, *M.B.*, 27 mars 1991.

magnétique »[136]. Cette interprétation a pour conséquence d'inclure les messages envoyés par téléphone portable et les courriers électroniques[137]. Le courrier électronique n'est donc pas un courrier au sens des articles 46*ter*, § 1er, du C.I.cr. et 88*sexies*, § 1er, du C.I.cr.[138]. En principe, il est interdit de prendre connaissance du contenu des (télé)communications privées sans y être autorisé au risque de sanctions pénales[139]. Le droit au secret des communications est, en effet, une facette du droit à la vie privée au sens de l'article 22 de la Constitution[140] et de l'article 8, § 1er, de la Convention européenne des droits de l'homme[141]. Ce principe n'est pas absolu, les autorités compétentes peuvent intercepter des communications dans certains cas strictement définis par la loi[142]. Cette mesure exceptionnelle doit être mise en œuvre à la lumière des principes de proportionnalité et de subsidiarité[143]. De plus, l'interception des (télé)communications est limitée aux investigations liées aux infractions et tentatives d'infractions les plus graves[144]. Elle relève donc de la compétence du juge d'instruction et dans certains cas du procureur du Roi notamment en cas de flagrant délit[145].

136. Projet de loi relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées, exposé des motifs, *Doc. parl.*, Sénat, n° 843-1, p. 7.
137. D. VANDERMEERSCH, *Les recherches en matière de téléphonie et de (télé)communications*, Bruxelles, éd. Jeune Barreau, 2006, p. 49.
138. En effet, le terme « courrier » est défini par les travaux préparatoire de la loi du 6 janvier 2003 relative au méthode particulières de recherche comme les « lettres et petits paquets postaux » traditionnels, à savoir les « courriers ouverts et fermés, cartes postales, imprimés, circulaires, paquets postaux, avis, télégrammes, envois recommandés, courriers transfrontaliers, etc. ». Voy. projet de loi relatif à la loi concernant les méthodes particulières de recherche et autres méthodes d'investigation, exposé des motifs, *Doc. parl.*, Ch. repr., n° 50-1688/1, pp. 55-56.
139. Voy. art. 314*bis* et 259*bis* du C. pén. introduits par 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.*, 24 janvier 1995. En outre, l'article 124 de la loi du 13 juin 2005 relative aux communications électroniques interdit de prendre connaissance d'une information transmise par voie électronique sans y être autorisé. Voy. L. du 13 juin 2005 relative aux communications électroniques, *M.B.*, 20 juin 2005.
140. À cet égard voy. R. ROBERT et K. ROSIER, « Réglementation et contrôle de l'utilisation des technologies de la communication et de l'information sur le lieu de travail », *in Le droit du travail à l'ère du numérique*, Limal, Anthemis, 2011, pp. 241 et s.
141. Cour eur. D.H., 18 mai 2010, *Kennedy c. Royaume-Uni*, § 118. Notons que la doctrine et les cours et tribunaux du travail sont divisés quant à l'extension du droit au secret des lettres garanti par l'article 29 de la Constitution au courrier électronique. Voy. T. CLAYES et D. DEJONGHE, « Gebruik van *e-mail* en internet op de werkplaats en controle door de werkgever », *J.T.T.*, 2001, p. 129 ; K. ROSIER, « Droit social : contrôle de l'usage des technologies de l'information et de la communication dans les relations de travail », *R.D.T.I.*, 2009, n° 35, p. 128.
142. Art. 90*ter* et s. C.I.cr.
143. D. VANDERMEERSCH, « La loi belge du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement des communications et télécommunications privées », *Rev. dr. pén.*, 1995, p. 301.
144. Art. 90*ter*, §§2 et 3, C.I.cr.

Les articles 90*ter* et suivants du C.I.cr. habilitent les autorités compétentes à « prendre connaissance » des (télé)communications « en cours de transmission ». La notion « en cours de transmission » fait l'objet de controverses. Selon les travaux préparatoires de la loi en cause, il s'agit de l'interception effectuée « sur le trajet entre l'émetteur et le récepteur »[146]. La question se corse lorsqu'il s'agit de déterminer si un courrier électronique sur le serveur mail du fournisseur d'accès Internet sans être arrivé sur l'ordinateur du destinataire est « en cours de transmission ». Selon certains auteurs, il s'agit du moment où le courrier peut être lu par le destinataire et se trouve dans sa boîte à courrier électronique[147]. D'autres auteurs estiment par contre que le destinataire doit avoir lu le courrier électronique pour être « en cours de transmission »[148]. L'article 90*ter* du C.I.cr. précise : « le juge d'instruction peut, à titre exceptionnel, écouter, prendre connaissance et enregistrer, pendant leur transmission ». Selon P. Van Linthout et J. Kherkhofs, il faut prendre en considération l'endroit où l'on peut raisonnablement considérer que le courrier a atteint sa destination[149]. En cas d'utilisation d'un client mail type '*thunderbird*', '*outlook*', le mail ne sera plus « en cours de transmission » dès son stockage sur le système informatique. Par contre, en cas d'utilisation d'une messagerie type '*outlook.com*', il ne sera plus en « cours de transmission » dès la consultation de la boîte électronique par la personne. En outre, une fois les données stockées, un juge d'instruction pourra accéder aux données sur la base de l'article 88*ter* du C.I.cr. En pratique et pour éviter toutes erreurs, les enquêteurs pourraient envisager des ordonnances sur deux bases légales : la recherche informatique et l'interception des (télé)communications.

