Le cryptage et le droit au silence

Auteur : Nizet, Justine
Promoteur(s) : Franssen, Vanessa
Faculté : Faculté de Droit, de Science Politique et de Criminologie
Diplôme : Master en droit à finalité spécialisée en droit pénal (aspects belges, européens et internationaux)
Année académique : 2017-2018
URI/URL : http://hdl.handle.net/2268.2/4946

LIÈGE université
Droit, Science Politique & Criminologie
Département de Droit

Le cryptage et le droit au silence

Justine NIZET

Travail de fin d'études
Master en droit à finalité spécialisée en droit pénal
Année académique 2017-2018

Recherche menée sous la direction de :
Madame Vanessa FRANSSEN
Chargée de cours

RESUME

Cet exposé aura pour sujet « Le cryptage et le droit au silence ». Quelle sera la place du droit au silence à l'ère numérique?

La question qui se pose principalement est celle de savoir si les données cryptées sont protégées par le droit au silence, si elles peuvent l'être ou au contraire, s'il existe une obligation de parler ou de collaborer.

Pour répondre à cette question, il conviendra d'envisager ces deux notions au travers de différents systèmes juridiques, principalement, le Conseil de l'Europe, l'Union européenne et la Belgique.

REMERCIEMENTS

Je souhaite remercier Madame Vanessa Franssen pour ce sujet passionnant qui m'a poussé à me dépasser intellectuellement ainsi que pour ses conseils pour améliorer ce travail.

Je remercie également ma famille et mes amis pour le soutien qu'ils m'apportent.

TABLE DES MATIERES

1. INTRODUCTION

Cet exposé aura pour sujet « Le cryptage et le droit au silence ». Quelle sera la place du droit au silence à l'ère numérique?

La question qui se pose principalement est celle de savoir si les données cryptées sont protégées par le droit au silence, si elles peuvent l'être ou au contraire, s'il existe une obligation de parler ou de collaborer. Pour répondre à cette question centrale, plusieurs étapes seront nécessaires.

Dans cette analyse, le champ d'application personnel du droit au silence se limitera principalement aux personnes physiques. En effet, les personnes morales semblent avoir un statut plus particulier que les personnes physiques, la protection qui doit leur être accordée sera différente[1]. Dans ce contexte, limiter le champ d'application personnel de l'analyse aux personnes physiques permettra une meilleure compréhension ainsi qu'une meilleure précision.

Premièrement, il s'agira de déterminer la problématique et de voir quelle est l'interaction qui existe entre le droit au silence et le cryptage.

Deuxièmement, le droit au silence et le privilège contre l'auto-incrimination, souvent invoqués ensemble, seront définis au travers de divers systèmes juridiques: le pacte international relatif aux droits civils et politiques, le Conseil de l'Europe, l'Union européenne et le droit belge. Les sanctions applicables en cas de violations de ces droits seront également envisagées.

Troisièmement, le concept de cryptage sera défini et exposé en procédant de manière assez similaire au point précédant. Le cryptage sera appréhendé au travers du Conseil de l'Europe, de l'Union européenne et du droit belge.

Ensuite, il s'agira de confronter les concepts et de savoir si les données cryptées sont protégées par le droit au silence. Pour essayer de prendre position, la jurisprudence et la législation belges seront examinées.

Le sujet étant plutôt controversé, les palliatifs utilisés par les Etats seront analysés ainsi que leurs avantages et inconvénients.

Finalement, une conclusion permettra de faire le point à propos des éléments exposés.

2. QUESTIONNEMENT CENTRAL

Quel est le lien entre le cryptage et le droit au silence? La question se pose, lorsque dans une affaire pénale, les enquêteurs ont besoin d'avoir accès aux données cryptées d'un suspect. Ce suspect peut-il se retrancher derrière le droit au silence ou devra-t-il fournir la clé de cryptage pour accéder aux données et par conséquent, aux preuves pouvant l'incriminer?

Pour pouvoir répondre à cette question, il conviendra tout d'abord de définir et cerner les concepts utilisés.

---

[1] Directive (UE) 2016/343 du Parlement européen et du Conseil du 9 mars 2016 portant renforcement de certains aspects de la présomption d'innocence et du droit d'assister à son procès dans le cadre des procédures pénales, considérants 13 à 15, *J.O.U.E.*, L 65 du 11 mars 2016, p.3.

3. LE DROIT AU SILENCE ET LE PRIVILÈGE CONTRE L'AUTO-INCRIMINATION

Dans la présente section, le droit au silence et le privilège contre l'auto-incrimination seront analysés. Comment sont-ils définis, quelles sont leurs composantes, quelles sont les sources qui les mentionnent?

Que se passerait-il, par exemple, si vous étiez interrogé sur des faits qui constituent une infraction? Devriez-vous répondre à toutes les questions qui vous sont posées? Il convient de répondre par la négative.

Les adages latins « *nemo tenetur seipsum accusare* » et « *nemo tenetur prodere seipsum* » signifient que nul n'est tenu de s'accuser lui-même. « *La présomption d'innocence comprend le droit de ne pas contribuer à sa propre incrimination, qui inclut le droit de se taire et le droit de ne pas être contraint de produire des preuves à charge. La maxime « Nul n'est tenu de s'accuser lui-même » (Nemo tenetur prodere seipsum) s'applique. L'accusé peut refuser de répondre à des questions et de produire des preuves* »[2]. Notons que le droit au silence et le privilège contre l'auto-incrimination sont généralement invoqués ensemble. Cependant, ce privilège est plus large que le droit au silence, ce dernier étant une facette de l'interdiction contre l'auto-incrimination[3].

Pourquoi est-il important de garantir ces droits à l'inculpé? Personne n'a envie de s'incriminer lui-même, forcer quelqu'un à le faire serait totalement inhumain et contre nature[4]. Dans le même ordre d'idée, l'inculpé ne peut pas être entendu sous serment[5].

Il s'agit de garantir le droit à un procès équitable, en ce sens que ce sont les autorités de poursuite qui doivent fournir les preuves à charge[6]. Il convient d'éviter les erreurs judiciaires et d'atteindre les buts de l'article 6 de la Convention européenne des droits de l'homme[7]. En effet, « *[t]oute personne accusée d'une infraction est présumée innocente jusqu'à ce que sa culpabilité ait été légalement établie* »[8] et c'est à l'accusation qu'il revient de prouver la culpabilité d'un accusé[9]. La question de la coercition abusive des autorités sera examinée ultérieurement.

Pour appréhender de la manière la plus complète possible le droit au silence, il s'agira d'analyser différents systèmes juridiques, en partant du niveau international pour arriver au niveau national, à savoir la Belgique. En effet, chacun des niveaux supérieurs pourra avoir

---

[2] Commission européenne, Livre vert sur la présomption d'innocence, COM(2006) 174 final du 26.4.2006, p.8.

[3] Commission européenne, Livre vert sur la présomption d'innocence, COM(2006) 174 final du 26.4.2006, p.8.

[4] S. LAMBERIGTS, « The Privilege against Self-Incrimination: a Chameleon of Criminal Procedure », *NJECL*, 2016, vol. 7, p. 424.

[5] O. MICHIELS, P*rocédure pénale - notes sommaires et provisoires*, 5e éd., Presses Universitaires de Liège, 2016-2017, p. 327.

[6] M. FRANCHIMONT, A. JACOBS et A. MASSET, *Manuel de procédure pénale*, 4ème éd., Bruxelles, Larcier, 2012, p. 1138.

[7] S. LAMBERIGTS, *op. cit.*, pp. 425-426.

[8] Convention de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950, approuvée par la loi du 13 mai 1955, art. 6 §2, *M.B.*, 19 août 1955, *err.*, 29 juin 1961.

[9] D. VANDERMEERSCH, *Eléments de droit pénal et de procédure pénale*, 5e éd., Bruxelles, la Charte, 2015, p. 765.

une influence sur le niveau inférieur et il est important de voir comment le droit au silence est envisagé par chaque niveau.

