Quelles garanties entourent la saisie de données informatiques et l'exploitation d'un système de données informatiques ?, note sous Cour de cassation (2e ch.), 11/02/2015

Forget, Catherine

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

Publication date:
2015

Document Version
le PDF de l'éditeur

JURISPRUDENCE

Cass. (2e ch.), 11 février 2015

Note d'observations de Catherine Forget[1]

SAISIE DE DONNÉES INFORMATIQUES – RECHERCHE DANS UN SYSTÈME INFORMATIQUE – PREUVES – INFORMATION – INSTRUCTION

DATA SEIZURE – COMPUTER SEARCH – EVIDENCE – INVESTIGATION

La loi du 28 novembre 2000 relative à la criminalité informatique a introduit des nouvelles méthodes de recherche dans le Code d'instruction criminelle, en ce compris la saisie de données et la recherche dans les systèmes informatiques. Le législateur a conçu ces dispositions légales de manière large, afin qu'elles puissent s'adapter aux changements technologiques. Cependant, les mesures adoptées ne sont pas précisément définies par le droit national et sont source d'incertitude légale. Dans un arrêt du 11 février 2015, la Cour de cassation a tranché ces controverses. La Cour a, tout d'abord, revu la distinction entre saisie de données et recherche dans un système informatique. Ensuite, la Cour a reconnu la compétence des services de police pour effectuer une recherche dans un système informatique dans le cadre d'une saisie de données, sans intervention automatique d'un juge d'instruction. Cette interprétation proposée par la Cour de cassation requière certaines précisions.

• • •

The informatics criminal law of 28 November 2000 introduced in the Code of Criminal Procedure news methods of investigation, including data seizure and computer and network search. The legislator has drafted these provisions in broad terms so that they can adapt to technological change. However, these measures are not strictly defined by national law, they are the source of legal controversy. In a judgment of 11 February 2015, the Court of Cassation ruled on these controversies. First, the Court reconsidered the distinction between data seizure and computer search. Second, the Court recognized the competence of the police to operate a network search in the context of data seizure, without the intervention of an investigating judge. The interpretation of the Court needs some clarification.

Siège : Fr. Close (prés. sect.), B. Dejemeppe, P. Cornelis, G. Steffens et Fr. Roggen (cons.)

Av. gén. : D. Vandermeersch

Plaid. : Me P. Vanlersberghe

R.G. n° P.14.1739.F

I. LA PROCÉDURE DEVANT LA COUR

Les pourvois sont dirigés contre un arrêt rendu le 10 octobre 2014 par la cour d'appel de Bruxelles, chambre correctionnelle.

Le demandeur A.A. invoque deux moyens dans un mémoire annexé au présent arrêt, en copie certifiée conforme.

Le 28 janvier 2015, l'avocat général Damien Vandermeersch a déposé des conclusions au greffe.

À l'audience du 11 février 2015, le conseiller Benoît Dejemeppe a fait rapport et l'avocat général précité a conclu.

[1] Avocate au barreau de Bruxelles, chercheuse au CRIDS (Université de Namur).

II. LA DÉCISION DE LA COUR

A Sur le pourvoi d'E.V.D.

Les formalités substantielles ou prescrites à peine de nullité ont été observées et la décision est conforme à la loi.

B. Sur le pourvoi d'A.A.

Sur le premier moyen

1. Le moyen est pris de la violation des articles 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, 15 et 22 de la Constitution, 28*bis*, § 3, 39*bis*, § 2, 88*ter*, §§ 1 et 3, et 89 du Code d'instruction criminelle. Le demandeur soutient en substance que la prise de connaissance par les enquêteurs des messages enregistrés sur le téléphone portable du coprévenu relève d'une recherche informatique qui devait être autorisée par le juge d'instruction et qu'en décidant du contraire, l'arrêt viole les dispositions précitées.

2. En application des articles 28*bis*, § 3, et 35 du Code d'instruction criminelle, le procureur du Roi est autorisé à saisir toutes choses susceptibles de servir à la manifestation de la vérité et à demander au suspect de s'expliquer sur les choses saisies qui lui sont représentées.

En vertu de l'article 39*bis*, § 2, lorsque le procureur du Roi découvre dans un système informatique des données stockées qui sont utiles pour les mêmes finalités que celles prévues pour la saisie, mais que la saisie du support n'est néanmoins pas souhaitable, ces données, de même que les données nécessaires pour les comprendre, sont copiées sur des supports qui appartiennent à l'autorité.

L'article 88*ter*, § 1er, prévoit que, lorsque le juge d'instruction ordonne une recherche dans un système informatique ou une partie de celui-ci, cette recherche peut être étendue vers un système informatique ou une partie de celui-ci qui se trouve dans un autre lieu que celui où la recherche est effectuée aux conditions que la loi détermine.

3. Un téléphone portable est un dispositif assurant, en exécution d'un programme, un traitement automatisé de données et permettant notamment l'envoi et la réception de télécommunications électroniques.

L'exploitation de la mémoire d'un téléphone portable, dont les messages qui y sont stockés sous la forme de *sms*, est une mesure découlant de la saisie, laquelle peut être effectuée dans le cadre d'une information sans autres formalités que celles prévues pour cet acte d'enquête.

