Les nouvelles méthodes d'enquête dans un contexte informatique

Forget, Catherine

Published in:
Revue du Droit des Technologies de l'information

Publication date:
2017

Document Version
le PDF de l'éditeur

Les nouvelles méthodes d'enquête dans un contexte informatique : vers un encadrement (plus) strict ?

Catherine Forget[1]

La loi du 25 décembre 2016 modifie le Code d'instruction criminelle en vue de répondre aux besoins des enquêteurs dans un contexte informatique. Elle offre de nouvelles méthodes telles la préservation de données, l'infiltration informatique ou la pénétration dans un système informatique en vue d'une observation. Outre ces innovations, la loi du 25 décembre 2016 clarifie les compétences des enquêteurs dans le cadre de la saisie de données informatiques et de la recherche dans un système informatique tout en laissant transparaître un certain accroissement des compétences du procureur du Roi au détriment de celles réservées au juge d'instruction. Enfin, elle entérine la jurisprudence « Yahoo » et ce faisant, élargit le spectre des tiers tenus à collaborer dans le cadre d'une demande d'identification, de repérage ou d'interception des communications. Il s'agira donc par le biais de cette contribution de faire le point sur les modifications et d'attirer l'attention du lecteur sur certains éléments susceptibles d'entrer en contradiction avec la Convention de Budapest mais aussi la jurisprudence de la Cour européenne des droits de l'homme et de la Cour de justice de l'Union européenne.

The law of 25 December 2016 amends the Code of Criminal Procedure to meet the needs of investigators in a technological context. This legislative framework offers new methods such as data preservation, infiltration into information systems as well as penetration into such systems for observation purposes. In addition to these innovations, the law of 25 December 2016 clarifies the investigators' enquiry methods in the context of seizure and research in information systems while allowing some increase in the powers of the prosecutor, hence diminishing those traditionnallly reserved to the investigating judge. Finally, this law integrates the "Yahoo" case law and thus broadens the scope of third parties required to collaborate when requested to identify, track or intercept communications. Therefore, this article analyzes the above-mentionned modifications to the Code of Criminal Procedure and draws the reader's attention to certain elements which may contradict the Budapest Convention but also the case law of the European Court of Human Rights and of the Court of Justice of the European Union.

INTRODUCTION

Après l'adoption de la loi « Pot-pourri 2 » modifiant le droit pénal et la procédure pénale[2], le Code d'instruction criminelle a fait l'objet d'une profonde modification afin de s'adapter aux besoins des enquêteurs dans un contexte digital. À l'heure où le rôle et la place du juge d'instruction sont largement remis en question[3],

[1] Avocate au barreau de Bruxelles (DWL-LAW) et chercheuse au CRIDS (Université de Namur).

[2] Loi du 5 février 2016 modifiant le droit pénal et la procédure pénale et portant des dispositions diverses en matière de justice, *M.B.*, 19 février 2016.

[3] M.-A. Beernaert, « Du juge d'instruction au juge de l'enquête : raisons et contours de la réforme proposée », in *La figure du juge d'instruction : réformer ou supprimer ?*,

la loi du 25 décembre 2016[4] offre de nouvelles méthodes d'enquête et clarifie certaines controverses tout en laissant transparaître un certain accroissement des compétences du procureur du Roi au détriment de celles réservées au juge d'instruction.

À titre liminaire, il est important de rappeler qu'en principe, seul le juge d'instruction est habilité à poser un acte de contrainte susceptible de porter atteinte aux droits et libertés individuelles[5]. En effet, celui-ci instruit à charge et à décharge de manière « indépendante et impartiale » alors que le procureur du Roi assume « le rôle de la partie poursuivante »[6] et « ne peut donc être considéré comme impartial »[7]. Cette répartition des rôles semble toutefois s'assouplir compte tenu des nouvelles lois en vigueur et de la multiplication des exceptions permettant au procureur du Roi d'agir dans des matières réservées au juge d'instruction par exemple, en cas de flagrant délit ou dans les conditions prévues par la mini-instruction[8].

Dans le cadre de cette analyse, nous exposerons successivement certaines méthodes d'enquêtes récemment modifiées à savoir, la préservation de données, la saisie de données informatiques, la recherche dans un système informatique, le blocage de site Internet, l'identification et le repérage, l'infiltration dans un contexte informatique, la pénétration dans un système informatique en vue d'une observation, l'obligation de collaboration et l'interception des communications. Nous évoquerons également la loi du 25 décembre 2016 relative au traitement des données des passagers[9] imposant aux transporteurs de communiquer les données de leurs clients. Sans souhait d'exhaustivité, nous mettrons l'accent sur les modifications et attirerons l'attention du lecteur sur certains éléments susceptibles d'entrer en contradiction avec la jurisprudence de la Cour européenne des droits de l'homme (ci-après Cour eur. D.H.) et de la Cour de justice de l'Union européenne (ci-après C.J.U.E.).

En effet, si le choix entre différentes techniques relève essentiellement du pouvoir discrétionnaire des États, ceux-ci ne disposent pas d'une latitude illimitée[10]. Ces méthodes entraînent essentiellement une ingérence dans le droit au respect de la vie privée et exigent le respect des critères de légalité, nécessité et proportionnalité en vue de prémunir le risque d'atteintes illicites ou arbitraires des pouvoirs publics[11]. Plus précisément, le critère de légalité requiert une réglementation « claire, prévisible et accessible » assurant une protection contre les risques d'abus et d'arbitraire et permettant au justiciable, si besoin en s'entourant de conseils éclairés de régler sa conduite[12]. Les critères de nécessité et de proportionnalité supposent l'existence de garanties adéquates et suffisantes contre les abus en tenant compte de la nature du besoin social impérieux poursuivi, des conséquences pour la collectivité et

Bruxelles, Larcier, 2017, pp. 21-28 ; L. Kennes et D. Scalia, *Du juge d'instruction vers le juge de l'enquête : analyse critique et de droit comparé,* Limal, Anthemis, 2017.

4 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.

5 Art. 28, § 3, du Code d'instruction criminelle (ci-après C.i.cr.).

6 Art. 28*bis* C.i.cr.

7 C. const., 25 janvier 2017, arrêt n° 6/2017, C-6325 et 6326, B.5.2.

8 Art. 28*septies* C.i.cr.

9 Loi du 25 décembre 2016 relative au traitement des données des passagers, *M.B.*, 25 janvier 2017.

10 Cour eur. D.H., 6 septembre 1978, *Gerhard Klass e.a. c. Allemagne*, série A, vol. 28, § 49.

11 Art. 8 de la Convention européenne des droits de l'homme (ci-après C.E.D.H.).

12 Cour eur. D.H., 2 août 1984, *Malone c. Royaume-Uni*, série A, n° 82, § 67.

de la marge d'appréciation laissée aux États membres[13].

Nous examinerons également les méthodes d'enquête à la lumière de la Convention sur la cybercriminalité[14] ratifiée par la Belgique en 2012[15]. Cette Convention, également intitulée Convention de Budapest, offre aux États parties un cadre contraignant en matière de procédure pénale. Elle exige le respect du principe de proportionnalité[16] mais aussi, lorsque cela s'avère approprié, le respect de conditions et sauvegardes telles une supervision par une juridiction ou un organe indépendant, l'indication des motifs justifiant l'exécution de la mesure et la limitation de sa portée ou de sa durée[17]. À l'appui de notre analyse, nous évoquerons également la Recommandation n° R (95)13 offrant un cadre non contraignant cette fois relatif à certaines méthodes d'enquête pénale[18].

Nous verrons *in fine* que, sans constituer des conditions *sine qua non*, certaines garanties semblent constituer des standards minimums tels l'existence d'une autorisation préalable par un organe indépendant assurant la séparation des pouvoirs ou encore le droit à un recours effectif protégeant les droits de la défense.

I. LA PRÉSERVATION DE DONNÉES

La loi du 25 décembre 2016 innove en intégrant la « préservation de données » dans le Code d'instruction criminelle[19]. L'article 39*ter* C.i.cr. permet désormais à tout officier de police judiciaire de solliciter auprès d'une personne physique ou morale la conservation immédiate des données en sa possession ou sous son contrôle[20] pendant une période maximale de 90 jours, s'il existe des raisons de croire que ces données sont susceptibles de perte ou de modification[21]. Ce temps doit permettre aux autorités de mettre en place d'autres procédures nécessitant l'accomplissement de formalités supplémentaires[22], par exemple une saisie de données informatiques. La décision doit être écrite et motivée et indiquer : le nom et la qualité de l'officier de police judiciaire qui demande la conservation, l'infraction qui fait l'objet de la recherche, les données qui doivent être conservées et la durée de conservation des données[23]. En cas d'urgence, la conservation peut être ordonnée verbalement et doit être confirmée par écrit dans les plus brefs délais[24]. Les personnes conservant les données sont tenues de veiller à leur intégrité et leur

13 Voy. en ce sens la jurisprudence abondante reprise dans le rapport de la Division de la recherche du Conseil de l'Europe intitulé « Sécurité nationale et jurisprudence européenne », 2013, disponible sur le site du Conseil de l'Europe.

14 Convention sur la cybercriminalité, Budapest, 23 novembre 2001, *S.T.C.E.,* n° 185. (ci-après Convention sur la cybercriminalité ou Convention de Budapest).

15 Loi du 3 août 2012 portant assentiment à la Convention sur la cybercriminalité, faite à Budapest le 23 novembre 2001, *M.B.,* 21 novembre 2012.

16 Art. 15, § 1er, Convention sur la cybercriminalité.

17 Art. 15, § 2, Convention sur la cybercriminalité.

18 Recommandation n° R(95)13 du Comité des ministres aux États membres relative aux problèmes de procédure pénale liés à la technologie de l'information, 11 septembre 1995.

19 Art. 39*ter* et 39*quater* C.i.cr.

20 Dans le cadre de la méthode d'enquête dite « l'injonction de produire », la Convention de Budapest indique que l'expression « en sa possession » ou « sous son contrôle » fait référence d'une part, à la possession matérielle des données et d'autre part, à des situations dans lesquelles l'intéressé ne possède pas matériellement les données à produire mais peut en contrôler librement la production, par exemple si les données sont stockées sur un cloud qu'il met librement à disposition. Le rapport explicatif précise toutefois qu'un accès aux données par une liaison du réseau ne constitue pas nécessairement un « contrôle » au sens de la présente disposition. Rapport explicatif de la Convention sur la cybercriminalité, Conseil de l'Europe, Budapest, 23 novembre 2001, § 173 (ci-après Rapport explicatif de la Convention de Budapest).

21 Art. 39*ter,* § 1er, al. 1er, C.i.cr.

22 *Ibidem*.

23 Art. 39*ter,* § 1er, al. 2, C.i.cr.

24 Art. 39*ter,* § 1er, al. 3 et § 2, C.i.cr.

sécurité mais aussi de garder le secret dont le non-respect est sanctionné dans les mêmes conditions que celles de l'article 458 du Code pénal à savoir le secret professionnel[25]. Le refus de collaboration et la disparation, destruction ou modification des données conservées sont punis d'un emprisonnement de six mois à un an ou d'une amende de vingt-six euros à vingt mille euros ou d'une de ces peines seulement[26].

Cette méthode préconisée par la Convention de Budapest[27] est traditionnellement présentée comme mesure alternative à l'obligation de conservation généralisée des « métadonnées »[28] imposée aux opérateurs et fournisseurs de réseaux et services de communications électroniques en vertu de la loi du 27 mai 2016[29]. Celle-ci serait en effet tout aussi efficace pour lutter contre la criminalité sans pour autant engendrer une ingérence aussi grave dans l'exercice du droit à la vie privée[30]. Néanmoins, le champ d'application de l'article 39*ter* du Code d'instruction criminelle pourrait s'avérer plus large que ne le prévoit la Convention de Budapest[31]. L'officier de police judiciaire peut en effet requérir la conservation des données « stockées » mais aussi la conservation des données « traitées ou transmises au moyen d'un système informatique ». Cet élargissement pourrait entrer en contradiction avec la Convention précitée puisque le rapport explicatif précise que cette méthode « ne s'applique pas à la collecte en temps réel et à la conservation de futures données relatives au trafic ni à l'accès en temps réel au contenu des communications »[32] mais visent les données « qui existent déjà et sont en cours de stockage »[33].

25 Art. 39*ter*, § 3, al. 1er, C.i.cr.

26 Art. 39*ter*, § 3, al. 2, C.i.cr.

27 Art. 16 de la Convention sur la cybercriminalité. Le Rapport explicatif de la Convention de Budapest illustre l'importance de cette technique d'enquête dans le cadre de la lutte contre la criminalité informatique en trois points. En premier lieu, elle permet d'assurer l'intégrité de données volatiles et facilement manipulables tout en ayant des incidences moins importantes pour la réputation d'une entreprise qu'une saisie de données informatiques, par exemple. En second lieu, elle implique la conservation de données de trafic pouvant s'avérer essentielles pour obtenir l'identification de la source de communications et ainsi, l'identité des auteurs d'infractions. En troisième lieu, ce dispositif vise également la conservation des données de contenu, données susceptibles de révéler que des infractions ont été commises et de servir à titre de preuves. Rapport explicatif de la Convention de Budapest, § 154.