A. Le Pacte international relatif aux droits civils et politiques

L'article 14.3 du Pacte international relatif aux droits civils et politiques accorde des garanties aux personnes accusées d'une infraction pénale. Le point g) leur permet de « *(...) ne pas être forcée de témoigner contre elle-même ou de s'avouer coupable* »[10].

Ce pacte, adopté par l'Assemblée générale des Nations Unies, « *a pour vocation de s'appliquer dans l'ensemble du monde et ses dispositions sont d'application directe en droit interne* »[11]. Malgré le fait qu'il soit applicable directement en droit interne, « *[c]omme de nombreuses dispositions du Pacte international font double emploi avec celles de la Convention européenne des droits de l'homme et qu'aucune juridiction internationale n'est habilitée à en sanctionner la violation, celles-ci sont plus rarement invoquées devant les juridictions belges* »[12]. Toutefois, en analysant les arrêts rendus par la Cour constitutionnelle[13] et la Cour de cassation[14], on constate que le Pacte est invoqué à de nombreuses reprises.

B. Le Conseil de l'Europe

La Cour européenne des droits de l'homme ainsi que la Convention jouent un rôle essentiel sur les systèmes juridiques des États membres du Conseil de l'Europe[15].

L'article 6 de la Convention européenne des droits de l'homme concerne le droit au procès équitable. Force est de constater qu'il ne fait aucune mention du droit au silence. Toutefois, cela ne signifie pas que la Convention européenne des droits de l'homme ne reconnaît pas ce droit. En effet, la Cour interprète les articles dans sa jurisprudence[16]. Elle s'est exprimée maintes fois concernant le droit au silence.

- Reconnaissance des droits

L'arrêt Funke est le premier arrêt qui reconnaît expressément que l'article 6 de la Convention inclut le droit de se taire et de ne pas contribuer à sa propre incrimination[17].

---

[10] Pacte international relatif aux droits civils et politiques, fait à New York le 19 décembre 1966, approuvé par la loi du 15 mai 1981, art. 14, *M.B.*, 6 juillet 1983.

[11] D. Vandermeersch, *op. cit.*, p. 26.

[12] D. Vandermeersch, *op. cit.*, p. 26.

[13] A titre d'exemples concernant le droit au silence: C.A., 25 janvier 2001, n°4/2001; C.C., 13 mars 2008, n °50/2008.
Arrêts récents concernant le Pacte: C.C., 22 décembre 2016, n°168/2006; C.C., 15 juin 2017, n°76/2017.

[14] A titre d'exemples: Cass. (1ère ch.), 1er octobre 2009, n° D.07.0024.N; Cass. (2e ch.), 10 décembre 2002, P. 02.1146.N; Cass. (2e ch.), 15 décembre 2004, P.04.1189.F

[15] D. Vandermeersch, *op. cit.*, p. 25.

[16] N. Mole et C. Harby, « Le droit à un procès équitable - Un guide sur la mise en oeuvre de l'article 6 de la Convention européenne des Droits de l'Homme », *Précis sur les droits de l'homme*, n°3, 2002, p. 6.

[17] Cour eur. D.H., arrêt *Funke c. France*, 25 février 1993, §44; N. Mole et C. Harby, *op. cit.*, p. 42; voir à ce propos J. Jackson, « Re-conceptualizing the right of silence as an effective fair trial standard », *I.C.L.Q.*, 2009, vol.58, p. 835.

Depuis, la jurisprudence constante de la Cour reconnaît que le droit au silence est inclus dans l'article 6 de la Convention[18]. Auparavant, la Commission européenne, quant à elle, reconnaissait que le droit au silence était la contrepartie négative de la liberté d'expression[19].

L'arrêt Funke met également en avant le rôle des autorités. Elles ne peuvent pas contraindre un suspect à fournir la preuve de son infraction[20]. Cette notion de coercition sera examinée ultérieurement.

- Champ d'application

Toutes les infractions criminelles sont couvertes par le droit de ne pas contribuer à sa propre incrimination[21]. Le droit au silence est applicable à toute la procédure[22].

Dans un premier temps, il faudra déterminer si une personne est accusée d'une infraction pénale, au sens de l'article 6 de la Convention. Pour cela, il faudra avoir égard à trois critères, c'est-à-dire comment l'infraction est qualifiée en droit national, la nature de l'infraction ainsi que la sanction que risque de subir l'intéressé au point de vue de la nature et du degré de cette sanction[23]. En effet, cette notion d'accusation pénale a une définition autonome dans la Convention européenne, la jurisprudence Engel permet de considérer qu'une sanction administrative peut être qualifiée de pénale[24].

La question de la volonté du suspect est centrale en ce qui concerne le droit au silence et le privilège contre l'auto-incrimination. Pour la Cour de Strasbourg, les déclarations et preuves liées à la volonté du suspect sont protégées. Cependant, les données obtenues par voie de contrainte peuvent être utilisées mais uniquement si elles existent indépendamment de la volonté du suspect[25]. L'arrêt Saunders contre Royaume-Uni en est l'illustration, ces données sont par exemple les prélèvements d'haleine, de sang, d'urine ainsi que l'analyse ADN[26].

Pour répondre à la question centrale, il conviendra de déterminer ce qu'il faut entendre par « indépendamment de la volonté du suspect ».

---

[18] A titre d'exemple: Cour eur. D.H., arrêt *Heaney McGuiness c. Irlande*, 21 décembre 2000, §40.

[19] J. JACKSON, *op. cit.*, p. 835.

[20] Cour eur. D.H., arrêt *Funke* c. France, 25 février 1993, §44.

[21] Cour eur. D.H., arrêt *Saunders c. Royaume-Uni*, 17 décembre 1996, §74; Conseil de l'Europe/Cour européenne des droits de l'homme, Guide sur l'article 6 de la Convention européenne des droits de l'homme - Droit à un procès équitable (volet pénal), 2014, p. 25, disponible sur www.echr.coe.int (consulté le 18/04/2018).

[22] Cour eur. D. H. (gde ch.), arrêt *John Murray c. Royaume-Uni*, 8 février 1996, §45; Conseil de l'Europe/Cour européenne des droits de l'homme, Guide sur l'article 6 de la Convention européenne des droits de l'homme - Droit à un procès équitable (volet pénal), 2014, p. 25, disponible sur www.echr.coe.int (consulté le 18/04/2018).

[23] Cour eur. D.H., arrêt *Öztürk c. Allemagne*, 21 février 1984, §50; Cour eur. D.H., arrêt *J.B. c. Suisse*, 3 mai 2001, §44.

[24] Cour eur. D.H., arrêt *Engel et autres c. Pays-Bas*, 8 juin 1976.

[25] J. MEESE, « The sound of silence. Het zwijgrecht en het nemo tenetur-beginsel *in* strafzaken. Een historisch en rechtsvergelijkend overzicht » *in* VAN OEVELEN, A., ROZIE, J., RUTTEN, S. (sous la direction de), *Zwijgrecht versus spreekplicht*, Intersentia, 2013, p. 39.

[26] Cour eur. D.H., arrêt *Saunders c. Royaume-Uni*, 17 décembre 1996, §69.

- Raisons

Le droit au silence cherche à protéger deux garanties principales, à savoir la protection contre la coercition abusive des autorités[27] et le respect de la présomption d'innocence[28].

Premièrement, il s'agira d'approfondir la notion de coercition. La Cour européenne des droits de l'homme n'autorise pas la coercition abusive des autorités pour éviter les erreurs judiciaires et atteindre le résultat voulu par l'article 6[29]. La tâche de la Cour n'est pas de donner aux Etats les moyens à utiliser pour atteindre le but de l'article 6 mais de vérifier qu'ils le respectent[30].

Au regard de la jurisprudence, il faut constater que toute forme de coercition n'est pas prohibée, comme expliqué précédemment avec l'arrêt Saunders. Les arrêts rejettent la coercition dite abusive[31]. Il faut déterminer:

> « *si ces interdictions revêtent un caractère absolu en ce sens que l'exercice par un prévenu du droit de garder le silence ne pourrait jamais servir en sa défaveur au procès ou, à titre subsidiaire, qu'il y a toujours lieu de tenir pour une "coercition abusive" le fait de l'informer au préalable que, sous certaines conditions, son silence pourra être ainsi utilisé* »[32].