4. Lorsque la saisie du support du système informatique ne se justifie pas, le procureur du Roi peut prendre copie des données intéressant l'information sur des supports appartenant à l'autorité. L'accès à ce dispositif implique que les policiers chargés de l'enquête peuvent procéder à l'analyse des données stockées dans la mémoire.

La prise de connaissance et la saisie d'un message après son arrivée à destination sur un téléphone portable est étranger au champ d'application de l'article 88*ter*, § 1er, qui vise l'hypothèse de l'extension d'une recherche ordonnée par le juge d'instruction vers un système informatique ou une partie de celui-ci qui se trouve dans un autre lieu que celui où la recherche est effectuée.

5. La cour d'appel a considéré que les enquêteurs s'étaient bornés à consulter les données reprises dans le téléphone portable du coprévenu qui avait été saisi, sans qu'il ressorte d'aucune pièce du dossier ou allégation vraisemblable que ces policiers avaient dû mener une recherche étendue à partir et au-delà dudit téléphone.

6. En décidant, sur le fondement de ces considérations, qu'aucune condition ou forme particulière ne devait présider à l'accomplissement du devoir d'enquête critiqué par le demandeur, l'arrêt justifie légalement sa décision.

7. Pour le surplus, la violation des articles 8 de la Convention, 15 et 22 de la Constitution, est entièrement déduite de celle, vainement invoquée, des dispositions précitées du Code d'instruction criminelle.

8. Le moyen ne peut être accueilli.

Sur le second moyen

9. L'arrêt condamne le demandeur à une peine unique constituée d'un emprisonnement d'un an assorti d'un sursis pour la durée d'épreuve maximale et d'une amende de trois cents euros. Le moyen soutient que cette peine s'avère inhumaine au sens de l'article 3 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales. Selon le demandeur, la cour d'appel n'a pas tenu compte de ce qu'il n'a été reconnu coupable que d'un fait isolé, à la différence

de ceux imputés au coprévenu, ni des répercussions qu'une telle peine aura sur son activité professionnelle, notamment du point de vue disciplinaire.

10. En vertu de cette disposition, nul ne peut être soumis à la torture ni à des peines ou traitements inhumains ou dégradants.

Toute condamnation pénale peut être ressentie comme inhumaine ou dégradante. L'appréciation subjective de sa sévérité ne permet toutefois pas de la considérer comme telle au sens de la Convention. Ne tombent, en effet, sous l'application de l'interdiction prévue par l'article 3, que les peines dont ce caractère apparaît particulièrement grave compte tenu non seulement de l'ensemble des circonstances propres à la cause et à la personnalité du condamné, mais aussi de la nature de la peine, ainsi que du contexte et des modalités prévisibles de son exécution.

11. Le moyen ne soutient ni que, telles que définies par le législateur, l'incrimination et la mesure des peines applicables sont, en l'espèce, contraires aux exigences de l'article 3, ni que l'arrêt inflige au demandeur une sanction non prévue à l'article 550*bis*, § 6, du Code pénal, sur le fondement duquel elle a été prononcée. Il ne fait pas davantage grief aux juges d'appel de ne pas avoir indiqué de manière concrète et précise les raisons pour lesquelles ils ont choisi la nature et le taux des peines.

12. Le juge détermine souverainement la peine en fonction des éléments propres à la cause et notamment de la gravité des faits et de la personnalité de la personne poursuivie.

13. En fixant la peine dans les limites de la loi et de la Convention et en indiquant les raisons concrètes et précises de sa décision, la cour d'appel n'a pas infligé au demandeur un traitement inhumain ou dégradant.

14. Le moyen ne peut être accueilli.

Le contrôle d'office

15. Les formalités substantielles ou prescrites à peine de nullité ont été observées et la décision est conforme à la loi.

Par ces motifs,

la Cour,

Rejette les pourvois ;

Condamne chacun des demandeurs aux frais de son pourvoi.

Note d'observations[1]

Quelles garanties entourent la saisie de données informatiques et l'exploitation d'un système de données informatiques ?

La loi du 28 novembre 2000 relative à la criminalité informatique[2] introduit dans le Code d'instruction criminelle (ci-après C.i.cr.) de nouvelles méthodes d'enquête et notamment la saisie de données informatiques et la recherche de données informatiques. Le législateur a rédigé ces dispositions en termes larges afin qu'elles puissent s'adapter aux évolutions technologiques[3]. Toutefois, les mesures n'étant pas strictement définies par le droit interne, elles sont la source de controverses juridiques. Dans un arrêt du 11 février 2015[4], la Cour de cassation tranche certains points liés aux mesures en cause. Premièrement, la Cour reconsidère la distinction entre recherche de données informatiques et extension de recherche de données informatiques. Deuxièmement, elle reconnaît la compétence des services de police pour exploiter un système informatique dans le cadre d'une saisie de données informatiques et donc, sans l'intervention d'un juge d'instruction. L'interprétation de la Cour mérite certains éclaircissements. Reprenons dès lors les dispositions légales en cause avant de nous plonger dans le cœur de l'arrêt. Ensuite, nous examinerons la procédure relative à la saisie de données informatiques au regard de la jurisprudence de la Cour européenne des droits de l'homme afin de mettre en perspective les garanties balisant l'article 39*bis* du C.i.cr.

