Institutional Repository - Research Portal
Dépôt Institutionnel - Portail de la Recherche
researchportal.unamur.be
University of Namur

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

La collecte de preuves sur le darknet et les espaces "accessibles au public"

Forget, Catherine

Published in:
Revue de droit pénal et de criminologie

Publication date:
2019

Document Version
le PDF de l'éditeur

Link to publication

Citation for pulished version (HARVARD):
Forget, C 2019, 'La collecte de preuves sur le darknet et les espaces "accessibles au public": note sous Cour de cassation (2e ch., N.), 28 mars 2017 (extraits)', *Revue de droit pénal et de criminologie*, numéro 5, pp. 702-715.

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 04. May. 2026

Cour de cassation (2e ch., N.), 28 mars 2017

P.16.1245.F.

(extraits)

Président : M. Van Volsem, président ff,
Rapporteur : M. Francis, conseiller,
Ministère public : M. Decreus, avocat général,
Pl. : Mes H. Geinger (du barreau de cassation).

Informatique – site accessible au public sur Internet – recueil de preuves par la police – modalités – utilisation d'un alias – légalité

Les services de police peuvent rassembler toutes les preuves sur les sites accessibles au public sur Internet, de la même manière que le public peut avoir accès à ces sites et nonobstant l'application des dispositions du Code d'instruction criminelle relatives aux méthodes particulières de recherche et aux recherches et pratiques d'écoute sur Internet. À cet égard, l'utilisation d'un alias peut relever du mode normal de la consultation de pages d'Internet, sous réserve que cette utilisation ne consiste pas à endosser une identité fictive crédible et que l'alias utilisé n'est pas de nature à provoquer la commission d'une infraction[1]. (L. 5 août 1992, art. 26 ; C. i. cr., art. 8)

ARRÊT

I La procédure devant la Cour

Le pourvoi est dirigé contre un arrêt rendu le 10 novembre 2016 par la cour d'appel d'Anvers, chambre correctionnelle.

(…)

1 Voy. la note, ci-après, de Mme. C. Forget. Voy. également J. Kerkhofs et Ph. Van Linthout, *Cybercrime*, Brussel, Politeia, 2013, pp. 248 et 249.
Il est à noter que la Cour constitutionnelle, saisie d'un recours en annulation de l'article 46*sexies*, alinéa 4, du Code d'instruction criminelle, n'a pas annulé cette disposition en ce qu'elle permet, sans contrôle des autorités judiciaires, l'interaction personnelle de fonctionnaires de police, dans l'exercice de leurs missions de police judiciaire, avec une ou plusieurs personnes sur Internet, interaction qui n'a pour finalité directe qu'une vérification ciblée ou une arrestation, et ceci sans utiliser d'identité fictive crédible (C.C., arrêt du 6 décembre 2018, n° 174/2018, spéc. B.35.1 et suivants ; cette décision est publiée par extraits, ci-avant). Toutefois, dans l'espèce ici tranchée par la Cour de cassation, cette disposition n'était en tout état de cause pas applicable, dès lors qu'aucune interaction n'avait eu lieu entre suspect et policiers.

this jurisquare copy is licenced to Université de Namur- Faculté de droit

II La décision de la Cour

Sur le moyen :

1. Le moyen invoque la violation des articles 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, 15 de la Constitution, 46*quinquies*, 47*sexies*, 56*bis*, 88*ter*, 89*ter* du Code d'instruction criminelle et 32 de la loi du 17 avril 1878 contenant le titre préliminaire du Code de procédure pénale : l'arrêt condamne le demandeur du chef de vente et exportation de stupéfiants, sur la base de constatations relatives à sa présence et à son comportement sur un forum sur le « darknet » ; la police a pu procéder à ces constatations après le chargement et l'utilisation de software spécifique, de moteurs de recherche, d'un site web qui surveille avec un moniteur ces marchés du *darknet* afin d'obtenir un lien d'invitation à ce forum, de l'enregistrement à ce forum sous un alias et de la visite de ce forum ; l'arrêt décide que la police a ainsi obtenu l'accès à un lieu accessible au public et que l'instruction n'a pas été étendue à des parties de l'Internet qui sont inaccessibles au public ; le forum était uniquement accessible lorsqu'un membre de la communauté donnait un lien d'invitation à un non-membre ; le forum constituait, partant, un club privé virtuel uniquement accessible à un groupe limité de personnes et qui faisait l'objet de communications d'ordre privé, auquel la police ne pouvait obtenir l'accès que sous réserve d'une autorisation du juge d'instruction de procéder à des recherches sur le réseau ; même si un mandat pour faire des recherches sur le réseau n'était pas nécessaire pour visiter ce forum parce qu'il n'y a pas eu irruption sur le compte privé du demandeur, le fait de visiter une telle partie privée d'Internet n'est possible que s'il est satisfait aux conditions d'un contrôle visuel discret, ce qui n'était pas le cas ; à tout le moins, la police a procédé à une observation sans que les conditions légales aient été observées à cet égard ; ainsi, les éléments de preuve ont été obtenus illégalement et ne pouvaient être utilisés sans constater que l'illégalité commise n'a pas entaché la fiabilité de la preuve et que son usage n'est pas contraire au droit à un procès équitable.