La torture est quant à elle totalement bannie[33], l'article 3 de la Cour européenne des droits de l'homme ne connaît aucune exception.

Deuxièmement, le respect de la présomption d'innocence oblige l'accusation à fournir les éléments de preuve servant à fonder la culpabilité. Ces preuves ne peuvent pas être obtenues par la contrainte ou la pression, au mépris de la volonté de l'accusé[34].

De plus, le suspect doit également avoir le choix de parler ou de se taire. Par conséquent, les autorités ne peuvent pas non plus utiliser des subterfuges pour faire parler le suspect afin d'obtenir des aveux qu'elles n'auraient pu obtenir durant l'interrogatoire et les utiliser en justice[35].

---

[27] Cour eur. D.H. (gde ch.), arrêt *John Murray c. Royaume-Uni*, 8 février 1996, §45.

[28] Cour eur. D.H., arrêt *Saunders c. Royaume-Uni*, 17 décembre 1996, §68.

[29] Cour eur. D.H. (gde ch.), arrêt *John Murray c. Royaume-Uni*, 8 février 1996, §45.

[30] Cour eur. D.H., arrêt *J.B. c. Suisse*, 3 mai 2001, §70.

[31] A titre d'exemples: Cour eur. D.H. (gde ch.), arrêt *John Murray c. Royaume-Uni*, 8 février 1996, §45-46; Cour eur. D.H., arrêt *Saunders c. Royaume-Uni*, 17 décembre 1996, §68; Cour eur. D.H., arrêt *Heaney McGuiness c. Irlande*, 21 décembre 2000, §40.

[32] Cour eur. D.H. (gde ch.), arrêt *John Murray c. Royaume-Uni*, 8 février 1996, §46.

[33] Cour eur. D.H., arrêt *Shlychkov v. Russia*, 9 février 2016.

[34] Cour eur. D.H., arrêt *Saunders c. Royaume-Uni*, 17 décembre 1996, §68.

[35] Conseil de l'Europe/Cour européenne des droits de l'homme, Guide sur l'article 6 de la Convention européenne des droits de l'homme - Droit à un procès équitable (volet pénal), 2014, p. 25, disponible sur www.echr.coe.int (consulté le 18/04/2018); Cour eur. D.H., arrêt *Allan c. Royaume-Uni*, 5 novembre 2002, §50.

- Un droit relatif[36]

La jurisprudence reconnaît que le droit au silence n'est pas absolu. Cette affirmation trouve son fondement dans l'arrêt John Murray[37]. S'il est vrai qu'une condamnation ne peut se fonder exclusivement sur le refus de parler du prévenu, certaines questions nécessitent des réponses. Garder le silence durant toute la procédure peut s'avérer préjudiciable[38]. Pour entraîner la condamnation d'un suspect ayant refusé de parler, des preuves suffisantes de sa culpabilité devront être apportées et démontrées par l'accusation. Le silence seul ne pourra pas pousser le juge à le condamner. Tous les éléments du cas d'espèce devront être pris en considération comme, notamment, le poids accordé à la preuve par les juridictions nationales[39].

La jurisprudence Jalloh précise encore que « *[p]our rechercher si une procédure a anéanti la substance même du droit de ne pas contribuer à sa propre incrimination, la Cour doit examiner en particulier les éléments suivants : la nature et le degré de la coercition, l'existence de garanties appropriées dans la procédure et l'utilisation qui est faite des éléments ainsi obtenus* »[40].

Tout d'abord, il faudra vérifier la nature et le degré de la coercition. Comme exposé précédemment, toute forme de coercition n'est pas prohibée.

Ensuite, la Cour vérifiera qu'il existe des garanties appropriées dans la procédure. Il s'agit par exemple d'examiner si les enquêteurs sont indépendants et soumis à un contrôle juridictionnel[41] ou au contraire le pouvoir discrétionnaire accordé des autorités[42], l'accès à un avocat[43] ou encore des garanties légales concernant la détention[44]. Il est également important de prendre en considération les présomptions, le recours à celles-ci n'est pas interdit. Il faut néanmoins que les présomptions soient limitées afin de permettre au suspect d'assurer ses droits de la défense et de ne pas vider la présomption d'innocence de sa substance[45]. Il semblerait donc que recourir à une présomption irréfragable serait difficilement compatible avec la présomption d'innocence, il faudra tenir compte des limites imposées par les états du point de vue de la gravité de la situation et afin de respecter les droits de la défense[46].

---

[36] Conseil de l'Europe/Cour européenne des droits de l'homme, Guide sur l'article 6 de la Convention européenne des droits de l'homme - Droit à un procès équitable (volet pénal), 2014, p. 26, disponible sur www.echr.coe.int (consulté le 18/04/2018).

[37] Cour eur. D.H. (gde ch.), arrêt *John Murray c. Royaume-Uni*, 8 février 1996.

[38] Conseil de l'Europe/Cour européenne des droits de l'homme, Guide sur l'article 6 de la Convention européenne des droits de l'homme - Droit à un procès équitable (volet pénal), 2014, p. 26, disponible sur www.echr.coe.int (consulté le 18/04/2018).

[39] Cour eur. D.H. (gde ch.), arrêt *John Murray c. Royaume-Uni*, 8 février 1996, §47.

[40] Cour eur. D.H., arrêt *Jalloh c. Allemagne*, 11 juillet 2006, §101.

[41] Cour eur. D.H., arrêt *Saunders c. Royaume-Uni*, 17 décembre 1996, §63.

[42] Cour eur. D.H., arrêt *Bykov c. Russie*, 10 mars 2009, §80.

[43] Cour eur. D.H., arrêt *Salduz c. Turquie*, 27 novembre 2008, §54.

[44] Cour eur. D.H., arrêt *Heaney McGuiness c. Irlande*, 21 décembre 2000, §15.

[45] Cour eur. D.H., arrêt *Salabiaku c. France*, 7 octobre 1988, §28.

[46] Cour eur. D.H., arrêt *Salabiaku c. France*, 7 octobre 1988, §28 in fine.

Et finalement, il sera possible de considérer qu'il n'y a pas eu de violation de l'article 6 si la pièce obtenue a un caractère limité dans l'ensemble des documents et ne permet pas d'établir à elle seule la culpabilité du prévenu[47].

- Intérêt public

En 1996, la Cour considérait qu'utiliser des données obtenues par la contrainte dans une enquête non judiciaire pour incriminer un suspect au niveau pénal ne pouvait être justifié par l'intérêt public[48]. Depuis, cette position a évolué. En effet, l'intérêt public peut être pris en considération pour poursuivre une infraction et sanctionner l'auteur. Il faudra le confronter avec un autre intérêt, celui de l'individu au recueil légal des preuves qui seront retenues contre lui. Toutefois, il ne faut pas vider de leur substance les droits de la défense[49].

- Rôle de l'avocat et notification des droits

Le droit au silence et l'accès à un avocat sont garantis par l'article 6 de la Convention. Ces droits sont distincts puisque renoncer à l'un ne signifie pas que l'on renonce à l'autre. Ils sont pourtant complémentaires[50]. En effet, la Cour affirme que si un suspect parle sans avoir été expressément informé de son droit à garder le silence et qu'il a pris cette décision sans être assisté de son avocat, alors ses déclarations ne pourront pas servir de preuve contre lui[51].

Dès lors, de manière extrêmement synthétique, il faut retenir qu'un suspect dans une affaire pénale a le droit de garder le silence et de ne pas collaborer pour fournir des preuves qui pourraient l'incriminer. Les autorités ne peuvent l'y contraindre lorsque les éléments de preuve ont été obtenus au mépris de la volonté du suspect[52]. Cependant, il conviendra de remarquer que ces droits sont difficiles à appréhender avec précision, la jurisprudence de la Cour a considérablement évolué et elle examinera tous les éléments propres au cas d'espèce[53].