I. LA SAISIE DE DONNÉES INFORMATIQUES ET LA RECHERCHE DE DONNÉES INFORMATIQUES

L'article 39*bis* du C.i.cr. ne donne pas de définition de la saisie de données informatiques. Le paragraphe premier dudit article se réfère toutefois aux dispositions relatives à la saisie pénale. La Cour de cassation définit la saisie pénale comme une « mesure conservatoire par laquelle l'autorité compétente, selon la loi et à propos d'une infraction, soustrait une chose à la libre disposition de son propriétaire ou de son possesseur et, en vue de la manifestation de la vérité, de la confiscation, de la restitution ou de la sécurité des intérêts civils, et la place sous elle »[5]. Une mesure de saisie vise dès lors l'appropriation temporaire de choses ayant servi à commettre une infraction, produites par une infraction, ou encore d'avantages patrimoniaux tirés directement d'une infraction[6]. L'article 39*bis* du C.i.cr. s'applique spécifiquement à la saisie de choses « immatérielles » n'impliquant pas forcément la saisie d'un support[7]. L'enquêteur peut se limiter à la simple copie des données stockées notamment si la saisie entraîne des conséquences disproportionnées par exemple, si elle empêche le fonctionnement du système informatique d'une entreprise[8]. Par ailleurs, les données peuvent être bloquées si leur copie s'avère impossible

1 Catherine Forget. Avocate au Barreau de Bruxelles, Chercheuse au CRIDS (Université de Namur).
2 Loi du 28 novembre 2000 relative à la criminalité informatique, *M.B.*, 3 février 2001.
3 Exposé des motifs, *Doc. parl.*, Ch. repr., 0213/001, p. 12.
4 Cass., 11 février 2015, R.G. n° P.14.1739.F, www.cass.be.
5 Cass., 25 février 2003, *Pas.*, 2003, p. 412.
6 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.
7 Art. 39*bis*, § 6, du C.i.cr.
8 *Doc. parl.*, Ch. repr., n° 50-213/1, p. 21.

pour des questions techniques ou pratiques[9]. Il s'agit alors d'une « mise sous scellés » des données[10] effectuée dans l'attente d'une copie ultérieure[11]. Les données contraires à l'ordre public et aux bonnes mœurs ou risquant d'endommager le système informatique – un virus par exemple – peuvent également être retirées du système informatique[12]. En outre, les autorités compétentes doivent s'assurer de la confidentialité et de l'intégrité des données saisies au moyen de techniques appropriées[13]. Ils ont, enfin, l'obligation d'informer le responsable du système informatique des données saisies et doivent fournir un résumé des données copiées, rendues inaccessibles ou retirées[14].

La saisie de données informatiques relève de la compétence du procureur du Roi et peut être exécutée dès le stade de l'information[15]. La recherche de données informatiques, par contre, relève en vertu de l'article 88*ter* du C.i.cr. de la compétence exclusive du juge d'instruction sauf exceptions strictement définies par le droit interne[16]. À l'instar de la saisie de données informatiques, la loi ne donne pas de définition de la recherche de données informatiques. Il s'agit selon nous d'une exploitation du système informatique par l'enquêteur dépassant la notion de « mesure conservatoire » que constitue la saisie[17]. En outre, la recherche de données informatiques peut être étendue à d'autres systèmes informatiques si les données se trouvent dans un autre lieu que celui où la recherche est effectuée[18]. L'extension de la recherche de données informatiques, pour être mise en œuvre, suppose le respect de deux conditions cumulatives. Premièrement, la mesure doit être nécessaire à la manifestation de la vérité en fonction de l'infraction visée dans l'ordonnance de recherche. Deuxièmement, soit l'exécution d'autres mesures serait disproportionnée, soit il existe un risque de perdre certains éléments de preuve. L'ordonnance autorisant l'extension de la recherche doit déterminer le système concerné par la mesure. Celle-ci doit également être limitée aux systèmes informatiques accessibles aux personnes autorisées à les utiliser[19] afin d'éviter une intrusion illimitée dans les systèmes informatiques[20]. Cette distinction entre recherche de données informatiques et extension de cette recherche est récemment remise en

9 Art. 39*bis*, § 4, du C.i.cr.

10 O. Klees, F. Roggen et D. Vandermeersch, « Les saisies en matière pénale et référé pénal », in *Droit pénal et procédure pénale*, Malines, Kluwer, 2006, p. 71.

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

12 *Doc. parl.*, Ch. repr., n° 50-213/1, pp. 20-21.

13 Art. 39*bis*, § 6, du C.i.cr.

14 Art. 39*bis*, § 5, du C.i.cr.

15 Art. 35 du C.i.cr.

16 O. Klees, F. Roggen et D. Vandermeersch, « Les saisies en matière pénale et référé pénal », in *Droit pénal et procédure pénale*, Malines, Kluwer, p. 67.

17 *A contrario*, certains auteurs considèrent 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.