28 Cette obligation consiste en la collecte et le stockage systématique et *a priori* de l'ensemble des données traitées et générées lors d'une communication électronique à l'exception du contenu de celle-ci. Elle implique donc une ingérence « particulièrement grave » dans le droit au respect de la vie privée et à la protection des données à caractère personnel. Sur ces notions, voy. Comité de la Convention sur la cybercriminalité du Conseil de l'Europe, « Rapport d'évaluation », 5-6 décembre 2012.

29 Loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques, *M.B.*, 18 juillet 2016. Pour un commentaire, voy. C. Forget, « L'obligation de conservation des "métadonnnées": la fin d'une longue saga juridique ? », *J.T.*, n° 6683, 2017, pp. 233-239. À l'heure où nous écrivons ces lignes, un recours en annulation est toujours pendant devant la Cour constitutionnelle introduit par l'Ordre des barreaux francophones et germanophone et les ASBL Liga voor Mensenrechten et Ligue des Droits de l'Homme.

30 Groupe Article 29, Avis 9/2004 sur le projet de décision-cadre sur la conservation de données traitées et stockées en relation avec la mise à disposition de services de communications électroniques disponibles publiquement ou de données sur les réseaux de communications publiques aux fins de la prévention, l'étude, la détection et la poursuite des actes criminels, y compris le terrorisme, 9 novembre 2004. Le Groupe de Travail de l'Article 29 est institué par la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses missions sont précisées à l'article 30 de la directive 95/46/CE et à l'article 15 de la directive 2002/58/CE.

31 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,* Limal, Anthemis, 2017, p. 226.

32 Rapport explicatif de la Convention de Budapest, § 149.

33 *Ibidem*, § 150.

Enfin, sans préjudice des possibilités de collaboration directe avec des opérateurs de réseaux de communications électroniques et des fournisseurs de services de communications électroniques étrangers[34], l'article 39*quater*, § 1er, du Code d'instruction criminelle prévoit des dispositions analogues à l'égard du procureur du Roi sollicitant la conservation des données se trouvant sur le territoire d'une autorité étrangère et nécessitant d'émettre une demande d'entraide judiciaire[35]. L'article 39*quater*, § 2 traite de manière similaire à la demande d'un autre État de conserver des données se trouvant sur le territoire belge. Ainsi, lorsqu'une telle possibilité est prévue dans un instrument de droit international liant la Belgique et cet autre État, l'autorité judiciaire compétente ayant l'intention de soumettre une demande d'entraide judiciaire peut « demander au service de police désigné par le Roi d'ordonner ou d'imposer d'une autre manière la conservation rapide de données stockées, traitées ou transmises au moyen d'un système informatique »[36]. Dans le cas où les données transitent ou sont transmises par la Belgique, les autorités belges doivent divulguer « dans les meilleurs délais, à l'autorité étrangère compétente une quantité de données d'identification ou d'appel suffisante pour retrouver qui est l'opérateur du réseau de communications électroniques ou le fournisseur du service de communications électroniques et par quelle voie la communication a été envoyée »[37].

II. LA SAISIE DE DONNÉES INFORMATIQUES, LA RECHERCHE ET L'EXTENSION DE RECHERCHE DANS UN SYSTÈME INFORMATIQUE « SANS BUT SECRET »

Avant l'adoption de la loi du 25 décembre 2016, la procédure en vigueur prévoyait une distinction entre la saisie de données informatiques, relevant de la compétence du procureur du Roi, et la recherche ou l'extension de recherche dans un système informatique, relevant de la compétence du juge d'instruction[38]. Ce régime faisait l'objet de controverses, le Code d'instruction criminelle ne précisant pas si les enquêteurs pouvaient exploiter un système informatique sans disposer d'une ordonnance du juge d'instruction[39]. La question fut tranchée par la Cour de cassation dans un arrêt du 11 février 2015. La Cour dit pour droit 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 »[40]. Cette jurisprudence fut entérinée par la loi du 25 décembre 2016 faisait fi de la nécessité de distinguer la « saisie » de données de la « recherche » dans un système dont la

34 Art. 39*quater,* § 1er, C.i.cr. Le législateur précise à ce propos créer un cadre légal « pour une collaboration directe avec des ISP étrangers conformément aux pratiques existantes ». Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n° 54-1966/001, p. 30. À ce propos, voy. V. Franssen et S. Tosza, *op. cit.*, p. 231.

35 Cette disposition transpose l'article 29 de la Convention de Budapest.

36 V. Franssen et S. Tosza, *op. cit.*, pp. 232 et s.

37 Art. 39*quater,* § 7, C.i.cr. Cette disposition transpose l'article 30 de la Convention de Budapest.

38 Art. 39*bis* C.i.cr. et 88*ter* C.i.cr.

39 Certains auteurs considéraient que « Ne constitue pas une recherche informatique l'exploitation d'un système informatique qui a été légalement saisi et qui se trouve entre les mains des enquêteurs (un smartphone, une tablette, un ordinateur…) ». O. Leroux, « Criminalité informatique », in X., *Postal Mémorialis, Lexique du droit pénal et des lois spéciales*, juillet 2014, C-362/46, p. 58. *A contrario*, voy. C. Forget, « Quelles garanties entourent la saisie de données informatiques et l'exploitation d'un système de données informatiques », *R.D.T.I.*, n° 61, décembre 2015, pp. 79-90.

40 Cass., 11 février 2015, R.G. n° P.14.1739.F, www.cass.be. Pour un commentaire d'arrêt, voy. C. Conings, « Het uitlezen van een gsm of een ander privaat IT-systeem: This is not America », noot onder Cass., 11 februari 2015, *R.W.*, 2015-16, pp. 622-626.

portée de l'ingérence dans le droit au respect de la vie privé diffère[41].

Par souci de lisibilité, nous exposerons successivement le régime relatif à la recherche et l'extension de recherche dans un système informatique « sans but secret » (A) puis, la saisie de données informatiques (B) et enfin, les possibilités de procéder au déverrouillage d'un système en vue de permettre l'exécution des mesures précitées (C).

A. La recherche et l'extension de recherche dans un système informatique « sans but secret »

La recherche et l'extension de recherche dans un système informatique « sans but secret » relèvent désormais de la compétence de l'officier de police judiciaire, du procureur du Roi ou du juge d'instruction selon la saisie, la saisie éventuelle ou subsidiairement, l'absence de saisie du support. Si cette recherche est effectuée « dans un but secret », elle relève de la compétence unique du juge d'instruction conformément à l'article 90*ter* C.i.cr. et sera exposée *infra* dans le cadre de l'interception des communications non accessibles au public.

Selon les travaux parlementaires, la distinction entre « secret » et « non secret » dépend, premièrement, de l'intention des enquêteurs « de prendre connaissance des communications ou des données à l'insu des acteurs de ces communications ou à l'insu du propriétaire, du détenteur ou de l'utilisateur du système informatique »[42]. À titre illustratif, si un téléphone portable est trouvé dans une voiture, il peut être exploité dans les conditions prévues par l'article 39*bis*, § 2, alinéa 1er, C.i.cr., l'objectif des enquêteurs n'étant pas d'effectuer une surveillance en secret[43]. Deuxièmement, le caractère non secret découle de l'obligation faite aux autorités de notifier « dans les plus brefs délais » au « responsable du système informatique » la recherche ou son extension, sauf si son identité ou son adresse ne peut « raisonnablement » être trouvée[44]. Il est important de noter que le « responsable du système informatique » est la personne disposant du contrôle réel ou juridique sur le système[45], elle ne s'identifie donc pas forcément avec la personne dont les données sont exploitées[46]. Il pourrait s'agir, par exemple, de l'utilisateur d'un système, de la personne suspectée ou encore de l'opérateur[47]. Ainsi, dans le cas où un ordinateur situé dans un cybercafé est exploité par les autorités, la notification pourrait être faite tant au propriétaire qu'à l'utilisateur du système. En outre, les travaux parlementaires ne précisent pas ce qu'il y a lieu d'entendre par « raisonnablement » être trouvé laissant une certaine marge d'appréciation aux enquêteurs.

Sur la base de ces deux motifs, à savoir, l'intention de l'enquêteur et la notification au responsable du système informatique, la recherche sera ou non secrète et devra respecter les conditions prévues par les articles 39*bis* C.i.cr. ou 90*ter* C.i.cr. Difficile donc de ne pas « raisonnablement » s'interroger sur la pertinence de cette justification au fondement de la différence de traitement procédurale entre deux types de recherche dans un système informatique. Celles-ci présentent en effet des similitudes quant au degré d'ingérence mais offrent des garanties radicalement différentes voire un

41 Pour un commentaire, voy. également C. Conings et S. Royer, « Verzamelen en vastleggen van digitaal bewijs in strafzaken », *N. C.*, 2017/4, pp. 313-320.

42 Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n° 54-1966/001, p. 54.

43 Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n° 54-1966/001, p. 54.

44 Art. 39*bis*, § 7, C.i.cr.

45 Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n° 54-1966/001, p. 21.

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

47 Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n° 54-1966/001, p. 19.

cadre nettement plus souple si elle est exercée « sans but secret ».

1. *La recherche dans le cadre d'une saisie éventuelle du support*

Tout officier de police judiciaire peut effectuer une recherche dans un système informatique c'est-à-dire « lire, inspecter ou examiner des données »[48] après avoir saisi le support pour autant que l'appareil ne soit pas verrouillé ou si l'enquêteur dispose du code d'accès[49]. Dans l'hypothèse où le support n'est pas saisi mais pourrait l'être, par exemple si l'ordinateur est situé dans un cybercafé ou si l'enquête se déroule dans une banque, l'officier de police judiciaire doit requérir l'autorisation du procureur du Roi avant d'entamer une recherche[50]. Le texte ne précise pas si cette autorisation peut être donnée oralement. En outre, la recherche effectuée dans ce cadre doit être limitée aux données sauvegardées sur l'appareil[51]. À cette fin, l'enquêteur est tenu de couper les liaisons externes en activant par exemple, le mode avion du téléphone[52]. Ainsi, des informations circulant par des services types WhatsApp, Viber, Hotmail, Gmail ou Facebook ne seront donc pas directement accessibles aux enquêteurs à moins d'être stockées et accessibles « hors connexion »[53].

L'exploitation des données contenues dans un système informatique et la compétence des enquêteurs, sont donc tributaires de la saisie d'un support. Ce régime semble peu conciliable avec la Recommandation n° R (95)13 du Conseil de l'Europe[54] et la Convention de Budapest[55]. Selon ces dispositions, dans le cas d'une intrusion dans un système par des autorités en vue de saisir des données, la procédure applicable dans le contexte digital devrait s'aligner sur celle prévue « dans le cadre des pouvoirs traditionnels » de perquisition et de saisie. Or, la loi du 25 décembre 2016, plutôt que d'aligner la procédure relative à la recherche dans un système informatique sur la « perquisition », aligne celle-ci sur celle prévue en cas de saisie. Ce faisant, elle offre peu de garanties au justiciable en dépit d'une ingérence importante dans le droit au respect de la vie privée[56].

48 Rapport explicatif de la Convention de Budapest, § 191.

49 Art. 39*bis*, § 2, al. 1er et § 5, C.i.cr.

50 Art. 39*bis*, § 2, C.i.cr.

51 Art. 39*bis*, § 2, al. 3, C.i.cr.

52 *Ibidem*.

53 Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n° 54-1966/001, p. 17.

54 Recommandation n° R(95)13 du Comité des ministres aux États membres relative aux problèmes de procédure pénale liés à la technologie de l'information, 11 septembre 1995, § 2.

55 Rapport explicatif de la Convention sur la cybercriminalité, § 191.

56 Nous rejoignons l'analyse de certains auteurs selon laquelle toute recherche dans un système informatique par les autorités devrait être encadrée par les mêmes garanties qu'une mesure de perquisition (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). Un système informatique tel un ordinateur, un serveur ou encore un téléphone portable, est protégé par l'article 8 de la CEDH (à titre illustratif, le considérant 24 de la directive 2002/58/CE précise que : « L'équipement terminal de l'utilisateur d'un réseau de communications électroniques ainsi que toute information stockée sur cet équipement relèvent de la vie privée de l'utilisateur, qui doit être protégée au titre de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales » (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, *J.O.*, C.E. L201/37, 31 juillet 2002, pp. 0037-0047)). Un tel système comprend en effet, des données relevant de la vie privée des personnes, par exemple, des données personnelles, des données professionnelles ou encore des données médicales. Il s'agit d'un espace virtuel pouvant être perçu par son utilisateur comme un lieu d'activité « au sein duquel un individu a le sentiment d'être dans

De plus, l'argument couramment invoqué selon lequel le caractère volatil de certaines données et le risque de perdre certains éléments de preuves nécessitent une consultation rapide et immédiate des données, ce que ne permet pas une procédure plus « lourde », n'est pas pertinent en l'espèce. En effet, les enquêteurs étant tenus de couper les liaisons externes de l'appareil, le risque de suppression des données par le suspect ou par un tiers n'est pas envisageable. Autrement dit, une fois les connexions réseaux désactivées, les données restent stockées sur l'appareil et ne sauraient disparaître. Dès lors, aucun motif ne semble justifier l'absence d'intervention du juge d'instruction ou, à tout le moins, du procureur du Roi d'autant qu'aucune protection particulière n'est prévue pour les données soumises au secret professionnel tels les avocats et les médecins.