De plus, le droit au silence et le privilège contre l'auto-incrimination ne sont pas des droits absolus. La Cour prend également en compte l'intérêt public. Cela a fait dire à certains que la force de ces droits s'en trouvait diminuée. Il lui est également reproché de ne pas différencier le droit au silence et le privilège contre l'auto-incrimination[54].

---

[47] Cour eur. D.H., arrêt *Bykov c. Russie*, 10 mars 2009, §104; Cour eur. D.H., arrêt *O'Halloran et Francis c. Royaume-Uni*, 29 juin 2007, §62; Conseil de l'Europe/Cour européenne des droits de l'homme, Guide sur l'article 6 de la Convention européenne des droits de l'homme - Droit à un procès équitable (volet pénal), 2014, p. 25-26, disponible sur www.echr.coe.int (consulté le 18/04/2018).

[48] Cour eur. D.H., arrêt *Saunders c. Royaume-Uni*, 17 décembre 1996, §74.

[49] Cour eur. D.H., arrêt *Jalloh c. Allemagne*, 11 juillet 2006, §97.

[50] Conseil de l'Europe/Cour européenne des droits de l'homme, Guide sur l'article 6 de la Convention européenne des droits de l'homme - Droit à un procès équitable (volet pénal), 2014, p. 25, disponible sur www.echr.coe.int (consulté le 18/04/2018).

[51] Conseil de l'Europe/Cour européenne des droits de l'homme, Guide sur l'article 6 de la Convention européenne des droits de l'homme - Droit à un procès équitable (volet pénal), 2014, p. 25, disponible sur www.echr.coe.int (consulté le 18/04/2018); Cour eur. D.H., arrêt *Brusco c. France*, 14 octobre 2010, §54; Cour eur. D.H., arrêt *Stojkovic c. France et Belgique*, 27 octobre 2011, §54; Cour eur. D.H., arrêt *Navone et autres c. Monaco*, 24 octobre 2013, §74.

[52] Cour eur. D.H., arrêt *Saunders c. Royaume-Uni*, 17 décembre 1996, §69.

[53] Cour eur. D.H., arrêt *Jalloh c. Allemagne*, 11 juillet 2006, §101.

[54] J. JACKSON, *op. cit.*, p. 836.

A présent, il s'agira de s'intéresser à l'Union européenne. Comment envisage-t-elle ces droits?

C. L'UNION EUROPÉENNE

Tout d'abord, il semble important de noter que l'Union européenne respecte la Convention européenne des droits de l'homme comme précisé à l'article 6 du Traité sur l'Union européenne. Cet article mentionne également la Charte des droits fondamentaux de l'Union européenne. L'article 48 de cette Charte concerne la présomption d'innocence et les droits de la défense. Cependant, la disposition ne mentionne pas le droit au silence en tant que tel.

Depuis quelques années déjà, l'Union européenne désire inciter les états à prévoir des garanties procédurales dans les affaires pénales et notamment, à garantir le droit au silence. Divers documents laissent transparaître cette volonté comme une résolution de 2003[55] ou encore une communication de 2013[56]. Le but de la Commission est de garantir aux citoyens un procès équitable dans l'ensemble de l'espace juridique européen.

La Commission avait constaté que les droits au silence, à ne pas s'auto-incriminer ainsi qu'à ne pas devoir collaborer étaient insuffisamment protégés. En effet, dans certaines situations, garder le silence peut s'avérer incriminant. De plus, le droit d'appel est un recours insuffisant puisqu'il n'exclut pas les preuves obtenues illégalement[57].

Actuellement, la matière est réglée par la directive 2016/343[58]. Les considérants 24 à 30 apportent des précisions concernant le droit au silence et le droit de ne pas s'auto-incriminer. L'article 7 de la directive garantit ces droits[59], il convient de l'examiner.

L'Union européenne considère que le droit au silence et le privilège contre l'auto-incrimination doivent être interprétés à la lumière de la jurisprudence de la Cour européenne des droits de l'homme[60]. Mais elle regrette aussi leur insuffisance. Au regard de ces

---

[55] Résolution du Parlement européen sur la proposition de recommandation du Parlement européen au Conseil sur les normes minimales en matière de garanties procédurales accordées aux suspects et aux personnes mises en cause dans des procédures pénales dans l'Union européenne (2003/2179(INI)), P5_TA(2003)0484, 6 novembre 2003, *J.O.U.E.*, C 83 E/180 du 2 avril 2004, pp. 180-185.

[56] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions relative aux avancées dans le programme de l'Union européenne relatifs aux garanties procédurales accordées aux suspects et aux personnes poursuivies - Renforcer les fondements de l'espace européen de justice pénale, Bruxelles, 27 novembre 2013, COM/2013/0820 final, pp. 1-14.

[57] Commission européenne, Commission staff working document impact assessment - Accompanying the document Proposal for measures on the strengthening of certain aspects of the presumption of innocence and of the right to be present at trial criminal proceedings, 27 novembre 2013, SWD/2013/0478 final, point 4.2.3.

[58] Directive (UE) 2016/343 du Parlement européen et du Conseil du 9 mars 2016 portant renforcement de certains aspects de la présomption d'innocence et du droit d'assister à son procès dans le cadre des procédures pénales, *J.O.U.E.*, L 65 du 11 mars 2016, pp. 1-11.

[59] Directive (UE) 2016/343 du Parlement européen et du Conseil du 9 mars 2016 portant renforcement de certains aspects de la présomption d'innocence et du droit d'assister à son procès dans le cadre des procédures pénales, art. 7, *J.O.U.E.*, L 65 du 11 mars 2016, pp. 8-9.

[60] Directive (UE) 2016/343 du Parlement européen et du Conseil du 9 mars 2016 portant renforcement de certains aspects de la présomption d'innocence et du droit d'assister à son procès dans le cadre des procédures pénales, considérant n°27, *J.O.U.E.*, L 65 du 11 mars 2016, p. 4.

considérations, est-ce que le champ d'application qui leur est reconnu est le même que celui reconnu par le Cour européenne des droits de l'homme?

Tout d'abord, la directive s'appliquera, en principe, uniquement aux procédures pénales. Les procédures civiles et administratives seront exclues bien qu'il faille tenir compte de la jurisprudence de la Cour européenne des droits de l'homme[61]. Tandis que la Cour européenne considère que des procédures administratives peuvent être qualifiées de pénales[62].

De plus, le champ d'application personnel de la directive inclut uniquement les personnes physiques[63]. Alors que les personnes morales ne sont pas exclues par la jurisprudence strasbourgeoise[64].

L'article 7.3 de la directive confirme la jurisprudence de la Cour européenne[65]. Il est également précisé que l'attitude coopérative du suspect peut être prise en considération[66], la Cour européenne des droits de l'homme ne semble pas donner une telle indication mais rien ne l'empêcherait de prendre cet élément en considération dans son analyse. En effet, dans tous les arrêts, elle examine toutes les circonstances de l'espèce[67].

L'article 7 précise encore que rien ne s'oppose à ce qu'une partie de la procédure soit menée par écrit ou sans interrogatoire en veillant toutefois à respecter le droit au procès équitable[68]. Cela est conforme à la jurisprudence de la Cour européenne des droits de l'homme lorsqu'elle affirme qu'il faudra analyser l'existence de garanties dans la procédure et de l'utilisation faite des pièces[69].

Toutefois, l'Union européenne ne se contente pas de répéter la jurisprudence strasbourgeoise. En effet, il existe une volonté de renforcer les droits au silence et à ne pas s'incriminer soi-même, la Commission reprochait que les Etats membres puissent tirer des preuves à charge, du silence de l'accusé[70]. L'article 7.5 de la directive se montre strict,

---

[61] Directive (UE) 2016/343 du Parlement européen et du Conseil du 9 mars 2016 portant renforcement de certains aspects de la présomption d'innocence et du droit d'assister à son procès dans le cadre des procédures pénales, considérant n°11, *J.O.U.E.*, L 65 du 11 mars 2016, p. 2.