Conclusion

Les nouvelles méthodes d'enquêtes liées à l'informatique peinent parfois à s'intégrer dans le Code d'instruction criminelle suscitant dès lors certaines inquiétudes. Si les règles de procédure pénale peuvent par-

145. Art. 90*ter*, § 5, C.I.cr.
146. Projet de loi relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées, exposé des motifs, *Doc. parl.*, Sénat, n° 843-1, p. 6.
147. F. DE VILLENFAGNE, « Criminalité informatique », *in Chronique de jurisprudence en droit des technologies de l'information (2002-2008) (2e partie)*, *R.D.T.I.*, n° 39, p. 22.
148. C. DE VALKENEER, « Les infractions en matière d'écoutes, de prise de connaissance et d'enregistrement de communications et de télécommunications », *in Les infractions – Volume 5 : les infractions contre l'ordre public* (H.-D. BOSLY et C. DE VALKENEER dir.), Bruxelles, Larcier, 2013, p. 399.
149. P. VAN LINTHOUT et J. KERKHOFS, « Internetrecherche : informaticatap en netwerkzoeking, licht aan het eind van de tunnel », *T. Strafr.*, 2008/2, p. 82.

fois sembler vieillies et révolues, elles sont les remparts contre les risques d'abus et d'arbitraire. En effet, une mesure d'investigation est susceptible de porter atteinte à certains droits fondamentaux. Ces ingérences sont justifiables pour autant qu'elles soient prévisibles, nécessaires, appropriées et proportionnées par rapport aux buts poursuivis[150]. Tant la jurisprudence de la Cour européenne des droits de l'homme que la Cour de justice de l'Union européenne ont étayé les conditions susmentionnées[151].

Si les nouvelles technologies confèrent de nouveaux moyens d'investigation, l'usage de ceux-ci ne peut se faire à n'importe quel prix. Ainsi, la mesure doit être prévisible et requiert une qualité légistique suffisante. L'étendue et les moyens d'action des autorités compétentes doivent être clairement et précisément encadrés. À cet égard, la Cour de Strasbourg souligne qu'une disposition légale doit « user de termes assez clairs pour indiquer à tous de manière suffisante en quelles circonstances et sous quelles conditions elle habilite la puissance publique à opérer pareille atteinte secrète, et virtuellement dangereuse, au droit au respect de la vie privée et de la correspondance »[152]. Une loi autorisant une méthode d'enquête doit donc être accessible et prévisible par l'intermédiaire de règles limpides et détaillées[153].

Or, comme nous l'avons vu, les règles relatives aux nouvelles technologies en procédure pénale laissent en suspend de nombreuses questions. Même si la jurisprudence et la doctrine tendent à apporter certaines réponses, celles-ci ne permettent pas d'encadrer la totalité des nouvelles mesures pour leur conférer, selon nous, une qualité légistique suffisante. Ce flou artistique suscite dès lors des inquiétudes légitimes quant au risque d'arbitraire et d'abus dans un domaine où l'équilibre entre les intérêts des services judiciaires et policiers et le respect des droits et libertés fondamentaux est parfois très fragile.

150. Art. 52, § 1er, de la Charte des droits fondamentaux et les § 2 des articles 8 à 11 de la Convention européenne des droits de l'homme.

151. Le caractère proportionné d'une mesure s'évalue au regard de l'objectif poursuivi, celui-ci doit être légitime et nécessaire dans une société démocratique. En outre, les États doivent mettre en balance les intérêts en cause à la lumière « des avantages pouvant résulter d'un large recours à ces techniques, d'une part, et des intérêts essentiels s'attachant à la protection de la vie privée, d'autre part ». Cour eur. D.H., 4 décembre 2008, *S. et Marper c. Royaume-Uni*, § 112. Voy. not. Cour eur. D.H., 3 avril 2007, *Copland c. Royaume-Uni*; Cour eur. D.H., 4 décembre 2008, *S. et Marper c. Royaume-Uni*, p. 30; C.J.U.E., aff. C-92/09, arrêt *Schecke et Eifert*.

152. Cour eur. D.H., *Malone c. Royaume-Uni*, 2 août 1984, § 67.

153. Cour eur. D.H., *Huvig c. France*, 24 avril 1990, § 32 et Cour eur. D.H., *Kruslin c. France*, 24 avril 1990, § 33.