Selon la Cour eur. D.H., à l'instar d'une mesure de perquisition, la recherche dans un système informatique requiert en principe l'existence d'une autorisation préalable sauf exceptions[57]. Cette autorisation permet de s'assurer de l'existence de soupçons raisonnables à l'encontre de l'intéressé avant l'intervention des enquêteurs dans le système[58] et ainsi éviter une mesure exercée de manière arbitraire mais aussi une « saisie » « massive et indifférenciée »[59]. Cette dernière également désignée « fishing expeditions » consiste en une fouille exercée dans l'espoir d'y trouver la preuve d'une infraction et en ce sens, viole le droit au respect de la vie privée[60]. La Cour eur. D.H. autorise néanmoins une recherche effectuée de manière large c'est-à-dire sans cibler les dossiers à consulter, sur base de 35 mots-clés par exemple, pour autant que des garanties soient offertes à l'in-

l'intimité, en sécurité contre l'immixtion de personnes contre sa volonté, indépendamment de la durée et de l'intensité d'utilisation » à l'instar du domicile privé au sens de la jurisprudence de la Cour eur. D.H. (Cour eur. D.H., 16 décembre 1992, *Niemietz c. la République fédérale d'Allemagne*, *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'avocat ».) L'intrusion dans ce système « privé » peut donc *a priori* être perçue pareillement à une mesure de perquisition au sens classique du terme et requiert donc le respect de garanties contre le risque d'accès illicite ou arbitraires aux données qui y sont stockées.

57 Dans l'arrêt *Trabajo Rueda*, la Cour semble avoir implicitement reconnu qu'une recherche dans un système informatique requiert en principe une autorisation préalable sauf exceptions. Celle-ci précisa en effet en ces termes : « 35. La Cour constate que, en ce qui concerne l'accès au contenu d'un ordinateur personnel par la police, la jurisprudence du Tribunal constitutionnel a établi la règle de l'autorisation judiciaire préalable, condition exigée en tout état de cause par l'article 8 de la Convention (qui requiert la délivrance d'un mandat par un organe indépendant) lorsqu'une atteinte à la vie privée d'une personne est en jeu. La jurisprudence constitutionnelle espagnole permet toutefois, à titre exceptionnel, de passer outre une telle autorisation dans des situations d'urgence ("nécessité urgente") pouvant faire l'objet d'un contrôle judiciaire postérieur ». Ce contrôle doit permettre de vérifier la réalité de l'urgence c'est-à-dire d'examiner l'existence de raisons pour lesquelles l'attente de cette autorisation risque d'entraver le bon déroulement de l'enquête. En l'espèce, les services de police avaient consulté les données contenues dans un ordinateur portable qui leur avait été remis. La Cour a considéré qu'il était difficile d'apprécier la réalité de l'urgence, la consultation de données informatiques visant les archives d'un système entre les mains des autorités et par ailleurs déconnecté d'Internet. Cour eur. D.H., 30 mai 2017, *Trabajo Rueda c. Espagne*, n° 32600/12, § 35.

58 Comme le souligne le juge Zupančič, « l'intrusion n'est donc justifiée qu'une fois le soupçon est déjà "raisonnable", c'est-à-dire lorsqu'il est très probable que le suspect a déjà enfreint la loi ». Selon ce dernier, le soupçon raisonnable devrait être « *a priori* », « concret », « spécifique » et « articulable » afin de permettre au juge de disposer au préalable d'informations réelles et pas seulement de l'intuition de l'autorité auteur de l'intrusion. Opinion concordante de juge Zupančič, à laquelle se rallie le juge De Gaetano, Cour eur. D.H., 2 avril 2014, *Vinci construction et GMT Génie Civil et services c. France*, n° 63629/10, §§ 78-79.

59 Cour eur. D.H., 16 octobre 2008, *Maschino c. France*, n° 10447/03, § 34.

60 Opinion concordante de juge Zupančič, à laquelle se rallie le juge De Gaetano Cour eur. D.H., 2 avril 2014, *Vinci construction et GMT Génie Civil et services c. France*, n° 63629/10, §§ 78-79.

téressé, en l'espèce, la présence de l'avocat mis en examen et d'un membre de l'ordre pendant la recherche dans le système ainsi que la rédaction d'un procès-verbal décrivant le déroulement des opérations[61].

En l'occurrence, le régime prévu par l'article 39*bis,* § 2, C.i.cr., à savoir la recherche dans un système informatique dans le cadre d'une éventuelle saisie du support, ne requiert ni d'autorisation préalable ni d'indiquer le respect des critères de nécessité et de proportionnalité pourtant requis par la Cour eur. D.H. en cas d'ingérence dans les droits fondamentaux. Par ailleurs, cette absence d'autorisation préalable implique un risque de connaître des « fishing expeditions », voire de connaître des abus, même si, selon le législateur, l'enquêteur est tenu de respecter les finalités visées par l'article 35 C.i.cr., à savoir conserver des données à titre de preuve ou saisir les données susceptibles de servir à la manifestation de la vérité[62].

2. *L'extension de recherche dans le cadre d'une saisie éventuelle du support*

Le procureur du Roi peut autoriser l'extension de recherche entamée sur base d'une saisie éventuelle du support, vers d'autres systèmes ou parties de ceux-ci[63] et pour autant que l'enquêteur ne doive introduire aucun mot de passe, par exemple si celui-ci a été « retenu », peu importe que ce mot de passe soit identique ou différent à chaque fois[64]. L'extension de recherche doit être limitée aux parties auxquelles « les personnes autorisées à utiliser le système informatique » ont spécifiquement accès[65]. L'autorisation doit être écrite, ou orale en cas d'urgence sous réserve de la confirmer dans les plus brefs délais[66]. Elle doit par ailleurs être motivée et indiquer les raisons pour lesquelles la mesure est, d'une part, nécessaire à la manifestation de la vérité et d'autre part, préciser en quoi l'exécution d'autres mesures serait disproportionnée ou s'il existe un risque de perdre certains éléments de preuve[67]. Comme le souligne le Conseil d'État, il est loisible de se demander si « l'intervention ou non du juge d'instruction, et partant l'existence d'une garantie supplémentaire, peut être tributaire de la simple possibilité qu'un système informatique "retienne" un mot de passe »[68].

Par ailleurs, la loi confie d'importants pouvoirs au procureur du Roi. Selon les travaux parlementaires, l'intervention de ce dernier offrirait une garantie suffisante, l'article 39*bis* C.i.cr. étant utilisé de manière réactive et requiert donc le respect des finalités visées par l'article 35 C.i.cr. à savoir, conserver des données à titre de preuve ou saisir les données susceptibles de servir à la manifestation de la vérité[69]. En outre, le législateur précise que, même si l'extension de la recherche dans un système informatique relevait antérieurement de la compétence du juge d'instruction[70], eu égard à l'évolution des nouvelles technologies, la distinction entre données stockées sur un appareil et données

61 Cour eur. D.H., 3 septembre 2015, *Sérvulo & Associados Advogados rl c. Portugal*, n° 27013/10, § 103. Voy. dans le même sens Cour eur. D.H., 16 octobre 2007, *Wieser et Bicos Beteiligungen GmbH c. Autriche,* n° 74336/01.

62 Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n° 54-1966/001, p. 19.

63 Art. 39*bis,* § 3, C.i.cr.

64 Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n° 54-1966/001, p. 20.

65 Art. 39*bis,* § 3, al. 3, C.i.cr. Cette limite également prévue sous l'empire de l'ancienne loi vise à empêcher tout « hacking externe » des enquêteurs. *Doc. parl.,* Ch. repr. 1999-2000, n° 50-213/1, p. 23. Le hacking externe est sanctionné par l'article 550*bis* du Code pénal. À cet égard, voy. : F. de Villenfagne et S. Dusollier, « La Belgique sort enfin ses armes contre la cybercriminalité : à propos de la loi du 28 novembre 2000 sur la criminalité informatique », *A&M,* 2002/1, pp. 60-81.

66 Art. 39*bis,* § 3, al. 6, C.i.cr.

67 Art. 39*bis,* § 3, C.i.cr.

68 Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n° 54-1966/001, p. 20.

69 *Ibidem*, p. 19.

70 Art. 88*ter* C.i.cr.

stockées sur un autre système informatique, type cloud, ne se justifie plus[71].

3. *La recherche et l'extension de recherche indépendamment de la saisie éventuelle du support*

Dans le cadre d'une instruction judiciaire ou d'une mini-instruction, le juge d'instruction est compétent pour ordonner une recherche dans un système informatique ou une partie de celui-ci autres que celles visées par l'article 39*bis*, § 2 et § 3 C.i.cr.[72]. Ainsi, par exemple, un juge d'instruction pourra ordonner une recherche dans le compte Gmail d'un suspect sans qu'aucun appareil connecté à ce compte n'ait été saisi[73] pour autant qu'il n'agisse pas « dans un but secret ».

La possibilité d'étendre la recherche à d'autres systèmes n'est pas expressément prévue par la loi mais elle se déduit du dernier alinéa de l'article 39*bis,* § 4 C.i.cr. lequel permet au juge d'instruction d'autoriser oralement en cas d'urgence « l'extension » de recherche visée au premier alinéa. De plus, à la différence de l'article 39*bis,* § 3 C.i.cr., le texte ne précise pas si la recherche doit être limitée aux systèmes auxquels « les personnes autorisées à utiliser le système informatique qui fait l'objet de la mesure ont spécifiquement accès »[74]. Toutefois, les travaux préparatoires précisent que les conditions prévues par l'article 39*bis,* § 3, C.i.cr. sont « naturellement » celles de l'article 39*bis,* § 4, C.i.cr. de sorte qu'une telle limitation lui serait applicable. En outre, si la recherche est effectuée dans un « but secret » seul le juge d'instruction est compétent conformément à l'article 90*ter* C.i.cr. sur lequel nous reviendrons *infra*.

71 Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n° 54-1966/001, p. 19.

72 Art. 39*bis,* § 4, C.i.cr.

73 Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n° 54-1966/001, p. 21.

74 Art. 39*bis,* § 3, al. 3 C.i.cr.

B. La saisie de données informatiques

Le législateur ne distingue pas expressément la recherche dans un système informatique de la saisie de données informatiques partant du postulat que l'exploitation du système informatique est une mesure découlant de la saisie[75]. En conséquence, le cadre applicable relatif à la saisie de données informatiques est calqué sur celui de la recherche et de l'extension de recherche dans un système informatique tel que mentionné *supra*[76].

Par ailleurs, à l'instar du régime prévu avant l'adoption de la loi du 25 décembre 2016, une fois la recherche effectuée, l'enquêteur peut décider de copier les données sur un support appartenant aux autorités ou sur des supports disponibles pour des personnes autorisées à utiliser ledit système et ce, en cas d'urgence ou pour des raisons techniques[77]. Dans le cas où la copie n'est pas possible en raison d'un volume trop important ou pour des raisons techniques, le procureur du Roi peut à l'aide de moyens techniques appropriés, se limiter à empêcher l'accès aux données saisies et à leurs copies tout en s'assurant à nouveau de leur intégrité. Cette mesure s'apparente à une « mise sous scellés » des données saisies dans l'attente d'une copie ultérieure[78]. En outre, les données peuvent être

75 Cette interprétation découle de l'arrêt de la Cour de cassation du 11 février 2015 déjà mentionné *supra*, Cass., 11 février 2015, R.G. n° P.14.1739.F, www.cass.be.

76 Art. 39*bis,* §§ 1er et s. C.i.cr.

77 Art. 39*bis,* § 6, C.i.cr.

78 F. Roggen, « L'extension des moyens d'investigation et des mesures de contrainte en procédure pénale », *R.G.C.F.*, 2003/5, p. 113. Notons que dans un arrêt du 22 octobre 2013, la Cour de cassation dit pour droit que la saisie de données informatiques est une base légale suffisante pour le blocage de site internet, étendant ainsi la portée de l'article 39*bis* C.i.cr. En effet, l'article précité ne vise pas, à notre sens, le blocage de site internet au stade de l'information. À cet égard voy. 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) ;

rendues inaccessibles ou, après en avoir pris copies, être retirées 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 des systèmes informatiques ou pour des données stockées, traitées ou transmises par le biais de tel systèmes ». Il s'agira par exemple, de retirer un virus informatique ou des images pédopornographiques[79].

La loi du 25 décembre 2016 apporte une certaine nouveauté. Désormais, le procureur du Roi peut autoriser l'utilisation ultérieure des données saisies ou d'une partie de celles-ci sauf si celles-ci « forment l'objet de l'infraction ou ont été produites par l'infraction et si elles sont contraires à l'ordre public ou aux bonnes mœurs ou constituent un danger pour l'intégrité des systèmes informatiques ou pour des données stockées, traitées ou transmises par le biais de tels systèmes »[80] et pour autant « que cela ne présente pas de danger pour l'exercice des poursuites »[81]. La loi ne précise pas si cette utilisation ultérieure est permise à l'égard de la personne dont les données ont été saisies ou à l'égard des enquêteurs en vue de procéder à une technique de « honeypot ». Cette mesure permet de « piéger » un internaute en laissant, par exemple, un lien renvoyant vers des sites de téléchargements illégaux ou des images pédopornographiques. L'enquêteur pourra collecter les adresses IP des personnes cherchant à s'y connecter[82]. En France, un tel système a été validé par la Cour de cassation sous le couvert d'une infiltration informatique[83].