[62] Cour eur. D.H., arrêt *Engel et autres c. Pays-Bas*, 8 juin 1976.

[63] Directive (UE) 2016/343 du Parlement européen et du Conseil du 9 mars 2016 portant renforcement de certains aspects de la présomption d'innocence et du droit d'assister à son procès dans le cadre des procédures pénales, art. 2, *J.O.U.E.*, L 65 du 11 mars 2016, p. 7.

[64] S. CRAS et A. ERBEŽNIK, « The Directive on the Presumption of Innocence and the Right to Be Present at Trial », *eucrim*, 2016, p. 28; voir aussi E. MONCEAUX, Quel droit au silence en procédure pénale?, Université Panthéon-Assas, 2011, p.28 (disponible sur docassas.u-paris2.fr).

[65] Cour eur. D.H., arrêt *Saunders c. Royaume-Uni*, 17 décembre 1996, §69.

[66] Directive (UE) 2016/343 du Parlement européen et du Conseil du 9 mars 2016 portant renforcement de certains aspects de la présomption d'innocence et du droit d'assister à son procès dans le cadre des procédures pénales, art.7.4, *J.O.U.E.*, L 65 du 11 mars 2016, p. 8.

[67] A titre d'exemple: Cour eur. D.H., arrêt *Jalloh c. Allemagne*, 11 juillet 2006, §101.

[68] Directive (UE) 2016/343 du Parlement européen et du Conseil du 9 mars 2016 portant renforcement de certains aspects de la présomption d'innocence et du droit d'assister à son procès dans le cadre des procédures pénales, art.7.6, *J.O.U.E.*, L 65 du 11 mars 2016, p. 9.

[69] Cour eur. D.H., arrêt *Jalloh c. Allemagne*, 11 juillet 2006, §101.

[70] Commission européenne, Commission staff working document impact assessment - Accompanying the document Proposal for measures on the strengthening of certain aspects of the presumption of innocence and of the right to be present at trial criminal proceedings, 27 novembre 2013, SWD/2013/0478 final, point 4.2.3.

l'exercice de ces droits par le suspect ne pourra pas se retourner contre lui, les autorités ne pourront pas en tirer des conclusions défavorables[71].

Il convient également d'ajouter que le droit de l'Union européenne est contraignant pour les Etats membres qui ont accepté d'abandonner une partie de leur souveraineté[72]. Les Etats membres doivent se conformer à la directive et la transposer[73].

A présent, il s'agira d'appréhender les droits au silence et à ne pas s'incriminer soi-même au niveau de la Belgique.

D. LA BELGIQUE

- Droits internationaux et européens

En Belgique, le droit au silence et le principe qui consiste à ne pas s'incriminer soi-même ont été fortement influencés et ont considérablement évolué grâce à la Cour européenne[74]. Les juridictions belges ainsi que la doctrine invoquent régulièrement le Pacte international relatif aux droits civils et politiques et la Convention européenne des droits de l'homme en ce qui concerne ces droits[75] tandis qu'après recherches, il semble que le droit européen est très peu analysé.

- Champ d'application

Il n'est pas aisé de définir le champ d'application du droit au silence et du principe d'auto-incrimination dans notre système juridique. Et il n'est pas possible d'en trouver une définition dans la législation. C'est la jurisprudence qui a reconnu ce droit et depuis longtemps[76] et ce n'est que plus tard que la jurisprudence a eu un impact en Belgique[77].

« *En 1986, notre Cour de cassation consacre le droit au silence de l'inculpé comme faisant partie des droits de la défense et, à ce titre, participant d'un principe général de droit* »[78]. Le droit au silence est donc vu en Belgique comme faisant partie des droits de la

---

[71] Directive (UE) 2016/343 du Parlement européen et du Conseil du 9 mars 2016 portant renforcement de certains aspects de la présomption d'innocence et du droit d'assister à son procès dans le cadre des procédures pénales, art.7.5, *J.O.U.E.*, L 65 du 11 mars 2016, p. 8.

[72] E. MONCEAUX, Quel droit au silence en procédure pénale ?, Banque des mémoires, Université Panthéon-Assas, 2011, p.18 (disponible sur docassas.u-paris2.fr).

[73] Directive (UE) 2016/343 du Parlement européen et du Conseil du 9 mars 2016 portant renforcement de certains aspects de la présomption d'innocence et du droit d'assister à son procès dans le cadre des procédures pénales, art.14, *J.O.U.E.*, L 65 du 11 mars 2016, p. 10.

[74] I. DE LA SERNA, « Le droit au silence - discours prononcé par le Procureur général I. de la Serna à l'occasion de la rentrée solennelle de la Cour d'appel de Mons le 1er septembre 2014 », *Pli juridique*, n°32, juin 2015, p. 5.

[75] A titre d'exemples: F. KUTY, « L'étendue du droit au silence en procédure pénale », *Rev. dr. pén.*, 2000/3, p. 309-334 et M. FRANCHIMONT, A. JACOBS et A. MASSET, *Manuel de procédure pénale*, 4ème éd., Bruxelles, Larcier, 2012, p. 1131-1136; Cass. (2ème Ch.), 22 juin 2010, P.10.0872.N, §12, p.5; Cass. (2ÈME ch.), 7 février 2001, P.00.1532.F ; C.C., 13 mars 2008, arrêt n°50/2008, B.9 et suivants; C.A., 25 janvier 2001, arrêt n°4/2001.

[76] F. KUTY, *op. cit.*, p. 320.

[77] F. KUTY, o*p. cit.*, p. 321.

[78] I. DE LA SERNA, « Le droit au silence - discours prononcé par le Procureur général I. de la Serna à l'occasion de la rentrée solennelle de la Cour d'appel de Mons le 1er septembre 2014 », *Pli juridique,* n°32, juin 2015, p. 5 et Cass., 13 mai 1986, *Rev. dr. pén. crim.*, 1986, p.905, concl. Avocat général Du Jardin.

défense. Les droits de la défense s'appliquent à toutes les phases de la procédure[79]. De ces éléments, il peut donc être postulé qu'en Belgique, le droit au silence s'applique à toute la procédure.

Personne ne peut être obligé de s'avouer coupable, peu importe qu'on ait été inculpé ou mis en prévention. C'est également pour cette raison que le suspect ne peut pas être entendu sous serment[80].

Toute personne faisant l'objet d'une accusation pénale[81], sans exception, a droit au respect de son droit au silence et à choisir à quelle question il répondra, afin, notamment, de ne pas témoigner contre lui-même et de ne pas s'auto-incriminer[82]. La Cour de cassation reprend la jurisprudence de la Cour européenne des droits de l'homme en affirmant que « *le droit au silence et l'interdiction de forcer l'auto-incrimination ne s'appliquent pas aux éléments de preuve qui peuvent être obtenus par le recours à la contrainte et qui existent indépendamment au mépris de la volonté de l'accusé* »[83]. Le juge pourra également tirer des conséquences défavorables de ce silence[84].

- Article 47*bis* du Code d'instruction criminelle

Le Code d'instruction criminelle belge contient un article très important concernant le droit au silence, il semble opportun d'en faire l'analyse. Il s'agit de l'article 47*bis*, il traite des auditions et a été modifié récemment par une loi du 21 novembre 2016.

A la lecture de cet article, plusieurs éléments doivent être pris en considération. Tout d'abord, il convient d'informer les personnes interrogées, auxquelles il n'est imputé aucune infraction, qu'elles ne peuvent pas être contraintes de s'accuser elles-mêmes[85], cela inclut le droit au silence puisqu'il en est l'une des composantes. Ce droit est qualifié par les députés belges de « *droit au silence version light* »[86].

Les personnes, suspectées d'avoir commis une infraction, sont informées du même droit mais également qu'elles peuvent répondre aux questions posées ou qu'elles ont le droit de se taire[87]. Le droit de ne pas être contraint de se s'accuser soi-même couplé à celui de se

---

[79] J. DU JARDIN, « Les droits de la défense dans la jurisprudence de la Cour de cassation (1990-2003), p. 10, disponible sur www.justice.belgium.be (consulté le 24/04/2018).