2. L'article 8 du Code d'instruction criminelle dispose que la police judiciaire recherche les crimes, les délits et les contraventions, en rassemble les preuves, et en livre les auteurs aux tribunaux chargés de les punir. L'article 26, alinéas 1 et 2, de la loi du 5 août 1992 sur la fonction de police prévoit que les fonctionnaires de police peuvent toujours pénétrer dans les lieux accessibles au public ainsi que dans les biens immeubles abandonnés, afin de veiller au maintien de l'ordre public et au respect des lois et règlements de police, ainsi qu'afin d'exécuter des missions de police judiciaire.

3. Sur la base de ces dispositions, les services de police peuvent rassembler toutes les preuves sur les sites accessibles au public sur Internet, de la même manière que le public peut avoir accès à ces sites et nonobstant l'application des dispositions du Code d'instruction criminelle relatives aux méthodes particulières de recherche et aux recherches et pratiques d'écoute sur Internet. À cet égard, l'utili-

this jurisquare copy is licenced to Université de Namur- Faculté de droit

sation d'un alias peut relever du mode normal de la consultation de pages d'Internet, sous réserve que cette utilisation ne consiste pas à endosser une identité fictive plausible et que l'alias utilisé n'est pas de nature à provoquer la commission d'une infraction.

4. Un site Internet n'est pas supposé inaccessible au public du seul fait que la visite de ce site est subordonnée à des conditions d'accès purement formelles, à savoir non liées à un quelconque contrôle de contenu ou de qualité personnel. De telles conditions d'accès ne sont effectivement pas de nature à laisser croire que l'accès à ce site est limité à un cercle privé. Lorsque la police satisfait à ces conditions d'accès, elle peut visiter cette page Internet sans autorisation particulière.

5. L'arrêt décide souverainement que :

- Agora est un forum/une communauté fermé(e) sur le *Darknet* ou le *Deepweb* où notamment des drogues font l'objet d'un trafic de manière anonyme et qui peut être visité(e) uniquement sur invitation d'un membre et n'est accessible que par le biais du navigateur TOR que l'on peut librement se procurer ;
- la police a obtenu un lien d'invitation vers Agora par le biais d'un site Internet qui surveille avec un moniteur les marchés du *Darknet* et constitue un fichier automatisé ;
- les enquêteurs se sont enregistrés sous un alias ;
- la police a, au moyen d'une fonction de recherche, consulté dans Agora la page de profil et les critiques du demandeur, qui étaient consultables par tous les visiteurs d'Agora ;
- les enquêteurs n'ont, à aucun moment, eu recours à un mot de passe, un login ou une clé appartenant au demandeur ou à une autre personne.

Sur la base de ces constatations, l'arrêt a pu légalement décider que les enquêteurs ont visité un lieu accessible au public et par conséquent qu'une ordonnance d'extension de la recherche vers un système informatique qui se trouve dans un autre lieu que celui où la recherche est effectuée n'était pas requise, et qu'il n'était pas question d'un quelconque procédé de piratage dans le chef de la police.

Dans cette mesure, le moyen ne peut être accueilli.

(…)

PAR CES MOTIFS,

LA COUR

Rejette le pourvoi ;

Condamne le demandeur aux frais.

(…)

this jurisquare copy is licenced to Université de Namur- Faculté de droit

Note

La collecte de preuves sur le *darknet* et les espaces « accessibles au public »

A Contexte et résumé de l'arrêt

L'arrêt de la Cour de cassation du 28 mars 2017[1] a trait à une enquête relative à des faits de ventes de stupéfiants. Suite à une dénonciation anonyme, les services de police procédèrent à une perquisition dans un domicile. Sur les lieux, ils trouvèrent de nombreux éléments confortant leurs suspicions à savoir, une quantité importante de drogues, des sachets en plastique et autres matériels de conditionnement, des enveloppes vides et des restes de poudre. Ils trouvèrent également un ordinateur connecté à « Agora », une place de marché en ligne hébergée sur le *darknet*[2] où s'échangent notamment des drogues illicites. Après avoir pris copie des éléments pertinents du système informatique à distance, les officiers de police judiciaire s'étaient également enregistrés sur « Agora » en faisant usage du navigateur *Tor Browser*, navigateur permettant de surfer sur le réseau *Tor* de manière anonyme, et ainsi se connecter sur le *darknet*. Pour obtenir l'adresse du site, ils avaient reçu un lien d'invitation d'un membre de la communauté généré automatiquement. Une fois connectés sur cette place, ils procédèrent à des constatations relatives au profil et aux commentaires du suspect. Au terme de l'enquête, celui-ci fut poursuivi devant les juridictions pénales et condamné par la cour d'appel d'Anvers à une peine principale de quatre ans d'emprisonnement et à une peine d'amende fixée à dix-huit mille euros pour le trafic d'amphétamines (speed) et de MDMA / MDEA (XTC).

En cassation, le demandeur contestait la recevabilité des preuves recueillies sur Agora car en violation du droit au respect de la vie privée.

En effet, selon lui, cette place devait être considéré comme un « lieu privé » ou un « club virtuel » accessible à un nombre limité de personnes compte tenu des modalités d'inscription. En conséquence, les enquêteurs auraient dû obtenir l'ordonnance d'un juge d'instruction, conformément aux dispositions relatives à l'extension de recherche dans un système informatique[3] ou, à tout le moins, même à considérer qu'il n'y avait pas eu d'intrusion dans son compte privé, respecter les

1 Cass., 28 mars 2017, P.16.1245.N, www.cass.be.

2 Un réseau de type « darknet » permet en théorie de rester anonyme puisqu'il n'implique pas un partage public des adresses IP.