18 Art. 88*ter*, § 1^er^, du C.i.cr.

19 Art. 88*ter*, § 2, du C.i.cr.

20 *Doc. parl.*, Ch. repr., n° 50-213/1, p. 22.

cause par la Cour de cassation dans un arrêt du 11 février 2015[21].

II. L'ARRÊT DE LA COUR DE CASSATION DU 11 FÉVRIER 2015

Dans un arrêt du 11 février 2015, la Cour de cassation tranche certains points de controverses relatifs à la saisie de données informatiques, à la recherche de données informatiques et à l'extension de cette recherche. Les faits peuvent être résumés comme suit. Un téléphone portable est saisi par des agents de police. Il appert que ces derniers ont consulté les données stockées et notamment les messages stockés dans la mémoire du téléphone portable sur base de l'article 39*bis* du C.i.cr. régissant la saisie de données informatiques. Or, selon les intéressés, la consultation des données stockées est une recherche de données informatiques au sens de l'article 88*ter* du C.i.cr. et relève de la compétence du juge d'instruction.

La Cour ne souscrit toutefois pas aux arguments des requérants. Celle-ci 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 ». Selon la Cour de cassation, la recherche de données informatiques au sens de l'article 88*ter* du C.i.cr. ne vise donc pas la consultation de données stockées dans un système informatique. Celle-ci tomberait dans le champ d'application de la saisie de données informatiques et peut être exécutée dès le stade de l'information. Et la Cour de compléter en soulignant que l'article 88*ter* du C.i.cr. doit être limité à « l'hypothèse de l'extension d'une recherche ordonnée par le juge d'instruction vers un système informatique ou une partie de celui-ci qui se trouve dans un autre lieu que celui où la recherche est effectuée »[22].

Ce faisant, premièrement, la Cour étend les pouvoirs des enquêteurs, ces derniers pouvant désormais exploiter les données stockées dans un système informatique, en l'occurrence un téléphone portable, sans l'intervention d'un juge d'instruction. Or, il est piquant de constater que l'article 39*bis,* § 2 du C.i.cr. autorise le procureur du Roi de saisir les données « lorsqu'il les découvre » sans pour autant lui conférer le pouvoir d'effectuer une recherche au sens « consultation » dans le système visé. Selon nous, le législateur ne prévoit donc pas la possibilité d'exploiter les données stockées sur un téléphone portable ou un ordinateur sans l'autorisation d'un magistrat[23]. Ce raisonnement est conforme à la *ratio legis* de l'article 35 du C.i.cr. selon lequel la saisie de données informatiques est une mesure conservatoire visant à emporter, copier voire bloquer des données pouvant servir à la manifestation de la vérité. Cette dernière ne peut donc s'entendre comme une mesure « d'exploitation » d'un système informatique. Cette analyse rejoint également l'interprétation du rapport explicatif de la Convention sur la cybercriminalité du Conseil de l'Europe[24] selon lequel

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

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

23 En ce sens voy. L. Kennes, « Les actes de recherche de la preuve et les modes de preuve », in *Manuel de la preuve en matière pénale*, Kluwer, Malines, 2009, p. 238. Notons que la prise de connaissances des données de (télé)communications en « cours de transmission » relève des articles 90*ter* et suivants du C.i.cr. À cet égard voy. 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 ; C. De Valkeneer, « Les infractions en matière d'écoutes, de prise de connaissance et d'enregistrement de communications et de télécommunications », in *Les infractions – Volume 5 : les infractions contre l'ordre public* (sous la dir. de H.-D. Bosly et C. De Valkeneer), Bruxelles, Larcier, 2013, pp. 399 et s. ; D. Vandermeersch, *Les recherches en matière de téléphonie et de (télé)communications*, Bruxelles, Éd. du Jeune Barreau, 2006, pp. 49 et s.

24 Loi du 3 août 2012 portant assentiment à la Convention sur la cybercriminalité, faite à Budapest le

la « saisie » implique de « réaliser ou conserver une copie de ces données ou informations »[25] *a contrario* donc de l'interprétation effectuée par la Cour de cassation. Notons néanmoins que l'arrêt susmentionné s'inscrit dans une analyse déjà développée par la Cour de cassation selon laquelle les enquêteurs peuvent se saisir de données téléphoniques, de messages stockés dans un répondeur téléphonique dans le cadre d'une visite domiciliaire sans devoir solliciter l'intervention d'un juge d'instruction[26]. Toutefois, comme nous le verrons ci-après, l'intrusion dans un « système informatique » n'a pas la même incidence que la consultation d'un répondeur téléphonique de sorte que la Cour aurait pu s'écarter de cette analyse.