[80] F. KUTY, *op. cit.*, p.320.

[81] Cass., 13 janvier 1999, P.98.0412.F.

[82] M.-A. BEERNAERT, H.-D. BOSLY et D. VANDERMEERSCH, *Droit de la procédure pénale*, 8ème éd., Brugge, la Charte, 2017, p. 690 et Cass. (2e ch.), 19 juin 2013, P.12.1150.F, concl. M.P.

[83] Cass. (2e ch.), 14 mars 2017, Larcier Cassation 2018, sommaire n°1, p.21.

[84] N. BLAISE et N. COLETTE-BASECQZ, *Manuel de droit pénal général*, 3e éd., Limal, Anthémis, 2016, p.411.

[85] Art. 47*bis,* §1 du Code d'instruction criminelle belge.

[86] Rapport concernant le relevé des lois qui ont posé des difficultés d'application ou d'interprétation pour les cours et tribunaux, *Doc. parl.*, Ch. Repr., sess. ord. 2010-2011, n°1414/006 du 8 février 2012, pp. 10 et 25.

[87] Art. 47*bis*, §2 du Code d'instruction criminelle belge.

taire est appelé « droit au silence version étendue »[88]. Cependant, leur identité est la seule information que les suspects ne peuvent refuser de donner[89].

Finalement, le sixième paragraphe est applicable à toutes les auditions[90]. L'avocat joue un rôle essentiel lors de celles-ci. Il veille notamment au respect du droit au silence[91].

Par conséquent, le droit belge fait la distinction entre le droit de ne pas s'accuser soi-même et le droit de se taire. Mais ce sont tout de même des éléments liés. Les droits garantis aux personnes auditionnées varieront en fonction de leur statut.

Si des preuves ont été obtenues en violation des droits au silence et à ne pas s'auto-incriminer, quel sort faudra-il leur réserver?

E. SANCTIONS

Tout d'abord, la Cour européenne des droits de l'homme considère que c'est le rôle des Etats de réglementer l'admissibilité des preuves[92]. En principe, il conviendrait d'écarter les preuves obtenues en contrariété au droit au silence. Dans le cas contraire, il existe une violation du droit au procès équitable. Cependant, il faudra avoir égard à tous les éléments propres au cas d'espèce[93] et regarder si la procédure était équitable dans son ensemble[94]. L'appréciation faite par la Cour est, par conséquent, très nuancée.

Ensuite, l'Union européenne apporte des précisions dans sa directive de 2016. L'article 10 de la même directive requiert des Etats membres qu'ils veillent à l'appréciation des éléments de preuve obtenus en violation du droit au silence et celui de ne pas s'auto-incriminer[95]. L'Union semble se montrer plus stricte en ce qui concerne les éléments de preuves car elle n'autorise pas les Etats à tirer des conséquences négatives de l'utilisation du droit au silence[96].

---

[88] Rapport concernant le relevé des lois qui ont posé des difficultés d'application ou d'interprétation pour les cours et tribunaux, *Doc. parl.*, Ch. Repr., sess. ord. 2010-2011, n°1414/006 du 8 février 2012, pp. 12 et 64.

[89] Art. 47*bis*, §2, 2) du Code d'instruction criminelle belge.

[90] Art. 47*bis*, §6 du Code d'instruction criminelle belge.

[91] Art. 47*bis*, §6, 7) du Code d'instruction criminelle belge.

[92] Cour eur. D.H., arrêt *Schenk c. Suisse*, 12 juillet 1988, §46; note à ce propos dans Conseil de l'Europe/Cour européenne des droits de l'homme, Guide sur l'article 6 de la Convention européenne des droits de l'homme - Droit à un procès équitable (volet pénal), 2014, p. 26, disponible sur www.echr.coe.int (consulté le 18/04/2018).

[93] O. MICHIELS, *Procédure pénale - notes sommaires et provisoires*, 5e éd., Presses Universitaires de Liège, 2016-2017, p. 326.

[94] Cour eur. D.H., arrêt *Allan c. Royaume-Uni*, 5 novembre 2002, §42.

[95] Directive (UE) 2016/343 du Parlement européen et du Conseil du 9 mars 2016 portant renforcement de certains aspects de la présomption d'innocence et du droit d'assister à son procès dans le cadre des procédures pénales, art. 10, *J.O.U.E.*, L 65 du 11 mars 2016, p. 10.

[96] Commission européenne, Commission staff working document impact assessment - Accompanying the document Proposal for measures on the strengthening of certain aspects of the presumption of innocence and of the right to be present at trial criminal proceedings, 27 novembre 2013, SWD/2013/0478 final, point 4.2.3 et sa mise en oeuvre dans la Directive (UE) 2016/343 du Parlement européen et du Conseil du 9 mars 2016 portant renforcement de certains aspects de la présomption d'innocence et du droit d'assister à son procès dans le cadre des procédures pénales, art. 7.5, *J.O.U.E.*, L 65 du 11 mars 2016, p. 8.

Du côté belge, l'article 47*bis*, §6, 9) du Code d'instruction criminelle exclut qu'une condamnation puisse se fonder sur des déclarations qui ont été faites en violation de certains paragraphes du même article, notamment, le droit à l'assistance d'un avocat. La Cour européenne se montre donc plus nuancée puisqu'elle regardera si la violation a vidé le droit au silence de sa substance[97]. Et la directive de l'Union européenne permet également leur utilisation[98].

Pendant plusieurs années, toutes les preuves obtenues illégalement étaient exclues[99]. Il était reconnu qu' « *est illégale la preuve obtenue par un acte qui est inconciliable avec les principes généraux du droit régissant la procédure pénale, notamment le respect des droits de la défense, même si cet acte n'est pas expressément interdit par la loi* »[100]. Comme il l'a été expliqué précédemment, le droit au silence fait partie des droits de la défense[101].

Petit à petit, la Cour de cassation a revu sa position concernant ces preuves et a accepté leur utilisation en justice[102] jusqu'à changer complètement sa vision dans l'arrêt Antigone[103]. Cependant, il conviendra d'exclure la preuve contraire au droit au procès équitable[104]. Cela sera le cas d'une preuve obtenue en violation du droit du prévenu à garder le silence. Cette jurisprudence Antigone a été intégrée dans le droit belge par le biais de l'article 32 du Titre préliminaire du Code de procédure pénale[105].

Dans les faits, le juge aura un pouvoir d'appréciation pour déterminer s'il y a eu une atteinte au droit au procès équitable en prenant en considération les circonstances[106]. Il appréciera le caractère intentionnel ou non de l'irrégularité, mettra en balance la gravité de l'infraction et la gravité de l'irrégularité, l'incidence de l'irrégularité sur le droit protégé ainsi que le caractère formel de l'irrégularité, …[107] La Cour va même plus loin car elle ne fait pas

---

[97] Cour eur. D.H., arrêt *Jalloh c. Allemagne*, 11 juillet 2006, §101.

[98] Directive (UE) 2016/343 du Parlement européen et du Conseil du 9 mars 2016 portant renforcement de certains aspects de la présomption d'innocence et du droit d'assister à son procès dans le cadre des procédures pénales, art.7 et 10, *J.O.U.E.*, L 65 du 11 mars 2016, respectivement p. 8-9 et 10.

[99] M.-A. BEERNAERT, « Antigone: les prémices de l'arrêt du 14 octobre 2003 », *in L'évolution de la jurisprudence Antigone sous le triple axe pénal, social et fiscal*, 2016, p. 10 (disponible sur dial.uclouvain.be).

[100] Cass., 13 mai 1986, RG 9136, sommaire, *Pas.*, 1986, p. 1107.

[101] I. DE LA SERNA, « Le droit au silence - discours prononcé par le Procureur général I. de la Serna à l'occasion de la rentrée solennelle de la Cour d'appel de Mons le 1er septembre 2014 », *Pli juridique,* n°32, juin 2015, p. 5 et Cass., 13 mai 1986, *Rev. dr. pén. crim.*, 1986, p.905, concl. Avocat général Du Jardin.