3 Il s'agissait de l'article 88*ter* du Code d'instruction criminelle (ci-après C. i. cr.). Cette disposition est à présent inclue dans l'article 39*bis* C. i. cr. suite à l'adoption de la loi du 25 décembre 2016 portant des modifications diverses au Code d'instruction criminelle et au Code pénal, en vue d'améliorer les méthodes particulières de recherche et certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications et créant une banque de données des empreintes vocales, *M.B.*, 17 janvier 2017.

this jurisquare copy is licenced to Université de Namur- Faculté de droit

dispositions relatives au contrôle visuel discret ou à l'observation systématique[4]. La Cour de cassation rejeta l'argument et considéra qu'Agora ne pouvait être qualifiée « d'espace non accessible au public » compte tenu des modalités purement formelles pour y pénétrer. Pour le surplus, appliquant par analogie au contexte digital les méthodes d'enquête du monde réel, la Cour rappela qu'en vertu de l'article 26 de la loi sur la fonction de police, les officiers de police judiciaire peuvent toujours pénétrer dans les lieux accessibles au public[5]. Dès lors, selon la Cour, les services de police n'avaient pas outrepassé leurs compétences de police judiciaire.

Cet arrêt nous donne l'occasion de nous pencher sur la collecte de preuves dans les espaces en ligne « accessibles au public » mais aussi sur certaines méthodes d'enquête aux délimitations parfois floues telles l'infiltration, l'enquête sous pseudonyme et l'observation systématique.

B La collecte de preuves dans les espaces virtuels « accessibles au public » : une ingérence dans le droit au respect de la vie privée ?

a) Les sources ouvertes et les espaces « accessibles au public » dans un contexte virtuel

Les sites Internet accessibles via des moteurs de recherche tels « Google » ou « Bing », sont qualifiés de « sources ouvertes » dans la mesure où tout le monde peut y avoir accès, que cet accès soit gratuit ou payant. Selon la Convention de Budapest[6], ces pages web sont consultables par les enquêteurs comme par le public, quelle que soit la localisation de ces données[7].

De manière plus nuancée, certains sites Internet nécessitent l'accomplissement de formalités pour pouvoir y accéder sans toutefois être limités à un nombre restreint de personnes ou à un cercle privé. En ce sens, dans le cadre de l'arrêt commenté, la Cour de cassation a considéré qu'une place de marché sur le *darknet*, en l'occurrence, « Agora », n'était pas inaccessible au public même si cet accès supposait l'accomplissement de certaines modalités pour pouvoir y pénétrer. En effet, selon la Cour, l'utilisation du navigateur *Tor Browser* et l'enregistrement via un lien d'invitation généré automatiquement sont des conditions d'accès purement formelles, c'est-à-dire « non liées à un quelconque contrôle de contenu ou de qualité personnel ». Et de préciser, « de telles conditions ne sont pas de nature à laisser croire que

4 Art. 46*quinquies*, 47*sexies*, 56*bis* et 89*ter* C. i. cr.

5 M. Franchimont, A. Jacobs et A. Masset, *Manuel de procédure pénale*, Bruxelles, Larcier, 2012, pp. 515-531.

6 Cette Convention offre aux États parties un cadre contraignant en matière de procédure pénale. (Convention sur la cybercriminalité, Budapest, 23 novembre 2001, *S.T.C.E.*, n° 185). Elle a récemment été ratifiée par la Belgique (voy. 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).

7 Art. 32, a) de la Convention sur la cybercriminalité, Budapest, 23 novembre 2001, *S.T.C.E.*, n° 185 ; voy. également art. 25, § 4, de la Décision du Conseil du 6 avril 2009 portant création de l'Office européen de police (Europol), *O.J. L. 121*, 15 mai 2009, pp. 37-66.

this jurisquare copy is licenced to Université de Namur- Faculté de droit

ce site est limité à un cercle privé » d'autant que les enquêteurs n'avaient pas fait usage de « fausses clés » tel un mot de passe, ou encore « hacké » le système visé[8]. Il ne pouvait donc s'agir d'une recherche ou d'une extension de recherche dans un système informatique comme le soutenait le demandeur[9].

Par analogie, dans un contexte réel, certains espaces, tels une auberge ou un bar[10], impliquent le respect de conditions pour pouvoir y pénétrer sans toutefois être qualifiés de lieux privés ou être considérés comme « inaccessibles au public ». En effet, déjà dans un arrêt du 16 mars 1842, la Cour de cassation a relevé deux sortes de lieux publics : « ceux dont l'accès est ouvert indistinctement et à toute heure à tout le monde, tels que les rues, places, etc., et ceux qui ne sont accessibles qu'à certaines personnes, à certaines heures ou sous certaines conditions »[11]. Il faut toutefois s'assurer de l'effectivité de ces conditions et vérifier si, en pratique, cet espace est limité à certaines personnes[12]. Dès lors, la destination donnée par le propriétaire importe peu, le critère retenu étant la possibilité concrète pour le public d'y avoir accès habituellement[13]. En conséquence, les clubs privés accessibles sur base d'une carte de membre doivent être considérés comme des lieux privés, sauf si une simple inscription nominative dans un registre suffit pour pouvoir y pénétrer[14]. L'accessibilité d'un lieu est donc une question de fait soumise, au besoin, à l'appréciation du juge du fond[15].