Quoi qu'il en soit, outre l'élargissement des pouvoirs d'enquête du procureur du Roi, notre régime est pauvrement encadré. La Cour eur. D.H. considère, par exemple, qu'une saisie opérée sur plus de 89.000 fichiers et plus de 29.000 messages électroniques peut s'avérer compatible avec la Convention compte tenu des garanties offertes à l'intéressé en l'espèce, à savoir : l'interdiction de saisir des documents couverts par le secret professionnel d'un avocat non visé par l'enquête, la mise sous scellées immédiates des documents saisis, le visionnage des documents saisis par un juge d'instruction ainsi que leur suppression s'ils ne sont pas utiles dans le cadre de l'enquête et enfin, la possibilité pour les intéressés d'introduire une réclamation auprès du président de la cour d'appel avec une mise sous scellées des données sans consultation possible dans

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 ; C. Forget, « La collecte de preuves informatiques en matière pénale », in *Pas de droit sans technologie* (sous la dir. de J.-F. Henrotte et F. Jongen), Bruxelles, Larcier, 2015, pp. 260 et s.

79 *Doc. parl.,* Ch. repr., sess. ord., 1999-2000, n° 50-213/1, pp. 20-21.

80 Art. 39*bis,* § 6, al. 4, C.i.cr.

81 Art. 39*bis,* § 6, al. 5, C.i.cr.

82 Le « honeypot » permet d'enregistrer passivement les activités et les flux de données qui lui sont envoyés. Un tel système peut s'avérer particulièrement controversé vu le risque de provocation. Pour une analyse, voy. M. Barel, *Honeypot : un pot-pourri…juridique*, Actes du symposium SSTIC04, disponible sur http://actes.sstic.org/SSTIC04/Droit_et_honeypots/SSTIC04-article-Barel-Droit_et_honeypots.pdf.

83 Cass. (ch. crim.), 30 avril 2014, 13-88.162, *Publié au bulletin*. En l'espèce, le FBI avait mis en place un forum de carding d'infiltration dénommé « Carderprofit » permettant aux utilisateurs de discuter de divers sujets liés à la fraude à la carte bancaire et de communiquer d'offres d'achats, de vente et d'échanges de biens et services qui y sont liées Le site était configuré pour permettre aux enquêteurs de surveiller et d'enregistrer les discussions en ligne publiées sur le site, ainsi que des messages envoyés par l'intermédiaire du site entre utilisateurs enregistrés ainsi que le protocole internet (IP) de l'ordinateur des utilisateurs lors de la consultation de leurs compte. La Cour de cassation française considéra que « le site de surveillance et d'enregistrement des messages échangés a seulement permis de rassembler les preuves de la commission de fraudes à la carte bancaire et d'en identifier les auteurs, aucun élément ne démontrant qu'il ait eu pour objet d'inciter les personnes qui l'ont consulté à passer à l'acte ».

l'attente de sa décision[84]. Autant de garanties que ne prévoit pas l'article 39*bis* C.i.cr. et ce, alors que pour rappel, aucune protection particulière n'est prévue pour les données soumises au secret professionnel telles les avocats et les médecins.

Enfin, le procureur du Roi est tenu de fournir au responsable du système informatique un résumé des données copiées, rendues inaccessibles ou retirées[85]. Ce document devrait lui permettre d'exercer un recours dans les conditions prévues par l'article 28*sexies* C.i.cr. et d'exiger la levée d'un acte d'enquête pour autant qu'il démontre « être lésé » par cette mesure. Or, selon la Cour eur. D.H., un recours effectif implique de pouvoir contester la régularité de la mesure devant un juge et d'obtenir la restitution voire l'effacement des documents saisis[86]. À cet égard, les intéressés devraient, par exemple, disposer d'un inventaire détaillant le nom des fichiers, leur extension, leur provenance, leur emprunte numérique ainsi qu'une copie des documents saisis pour être en mesure de vérifier que seules les données en lien avec l'objet de l'enquête ont été emportées[87]. En l'occurrence, seule la pratique nous permettra de constater si l'article 39*bis*, § 7, C.i.cr. combiné à l'article 28*sexies* C.i.cr. offrent un droit à un recours effectif au sens de la jurisprudence de la Cour de Strasbourg.

C. Le « déverrouillage » d'un système informatique

En vue de pouvoir effectuer une recherche dans un système informatique et d'y saisir les données, le procureur du Roi ou le juge d'instruction peut, sans le consentement de l'utilisateur, faire usage de « fausses clés » c'est-à-dire de « 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 »[88]. Il s'agit par exemple, de l'utilisation de logiciel malveillant, de l'utilisation de données biométriques telles des empreintes digitales, ou de mettre à profit des mots de passe révélés par des hackers sur des sites Internet[89]. Les travaux préparatoires précisent que le propriétaire ne doit pas avoir préalablement la possibilité d'introduire lui-même le mot de passe au risque d'avoir la possibilité d'effacer certaines données et de faire disparaître des éléments de preuve[90]. Si le système est chiffré, le procureur du Roi ou le juge d'instruction peut également autoriser « l'installation de dispositifs techniques dans les systèmes informatiques concernés en vue de décryptage et du décodage de données stockées, traitées ou transmises par ce système »[91].

Soulignons que, dans le cadre d'une extension de recherche, seul le juge d'instruction est compétent pour faire usage de fausses clés[92], par exemple, dans le cas où les enquêteurs souhaiteraient se connecter au réseau VPN verrouillé d'une entreprise à partir de l'ordinateur d'un employé[93]. En revanche, si le mot

84 Cour eur. D.H., 3 septembre 2015, *Sérvulo & Associados Advogados rl c. Portugal*, n° 27013/10, § 100.

85 Art. 39*bis,* § 5, C.i.cr.

86 Cour eur. D.H., 21 mars 2017, *Société Janssen Cilag c. France*, n° 33931/12, § 23 ; Cour eur. D.H., 2 avril 2014, *Vinci construction et GMT Génie Civil et services c. France*, n° 63629/10, § 78.

87 Cour eur. D.H., 2 avril 2014, *Vinci construction et GMT Génie Civil et services c. France*, n^{os} 63629/10 et 60567/10, § 76.

88 Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n° 54-1966/001, p. 22.

89 Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n° 54-1966/001, p. 22.

90 *Ibidem*.

91 Art. 39*bis,* § 5, C.i.cr.

92 *Ibidem*.

93 Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n° 54-1966/001, p. 19.

de passe est « retenu », le procureur du Roi est également compétent[94]. La loi ne précise pas si un officier de police judiciaire peut faire usage de fausses clés sans l'intervention du procureur du Roi, sous le couvert du consentement du responsable du système informatique laquelle s'apparenterait alors à, selon nous, une sorte de « visite domiciliaire » sur consentement.

III. LE BLOCAGE DE SITE INTERNET

Le blocage de site Internet n'est pas spécifiquement réglementé par le Code d'instruction criminelle mais s'inscrit dans le cadre de la saisie de données informatiques[95]. On peut regretter l'absence de clarifications apportées par la loi du 25 décembre 2016. L'affaire « *Piratebay* » témoigne de l'importance d'encadrer toute mesure de blocage de site Internet, celle-ci étant susceptible de mettre à mal tant le droit au respect de la vie privée que le droit à la liberté d'expression garanti respectivement par les articles 8 et 10 de la CEDH. En l'espèce, en vue de faire cesser une violation des droits de la propriété intellectuelle, une ordonnance du juge d'instruction prise sur base de l'article 39*bis* C.i.cr. encadrant la saisie de données informatiques, enjoignait aux opérateurs de rendre inaccessible l'accès au contenu des sites liés à l'adresse IP du nom de domaine « thepiratebay.org ». Ces derniers devaient effectuer un procédé technique « reverse IP domain check » afin de déterminer les noms de domaines renvoyant au serveur lié à « thepiratebay.org » et y bloquer l'accès[96]. La Cour de cassation confirma la base légale applicable considérant que le blocage de site Internet découlerait de la saisie de données informatiques, la disposition susmentionnée permettant au procureur du Roi de rendre inaccessibles les données formant l'objet de l'infraction, produites par l'infraction ou contraires à l'ordre public et aux bonnes mœurs ou encore risquant d'endommager un système informatique[97].

Cette interprétation fut vivement critiquée en raison de la nature provisoire et temporaire de la saisie, celle-ci visant à conserver des données à titre de preuve ou pouvant servir à la manifestation de la vérité et ne saurait donc

94 *Ibidem*, p. 20.

95 D'autres lois particulières encadrent l'effacement ou le retrait de données. Par exemple, les articles 39 et 41 de la loi sur la protection de la vie privée (ci-après LVP) permettent au juge d'ordonner l'effacement de données à caractère personnel traitées en violation de la loi sur la protection de la vie privée. De même, les fournisseurs de services internet peuvent être tenus de supprimer les données traitées en violation de la LVP sur base d'une décision du président du tribunal de première instance (loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993). En outre, en matière de droits de propriété intellectuelle, la personne préjudiciée peut également agir par le biais d'une action en cessation (art. XI.334, § 1er, Code de droit économique).

96 Notons que les demandeurs en cassation contestaient également l'obligation de collaboration qui leur était due. Ils invoquaient l'article 21 de la loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information (actuellement XII.20 du Code de droit économique). En effet, l'article précité réfère *in fine* à l'article 39*bis* C.i.cr. en précisant que le prestataire *peut* empêcher l'accès aux données, le temps nécessaire au procureur du Roi de prendre des dispositions, par exemple requérir un mandat de perquisition. Ce dernier n'a pas l'obligation de prendre des mesures. La Cour n'a pas retenu cet argument et, se basant sur le § 4 de l'article 39*bis* C.i.cr. (actuellement art. 39*bis,* § 6, C.i.cr.), considéra que cette disposition « n'exclut pas que cet ordre soit adressé à des tiers » obligeant dès lors ces derniers à collaborer (Cass. (2e ch., sect. nl.), 22 octobre 2013, R.G. n° P.13.0550.N, www. cass.be. Pour un commentaire, voy. 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) ; 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).

97 Art. 39*bis,* § 6, C.i.cr.

recouvrir un caractère permanent[98]. De plus, si en l'espèce, le blocage de site Internet fut certes souhaité compte tenu de la violation flagrante des droits de propriété intellectuelle, une telle jurisprudence comporte un certain danger. En effet, ce faisant, la Cour de cassation attribue au procureur du Roi une mesure de contrainte susceptible de porter atteinte à la fois à l'exercice du droit au respect de la vie privée et au droit la liberté d'expression dont l'exercice devrait relever de la compétence du juge d'instruction, ou à tout le moins, être spécifiquement encadré.

La Cour eur. D.H. dispose d'une jurisprudence abondante sur les responsabilités – civile et pénale[99] –, des hébergeurs et des éditeurs de contenu[100]. Par contre, dans le domaine spécifique du blocage de site Internet, elle n'a pas encore eu l'occasion de baliser les bonnes pratiques à suivre afin de s'assurer que l'ingérence soit conforme à la CEDH. Notons toutefois que dans le cadre de l'arrêt *Ahmet Yildirim contre Turquie*[101], la Cour eur. D.H. fut saisie d'un litige relatif à une mesure de blocage de site internet. Un tribunal avait ordonné de bloquer l'accès à « Google sites » afin d'empêcher la consultation d'un site Internet dont le propriétaire était poursuivi pour outrage à la mémoire d'Atatürk. Le requérant, personne tierce à la procédure, invoquait la violation du droit à la liberté d'expression, celui-ci ne pouvant plus accéder à son propre site internet alors qu'il n'était pas lié aux poursuites pénales entamées. La Cour constata l'absence de base légale suffisante mais aussi l'absence de garanties suffisantes contre les risques d'abus et d'arbitraire.

Au terme de cette décision, le juge Pinto De Albuquerque édicta dans une opinion concordante[102] un ensemble de lignes directrices claires à suivre en la matière à savoir :

1) une définition des catégories de personnes et d'institutions susceptibles de voir leurs publications bloquées (les propriétaires nationaux ou étrangers de contenus, sites ou plates-formes illicites, les utilisateurs de ces sites ou plates-formes, etc.) ;
2) une définition des catégories d'ordonnances de blocage, par exemple celles qui visent le blocage de sites, d'adresses IP, de ports, de protocoles réseaux, ou le blocage de types d'utilisation, comme les réseaux sociaux ;
3) une disposition sur le champ d'application territoriale de l'ordonnance de blocage ;
4) une limite à la durée d'une telle ordonnance de blocage ;
5) l'indication des « intérêts » justifiant la mesure, du critère de proportionnalité et de nécessité ;
6) la détermination des autorités compétentes pour émettre une ordonnance de blocage motivée ;
7) une procédure à suivre pour l'émission de cette ordonnance, comprenant l'examen par l'autorité compétente du dossier à l'appui de la demande d'ordonnance et l'audition de la personne ou institution lésée, sauf si cette audition est impossible ou se heurte aux « intérêts » poursuivis ;

98 F. Lugentz et D. Vandermeersch, « Chapitre 2 – Les choses susceptibles d'être saisies », in *Saisie et confiscation en matière pénale*, Bruxelles, Bruylant, 2015, pp. 103-128.

99 E. Montero, « "La responsabilité des prestataires intermédiaires sur les réseaux", Le commerce électronique sur les rails ? », *Cahiers CRID*, Bruxelles, Bruylant, 2001, n° 453.

100 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.*, n° 96, pp. 879 et s.

101 Cour eur. D.H., 18 décembre 2012, *Ahmet Yildirim c. Turquie,* n° 3111/10.

102 Opinion concordante du juge Pinto De Albuquerque, Cour eur. D.H., 18 décembre 2012, *Ahmet Yildirim c. Turquie,* n° 3111/10.