[102] M.-A. BEERNAERT, « Antigone: les prémices de l'arrêt du 14 octobre 2003 », *in L'évolution de la jurisprudence Antigone sous le triple axe pénal, social et fiscal*, 2016 (disponible sur dial.uclouvain.be).

[103] O. MICHIELS, *Procédure pénale - notes sommaires et provisoires*, 5e éd., Presses Universitaires de Liège, 2016-2017, p. 328.

[104] O. MICHIELS, *La jurisprudence de la Cour constitutionnelle en procédure pénale: le Code d'instruction criminelle remodelé par le procès équitable?*, Limal, Anthémis, 2015, p. 476-477.

[105] La preuve obtenue en violation de l'organisation des Cours et Tribunaux n'a pas été intégrée dans l'article 32 du Titre préliminaire du Code de procédure pénale.

[106] Cass. (2e ch.), 28 mai 2013, P. 13.0066.N, point 28.

[107] Cass. (2e ch.), 28 mai 2013, P.13.0066.N, point 28; voir aussi O. MICHIELS, *La jurisprudence de la Cour constitutionnelle en procédure pénale: le Code d'instruction criminelle remodelé par le procès équitable?*, Limal, Anthémis, 2015, p.331.

d'obligation au juge de stipuler si la preuve a violé le droit au silence ou celui interdisant l'auto-incrimination[108].

Il ne faut cependant pas négliger la question de la purge des nullités dans cette approche. Ce mécanisme trouve son assise dans l'article 235*bis* du Code d'instruction criminelle, plus précisément au paragraphe 6. La chambre des mises en accusation statue sur les pièces irrégulières et autorise ou non qu'elles soient utilisées en justice. Dans ce cas, les preuves irrégulières pourront être utilisées en justice. En effet, il pourrait notamment y avoir un intérêt pour les droits de la défense que ces pièces ne soient pas écartées.

Au regard des éléments précédents, la Cour de cassation belge laisse transparaître une jurisprudence plutôt souple. Cette jurisprudence, analysant tous les éléments propres à la situation, a été jugée conforme à l'article 6 de la Convention européenne des droits de l'homme[109]. Cependant, le juge belge peut tirer des conséquences du silence de l'inculpé[110], c'est ce que reproche l'Union européenne[111], la jurisprudence belge y semble donc contraire.

4. LE CRYPTAGE

Les interventions législatives, jurisprudentielles ou encore doctrinales en ce qui concerne le droit au silence n'ont pas manqué. La situation est-elle identique en ce qui concerne le cryptage? Dans un premier temps, le concept de cryptage sera défini. Ensuite, nous nous pencherons sur la place qu'il occupe dans les différents systèmes juridiques. Pour garder une certaine cohérence, ils seront analysés en procédant de manière assez similaire au point précédent, c'est-à-dire en partant du niveau international pour finir par la Belgique.

A. DÉFINITION

Cette section aura vocation à définir le concept de cryptage. Cependant, elle se veut simpliste, le but étant de faire une courte analyse permettant de comprendre l'essentiel du mécanisme, important pour la suite de l'exposé[112].

---

[108] Cass. (2e ch.), 28 mai 2013, P. 13.0066.N, point 28.

[109] F. LUGENTZ, *La preuve en matière pénale - sanction des irrégularités*, Limal, Anthémis, 2017, p.51 et Cour eur. D.H., arrêt *Kalnénienė c. Belgique*, 31 janvier 2017, §48 à 54.

[110] Cass. (2e ch.), 5 octobre 2010, P.10.0703.N, point 15.

[111] Commission européenne, Commission staff working document impact assessment - Accompanying the document Proposal for measures on the strengthening of certain aspects of the presumption of innocence and of the right to be present at trial criminal proceedings, 27 novembre 2013, SWD/2013/0478 final, point 4.2.3 et mis en oeuvre dans: Directive (UE) 2016/343 du Parlement européen et du Conseil du 9 mars 2016 portant renforcement de certains aspects de la présomption d'innocence et du droit d'assister à son procès dans le cadre des procédures pénales, art.7.5, *J.O.U.E.*, L65 du 11 mars 2016, p.8.

[112] Pour plus d'informations, voir C. PAAR et J. PELZL, *Understanding Cryptography - A textbook for students and practitioners*, Berlin, Springer, 2010, 372 p.; W. STALLINGS, *Cryptography and Network security - Principles and Practices*, 4e éd., Prentice Hall, 592 p.

Les termes cryptographie et chiffrement peuvent également être utilisés. Le cryptage est utilisé pour protéger ses données. L'idée n'est pas nouvelle, elle a cependant connu un essor considérable et plus la technologie progresse, plus le cryptage est utilisé[113].

Le cryptage peut être défini comme étant la « *transformation d'un message en clair en un message codé compréhensible seulement par qui dispose du code* »[114].

Il s'agit, en effet de partir d'un message clair et de le transformer en une série de chiffres. Pour pouvoir lire ce message, il sera nécessaire de faire l'opération inverse et de déchiffrer le message à l'aide d'une clé de déchiffrement composée de bits[115]. Les bits sont une séquence d'unités d'informations élémentaires ne pouvant avoir que 0 ou 1 comme valeur[116].

Il est également important que la clé remplisse certains critères afin d'être considérée comme sûre et rester secrète, le but étant qu'il soit impossible de la déchiffrer même si on est en possession du texte ou de la donnée cryptée, cela doit être purement aléatoire[117]. Le message ou les données seront dès lors illisibles pour la personne qui ne possède pas la clé de déchiffrement[118].

Lorsque la même clé est utilisée pour le chiffrement et le déchiffrement, la méthode sera appelé cryptographie symétrique[119]. Tandis que plus tardivement est apparu ce qu'on appelle le cryptage à clé publique[120]. L'utilisateur possède une clé privée, dont seul lui a la connaissance et il donne ce qu'on appelle une clé publique aux personnes qu'il autorise à décrypter les données[121].

- La sécurité

La population utilise de plus en plus internet et les nouvelles technologies. Elle requiert de la part des fournisseurs de services une forme de sécurité. C'est un besoin totalement légitime. En effet, énormément d'informations personnelles sont stockées sur les ordinateurs, smartphones, tablettes, … Cela peut concerner des informations sur notre identité, sur notre compte bancaire ou encore de dossiers professionnels. Plusieurs éléments vont motiver une personne à vouloir protéger ses données: « *Si je transfère des informations sensibles (par exemple, couvertes par le secret professionnel) ou si je veux protéger des sources qui doivent rester confidentielles (par exemple des fonctionnaires qui dénoncent des collègues ripoux) ou tout simplement pour protéger ma vie privée ou sentimentale, j'ai tout*

---

[113] J.-N. COLIN, « Du secret à la confiance… quelques éléments de cryptographie » *in* H. JACQUEMIN (sous la direction de), *L'identification électronique et les services de confiance depuis le règlement eIDAS*, CRIDS, 39, Bruxelles, Larcier, 2016, p. 8.

[114] « cryptage » dans Le petit Larousse illustré 2002, Paris, Larousse, 2001, p. 286.

[115] D. DENNING, *Cryptography and data security*, United States, Addison-Wesley Publishing Compagny, 1982, p. 1-2; voir aussi J.-N. COLIN, *op. cit.*, p.9.

[116] J.-N. COLIN, *op. cit.*, p.8.

[117] J.-N. COLIN, *op. cit.*, p.9 voir aussi W. STALLINGS, *Cryptography and Network security - Principles and Practices*, 4e éd., Prentice Hall, p.30.

[118] J.-N. COLIN, *op. cit.*, p.10.

[119] J.-N. COLIN, *op. cit.*, p.10.

[120] W. STALLINGS, *Cryptography and Network security - Principles and Practices*, 4e éd., Prentice Hall, p.30.

[121] J.-N. COLIN, *op. cit.*, p.11.

intérêt à crypter (ou encoder) mes communications »[122]. Personne n'a envie que ce type de données tombent entre de mauvaises mains.