Deuxièmement, dans l'arrêt du 11 février 2015, la Cour ne distingue plus les notions de recherche et d'extension de recherche de données informatiques. Selon celle-ci, l'article 88*ter* du C.i.cr. n'a trait qu'à « l'extension » de la recherche. Pourtant, la différenciation entre les deux notions n'est pas dénuée de fondement. En effet, le législateur constatant l'importance des systèmes en réseaux, permet d'étendre la recherche de données informatiques à d'autres systèmes[27]. Les travaux préparatoires précisent en ces termes : « lorsque les systèmes informatiques pour lesquels une recherche semble nécessaire sont dispersés en différents endroits, plusieurs mandats de perquisition ou de saisie doivent être délivrés »[28]. Ainsi, le juge d'instruction est tenu de localiser préalablement le ou les systèmes faisant l'objet d'une recherche de données informatiques empêchant tout « hacking externe » des enquêteurs[29]. La Cour de cassation, en ne distinguant plus la recherche de données informatiques *stricto sensu* de l'extension de la recherche vide partiellement l'article 88*ter* du C.i.cr. de son contenu. Sur base d'une définition très large de la saisie de données informatiques, la Cour limite l'article 88*ter* du C.i.cr. et s'en réfère à l'article 39*bis* du C.i.cr. avec pour conséquence d'assouplir les conditions permettant d'exploiter un système informatique légalement saisi. En tout état de cause, l'arrêt du 11 février 2015 a une incidence certaine sur les droits fondamentaux et en particulier sur les garanties prévues en cas d'ingérence dans le droit à la vie privée. La consultation des données stockées dans un système informatique peut s'avérer particulièrement intrusive de sorte que, selon certains auteurs, un rapprochement peut être effectué entre mesure de perquisition et intrusion dans un système informatique[30].

23 novembre 2001, *M.B.*, 21 novembre 2012.

25 Rapport explicatif de la Convention sur la cybercriminalité, STE n° 185, n° 197.

26 Notons que selon certains auteurs, cette interprétation rejoint l'analyse déjà développée par la Cour de cassation selon laquelle les enquêteurs peuvent se saisir de données téléphoniques, de messages stockés dans un répondeur téléphonique dans le cadre d'une visite domiciliaire (Cass., 27 octobre 1999, *J.T.*, 2000, p. 522). À cet égard, voy. J. De Codt, *Des nullités de l'instruction et du jugement*, Bruxelles, Larcier, 2006, p. 51 ; F. Lugentz et D. Vandermeersch, « Chapitre 2 – Les choses susceptibles d'être saisies », in *Saisie et confiscation en matière pénale*, Bruxelles, Bruylant, 2015, p. 140.

27 C. Meunier, « La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique », *Rev. dr. pén.*, 2001, p. 663.

28 *Doc. parl.*, Ch. repr. 1999-2000, n° 50-213/1, p. 22.

29 *Doc. parl.*, Ch. repr. 1999-2000, n° 50-213/1, p. 23. Notons que 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*, 2001/1, pp. 60-81.

30 Voy. not. C. Meunier, « La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique », *Rev. dr. pén.*, 2001/7-8, pp. 663-664 ; T. Incalza, « Strafonderzoek in het digitale tijdperk : zoeking en inbeslagneming », *Jura Falc.*, 2010-2011/2, pp. 329-383 ; B. Losdyck, « Les saisies et perquisitions de matériel informatique : les "garde-fous" entourant leur mise en œuvre », *R.D.T.I.*, 2013/3, n° 52.

III. LA CONSULTATION DES DONNÉES STOCKÉES DANS UN SYSTÈME INFORMATIQUE ET LA PERQUISITION

Les travaux préparatoires de la loi du 28 novembre 2000 relative à la criminalité informatique définissent le système informatique comme « tout système permettant le stockage, le traitement ou la transmission de données »[31]. Selon la directive 2002/58/CE dite directive « vie privée et communications électroniques »[32], un système informatique entre dans le champ d'application de l'article 8 de la Convention européenne des droits de l'homme[33]. Celui-ci comprend en effet des données relevant de la vie privée des personnes notamment des données personnelles, des données professionnelles ou encore des données médicales. Le système informatique est un espace virtuel pouvant être perçu par son propriétaire comme un lieu d'activité « au sein duquel un individu a le sentiment d'être dans l'intimité, en sécurité contre l'immixtion de personnes contre sa volonté, indépendamment de la durée et de l'intensité d'utilisation »[34]. Cette approche rejoint la définition du domicile privé de la Cour européenne des droits de l'homme[35]. L'intrusion dans ce système « privé » peut donc *a priori* rejoindre la notion de perquisition au sens plus classique.

Le rapprochement entre perquisition et exploitation de données stockées dans un système informatique trouve également écho au sein de hautes instances internationales. Ainsi, selon le Rapport explicatif de la Convention sur la cybercriminalité, la pénétration dans un système informatique et la consultation de ce système suppose une mesure de perquisition. Le rapport relève en effet que « les enquêteurs perquisitionnent ou inspectent ces données ainsi enregistrées et saisissent ou emportent physiquement des données tangibles. La collecte des données a lieu pendant la perquisition et porte sur les données existant à ce moment-là »[36]. Le texte souligne également que

31 *Doc. parl.,* Ch. repr., n° 50-213/1, p. 3. À titre informatif, le Conseil de l'Europe définit le système informatique comme « un dispositif composé de matériel et de logiciels, conçus pour le traitement automatisé des données numériques. Il peut comprendre des moyens d'acquisition, de restitution et de stockage des données. Il peut être isolé ou connecté à d'autres dispositifs similaires au sein d'un réseau ». Voy. rapport explicatif de la Recommandation R(89) 9 du Conseil de l'Europe, éd. du Conseil de l'Europe, Strasbourg, 1990, § 23.