8) la notification de l'ordonnance de blocage et de sa motivation à la personne ou institution lésée ;
9) une procédure de recours de nature judiciaire contre l'ordonnance de blocage.

Ces critères illustrent la nécessité de prévoir des garanties suffisantes et, en conséquence, d'encadrer le blocage de site Internet en tant que mesure à part entière et non de l'intégrer dans une mesure préexistante telle la saisie de données informatiques.

IV. L'IDENTIFICATION ET LE REPÉRAGE

La loi du 25 décembre 2016 entérine la jurisprudence «Yahoo»[103] et ce faisant, élargit le spectre des tiers tenus à collaborer dans le cadre d'une demande d'identification, de repérage ou d'interception des communications (voy. *infra*). Ces méthodes d'enquêtes ne visent plus uniquement la collaboration des «opérateurs de réseaux de communications électroniques» traditionnels tels Base, Orange, Proximus, mais visent de manière plus générale la coopération de «toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste 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» en ce inclus «le fournisseur d'un service de communications électroniques» (ci-après «opérateurs et fournisseurs de communications électroniques»)[104]. Ce faisant, le législateur inclut désormais la collaboration des services dits «over the top» tels WhatsApp, Viber, Facebook ou encore Skype[105] à savoir, des services utilisant les réseaux de communications existants pour fournir des services de communications.

A. Les données d'identification

Le procureur du Roi peut solliciter le concours des opérateurs et fournisseurs de communications électroniques afin de procéder à l'identification d'un utilisateur de ses services en obtenant par exemple, les informations relatives à une ligne téléphonique, une adresse de courrier électronique, une adresse IP, un code

103 En l'espèce, Yahoo considérait ne pouvoir être qualifiée de «fournisseurs de service de communications électroniques» eu égard à la loi du 13 juin 2005 sur les communications électroniques. Au terme d'une longue saga judiciaire, la Cour de cassation considéra devoir interpréter la notion de «fournisseur d'un service de communication électronique» de manière autonome par rapport à la loi du 13 juin 2005, la société étant dès lors tenue de fournir les données requises (Cass., 18 janvier 2011). Pour une analyse, voy. K. De Schepper et F. Verbruggen, «Ontsnappen space invaders aan onze pacmannen? De materiële en formele strafrechtsmacht van België bij strafbare weigering van medewerking door elektronische dienstverleners», *T. Straf.,* 2013, pp. 143-166. Notons que l'affaire est remontée une seconde fois devant la Cour de cassation en raison de la problématique de la territorialité. La Cour rejeta le pourvoi en cassation considérant que "Yahoo!" dispose de suffisamment de points de repère sur le territoire belge de sorte qu'une commission rogatoire internationale n'était pas requise (Cass., 11 décembre 2015, R.G. n° P.13.2082.N).

104 Art. 46*bis*, § 1er, al. 3, art. 88*bis*, § 1er, al. 2 et art. 90*quater*, § 2, C.i.cr.

105 L'approche retenue dans l'affaire *Yahoo* fut également retenue par le tribunal correctionnel de Malines à l'égard de Skype estimant que ce dernier devait collaborer dans les conditions prévues par l'article 88*bis*, § 2 et 90*quater* § 2, C.i.cr. en tant que fournisseurs de services de communications électroniques (Corr. Anvers (div. Malines), 27 octobre 2016, *N.j.W.*, 2016/20, pp. 921-928. Pour un commentaire, voy. J. Flo, «Skype moet onderzoekers toegang geven tot communicatie verdachte», *Juristenkrant,* n° 337). Cette approche fut confirmée par la cour d'appel d'Anvers (Anvers, 15 novembre 2017, C.1288.2017, inédit). Voy. J. Flo, «Skype opnieuw veroordeeld voor belemmering strafonderzoek», *Juristenkrant*, 2017, n° 359.

«IMEI» d'un téléphone[106], l'adresse «MAC» d'un ordinateur[107].

Dans le cas où l'infraction n'est pas de nature à emporter une peine d'emprisonnement correctionnel principal d'un an ou une peine plus lourde, le procureur du Roi ne peut accéder qu'aux données d'indentification conservées depuis six mois à partir de sa décision[108]. Ces données doivent être fournies sur demande «en temps réel» sous peine d'une amende de vingt-six euros à dix mille euros en cas de refus ou d'absence de réaction[109]. En outre, la loi prévoit une obligation à l'égard des tiers de «garder le secret» sanctionnée dans les mêmes conditions que celles prévues par l'article 458 du Code pénal garantissant le secret professionnel[110].

B. Les données de trafic et de localisation

Le juge d'instruction peut solliciter le concours des opérateurs et fournisseurs de communications électroniques afin de procéder «au repérage des données de trafic de moyens de communication électronique à partir desquels ou vers lesquels des communications électroniques sont adressées ou ont été adressées» ou à «la localisation de l'origine ou de la destination de communications électroniques»[111]. Autrement dit, le juge d'instruction est compétent pour demander l'isolement de certaines données d'appel, par exemple, les différents numéros de téléphone composés ou reçus par un téléphone, leur durée, le moment de la prise de contact, etc. Il peut également par ce biais localiser le signal émis par un appareil en fonctionnement sans qu'une communication ne soit émise ou reçue[112] et ainsi, géolocaliser une personne[113].

Cette mesure ne peut être ordonnée qu'en présence d'indices sérieux d'infractions de nature à entraîner un emprisonnement correctionnel principal d'un an ou une peine plus lourde et pour autant que sa mise en œuvre s'avère nécessaire à la manifestation de la vérité[114]. Le juge d'instruction indique les circonstances de fait de la cause qui justifient la mesure, son caractère proportionnel eu égard au respect de la vie privée et subsidiaire à tout autre devoir d'enquête, dans une ordonnance motivée[115]. Cette mesure doit être limitée dans le temps, deux mois maximums à dater de l'ordonnance postérieure ou antérieure sans préjudice de renouvellement[116].

À noter que l'accès aux données de trafic et de localisation conservées par les opérateurs sur base de l'article 126 de la loi du 13 juin 2005, soit l'obligation de conservation des métadonnées[117], ne sont accessibles au juge

106 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.

107 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. Art. 46*bis* C.i.cr. Voy. 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.

108 Art. 46*bis*, § 1er, dernier alinéa C.i.cr.

109 Art. 46*bis*, § 2, dernier alinéa C.i.cr.

110 Art. 46*bis*, § 2, al. 3, C.i.cr.

111 Art. 88*bis*, § 1er, C.i.cr.

112 Cass., 24 mai 2011, R.G. nº P.11.0909.N, *Pas.*, 2011.

113 La différence entre la notion de repérage au sens de l'article 88*bis* C.i.cr. et d'identification au sens de l'article 46*bis* C.i.cr. est parfois ténue. À cet égard, voy. 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*?», *op. cit.*

114 Art. 88*bis*, § 1er, al. 1er, C.i.cr.

115 Art. 88*bis*, § 1er, al. 4, C.i.cr.

116 Art. 88*bis*, C.i.cr.

117 Loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques, *M.B.*, 18 juillet 2016. Pour un état des lieux sur la question, voy. C. Forget, «L'obligation de conservation des "métadonnnées": la fin d'une longue saga juridique?», *J.T.*, nº 6683, 2017, pp. 233-239. Rap-

d'instruction que « s'il existe des indices sérieux que les infractions peuvent donner lieu à une peine d'emprisonnement correctionnel principal d'un an ou à une peine plus lourde »[118]. L'accès est limité aux données stockées depuis six mois pour les infractions punies d'un à cinq ans d'emprisonnement, neuf mois lorsque l'infraction est de nature à emporter une peine de cinq ans ou plus, douze mois lorsqu'il est question de terrorisme[119]. La loi prévoit par ailleurs des garanties supplémentaires pour les personnes soumises au secret, en l'occurrence les avocats et les médecins[120]. Ces données doivent être fournies sur demande « en temps réel » sous peine d'une amende de vingt-six euros à dix mille euros en cas de refus ou d'absence de réaction[121]. En outre, la loi prévoit une obligation à l'égard des tiers de « garder le secret » dont le non-respect est sanctionné dans les mêmes conditions que celles prévues par l'article 458 du Code pénal garantissant le secret professionnel[122].

En cas de flagrant délit, le procureur du Roi peut également ordonner le repérage, pour les infractions visées à l'article 90*ter*, §§ 2, 3 et 4 C.i.cr. avec confirmation de la mesure dans les vingt-quatre heures par le juge d'instruction[123]. En cas d'enquête relative à une infraction terroriste, prise d'otage, détention illégale ou extorsion, le procureur du Roi peut ordonner la mesure tant que la situation de flagrant délit perdure, sans qu'une confirmation par le juge d'instruction ne soit nécessaire[124]. Uniquement concernant les infractions terroristes, le procureur du Roi peut ordonner le repérage des communications dans les septante-deux heures suivant la découverte de cette infraction, sans qu'une confirmation par le juge d'instruction ne soit nécessaire[125]. En cas de harcèlement réalisé par le biais d'un réseau ou d'un service de communications électroniques au sens de l'article 145, § 3 et § 3*bis* de la loi du 13 juin 2005 relative aux communications électroniques[126], le procureur du Roi peut également ordonner un tel dispositif, sur demande du plaignant[127]. On peut s'étonner d'un tel élargissement pour une infraction qui ne requiert pas la répétition du comportement incriminé[128], à la différence du harcèlement de droit commun[129].

V. LA COMMUNICATION DES DONNÉES PASSAGERS

La loi du 25 décembre 2016 relative au traitement des données des passagers, intitulée loi « PNR » pour « Passenger Name Record »[130], introduit une obligation pour les transporteurs et opérateurs de voyage des différents secteurs de transport international (aérien, ferroviaire, routier et maritime) de transmettre les informations relatives à leurs passagers[131] à une banque

pelons que comme mentionné *supra* dans la section relative à la « préservation de données », un recours en annulation est actuellement pendant devant la Cour constitutionnelle.

118 Art. 88*bis*, § 2, C.i.cr.

119 *Ibidem*.

120 Art. 88*bis*, § 3, C.i.cr.

121 Art. 88*bis*, § 4, C.i.cr.

122 Art. 88*bis*, § 4, al. 2, C.i.cr.

123 Art. 88*bis*, § 1er, al. 6, C.i.cr.

124 Art. 88*bis*, § 1er, al. 7, C.i.cr.

125 Art. 88*bis*, § 1er, al. 8, C.i.cr.

126 *M.B.*, 20 juin 2005.

127 Art. 88*bis*, § 1er, al. 9, C.i.cr.

128 Selon O. Leroux, il est réducteur de qualifier cette disposition de harcèlement considérant que la loi ne requiert pas la répétition du comportement incriminé. Voy. O. Leroux, « Protection pénale des mineurs sur Internet : harcèlement, "Grooming" et cyberprédation », in *Pas de droit sans technologie* (sous la dir. de J.-F. Henrotte et F. Jongen), Bruxelles, Larcier, 2015, p. 222.

129 Art. 442*bis* Code pénal.

130 Loi du 25 décembre 2016 relative au traitement des données des passagers, *M.B.*, 25 janvier 2017.

131 L'article 9 de la loi PNR distingue les données API à savoir les données d'enregistrement et d'embarquement, des données PNR à savoir les données de réservation. Les données API sont des données authentiques, par exemple, données biographiques figurant sur une carte d'identité. Les données PNR

de données gérée par le Service public fédéral Intérieur [132]. Ces données ont vocation à être analysées avant l'arrivée, le transit ou le départ d'une personne sur le territoire national[133] par l'Unité d'Informations des Passagers (UIP) créée au sein du SPF Intérieur[134]. Cette méthode appliquée à des fins de « pre-screenning »[135], permettrait de « faire émerger des profils de passagers à risque qui ne sont pas nécessairement connus ou mentionnés dans les banques de données des services »[136]. En outre, les services compétents[137] ont la possibilité de procéder à des recherches ponctuelles dans les limites de leurs missions et des finalités prévues par la loi à savoir, notamment la lutte contre le terrorisme, la recherche et la poursuite de certaines infractions et la lutte contre l'immigration illégale[138].

Conformément à l'article 46*septies* C.i.cr., le procureur du Roi peut, sur base d'une décision écrite et motivée, charger l'officier de police judiciaire de requérir l'UIP afin d'obtenir la communication de données de passagers. L'article 46*septies*, § 2, C.i.cr. impose le respect des critères de proportionnalité et de subsidiarité par rapport à d'autres devoirs d'enquête. Si la demande porte sur un ensemble de données relatives à une enquête spécifique, celle-ci doit alors être limitée à une période d'un mois, sans préjudice de renouvellement[139].

Dans le cadre de cette contribution, nous n'aborderons pas l'épineuse question de la conformité de la loi relative au traitement des données des passagers aux droits fondamentaux[140]. Notons toutefois que l'avis « PNR » rendu récemment par la Cour de justice de l'Union européenne[141] aura très probablement des conséquences sur notre législation nationale d'autant qu'un recours en annulation est actuellement pendant devant la Cour constitutionnelle[142].