In casu, le caractère accessible du lieu *online* n'était pas réellement contestable. En revanche, on peut regretter que, en l'absence de critères prévus par la loi, la Cour de cassation n'ait pas été plus scrupuleuse quant aux critères retenus pour qualifier celui-ci[16]. En effet, comme l'indiquait la Commission de la protection de la vie privée (ci-après CPVP)[17] à propos d'un avant-projet de loi visant à légitimer l'accès des services de police à des sources du web dites « semi-publiques » du type

---

8 Dans le cadre d'une recherche de données informatiques ou d'une saisie de données informatiques, le procureur du Roi ou le juge d'instruction peut 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 ». Il s'agit, par exemple, de l'utilisation d'un logiciel malveillant ou de données biométriques telles des empreintes digitales en vue d'exploiter certaines données stockées dans un système informatique (Voy. art. 39*bis* C. i. cr., Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2016-2017, n° 1966/001, p. 22).

9 Notons que la Cour constitutionnelle a récemment annulé l'article 39*bis*, § 3, du Code d'instruction criminelle visant l'extension de recherche dans un système informatique considérant que cette mesure doit, à l'instar d'une mesure de perquisition, relever de la compétence du juge d'instruction. C.C., 6 décembre 2018, B.16.4.

10 *Doc. parl.,* Ch. repr., sess. 1990-1991, n° 1637/1, p. 44.

11 Cass., 16 mars 1842, *Pas.*, 1842, I, pp. 158-159.

12 Cass., 25 mai 1972, *Pas.*, 1972, I, p. 885.

13 L. Kennes, *Droit pénal et procédure pénale*, Malines, Kluwer, 2007 p. 17.

14 C. De Valkeneer, *Manuel de l'enquête pénale*, Bruxelles, Larcier, 2018, p. 516.

15 *Ibidem*, p. 516.

16 Dans le même sens, voy. C. Conings, « De politie op het darknet », *T. Strafr.* 2017/5, p. 331.

17 Précisons que, depuis le 25 mai 2018, la Commission de la protection de la vie privée a été remplacée par l'Autorité de protection des données.

this jurisquare copy is licenced to Université de Namur- Faculté de droit

réseaux sociaux, forums ou blogs[18], par conditions d'accès « purement formelles », il y a lieu d'entendre : « sans contrôle de l'exactitude des données et sans que cela n'empêche n'importe qui d'avoir accès »[19] et non pas, un contrôle « de contenu et de qualité personnel » comme l'a pointé la Cour de cassation.

b) L'existence d'une base légale accompagnée de garanties suffisantes

La consultation des sources ouvertes par les services de police n'est pas prévue par une loi spécifique. À l'instar d'autres méthodes d'enquête pénales, elle peut entraîner une ingérence dans le droit au respect de la vie privée des personnes concernées. En effet, en vertu de la jurisprudence de la Cour européenne des droits de l'Homme (ci-après Cour eur. D.H.), un individu dispose du droit au respect de la vie privée et ce, même dans un espace public[20]. À cet effet, la Cour eur. D.H. s'attache à déterminer « ce qu'un individu est raisonnablement en droit d'attendre quant au respect de sa vie privée » sans toutefois lui reconnaître un facteur nécessairement décisif[21]. À titre illustratif, l'accès de la police aux informations sur un abonné liées à une adresse IP, entraîne une ingérence dans le droit au respect de la vie privée, et ce même si cette personne est connectée à un réseau public. La Cour eur. D.H. prend en effet en considération le fait qu'en se connectant, cette personne s'attend à rester anonyme et à ce que ses données restent confidentielles[22]. Néanmoins, le droit au respect de la vie privée n'est pas absolu[23]. Pour être conforme à la Convention européenne des droits de l'Homme, toute ingérence doit poursuivre un but légitime tel que la sécurité nationale, mais aussi s'inscrire dans le respect des critères de légalité, nécessité et proportionnalité en vue de se prémunir contre les risques d'atteintes illicites ou arbitraires des pouvoirs publics[24]. À cet égard, la Cour eur. D.H. examine l'affaire dans son ensemble et vérifie si les motifs invoqués sont pertinents et suffisants et si la mesure paraît proportionnée aux buts légitimes poursuivis à la lumière des garanties offertes par la disposition soumise à son contrôle[25].

---

18 C.P.V.P., avis n° 13/2015 du 13 mai 2015 sur l'avant-projet de loi portant dispositions diverses – modifications de la loi portant création d'un organe de recours en matière d'habilitations de sécurité, de la loi sur la fonction de police et de la loi du 18 mars 2014 relative à la gestion de l'information policière (CO-A-2015-019) (ci-après avis n° 13/2015).

19 Point 27 de l'avis n° 13/2015.

20 Cour eur. D.H., *von Hannover c. Allemagne*, n° 59320/00, 24 juin 2004, § 68.

21 Cour eur. D.H., *P.G. ET J.H. c. Royaume-Uni*, n° 44787/98, 25 septembre 2001, § 57.

22 Cour eur. D.H., *Benedik c. Slovénie*, n° 62357/14, 24 avril 2018, § 117. Dans le cadre de cet arrêt, la Cour eur. D.H. a examiné la question de l'ingérence dans le droit au respect de la vie privée à la lumière des attentes raisonnables subjectives de l'intéressé. Selon la Cour, lors de l'échange de fichiers contenant du matériel pornographique via le réseau *Razorback*, le requérant espérait, sous un angle subjectif, que cette activité soit confidentielle et que son identité ne soit pas révélée. De plus, la Cour eur. D.H. indique que le fait de ne pas avoir caché son adresse IP dynamique, en supposant qu'il soit possible de faire, ne peut pas être un facteur décisif dans l'appréciation du critère des attentes raisonnables d'un point de vue objectif. À cet égard, elle constate que la question n'est clairement pas de savoir si le demandeur aurait pu raisonnablement dissimuler son adresse IP dynamique, mais s'il aurait pu raisonnablement s'attendre à ce que son adresse IP dynamique reste confidentielle.