32 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 (ci-après directive 2002/58/CE).

33 Le considérant 24 de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques 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 ».

34 Cour eur. D.H., arrêt *Niemietz c. la République fédérale d'Allemagne*, 16 décembre 1992, *Rev. trim. D.H.*, 1993, p. 467 et *J.T.*, 1994, p. 65, note E. Jakhian et P. Lambert, « Les perquisitions dans les cabinets d'avocat ».

35 Voy. not. Cour eur. D.H., arrêt *Société Colas Est et autres c. France*, 16 avril 2002, n° 37971/97, § 41 ; Cour eur. D.H., arrêt *Van Rossem c. Belgique*, 9 décembre 2004, n° 41872/98. Notons qu'une interprétation similaire à celle de la Cour européenne des droits de l'homme est retenue par la Cour constitutionnelle. La Cour de cassation a opté de manière constante pour une définition plus restrictive de la notion mais étant donné que les dispositions de la Convention priment sur celles de la Constitution, nous rejoignons L. Kennes lorsqu'il écrit qu'« il est donc évident que toute personne bénéficie de la protection de l'article 8 de la Convention, telle qu'interprétée par la Cour européenne des droits de l'homme ». Voy. L. Kennes, *Manuel de la preuve en matière pénale,* Malines, Kluwer, 2009, p. 24.

36 Rapport explicatif de la Recommandation R(89) 9 du Conseil de l'Europe, éd. du Conseil de l'Europe, Strasbourg, 1990, § 186.

« L'emploi du mot classique "perquisitionner" traduit l'idée de l'exercice par l'État d'un pouvoir coercitif et montre que le pouvoir visé dans cet article est analogue à la perquisition classique. "Perquisitionner" veut dire rechercher, lire, inspecter ou examiner des données, et inclut aussi les notions de recherche de données et d'examen de données »[37]. En outre, la Convention sur la cybercriminalité récemment ratifiée par la Belgique[38], suggère aux États membres d'adopter des « mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à accéder d'une façon similaire à un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées »[39].

Par conséquent, le rapprochement entre la perquisition et l'intrusion dans un système informatique pour y exploiter des données stockées traduit, en tout état de cause, l'importance de l'ingérence dans la vie privée d'une personne. De plus, cette « analogie » plaide pour l'existence de garanties suffisantes en cas d'exploitation d'un système informatique. Pourtant, la Cour de cassation dans l'arrêt du 11 février 2015 prive les personnes de certaines garanties visant à limiter le risque de consultation illicite ou arbitraire des données stockées dans un système informatique. Cet arrêt et de manière plus générale, l'article 39*bis* du C.i.cr. peine à s'intégrer adéquatement avec la jurisprudence de la Cour européenne des droits de l'homme selon laquelle une ingérence dans la vie privée suppose en tout état de cause le respect de certaines garanties.

IV. L'ARTICLE 39*BIS* DU C.I.CR., UNE MESURE PRÉVUE PAR LA LOI ET PROPORTIONNÉE ?

Outre les controverses tranchées dans l'arrêt de la Cour de cassation du 11 février 2015, l'article 39*bis* du C.i.cr. soulève certaines inquiétudes si l'on s'en tient à la procédure applicable. Le système informatique est en effet protégé par l'article 8 de la Convention européenne des droits de l'homme[40]. Toutefois cet article n'est pas absolu. Une ingérence est conforme aux droits fondamentaux à la condition d'être « prévue par la loi », « nécessaire » dans une société démocratique, à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui et proportionnée par rapport à l'objectif poursuivi[41]. Ces critères sont autant d'éléments susceptibles de conférer des garanties efficaces contre les atteintes arbitraires aux droits substantiels[42].

En effet, tout d'abord, une mesure est « prévue par la loi » si elle est « prévisible » et « accessible »[43]. Celle-ci doit avoir une base en droit interne suffisamment précise et détaillée pour permettre à chacun de connaître les conditions et les circonstances dans lesquelles les autorités publiques pourraient s'ingérer dans ce droit[44]. En l'occurrence, l'analyse de la Cour de cassation illustre l'absence de clarté des dispositions légales en cause et donc d'une poten-

37 *Ibidem*, § 191.

38 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.

39 Art. 19, § 1er, de la Convention de Budapest sur la cybercriminalité, Conseil de l'Europe, 23 novembre 2001.

40 Considérant 24 de la directive 2002/58/CE.

41 Art. 8, § 2, de la Convention européenne des droits de l'homme.

42 Cour eur. D.H., arrêt *Liberty et autres c. Royaume-Uni*, 1er juillet 2008, n° 58243/00, § 69.

43 Cour eur. D.H., arrêt *Bykov c. Russie*, 10 mars 2009, n° 4378/02.

44 Cour eur. D.H., arrêt *Huvig c. France*, 24 avril 1990, n° 11105/84, § 32 ; Cour eur. D.H., arrêt *Kruslin c. France*, 24 avril 1990, n° 11801/85, § 33.

tielle violation de l'article 8, § 2, de la Convention européenne des droits de l'homme.