VI. L'INFILTRATION DANS UN CONTEXTE INFORMATIQUE

L'article 46*sexies,* § 1er, C.i.cr. autorise désormais les services de police à « entretenir des contacts sur Internet avec une ou plusieurs personnes, sous une identité fictive ou non ». Il s'agit donc d'une nouvelle méthode d'enquête calquée sur l'infiltration classique mais présentant davan-

comprennent davantage d'informations. Il s'agit notamment de l'itinéraire complet pour le passager, l'agence de voyage, le numéro de siège, les informations relatives aux bagages, les données d'enregistrement et d'embarquement (type de document de voyage, numéro du document, nationalité, nombre poids et identification des bagages, numéro de transport, etc.), les modes de paiement et l'adresse de facturation, etc.

132 Art. 3 loi PNR.

133 Art. 15 loi PNR.

134 Art. 24 loi PNR.

135 Le « pre-screening » consiste en « l'évaluation du risque représenté par les passagers » et s'effectue par le biais d'une corrélation entre les banques de données des services compétents ou par le biais de critères préétablis par l'UIP.

136 Exposé des motifs, *Doc. parl.,* Chambre, sess. ord., 2015-2016, n° 54-2069/001, p. 29.

137 Par « services compétents », l'article 14, § 1er, 2°, précise qu'il s'agit des services de police, de la Sûreté de l'État, du Service général de Renseignement et de Sécurité, de services d'enquêtes liées aux infractions douanes et accises.

138 Art. 8 loi PNR.

139 Art. 46*septies,* § 3, C.i.cr.

140 La particularité du système PNR est l'exploration systématique de données afin de « situer » des passagers sur une échelle de risque et d'ainsi permettre l'identification de criminels « éventuels ou probables ». Selon le Conseil de l'Europe, un tel mécanisme ciblant des personnes « qui n'ont commis aucune infraction » ne pourrait en aucun cas viser « un but légitime » d'autant qu'il existe un risque d'erreur inévitable susceptible de mener à du profilage discriminatoire. Voy. en ce sens le rapport du Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé du Conseil de l'Europe, *Passenger Name Records, data mining & data protection : the need for strong safeguards*, 15 juin 2015, T-PD(2015)11.

141 C.J.U.E., 26 juillet 2017, avis 1/15, ECLI:EU:C:2017:592.

142 Recours en annulation totale ou partielle de la loi du 25 décembre 2016 relative au traitement des données des passagers, introduit par l'ASBL « Ligue des Droits de l'Homme ».

tage de souplesse. À l'instar de l'article 47*octies* C.i.cr., celle-ci requiert le respect de critères de subsidiarité et l'existence d'indices sérieux indiquant que les personnes visées commettent ou commettraient des infractions punissables d'un emprisonnement d'un an ou d'une peine plus lourde[143]. En outre, la période d'infiltration dans un contexte digital ne peut excéder trois mois, sans préjudice de renouvellement[144]. Cette limitation dans le temps pourrait poser problème en pratique, par exemple si l'enquêteur laisse son profil inactif et le réutilise après une certaine période, il dépassera rapidement le délai légal prescrit.

À l'instar de l'infiltration classique[145], la commission d'infractions de type échanger des fichiers illégaux via des réseaux *peer-to-peer* ou envoyer des messages sur un forum de radicaux ou extrémistes sur lequel on nie l'holocauste[146], suppose l'autorisation du procureur du Roi[147]. Par contre, la loi ne précise pas le type d'infractions admissibles et ne les limite pas au « cyberespace », *a contrario* de ce que recommandait pourtant le Conseil d'État[148]. En tout état de cause, l'agent ne peut se rendre coupable de provocation[149] ou faire usage d'un profil fictif explicite, trompeur ou provocant[150], au risque de rendre les poursuites irrecevables.

À la différence d'une infiltration dans un contexte réel, le procureur du Roi ne peut prendre des mesures visant à garantir la sécurité et l'intégrité physique ou psychiques du cyberinfiltrant. Selon les travaux parlementaires, cela se justifie en raison de l'absence de contact réel avec la personne infiltrée et de l'absence de nécessité de disposer d'une base légale pour prendre de telles mesures[151]. Par ailleurs, l'infiltrant ne doit pas appartenir aux unités spéciales de la police fédérale. Il revient au Roi de déterminer les conditions, la formation et les modalités de désignation des services de police habilités à exécuter la mesure[152]. Selon le Conseil d'État, il aurait été bienvenu de fixer de tels éléments dans la loi compte tenu de leur incidence en cas de mise à exécution de la mesure et ce, conformément au principe de légalité garanti par l'article 12 alinéa 2, de la Constitution[153]. La loi permet également de faire appel à un expert civil, dans des circonstances exceptionnelles et pour une courte durée[154], par exemple si des agents pénètrent dans un milieu où est utilisé un langage spécifique (langue étrangère, langage de jeunes…) ou dans certains milieux où des connaissances très spécialisées sont requises tels les hackers[155].

L'infiltration dans un contexte digital est encadrée de manière plus souple que dans un contexte réel[156]. Il ne s'agit pas d'une méthode particulière de recherche au sens des articles 47*ter* et suivants C.i.cr. Toutefois, un contrôle exercé par la chambre des mises en accusation dans le cadre de l'examen des méthodes particulières de recherche[157] est possible dans le cas où un dossier confidentiel est ouvert, c'est-à-dire dans le cas où l'enquê-

143 Art. 46*sexies*, § 1er, C.i.cr.
144 Art. 46*sexies*, § 2, C.i.cr.
145 Art. 47*octies,* § 4, C.i.cr.
146 Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n° 54-1966/001, p. 41.
147 Art. 46*sexies*, § 3, al. 2, C.i.cr.
148 Avis du Conseil d'État n° 59.199/3 du 9 mai 2016, p. 136, point 24.
149 Art. 30 du Titre préliminaire du Code pénal.
150 Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n° 54-1966/001, p. 36.
151 Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n° 54-1966/001, p. 42.
152 Art. 46*sexies*, § 1er, al. 2, C.i.cr.
153 Cet article précise que « Nul ne peut être poursuivi que dans les cas prévus par la loi, et dans la forme qu'elle prescrit ».
154 Art. 46*sexies*, § 1er, al. 3, C.i.cr.
155 Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n° 54-1966/001, p. 38.
156 *Ibidem*, p. 36.
157 Art. 235*ter* et 235*quater* C.i.cr.

teur est autorisé à commettre des infractions[158] ou s'il est fait appel à un expert civil[159]. Le législateur justifie cette différence de traitement en considérant que la mesure serait moins intrusive compte tenu de l'absence de contact physique entre l'infiltré et l'infiltrant et de l'obligation de retranscrire dans un procès-verbal les contacts pertinents. Cette obligation de retranscription assurerait une certaine transparence et limiterait ainsi le risque d'abus[160]. En tout état de cause, la question devra être tranchée par la Cour constitutionnelle, la Ligue des droits de l'Homme ayant annoncé avoir introduit un recours en annulation à l'encontre de cette disposition.

Enfin, l'article 46*sexies,* § 1er C.i.cr. ne s'applique pas si les services de police interagissent avec une personne uniquement à des fins d'arrestation ou en vue d'effectuer une vérification ciblée et ceci, sans utiliser une identité fictive crédible[161]. Il s'agira, par exemple, de prendre contact avec une personne sur un site de petites annonces et de lui fixer un rendez-vous ou d'échanger brièvement avec une personne pour s'assurer de sa dangerosité et qu'il ne s'agit pas d'un plaisantin. Comme le souligne la Commission de protection de la vie privée, cette exclusion manque de clarté et devrait être encadrée distinctement soit dans le Code d'instruction criminelle, soit dans la loi sur la fonction de police afin de respecter les exigences de prévisibilité établie par l'article 8, § 2, de la CEDH[162]. Toutefois, dans un arrêt du 28 mars 2017[163], la Cour de cassation dit pour droit que l'article 26 de la loi sur la fonction de police constitue une base légale suffisante pour permettre aux services de police de « patrouiller » sur Internet sur les « sources ouvertes » ou « semi publiques »[164]. Cette disposition permet en effet aux enquêteurs de pénétrer dans les lieux accessibles au public, types cafés ou restaurants, dans le cadre des missions de police judiciaire à savoir, en vue de rechercher les crimes, les délits et les contraventions, d'en rassembler les preuves et d'en livrer les auteurs aux tribunaux chargés de les punir[165].

VII. LA PÉNÉTRATION DANS UN SYSTÈME INFORMATIQUE À DES FINS D'OBSERVATION

En vertu de l'article 46*quinquies,* § 1er, C.i.cr., le procureur du Roi peut autoriser les services de police à pénétrer dans un lieu privé à l'insu du propriétaire, à ouvrir des objets fermés se trouvant sur les lieux ou à les emporter pour une durée limitée en vue de réunir des preuves. La mesure doit revêtir un caractère subsidiaire et nécessite la présence d'indices « sérieux que les faits punissables constituent ou constitueraient une infraction visée à l'article 90*ter*, §§ 2

158 Art. 46*sexies*, § 3, C.i.cr.
159 Art. 46*sexies*, § 1er, C.i.cr.
160 Art. 46*sexies,* § 4, al. 1er, C.i.cr.
161 Art. 46*sexies*, § 1er, al. 4, C.i.cr.
162 C.P.V.P., avis n° 21/2016 du 18 mai 2016, pp. 31-32, points 45 et 48.
163 Cass., 28 mars 2017, R.G. n° P.16.1245.N/4.
164 En l'espèce, des enquêteurs s'étaient enregistrés sur un forum de vente de drogues sur le darknet, via l'utilisation du navigateur Tor, après avoir reçu un lien d'invitation d'un membre de la communauté leur permettant de s'inscrire. La Cour considéra que les observations effectuées n'entraient pas dans le champ d'application de l'article 47*sexies,* § 1er, C.i.cr. à savoir l'observation systématique. En effet, selon la Cour, l'entrée dans cet « espace » dépendait de conditions d'accès purement formelles, sans contrôle sur le contenu ou sur la qualité des personnes de sorte qu'il ne pourrait s'agir d'un espace limité à un cercle privé inaccessible aux enquêteurs mais bien d'un espace accessible au sens de l'article 26 de la loi sur la fonction de police. On peut toutefois se demander si le fait d'épier en secret sur Internet pendant « plus de cinq jours consécutifs ou de plus de cinq jours non consécutifs répartis sur une période d'un mois » ne pourrait pas constituer une observation systématique au sens de l'article 47*sexies,* § 1er, C.i.cr. Néanmoins, l'arrêt ne nous dit pas quelle fut la durée de l'observation. Pour un commentaire, voy. C. Conings, « De politie op het darknet », *T. Strafr.*, 2017/5, pp. 331-334.
165 Art. 8 C.i.cr.

à 4, ou sont commis ou seraient commis dans le cadre d'une organisation criminelle visée à l'article 324*bis* du Code pénal »[166].

Dans ce cadre, le procureur du Roi peut désormais autoriser la pénétration dans un système informatique afin d'y placer, réparer, retirer un moyen technique à des fins d'observation au sens de l'article 47*sexies*, § 1er, C.i.cr.[167], par exemple, une caméra installée par un particulier dans un hangar. Si le système informatique est situé dans un lieu privé type un domicile ou un local professionnel ou s'il donne vue sur un domicile, les services de police devront disposer de l'autorisation du juge d'instruction[168]. Il s'agit donc d'une modification importante du Code d'instruction criminelle qui ne prévoyait pas la possibilité pour les enquêteurs d'exploiter un système informatique en temps réel installé par un tiers[169]. Outre les conditions classiques de l'observation, la pénétration ne peut excéder trois mois à dater de l'autorisation[170]. Par contre, il n'est pas exigé des enquêteurs de décrire dans un procès-verbal les techniques et tactiques employées, l'identité des personnes employées et le moment où l'observation a eu lieu[171].

L'article 89*ter* C.i.cr. prévoit par ailleurs la possibilité d'explorer le système informatique à l'insu de la personne concernée. Selon les travaux préparatoires, conformément aux finalités visées par l'article 46*quinquies*, § 2, C.i.cr., les enquêteurs peuvent vérifier si des preuves existent mais non les emporter, à l'exception de certains échantillons ou certaines copies ciblées d'un ordinateur[172]. Ainsi, en cas de consultation d'images pédopornographiques par exemple, l'enquêteur peut effectuer une recherche dans le système afin de prélever certaines images[173]. Par contre, à la différence de l'article 90*ter* C.i.cr., les preuves découvertes ne peuvent être entièrement collectées, utilisées et copiées[174]. La limite entre l'exploration d'un système dans le cadre d'une observation et interception des communications au sens de l'article 90*ter* C.i.cr. pourra toutefois s'avérer

166 Art. 46*quinquies,* § 1er, C.i.cr.

167 L'article 47*sexies*, § 1er, 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 » laquelle relève de la compétence générale des services de police. Cette dernière s'exerce à des occasions déterminées par exemple, lorsqu'un policier « en civil » épie des personnes organisant une manifestation sans autorisation. *Doc. parl.,* Ch. repr., n° 20/1688/001, p. 30 ; voy. également M. Beys, *Quels droits face à la police ?*, Couleur livres, J&D Éditions, 2014, pp. 323 et s.