23 Art. 8.2 de la Convention européenne des droits de l'Homme.

24 *Ibidem*.

25 Cour eur. D.H., *Z c. Finlande*, n° 22009/93, 25 février 1997.

this jurisquare copy is licenced to Université de Namur- Faculté de droit

En l'occurrence, la Cour de cassation n'a pas clairement tranché la question d'une éventuelle ingérence dans le droit au respect de la vie privée du demandeur. Elle s'est en effet limitée à constater que les conditions pour y pénétrer n'étaient « pas de nature à laisser croire » que cette place de marché en ligne était réservée à un cercle privé.

Au-delà du cas d'espèce, on peut toutefois considérer, compte tenu de la jurisprudence précitée que la collecte de données relative à un individu à des fins de poursuites pénales, peut constituer une ingérence dans le droit au respect de la vie privée, et ce même si les informations le concernant sont publiées dans un espace accessible au public.

Dès lors, concernant la base légale permettant aux autorités répressives de consulter les données pertinentes, la Cour de cassation s'est fondée sur l'article 26 de la loi sur la fonction de police. Cette disposition permet aux services de police de pénétrer[26], autrement dit accéder physiquement[27], dans les lieux qui leur sont légalement accessibles, à savoir, les lieux accessibles au public, les immeubles abandonnés et les établissements hôteliers ou autres établissements de logement[28]. Ils peuvent exercer cette compétence à des fins administratives[29] mais aussi judiciaires[30], c'est-à-dire, 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[31]. Pour le surplus, l'article 26 de la loi sur la fonction de police implique, pareillement à d'autres actes de police judiciaire tels la saisie[32], le contrôle d'identité[33] ou encore, la fouille de personnes[34], le respect de certaines garanties. En effet, la pénétration dans un lieu suppose l'existence d'une infraction, qu'elle soit ou non déjà constatée, ou d'indices qu'une infraction va être commise[35]. Autrement dit, les enquêteurs ne peuvent procéder à des recherches exploratoires[36] ou à une fouille de données dans l'espoir de trouver la preuve d'une infraction[37]. De plus, les officiers de police judiciaire agissant d'initiative, ont l'obligation d'in-

---

26 Dès lors, un policier observant attentivement des plantes dans un jardin depuis le domaine public ou procédant à des constatations depuis l'extérieur grâce à l'entrebâillement de la porte n'effectue pas une perquisition (Cass., 10 janvier 1995, P.94.1030.N. Pour un commentaire voy. L. Arnou, « Het betreden van de woning als noodzakelijke vereiste voor het bestaan van woonstschennis », *A.J.T.*, 1995-1996, pp. 354-357).

27 L. Kennes, *op. cit.*, p. 17.

28 Cette base légale avait déjà été suggérée par la doctrine. À ce propos, voy. J. Kerkhofs et P. Van Linthout, « Cybercrime », *Politeia*, 2013, ainsi que C. Conings et P. Van Linthout, « Sociale media – Een nieuwe uitdaging voor politie en justitie », *Panopticon*, 2012, vol. 3.

29 Art. 26, § 1er, de la loi du 5 août 1992 sur la fonction de police.

30 Art. 26, § 2, de la loi du 5 août 1992 sur la fonction de police.

31 Art. 8 C. i. cr. et art. 15 de la loi sur la fonction de police.

32 Art. 35 et suivants C. i. cr.

33 Art. 34 de la loi du 5 août 1992 sur la fonction de police.

34 Art. 28 de la loi du 5 août 1992 sur la fonction de police.

35 C. De Valkeneer, *Manuel de l'enquête pénale*, Bruxelles, Larcier, 2018, p. 515.

36 *Ibidem.*

37 Il est souvent fait mention de l'interdiction d'une recherche exploratoire dans le cadre de la saisie des données informatiques et de la recherche dans un système informatique. Voy. à ce propos : Cour eur. D.H., *Vinci construction et GMT Génie civil et services c. France*, 2 avril 2014, n° 63629/10, §§ 78-79.

this jurisquare copy is licenced to Université de Namur- Faculté de droit

former le procureur du Roi des recherches effectuées dans un délai et selon les modalités fixées par directive[38]. Cette obligation n'est ni substantielle ni prescrite à peine de nullité[39]. Elle vise à conforter l'autorité et la responsabilité du procureur du Roi quant à la conduite de l'information qu'il dirige et, partant, à assurer l'efficacité de celle-ci[40].

En l'espèce, on peut se demander si ces garanties suffisent à éviter le risque d'ingérences illicites ou arbitraires des autorités répressives. En effet, comme le recommandait la CPVP, il faudrait adapter la législation si l'on souhaite que des fonctionnaires de police puissent « visiter les espaces virtuels accessibles au public après enregistrement, et pour ainsi dire faire de la surveillance et des patrouilles sur Internet »[41]. Elle mettait l'accent sur le risque de confusion avec une méthode particulière de recherche telles une infiltration ou une observation systématique en cas de prise de contact « avec des cibles »[42].