Ensuite, toujours au regard de l'article 8, § 2, de la Convention, l'atteinte la vie privée doit être proportionnée au regard de l'objectif poursuivi. Celle-ci ne peut excéder ce qui est strictement nécessaire pour atteindre l'objectif visé. La Cour de Strasbourg examine ce critère en tenant compte de la marge d'appréciation laissée aux États membres[45]. Celle-ci vérifie si la législation et la pratique offrent des garanties suffisantes et adéquates contre les risques d'abus et d'arbitraire[46]. *In casu,* en vertu de l'article 39*bis,* § 5, du C.i.cr., l'enquêteur est tenu de faire un résumé au responsable du système informatique des données copiées et rendues inaccessibles suite à la « recherche effectuée dans le système ». On ne peut que s'étonner de l'usage du terme « recherche » par le législateur étant donné que la recherche de données informatiques est réglementée par l'article 88*ter* du C.i.cr. conformément à ce que nous avons exposé *supra*.

En tout état de cause, le procureur du Roi doit en principe établir dans un procès-verbal un résumé des données saisies. En ce sens, le cadre légal s'inscrit dans la lignée de la jurisprudence de la Cour européenne des droits de l'homme. Celle-ci s'oppose en effet à la saisie « massive et indifférenciée » de données informatiques[47]. Les enquêteurs doivent déterminer les données saisies et ne peuvent copier l'entièreté d'un disque dur sans critères limitatifs. Ainsi, dans l'arrêt *Vinci*, la Cour de Strasbourg précise que doit être établi « un inventaire suffisamment précis, indiquant le nom des fichiers, leur extension, leur provenance et leur empreinte numérique (…) ainsi qu'une copie des documents saisis »[48]. Au niveau du droit interne, il est toutefois loisible de se demander si le « résumé » établi *a posteriori* par le procureur du Roi permet à l'intéressé d'identifier de manière suffisante les données saisies et si les enquêteurs établissent effectivement ce résumé *in concreto*.

De plus, lorsque les enquêteurs consultent les données stockées soit avant la saisie de données informatiques *stricto sensu*, l'article 39*bis* du C.i.cr. n'impose pas de limiter préalablement la « fouille » à laquelle ils désirent procéder. Ces derniers disposent d'un blanc-seing quant à la saisie des données stockées dans le système informatique pour autant qu'ils disposent des autorisations nécessaires et ne doivent uniquement les identifier postérieurement. Or, selon la Cour européenne des droits de l'homme, la consultation des données stockées dans un système informatique doit être localisée. Les enquêteurs doivent s'efforcer de « circonscrire leurs fouilles et de ne procéder qu'à des saisies en rapport avec l'objet de leur enquête »[49]. À cet égard, le juge Zupancic dans une opinion concordante à laquelle se rallie le juge Gaetano fait le parallèle entre une recherche dans un système informatique assortie d'une saisie de ces données et une mesure de perquisition : « Lorsqu'est recherché un élément de preuve spécifique dans un lieu concret, la règle a toujours été bien sûr que la police ne peut fouiller que là où cet élément est susceptible d'être trouvé. Par exemple, si elle devait rechercher un fusil, elle ne serait pas

45 S. Greer, « La marge d'appréciation : interprétation et pouvoir discrétionnaire dans le cadre de la Convention européenne des droits de l'homme », *Dossiers sur les droits de l'homme*, n° 17, Strasbourg, Conseil de l'Europe, 2000, pp. 9 et s.

46 Cour eur. D.H., arrêt *Miailhe c. France*, 25 février 1993, n° 12661/87, § 37, série A, n° 256-C ; Cour eur. D.H., arrêt *Funke c. France,* 25 février 1993, n° 10828/84, § 56, série A, n° 256-A ; Cour eur. D.H., arrêt *Crémieux c. France*, 25 février 1993, n° 11471/85, § 39.

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

48 Cour eur. D.H., arrêt *Vinci construction et GMT Génie Civil et services c. France*, 2 avril 2014, n° 63629/10 et 60567/10, §76.

49 *Ibidem.*

autorisée à fouiller les petits tiroirs où l'arme ne pourrait être cachée. Si cette règle était enfreinte, les éléments recueillis, par exemple des stupéfiants retrouvés sur les lieux, ne pourraient être versés au dossier par l'effet de la règle de l'exclusion. Cette règle connaît toutefois une exception. Si, lorsqu'elle recherche légitimement un élément de preuve particulier, la police tombe par inadvertance sur une pièce prouvant qu'une autre infraction a été commise, le principe dit des « objets bien en vue » (*plain view doctrine*) entre en jeu : tout objet trouvé parce qu'il était bien en vue est une preuve admissible de l'infraction en question ou d'une autre. Le complément subjectif au principe des objets bien en vue est ce qu'il est convenu d'appeler la « découverte par inadvertance » (*inadvertent discovery*), c'est-à-dire que la police doit démontrer que la découverte de l'élément en question n'était pas prévue et qu'elle s'est donc faite « par inadvertance »[50]. Dès lors, les autorités compétentes ne peuvent consulter un système informatique sans but précis et mener une pêche à l'information dans l'espoir de trouver la preuve d'une infraction[51]. Or, l'article 39*bis* du C.i.cr. permet la pêche à l'information dans le sens où il n'oblige pas les enquêteurs à limiter la consultation du système à certains fichiers ou certaines données nécessaires dans le cadre de l'enquête. L'article précité peine donc à répondre aux exigences de proportionnalité de l'article 8, § 2, de la Convention interprété à la lumière de la jurisprudence de la Cour de Strasbourg.