168 Art. 89*ter* C.i.cr.

169 Par contre, si les services de police font usage d'un moyen technique installé par un tiers afin de tracer et de localiser des marchandises par exemple ou pour obtenir des images de caméras de surveillance *a posteriori*, la Cour de cassation considère qu'il ne s'agit pas d'une observation au sens de l'article 47*sexies* C.i.cr. (Cass., 19 juin 2012, R.G. n° P.12.0362.N, *Lar. Cass.*, 2012/10, p. 231) ; Y. Van Den Berge, « Le système informatique automatisé "tracking et tracing" aux fins de localisation de conteneurs n'est pas une observation au sens de l'article 47*sexies* C.I.cr. », *T. Strafr.*, 2013/3, p. 185 (note sous Cass., 19 juin 2012, R.G. n° P.12.0363.N) ; 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.

170 Art. 47*sexies,* § 3, C.i.cr. La période d'un mois prévue antérieurement a été portée à trois mois par la loi du 25 décembre 2016.

171 Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n° 54-1966/001, p. 36.

172 Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n° 54-1966/001, p. 51.

173 Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n° 54-1966/001, p. 51.

174 Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n° 54-1966/001, p. 52.

ténue en pratique[175]. En outre, le législateur ne semble pas avoir prévu la possibilité d'effectuer une observation par le biais d'un système informatique, indépendamment d'une pénétration dans un lieu privé ou un domicile si ce n'est dans les conditions prévues par l'article 90*ter* C.i.cr.

VIII. L'OBLIGATION DE COLLABORATION

L'article 88*quater* du Code d'instruction criminelle prévoit deux types de collaboration relevant de la compétence du juge d'instruction. La première est une obligation d'information consistant à enjoindre quiconque présumé disposer d'une connaissance particulière du système informatique faisant l'objet d'une recherche ou de son extension, de fournir dans une forme compréhensible, des informations sur le fonctionnement de ce système[176]. Un tiers pourrait par exemple, être tenu de fournir les clés de chiffrement ou les mots de passe dont il aurait connaissance sur demande des autorités[177]. La seconde est une obligation « d'agir » dans le sens où le juge d'instruction peut ordonner à toute personne appropriée de mettre ledit système en fonctionnement et de procéder à une saisie de données informatiques c'est-à-dire de copier les données, de les rendre inaccessibles ou encore de les retirer de l'appareil exploité[178].

On précisera que la mesure ne peut porter atteinte au droit au silence et aux règles de droit commun relatives aux personnes tenues au secret professionnel[179]. Sous réserve de ces exceptions, le défaut de collaboration est passible de sanctions pénales à savoir, une peine d'emprisonnement de six mois à trois ans et d'une amende de vingt-six euros à vingt mille euros ou d'une de ces peines seulement[180]. Cette sanction peut être portée d'un à cinq ans avec une amende de cinq cents euros à cinquante mille euros dans le cas où la collaboration aurait eu pour effet d'empêcher la commission d'un crime ou d'un délit ou d'en limiter les effets[181]. En outre, la loi prévoit une obligation à l'égard des tiers de « garder le secret » sanctionnée dans les mêmes conditions que celles prévues par l'article 458 du Code pénal garantissant le secret professionnel[182].

À la différence de l'article 88*quater* § 2, l'article 88*quater,* § 1er ne précise pas si l'obligation d'information peut être adressée à un inculpé et aux personnes visées par l'article 156 C.i.cr., à savoir, les ascendants ou descendants de la personne prévenue ainsi que ses proches. Dans un jugement du 17 novembre 2014, le tribunal correctionnel de Termonde a toutefois rappelé qu'aucun suspect ne peut être obligé de collaborer activement avec les autorités poursuivantes. Il estima qu'en ordonnant aux prévenus de rendre accessibles les supports de données, ils avaient été contraints, moyennant une prestation intellectuelle propre, de

175 Dans le même sens, voy. S. Tosza et V. Franssen, *op. cit.*, p. 236.

176 Art. 88*quater,* § 1er, C.i.cr.

177 L'article 88*quater* C.i.cr. s'inscrit dans la lignée de la Recommandation R (95) 13 du Conseil de l'Europe qui considère que les « autorités chargées de l'enquête devraient avoir le pouvoir d'ordonner aux personnes qui ont des données spécifiques sous leur contrôle de fournir toutes les informations nécessaires pour permettre l'accès au système informatique et aux données qu'il renferme ». Voy. Recommandation R (95) 13 du Conseil de l'Europe relative aux problèmes de procédure pénale liés à la technologie de l'information, adoptée le 11 septembre 1995.

178 Art. 88*quater,* § 2, C.i.cr.

179 *Doc. parl.*, Ch. repr., 1999-2000, n° 0213/001, p. 28. Voy. à cet égard la jurisprudence de la Cour constitutionnelle : C. const., 17 décembre 2015, n° 178/2015, § B.52.3 ; J. Coppens et C. Van De Heyning, « Het bevel tot medewerking van artikel 88*quater* Sv., het zwijgrecht en het verbod op zelfincriminatie », *T.S.*, n° 3, 2016, pp. 260-265.

180 Art. 88*quater,* § 3, al. 1er, C.i.cr.

181 Art. 88*quater,* § 3, al. 2 C.i.cr.

182 Art. 88*quater,* § 4, C.i.cr.

contribuer activement à l'administration de la preuve de sorte que les éléments de preuve fournis par les supports de données cryptées étaient frappés de nullité[183]. Cette approche fut confirmée par la cour d'appel de Gand[184].

Récemment toutefois, la cour d'appel d'Anvers, chambre des mises en accusation, a considéré que l'ordonnance d'un juge d'instruction imposant à un inculpé de dévoiler le code pin de son téléphone portable sous peine de sanctions pénales afin de permettre aux enquêteurs d'exploiter les données stockées, n'était pas incompatible avec les exigences du droit à un procès équitable[185]. Dans sa décision, la chambre des mises en accusation a notamment fait référence à l'arrêt *Saunders* où la Cour eur. D.H. a estimé qu'une donnée que l'on peut obtenir de l'accusé en recourant à des pouvoirs coercitifs mais qui existent indépendamment de sa volonté, tels des documents recueillis sur base d'un mandat, des empreintes ADN, haleine, sang, urine, n'entraient pas dans le champ d'application du droit au silence[186]. Cette interprétation mérite d'être nuancée puisqu'à la différence de documents fiscaux tenus en vertu d'une obligation légale et saisissables dans le cadre d'une perquisition par exemple, un mot de passe est créé sur initiative de son auteur et devrait donc être couvert par le droit au silence[187]. En effet, le droit au silence ne couvre pas uniquement le droit de se taire mais englobe également le droit de ne pas fournir des informations susceptibles d'affecter substantiellement la position de l'accusé ou de favoriser une incrimination[188], ce qui pourrait être le cas lorsqu'un suspect est tenu de donner accès aux données stockées sur son téléphone. Une interprétation différente peut être défendue si le mot de passe équivaut à l'empreinte ADN du suspect ou à son inis par exemple.

Concernant la collaboration de tiers, si l'article 88*quater*, § 2 précise que les personnes visées doivent donner suite à l'ordonnance du juge d'instruction « dans la mesure de leurs moyens », l'article 88*quater,* § 1er ne prévoit pas une telle limitation et ne précise pas les conséquences d'un défaut de collaboration en raison soit d'une impossibilité matérielle, soit d'un intérêt légitime invoqué par ce tiers. À ce propos, l'affaire *Apple* défraya la chronique en raison du refus de l'entreprise d'obtempérer à une injonction du FBI lui ordonnant de déchiffrer le téléphone portable d'un des auteurs de la tuerie de San Bernardino. Apple refusa d'agir invoquant le risque de mettre à mal la sécurité informatique de ses services[189]. *In fine*, le FBI trouva une faille et accéda aux données contenues sur le téléphone sans la collaboration de la multinationale. Cette affaire illustre l'équilibre difficile entre le besoin pour les autorités d'accéder à des données en imposant la collaboration de tiers[190] et la nécessité pour une entreprise d'assurer la protection des données

183 Corr. Termonde, 17 novembre 2014, *T. Strafr.*, 2016/3, pp. 255-260.

184 Gand, 23 juin 2015, *N.j.W.,* 2016, liv. 336, p. 134, note C. Conings.

185 Anvers (ch. mise acc.), 21 décembre 2017, R.G. n° K/2895/2017, inédit.

186 Cour eur. D.H., 17 décembre 1996, *Saunders c. Royaume-Uni*, n° 1187/91, § 69.

187 Cour eur. D.H., 25 février 1993, *Funke c. France*, n° 110588/83.

188 Cour eur. D.H., 19 février 2009, *Chabelnik c. Ukraine,* n° 16404/03.

189 Outre le déblocage du téléphone, le FBI souhaitait qu'Apple élabore une nouvelle version du système d'exploitation afin de faciliter de manière générale l'accès des autorités aux données stockées sur ses appareils, indépendamment de celui visé dans le cadre de l'enquête.

190 Europol est d'avis que certains systèmes de chiffrement ralentissent considérablement la poursuite des enquêtes pénales. Il en appelle à une solution viable permettant à la fois d'assurer la protection de la vie privée des utilisateurs et de permettre la lutte contre les infractions et menaces contre la sécurité. Europol, « The Internet Organised Crime Threat Assessment (IOCTA) 2015 », 30 septembre 2015, pp. 67 et s.

à caractère personnel par des méthodes de chiffrement[191] et en ce sens, contribuer à protéger le droit au respect de la vie privée[192].

Selon la Convention de Budapest, les autorités répressives se heurtant à des données chiffrées[193] peuvent imposer la collaboration de tiers afin d'obtenir les données en sa possession ou sous son contrôle[194] en « texte clair »[195] c'est-à-dire déchiffrées. Considérant qu'il s'agit d'une méthode d'enquête, elle exige le respect du critère de proportionnalité mais aussi de prendre en considération l'intérêt légitime de tiers[196]. Au niveau des instances internationales, le Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression des Nations Unies estime qu'une obligation de collaboration est une ingérence qui devrait « être strictement limitée, conformément aux principes de légalité, de nécessité, de proportionnalité et de légitimité des objectifs »[197]. Selon ce dernier, les États devraient « éviter toutes les mesures qui affaiblissent la sécurité en ligne des individus, telles que des portes dérobées, de faibles standards de cryptographie ou la rétention de clés de chiffrement »[198]. Dans le même sens, la Recommandation n° R(95)13 du Comité des ministres aux États membres relative aux problèmes de procédure pénale liés à la technologie de l'information dispose « des mesures devraient être examinées afin de minimiser les effets négatifs de l'utilisation du chiffrement sur les enquêtes des infractions pénales, sans toutefois avoir

191 Différents instruments internationaux préconisent le chiffrement de données en vue d'assurer la sécurité des flux et la protection des données à caractère personnel. L'article 31, § 1er, du règlement général sur la protection des données liste certaines mesures permettant de garantir un niveau de sécurité informatique adapté dont la première est « le chiffrement des données à caractère personnel ». De même, une Recommandation du Comité des ministres du Conseil de l'Europe préconise l'application de mesures de cryptage « de bout en bout » afin d'éviter l'accès illicite aux données par des tiers. Voy. Recommandation CM/Rec (2014)6 du Comité des ministres aux États membres sur un Guides des droits de l'homme pour les utilisateurs d'internet, adoptée par le Comité des ministres le 16 avril 2014 ; dans le même sens, l'Assemblée parlementaire du Conseil de l'Europe affirme qu'un « cryptage généralisé destiné à renforcer le respect de la vie privée reste la riposte la plus efficace pour permettre aux citoyens de protéger leurs données », voy. Rapport de la commission des questions juridiques et des droits de l'homme de l'Assemblée parlementaire du Conseil de l'Europe, rapporteur M. Pieter Omtzigt, Doc. 13734, 18 mars 2015, point 119.

192 Ce lien de dépendance a été illustré dans l'arrêt *I. c. Finlande* où la Cour eur. D.H. estima que le défaut de garanties relatives à la sécurisation des données contre des usages non autorisés constitue une violation de l'obligation positive d'assurer le respect du droit à la vie privée consacré à l'article 8 de la C.E.D.H. Cour eur. D.H., 17 juillet 2008, *I. c. Finlande*, n° 20511/03.

193 Europol affirme que le chiffrement des données ralentit considérablement la poursuite des enquêtes pénales. Europol, « The Internet Organised Crime Threat Assessment (IOCTA) 2015 », 30 septembre 2015, pp. 67 et s.

194 Comme déjà exposé *supra*, l'expression « en sa possession » ou « sous son contrôle » fait référence d'une part, à la possession matérielle des données et d'autre part, à des situations dans lesquelles l'intéressé ne possède pas matériellement les données à produire mais peut en contrôler librement la production, par exemple si les données sont stockées sur un cloud qu'elle met librement à disposition. Le rapport explicatif précise toutefois qu'un accès aux données par une liaison du réseau ne constitue pas nécessairement un « contrôle » au sens de la présente disposition. Rapport explicatif de la Convention sur la cybercriminalité, § 173.

195 Rapport explicatif de la Convention de Budapest, § 176.

196 Art. 18, § 2, de la Convention de Budapest.

197 Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, A/HRC/29/32, 22 mai 2015, § 56.

198 *Ibidem*, § 60.

des conséquences plus que strictement nécessaires sur son utilisation légale »[199].

La Cour eur. D.H. n'a pas été amenée à se prononcer sur la question mais fut saisie de litige relatif à la collaboration de tiers en raison de l'anonymat d'internautes. À cette occasion, elle déduisit du droit au respect de la vie privée une obligation positive à charge des États membres de prévoir dans leur droit interne des dispositions permettant d'exiger un fournisseur de service Internet à dévoiler l'identité d'un destinataire de leurs services[200]. La C.J.U.E. adopte une position similaire dans le domaine de la propriété intellectuelle en reconnaissant que des acteurs privés puissent être tenus de sécuriser une connexion Internet et d'imposer à l'utilisateur de s'identifier[201]. En définitive, le sujet est donc loin d'être clos.