C Les enquêtes à l'aide d'une « identité fictive crédible » ou d'un « pseudonyme »

Dans le cadre de l'arrêt commenté, les enquêteurs avaient fait usage d'un pseudonyme pour pouvoir se connecter à « Agora » sans toutefois procéder à une infiltration informatique. Précisons dès lors les distinctions entre ces différentes méthodes.

a) L'infiltration informatique suppose une interaction

L'infiltration informatique permet au procureur du Roi d'autoriser les services de police à entretenir des contacts sur Internet, avec une ou plusieurs personnes, « sous une identité fictive ou non »[43]. Le critère retenu est donc le but d'interaction avec un internaute pendant une certaine durée, à savoir, trois mois au maximum, sans préjudice du renouvellement[44]. Remarquons à ce propos que l'article 46*sexies* C. i. cr. ne s'applique pas en cas de contacts ponctuels entre un agent et un suspect en vue d'effectuer une vérification ciblée afin de s'assurer qu'il ne s'agit pas d'un plaisantin ou pour fixer un rendez-vous et procéder à son arrestation[45]. Néanmoins, en ce cas, les agents ne peuvent endosser une identité fictive crédible[46]

38 Art. 28*ter*, § 2, al. 1er, C. i. cr.
39 Cass., 20 octobre 2015, P.15.0789.N, *Pas.*, 2015/10, pp. 2379-2383.
40 *Ibidem.*
41 Point 27 de l'avis n° 13/2015.
42 Point 32 de l'avis n° 13/2015.
43 Art. 46*sexies*, § 1er, C. i. cr.
44 Art. 46*sexies*, § 2, C. i. cr.
45 Art. 46*sexies*, § 1er, al. 4, C. i. cr. Les travaux parlementaires précisent que l'arrestation doit être un objectif à court terme (« finalité directe »). Des interactions personnelles qui servent, par exemple, à collecter des éléments de preuve et qui ne doivent conduire qu'ensuite à une arrestation ne sont donc pas visées (Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n° 54-1966/001, p. 39).
46 Art. 46s*exie*s, § 1er, al. 4, C. i. cr.

this jurisquare copy is licenced to Université de Namur- Faculté de droit

mais peuvent interagir de manière anonyme puisqu'ils ne doivent pas indiquer leur qualité de policier[47].

L'infiltration informatique exige le respect des critères de nécessité et de subsidiarité mais aussi, l'existence d'indices sérieux que les personnes infiltrées commettent ou commettraient des infractions pouvant donner lieu à un emprisonnement correctionnel principal d'un an ou à une peine plus lourde[48]. En outre, la commission d'infractions comme échanger des fichiers pédopornographiques via des réseaux *peer-to-peer* ou envoyer des messages sur un forum extrémiste sur lequel on nie l'holocauste[49], suppose l'autorisation du procureur du Roi[50]. Enfin, l'agent ne peut se rendre coupable de provocation[51] ou faire usage d'un profil fictif explicite, trompeur ou provocant[52], au risque de violer irrémédiablement les droits de la défense du suspect et ainsi, rendre les poursuites irrecevables[53].

Dans l'arrêt commenté, il ne pouvait s'agir d'une infiltration informatique compte tenu de l'absence d'interactions entre le suspect et les autorités policières. De surcroît, conformément à l'article 46*sexies*, § 1er, al. 4, C. i. cr., les policiers auraient pu interagir ponctuellement avec le suspect en vue de s'assurer de la vente effective de stupéfiants sans tomber dans le champ d'application de l'infiltration informatique ou de la consultation des sources ouvertes accessibles au public. En ce cas, la limite entre les différentes méthodes peut paraître assez floue puisque comme le souligne la Commission de la protection de la vie privée, cette exception « apparaît pour le moins énigmatique »[54]. Elle s'interrogeait sur la nécessité de clarifier cette disposition et qu'elle soit intégrée soit dans le Code d'instruction criminelle ou soit dans la loi sur la fonction de police[55].

b) L'enquête sous pseudonyme : une absence d'interaction

L'utilisation d'un alias sur Internet permet aux services de police de collecter des preuves de manière anonyme sans attirer l'attention d'un suspect éventuel. En revanche, dans un contexte réel, en principe et sous réserve de certaines exceptions telles la technique du leurre ou la dissimulation, les officiers de police en service doivent pouvoir être identifiés en toutes circonstances[56]. À cette fin, ils sont en effet tenus de porter une plaque nominative apposée de manière visible

47 Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n° 54-1966/001, p. 38.
48 Art. 46*sexies*, § 1er, C. i. cr.
49 Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n° 54-1966/001, p. 41.
50 Art. 46*sexies*, § 3, al. 2, C. i. cr.
51 Précisons que, selon la Cour de cassation, il y a provocation lorsque, dans le chef de l'auteur, l'intention délictueuse est directement née ou est renforcée, ou est confirmée par l'intervention d'un fonctionnaire de police ou d'un tiers agissant à la demande expresse de ce fonctionnaire alors que l'auteur voulait y mettre fin (Cass., 28 mai 2014, *Pas.*, 2014/5, pp. 1336-1347).
52 Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n° 54-1966/001, p. 36.
53 Art. 30, al. 2, du Titre préliminaire du Code de procédure pénale.
54 C.P.V.P., avis n° 21/2016 du 18 mai 2016, pp. 31-32, pt. 45.
55 *Ibidem*, pt. 48.
56 Art. 41, § 1er, al. 1er, de la loi sur la fonction de police.

this jurisquare copy is licenced to Université de Namur- Faculté de droit

et lisible à un endroit déterminé sur leur uniforme[57]. Toutefois, le chef de corps, le commissaire général, le directeur général ou leur délégué peuvent, pour certaines interventions, décider de remplacer la plaquette nominative par un numéro d'intervention[58]. Lorsque les services de police interviennent en habits civils à l'égard d'une personne, ils doivent porter un brassard indiquant de manière visible et lisible le numéro d'intervention dont ils sont titulaires[59].