Enfin, selon la Cour européenne des droits de l'homme, la régularité d'une mesure de saisie doit pouvoir être appréciée *in concreto* devant un juge afin de permettre aux intéressés d'une part, d'apprécier l'opportunité de la saisie et d'autre part, d'obtenir l'effacement et/ou la récupération des données saisies[52]. Or, le Code d'instruction criminelle ne prévoit pas la possibilité de requérir l'effacement des données copiées. Il permet tout au plus à la personne préjudiciée de demander la récupération du support[53]. Se pose dès lors la question de la durée de conservation des données saisies par les enquêteurs sur base de l'article 39*bis* du C.i.cr. et la crainte d'une conservation illimitée. En outre, si le support de la personne est saisi, par exemple l'ordinateur, celui-ci ne pourra déterminer exactement quelles sont les données saisies. En pratique, le procès-verbal mentionnant la saisie du support n'indique pas, à notre connaissance, la saisie de données informatiques à moins que ces données soient exploitées à titre de preuve. Ce dernier ne sera donc pas en mesure d'en contester l'opportunité devant un juge à l'inverse de ce que préconise la Cour de Strasbourg.

CONCLUSION

La consultation de données stockées dans un système informatique est une mesure de contrainte emportant une atteinte certaine

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

51 Pour un parallèle en matière fiscale, voy. V. Dauginet et V. Vercauteren, « Fiscale huiszoekingen », *T.F.R.*, 2014/1-2, n° 453, pp. 76-87.

52 Cour eur. D.H., arrêt *Vinci construction et GMT Génie Civil et services c. France*, 2 avril 2014, n° 63629/10. « §. 78. La Cour relève ensuite que, pendant le déroulement des opérations en cause, les requérantes n'ont pu ni prendre connaissance du contenu des documents saisis, ni discuter de l'opportunité de leur saisie. Or, de l'avis de la Cour, à défaut de pouvoir prévenir la saisie de documents étrangers à l'objet de l'enquête et *a fortiori* de ceux relevant de la confidentialité qui s'attache aux relations entre un avocat et son client, les requérantes devaient pouvoir faire apprécier *a posteriori* et de manière concrète et effective leur régularité. Un recours, tel que celui ouvert par l'article L.450-4 du Code de commerce, devait leur permettre d'obtenir, le cas échéant, la restitution des documents concernés ou l'assurance de leur parfait effacement, s'agissant de copies de fichiers informatiques ».

53 Art. 28*sexies* du C.i.cr.

dans les droits fondamentaux des personnes. Elle suppose en effet l'intrusion dans un système informatique où s'exerce la vie privée de l'intéressé. Dans l'arrêt du 11 février 2015, la Cour de cassation facilite l'exploitation des données stockées dans un système informatique dans le sens où la mesure relève désormais de la compétence du procureur du Roi. Cette interprétation, bénéfique quant au risque de déperdition de la preuve, emporte certains risques de consultation illicite et arbitraire des systèmes informatiques. Par ailleurs, la distinction entre recherche de données informatiques et l'extension de cette recherche n'existe plus, la Cour interprétant de manière très large le terme « saisie ». Pourtant, les instances internationales et certains auteurs de doctrine préconisent une certaine prudence en cas d'exploitation de données informatiques et créent un parallèle avec la perquisition d'un domicile soulignant l'importance de l'ingérence dans la vie privée. Outre les éléments soulevés par la Cour dans l'arrêt du 11 février 2015, l'article 39*bis* du C.icr. présente plusieurs lacunes au regard de l'article 8, § 2, de la Convention européenne des droits de l'homme quant aux exigences de légalité et de proportionnalité. La mesure pourrait être considérée comme n'étant pas suffisamment claire et prévisible vu les controverses tranchées par la Cour de cassation. Par ailleurs, en l'état, les enquêteurs peuvent procéder à une « pêche à l'information » une fois le support légalement saisi. Ces derniers n'ont pas l'obligation de se limiter à la consultation de certains fichiers liés à l'enquête. De plus, les intéressés ne peuvent identifier les données consultées et copiées. Ils disposeront tout au plus d'un résumé mentionnant les données saisies sans autre précision. Enfin, une fois la saisie effectuée, aucune procédure ne permet explicitement au responsable du système informatique de requérir l'effacement des données copiées laissant planer certaines craintes quant au risque de conservation pour une période indéterminée. L'article 39*bis* du C.i.cr. a, par conséquent, de nombreuses raisons d'être remis en cause au regard de l'article 8, § 2, de la Cour européenne des droits de l'homme.

Catherine Forget