IX. L'INTERCEPTION DES COMMUNICATIONS NON ACCESSIBLES AU PUBLIC

Le juge d'instruction est compétent pour ordonner « en secret »[202] l'interception, la prise de connaissance, l'exploration, l'enregistrement de communications non accessibles au public ou de données informatiques[203]. Pour accéder au système, il peut ordonner l'utilisation de fausses clés[204], la suppression de manière temporaire des protections du système informatique ou en encore 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[205]. Ainsi libellée, la disposition permet, par exemple, aux enquêteurs de placer un logiciel espion sur l'ordinateur d'une personne en vue d'exploiter le contenu du disque dur ou d'intercepter une conversation et d'en prendre copie[206]. Ce type de programme peut être installé à l'insu de l'utilisateur par exemple, par le biais d'une mise à jour du système d'exploitation ou en envoyant un message électronique comprenant une pièce jointe qui, une fois ouverte, entraîne l'installation automatique[207]. Les enquêteurs pourront par ce biais accéder aux communications

199 Recommandation R (95) 13 du Comité des ministres aux États membres relative aux problèmes de procédure pénale liés à la technologie de l'information, 11 septembre 1995, § 14.

200 Cour eur. D.H., 2 décembre 2008, *K.U. c. Finlande*, n° 2872/02, § 49. Selon celle-ci, «Même si la liberté d'expression et la confidentialité des communications sont des préoccupations primordiales et si les utilisateurs des télécommunications et des services Internet doivent avoir la garantie que leur intimité et leur liberté d'expression seront respectées, cette garantie ne peut être absolue, et elle doit parfois s'effacer devant d'autres impératifs légitimes tels que la défense de l'ordre et la prévention des infractions pénales ou la protection des droits et libertés d'autrui».

201 C.J.U.E., 15 septembre 2016, *Tobias Mc Fadden c. Sony Music Entertainment Germany GmbH*, C-484/14.

202 En ce sens il se distingue de l'article 39*bis*, § 4, C.i.cr., voy. *supra*, « La saisie de données, informatiques, la recherche et l'extension de recherche dans un système informatique ».

203 Avant l'adoption de la loi du 25 décembre 2016, les articles 90*ter* et suivants C.i.cr. habilitaient les autorités compétentes à « prendre connaissance » des communications « en cours de transmission ». Cette notion était peu adéquate dans un contexte digital par exemple, lorsque les enquêteurs souhaitaient prendre connaissance d'un projet de courrier électronique. En pratique en effet, certains suspects utilisent une boîte mails et enregistrent leurs communications dans le dossier « brouillon » leur permettant d'éviter une interception de leurs communications. 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 (voy. l'analyse de E. Lecroart, « La prise de connaissance d'e-mails "en cours de transmission", un parcours sans fin ? », *R.D.T.I.*, 2014/4, n° 57, pp. 19-41).

204 Sur la notion de « fausses clés », voy. *supra*, La saisie de données informatiques.

205 Art. 90*ter*, § 1er, al. 3, C.i.cr.

206 Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n° 54-1966/001, p. 57.

207 M. Zwolinska, « Sécurité et les libertés fondamentales des communications électroniques en droit français, européen et international », thèse sous la direction de Louis Balmond, Nice, 2015, p. 300.

véhiculées par des dispositifs « VoIP »[208] soit par exemple, WhatsApp, Viber ou Skype lesquels ont la particularité d'être souvent chiffrés et inaccessibles. Outre l'interception des communications, la faculté de ces logiciels est infinie : certains peuvent surveiller un ordinateur et intercepter l'ensemble des données informatiques par exemple, les entrées clavier, les mots de passe, d'autres interceptent les échanges de flux de données circulant via l'appareil et par Internet[209]. La mesure peut donc s'avérer particulièrement intrusive pour la vie privée des personnes concernées.

À noter que cette méthode ne peut excéder un mois à dater de la première autorisation[210] sans préjudice de renouvellement avec une période maximale de six mois, sauf en cas de retard dû à sa préparation technique[211]. Elle ne peut être ordonnée que de manière exceptionnelle, lorsque les nécessités de l'instruction l'exigent, en présence d'indices sérieux d'une infraction visée par l'article 90*ter*, § 2, C.i.cr. et uniquement si d'autres moyens d'investigation ne paraissent pas suffire à la manifestation de la vérité[212]. Celle-ci ne peut être exécutée à des fins exploratoires ou dans le cadre d'une mini-instruction et reste donc de la compétence unique du juge d'instruction, sauf cas particulier du flagrant délit dans le cadre d'infractions terroristes par exemple, où le procureur du Roi disposera de compétences importantes[213].

L'article 90*novies* C.i.cr. prévoit par ailleurs une obligation d'informer toute personne ayant fait l'objet d'une mesure visée par l'article 90*ter* C.i.cr., de la nature de ladite mesure et des dates auxquelles elle a été exécutée. Cette notification doit intervenir au plus tard quinze jours après le moment où la décision sur le règlement de la procédure est devenue définitive ou après que la personne concernée ait été citée, sauf si son identité ou son adresse ne peut « raisonnablement » être trouvée.

En dépit des réserves émises par la Commission de la protection de la vie privée, la loi du 25 décembre 2016 a élargi de manière importante la liste des infractions visées par l'article 90*ter,* § 2, C.i.cr. en incluant par exemple, l'attentat à la pudeur, le viol, le grooming, le vol à l'aide de violence ou menaces, le trafic de stupéfiants, l'incendie et la tentative d'incendie, le hacking, le faux informatique, les infractions relatives au secret des communications, sans qu'un débat parlementaire approfondi n'ai eu lieu[214]. En ce sens, on peut s'interroger sur la compatibilité d'un tel dispositif avec la Convention de Budapest exigeant de limiter ce type de méthode aux enquêtes relatives à « un éventail d'infractions graves à définir en droit interne »[215].

Afin de mettre en œuvre un tel dispositif, le juge d'instruction peut requérir directement ou par l'intermédiaire du service de police désigné par le Roi, le concours « en temps réel » des opérateurs et fournisseurs de communi-

208 Ces services permettent de communiquer via le réseau Internet en faisant usage du protocole TCP/IP.

209 *Ibidem*.

210 Art. 90*quater,* § 1er, C.i.cr.

211 Art. 90*quinquies* C.i.cr.

212 Art. 90*ter,* § 1er, al. 4, C.i.cr.

213 L'article 90*ter,* § 5, C.i.cr. prévoit en effet que : « En cas de flagrant délit et tant que la situation de flagrant délit perdure, le procureur du Roi peut ordonner la mesure visée au paragraphe 1er 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 paragraphe 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 ». À ce propos, voy. C. Conings et S. Royer, « Verzamelen en vastleggen van digitaal bewijs in strafzaken », *N. C.*, 2017/4, pp. 319.

214 Avis de la Commission de la protection de la vie privée, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n° 54-1966/001, p. 34.

215 Art. 21, § 1er, de la Convention de Budapest.

cations électroniques tel qu'exposé *supra*[216]. De manière plus large, le juge d'instruction peut également faire appel à toute personne présumée disposer de connaissance particulière du système informatique qu'elles fournissent des informations sur le fonctionnement de ce moyen ou système et sur la manière d'accéder à son contenu qui est ou a été transmis, dans une forme compréhensible. Il peut ordonner aux personnes de rendre accessible ce contenu, dans la forme qu'il souhaite, notamment dans le cas où celui-ci est chiffré[217]. Le refus de collaboration « en temps réel » est puni de vingt-six euros à dix mille euros[218] tandis que le refus de prêter son concours technique en vue de déchiffrer les données est puni d'un emprisonnement de six mois à un an ou d'une amende de vingt-six euros à vingt mille euros ou d'une de ces peines seulement[219]. En outre, la loi prévoit une obligation à l'égard des tiers de « garder le secret » sanctionnée dans les mêmes conditions que celles de l'article 458 du Code pénal à savoir le secret professionnel[220].

L'affaire rendue récemment par la cour d'appel d'Anvers met en lumière la difficulté de placer une limite à l'obligation de collaboration[221]. En l'espèce, une ordonnance du juge d'instruction prise sur base des articles 88*bis* C.i.cr. et 90*quater* C.i.cr. imposait à Skype de collaborer en vue de permettre l'interception des données de communications électroniques. L'entreprise invoquait l'impossibilité matérielle de prêter son concours en raison du chiffrement des données depuis le destinateur et le déchiffrement une fois chez le destinataire. Néanmoins, selon la cour d'appel, en créant ses services, Skype aurait dû tenir compte des obligations de collaboration découlant du droit national belge. En effet, à la différence de l'article 88*quater*, § 2, C.i.cr. imposant une obligation de collaboration dans la limite des moyens dont dispose un tiers, l'article 90*quater* C.i.cr. ne prévoit aucune dérogation à l'obligation de collaboration. Ce faisant, la cour déduit de l'article 90*quater* C.i.cr. une obligation positive à charge des tiers dès la conception d'application. Cette obligation entre en résonnance avec les concepts développés en sécurité informatique types « privacy by design » ou « privacy by default » prévus par le Règlement général sur la protection des données. Ceux-ci imposent au responsable du traitement de prendre en considération dès la conception d'application des mesures techniques et organisationnelles appropriées relatives à la protection des données et au respect de la vie privée[222]. On peut toutefois s'interroger si le Code d'instruction criminelle prévoit une telle obligation « positive » à charge des tiers.

CONCLUSIONS

La loi du 25 décembre 2016 confie d'importants pouvoirs au procureur du Roi et laisse transparaître une volonté de modifier la place réservée au juge d'instruction. Au niveau de la Cour eur. D.H., le juge d'instruction n'est pas une figure indispensable en cas d'ingérence dans le droit au respect de la vie privée par des autorités publiques. En effet, l'examen d'une

216 Art. 90*quater*, § 2, C.i.cr. Il s'agit des opérateurs et fournisseurs de communications électroniques tels que définis *supra* dans le cadre de l'identification et du repérage au sens des articles 46*bis* et 88*bis* C.i.cr.

217 Art. 90*quater*, § 4, C.i.cr.

218 Art. 90*quater*, § 2, al. 4, C.i.cr.

219 Art. 90*quater*, § 4, al. 3, C.i.cr.

220 Art. 90*quater*, § 2, al. 3 et § 4, al. 4, C.i.cr.

221 Anvers, 15 novembre 2017, R.G. n° C.1288.2017, inédit.

222 Art. 25 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (texte présentant de l'intérêt pour l'EEE), *J.O.*, L 119, 4 mai 2016, p. 1 (ci-après le règlement général sur la protection des données).

technique d'enquête dépend de toutes les circonstances, notamment dans le cadre des mesures de surveillance secrète, de : « la nature, l'étendue et la durée des mesures éventuelles, les raisons requises pour les ordonner, les autorités compétentes pour les permettre, exécuter et contrôler, le type de recours fourni par le droit interne »[223].

Par ailleurs, comme l'a rappelé la Cour de cassation, « La mission impartie au ministère public ne se réduit pas à celle d'un accusateur. Il intervient aussi au procès pour proposer au juge une solution de justice. (…) La loyauté du ministère public se présume. Des éléments précis et objectifs sont requis pour renverser cette présomption. Le principe de loyauté implique que tous les éléments recueillis par le parquet soient versés au dossier répressif et, plus particulièrement, les éléments à décharge »[224].

Si on peut admettre que la place de notre magistrat instructeur soit remise en cause, il est par contre regrettable que le législateur ne se soit pas systématiquement aligné sur la Convention de Budapest pour offrir des garanties suffisantes aux justiciables. En effet, dans le cadre de la recherche et l'extension de recherche dans un système informatique « sans but secret » ainsi que la saisie de données informatiques, les protections contre le risque d'ingérence illicite ou arbitraire sont minces. De même, certaines méthodes d'enquêtes tels le blocage de site Internet ou l'infiltration dans un contexte informatique semblent manquer de clarté. En outre, les obligations de collaboration de tiers sont fortement accentuées et les limites sont parfois peu claires que l'entreprise invoque un intérêt légitime ou qu'un suspect soit contraint de fournir un mot de passe sous peine de sanctions pénales.

Enfin que l'article 32 du Titre préliminaire du Code de procédure pénale mentionné dans les travaux parlementaires en tant que garantie en cas de violation de droits fondamentaux ne paraît pas pertinent[225]. Celui-ci permet la « mise à l'écart » des preuves obtenues irrégulièrement en cas d'atteinte au procès équitable[226]. Il ne saurait donc réparer les manquements en cas d'ingérence illicite et arbitraire dans le droit au respect de la vie privée. Nous verrons si la jurisprudence permettra de clarifier certains points et si les garanties fournies au justiciable seront en pratique effectives et non théoriques et illusoires.

223 Cour eur. D.H., 6 septembre 1978, *Gerhard Klass e.a. c. Allemagne*, série A, vol. 28, § 41.

224 Cass., 19 décembre 2012, R.G. n° P.121310.F., www.cass.be.

225 Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n° 54-1966/001, p. 61.

226 Pour une analyse détaillée, voy. F. Lugentz, *La preuve en matière pénale*, Limal, Anthemis, 2017.