Sur Internet, il en va tout autrement puisque, comme le précise la Cour de cassation « l'utilisation d'un alias peut relever du mode normal de la consultation de pages d'Internet, sous réserve que cette utilisation ne consiste pas à endosser une identité fictive plausible et que l'alias utilisé n'est pas de nature à provoquer la commission d'une infraction ». L'utilisation d'un alias en l'absence d'interaction n'est certes pas une infiltration au sens de l'article 46*sexies* C. i. cr. Cette mesure semble par contre proche de l'observation systématique *online* par exemple lorsque les services de police scrutent pendant une certaine durée le comportement d'une personne ciblée sur Internet à l'aide d'un logiciel leur permettant de filtrer les données.

D L'observation systématique dans un contexte informatique

Sur Internet, la surveillance d'une personne ciblée ou d'un lieu particulier pourrait être qualifiée d'observation systématique au sens de l'article 47*sexies*, § 1er, C. i. cr. En effet, l'observation systématique peut être définie comme une observation « par un fonctionnaire de police, d'une ou de plusieurs personnes, de leur présence ou de leur comportement, ou de choses, de lieux ou d'événements déterminés ». Elle est dite « systématique » en raison de sa durée à savoir, plus de cinq jours consécutifs ou plus de cinq jours non consécutifs répartis sur une période d'un mois ou, en raison de l'utilisation de moyens techniques ou, en raison de son caractère international, ou encore, si elle est exécutée par des unités spécialisées de la police fédérale[60]. Une telle mesure peut être mise en œuvre par les services de police après autorisation du procureur du Roi si les nécessités de l'enquête l'exigent et si d'autres moyens d'investigation ne semblent pas suffire à la manifestation de la vérité[61]. Elle est par nature secrète puisqu'elle est mise en œuvre à l'insu des personnes concernées[62]. Cette méthode particulière de recherche se distingue de l'observation « non systématique » laquelle relève de la compétence générale des services de police, s'exerçant à des occasions déterminées, par

57 Art. 41, § 1er, al. 2, de la loi sur la fonction de police.
58 Art. 41, § 1er, al. 3, de la loi sur la fonction de police.
59 Art. 41, § 1er, al. 4, de la loi sur la fonction de police.
60 Art. 47*sexies*, § 2, C. i. cr.
61 Art. 47*sexies*, § 2, al. 1er, C. i. cr.
62 C. De Valkeneer, *Manuel de l'enquête pénale*, Bruxelles, Larcier, 2018, p. 358.

this jurisquare copy is licenced to Université de Namur- Faculté de droit

exemple lorsqu'un policier « en civil » épie des personnes organisant une manifestation sans autorisation[63].

Une observation effectuée à l'aide de moyens techniques suppose une condition supplémentaire puisqu'elle ne peut être autorisée qu'en présence d'indices sérieux d'infractions de nature à entraîner un emprisonnement correctionnel principal d'un an ou une peine plus lourde[64]. Par moyen technique, il y a lieu d'entendre « une configuration de composants qui détecte des signaux, les transmet, active leur enregistrement et enregistre les signaux »[65]. Il s'agit par exemple, d'un « GPS » ou d'une caméra, qu'elle soit installée par les services de police ou directement par un tiers[66], sans préjudice de la possibilité pour ce dernier de collaborer avec les autorités en divulguant les images enregistrées[67]. En revanche, ne constituent pas un moyen technique, un appareil photo sauf s'il est utilisé pour avoir une vue dans un domicile ou dans un local utilisé à des fins professionnelles ou encore dans la résidence d'un avocat ou d'un médecin dans les cas prévus par l'article 56*bis*, al. 2, C. i. cr., à savoir, le contrôle visuel discret[68]. Dans le même sens, une caméra thermique est considérée par la Cour de cassation, comme un appareil permettant des photographies thermiques de sorte qu'il ne s'agit pas d'un moyen technique au sens de l'article 47sexies, § 1er, al. 3, C. i. cr.[69]. Sont également exclus de cette définition, les appareils ne comprenant pas un certain degré de sophistication, par exemple des jumelles, un appareil photo muni d'un téléobjectif classique ou encore un caméscope[70]. Précisons à toutes fins utiles que selon la Cour de cassation, des critères subjectifs tels que le caractère accessoire, superficiel ou occasionnel de l'observation ou le degré d'ingérence dans la vie privée sont sans pertinence pour examiner le caractère systématique de l'observation en tant que méthode particulière de recherche[71].

Dans le cadre de l'arrêt commenté, on aurait pu considérer qu'il s'agissait d'une observation systématique compte tenu de l'utilisation du navigateur *Tor Browser*. Toutefois, ce navigateur ne vise pas à détecter, à transmettre ou à enregistrer des signaux mais permet de surfer de manière anonyme sur le réseau *Tor* de sorte qu'on ne pourrait considérer qu'il s'agit d'un moyen technique au sens de l'article 47*sexies*, § 1er, al. 3. En revanche, si les officiers de police judiciaire avaient fait usage d'un logiciel espion filtrant de manière continue les commentaires pu-

63 *Doc. parl.*, Ch. repr., sess. 2001-2002, n° 50-1688/001, p. 30 ; voy. également M. Beys, *Quels droits face à la police ?*, Mons-Liège, Couleur livres-J&D Éditions, 2014, pp. 323 et s.
64 Art. 47*sexies*, § 2, al. 2, C. i. cr.
65 Art. 47*sexies*, § 1er, al. 3, C. i. cr.
66 Bruxelles, 13 mai 2011, *J.L.M.B.*, 2012, p. 461.
67 La Cour de cassation a considéré que le visionnage *a posteriori* par les services de police d'une caméra de surveillance placée par la Ville de Charleroi afin de pouvoir identifier un véhicule impliqué dans un accident ne constitue pas une observation systématique (Cass., 16 mars 2016, P.15.1602.F, *Rev. dr. pén. crim.*, 2017/5, pp. 482-492, notes L. Kerzmann).
68 Art. 47*sexies*, § 1er, al. 4, C. i. cr.
69 Cass., 19 novembre 2013, P.13.1779.N.
70 C. De Valkeneer, *Manuel de l'enquête pénale*, Bruxelles, Larcier, 2018, p. 363.
71 Cass., 20 juin 2017, P.15.0464.N., *Lar. Cass.*, 2018/9, p. 206.

this jurisquare copy is licenced to Université de Namur- Faculté de droit

bliés sur un site ou sur un réseau social, une approche plus nuancée aurait pu être retenue dans la mesure où le moyen technique employé permettrait de détecter des signaux. En tout état de cause, en l'espèce, on peut se demander si du fait de sa durée, l'acte de recherche critiqué ne constituait pas une observation systématique de plus de cinq jours consécutifs ou de plus de cinq jours non consécutifs répartis sur une période d'un mois. Toutefois, il ressort de l'arrêt de la cour d'appel soumis à la censure de la Cour de cassation que l'observation avait été effectuée *a posteriori* sur les pages Internet relatives au profil suspect et aux commentaires, de sorte qu'en raison de ce décalage dans le temps, il ne s'agissait pas d'une telle observation systématique.

Conclusion

Sur le *darknet*, la commercialisation de produits illicites tels des médicaments, des stupéfiants, des armes à feu, de la fausse monnaie ou encore des images et vidéos pédopornographiques, s'effectue avec une simplicité déconcertante. En effet, l'anonymat des utilisateurs et l'usage de monnaies virtuelles, comme le *bitcoin*[72], facilitent la commission d'infractions et complexifient les poursuites pénales dans un contexte exempt de frontières nationales. En 2017, des enquêtes menées par Europol, le F.B.I. et la police néerlandaise, ont permis la fermeture de trois des plus grandes places de marché en ligne, ALPHABAY, Hansa et RAMP[73]. Néanmoins, plutôt qu'une fermeture définitive, ces démantèlements ont incité une migration des utilisateurs vers d'autres places de marché nouvellement créées ou d'autres plateformes plus sécurisées notamment en raison d'un chiffrement plus élevé des communications.

En dépit de ces difficultés, l'arrêt de la Cour de cassation du 28 mars 2017 nous rappelle que les espaces hébergés sur le *darknet* sont aussi susceptibles d'être qualifiés d'espaces « accessibles au public » et, dès lors, d'être consultés par les officiers de police judiciaire de la même manière qu'ils le sont par le public. Si la consultation des sources ouvertes par les autorités répressives est une pratique courante qui, *a priori*, ne semble pas problématique, le sujet pourrait encore à l'avenir faire débat. En effet, certains logiciels permettent de filtrer un ensemble très important de données disponibles sur des sources ouvertes et sont utilisés à des fins judiciaires ou de renseignement. À titre illustratif, la police de Liège a annoncé s'être dotée de programmes informatiques permettant de scruter les

72 Le *bitcoin* est une monnaie virtuelle dite « cryptographique ». Elle est indépendante de l'autorité et du contrôle des pouvoirs publics et utilisée comme moyen de paiement par voie électronique. Elle dispose d'un cours qui évolue en permanence, à l'instar des monnaies officielles reconnues par les États, et peut être achetée ou vendue au cours du jour (Corr. Liège, division Liège (15e ch.), 18 janvier 2018, *J.L.M.B.*, 2018/12, pp. 564-567). À ce propos, voy. S. Royer, « Bitcoins in het Belgische strafrecht en strafprocesrecht », *R.W.*, 2016-2017/13, pp. 483-501.

73 European Monitoring Centre for Drugs and Drug Addiction and Europol, « Drugs and the darknet: Perspectives for enforcement, research and policy », EMCDDA-Europol Joint publications, Publications Office of the European Union, 2017, Luxembourg.

this jurisquare copy is licenced to Université de Namur- Faculté de droit

réseaux sociaux afin de détecter des éventuels troubles à l'ordre public. On peut se demander si l'utilisation de ces logiciels ne devrait pas constituer une observation systématique au sens de l'article 47s*exies*, § 1er, C. i. cr. plutôt qu'une consultation de sources ouvertes au sens de l'article 26 de la loi sur la fonction de police, et donc impliquer le respect d'un cadre procédural plus strict.

Catherine Forget,
Avocate au Barreau de Bruxelles (JusCogens),
chercheuse au CRIDS (Université de Namur)

this jurisquare copy is licenced to Université de Namur- Faculté de droit