Le cryptage permet donc d'assurer cette sécurité. Mais de quelle façon? Il permet la confidentialité, l'intégrité et l'authenticité des données dans les échanges numériques. Par exemple, X envoie un message à Y. Le cryptage va protéger le contenu du message et il sera inchangé lorsque Y le lira, on parle d'intégrité. Y pourra être certain que le message provient de X, c'est l'authenticité[123]. La confidentialité de la communication sera assurée par le fait que seules les personnes à qui on a fait confiance pourront lire le message[124]. Certains auteurs qualifient également l'intégrité de non-répudiation[125].

Les motifs énoncés précédemment semblent nobles. Cependant, le cryptage est également un moyen utilisé par les criminels afin de rendre des preuves inaccessibles. Le cryptage entre en contradiction avec le droit des enquêteurs à avoir accès à des preuves, cela complique leur travail. Cette situation ambivalente n'est pas récente, elle a déjà été pointée du doigt par divers auteurs et ne concerne pas que la Belgique[126]. La balance d'intérêt entre les deux est délicate.

- Cas particulier: le code

Dans ce travail, les codes d'accès seront abordés de manière incidente.

Le code peut être envisagé de deux manières. Tout d'abord, il peut s'agir d'un code d'accès, c'est-à-dire une « *combinaison alphanumérique qui, composée sur un clavier électronique, autorise un accès* »[127]. Par exemple, le mot de passe pour déverrouiller un téléphone portable. Le mot de passe assure la sécurité des données, tout comme le cryptage.

Ensuite, le code peut être envisagé comme un chiffrement. Il peut être défini comme étant un « *système étant un système de symboles permettant d'interpréter, de transmettre un message, de représenter une information des données* »[128]. Et le codage ou l'encodage est l' « *action d'appliquer un code pour transformer un message, des données en vue de leur transmission ou de leur traitement* »[129]. Cela signifie qu'un message clair se verra appliquer

---

[122] M. BEYS, *Quels droits face à la police*, Bruxelles, J & D édition, 2014, pp. 326-327.

[123] Y. AKDENIZ et C. WALKER, « Whisper who dares: encryption, privacy rights and the new world disorder », *in* Y. AKDENIZ, C. WALKER et D. WALL, *The internet, Law and Society*, United Kingdom, Pearson Education, 2000, p. 320.

[124] S. BAKER et P. HURST, *The limits of Trust - Cryptography, Governments and Electronic Commerce*, The Hague, Kluwer Law International, 1998, p. 2.

[125] C. PAAR et J. PELZL, *Understanding Cryptography - A textbook for students and practitioners*, Berlin, Springer, 2010, p. 154.

[126] B.-J. KOOPS, « The Crypto Controversy - A Key Conflict in the Information Society », *Law and Electronic Commerce*, Vol. 6, London, Kluwer Law international, 1999, p. 1-2; S. BAKER et P. HURST, *The limits of Trust - Cryptography, Governments and Electronic Commerce*, The Hague, Kluwer Law International, 1998, pp. 5-7; M. SEPEC, « Digital data encryption - Aspects of criminal law and dilemmas in Slovenia », *Digi (Digital evidence and electronic signature law review)*, vol. 10, 2013, p. 147.

[127] « code » dans Le petit Larousse illustré 2002, Paris, Larousse, 2001, p. 230.

[128] « code » dans Le petit Larousse illustré 2002, *op. cit.*, p. 229.

[129] « codage » dans Le petit Larousse illustré 2002, *op. cit.*, p. 229.

un code pour permettre sa transmission. Il semblerait qu'il n'y ait pas vraiment de différence avec le chiffrement dans ce cas[130].

De plus, il faut constater que, généralement, le code ou le mot de passe ne seront pas distingués du cryptage et seront abordés ensemble[131].

Par conséquent, même si cet exposé n'a pas pour vocation de répondre à la question du droit au silence par rapport au code, la similitude avec le cryptage permettra la plupart du temps de ne pas faire de distinction.

Quelle approche les différents systèmes juridiques ont-ils du chiffrement?

B. Approche historique

Au XX^{ème} siècle, le cryptage faisait déjà l'objet de discussions. Les ouvrages mentionnent généralement des lignes directrices établies par l'organisation de Coopération et de Développement Economiques, connue sous le nom d'OCDE[132]. L'OCDE est une organisation mondiale qui s'intéresse au bien-être économique et social[133].

Ces lignes directrices désiraient que les Etats membres mettent en place une politique concernant l'utilisation du cryptage. De plus, les fournisseurs de services devaient faciliter l'accès aux clés de cryptage[134].

C. Conseil de l'Europe

Déjà en 1995, le Conseil de l'Europe faisait état du caractère ambivalent du chiffrement. Selon lui, il fallait réduire ses effets négatifs dans le cadre des enquêtes pénales sans toutefois le rendre inefficace[135].

En 2001, le Conseil de l'Europe a adopté la Convention de Budapest sur la cybercriminalité. Le souhait du Conseil est de protéger le cyber-espace et de faire en sorte

---

[130] A ce sujet, voir aussi la définition donnée par D. Denning, *Cryptography and data security*, United States, Addison-Wesley Publishing Compagny, 1982, p. 2.

[131] Projet de loi portant des modifications diverses au Code d'instruction criminelle et au Code pénal, en vue d'améliorer les méthodes particulières de recherche et certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications et créant une banque de données des empreintes, *Doc. parl.*, Ch. Repr., sess. ord. 2015-2016, n° 1966/001 du 8 juillet 2016, pp. 20 et 22: pas de différence entre les clés de cryptage et les mots de passe; 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.*, n°7, 2001, p. 675 et 682.

[132] T. Piette-Coudol, *Echanges électroniques Certification et sécurité*, Paris, Litec, 2000, p. 21-22; Y. Akdeniz et C. Walker, « Whisper who dares: encryption, privacy rights and the new world disorder », *in* Y. Akdeniz, C. Walker et D. Wall, *The internet, Law and Society*, United Kingdom, Pearson Education, 2000, p. 323; S. Baker et P. Hurst, *The limits of Trust - Cryptography, Governments and Electronic Commerce*, The Hague, Kluwer Law International, 1998, pp. 41-71.

[133] Informations disponibles sur le site de l'OCDE: oecd.org

[134] T . Piette-Coudol, *Echanges électroniques Certification et sécurité*, Paris, Litec, 2000, pp. 21-22.

[135] Conseil de l'Europe, 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, adoptée le 11 septembre 1995 lors de la 543e réunion des Délégués des Ministres, p.3.

qu'il ne serve pas à commettre ou stocker des infractions[136]. L'utilisation du cryptage sera nécessaire dans ce cadre.

Il convient, dans un premier temps, de définir la notion de fournisseur de service: « *i. toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique; ii. toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs* »[137]

Il est possible de recourir à des pouvoirs coercitifs pour faciliter l'accès à des preuves situées sur un support informatique. Dans ce cadre, des obligations pèseront sur les fournisseurs de services. La Convention autorise que les fournisseurs de services puissent être contraints à collaborer et à fournir des informations en vue, notamment de contourner le problème du cryptage[138]. La Belgique a été dans ce sens, comme nous le verrons ultérieurement[139].

Ensuite, il convient d'analyser les articles 4 et 25 de la Convention de Budapest. L'article 4 vise l'atteinte à l'intégrité des données[140]. Comme il l'a été montré précédemment, le cryptage est un outil qui permet de garder les données intègres. Cet article ne pénalise pas l'altération des données lorsqu'il existe un but commercial, afin notamment d'assurer la protection des communications comme c'est le cas du cryptage. Porter atteinte à l'intégrité des données peut être légitimé par un but supérieur, à savoir le respect de la vie privée[141]. Le cryptage est intimement lié à l'article 8 de la Convention européenne des droits de l'homme et son but est justement de protéger l'intégrité des données et d'empêcher à autrui d'y porter atteinte.

L'article 25, quant à lui, concerne l'entraide entre les Etats dans le cadre de la cybercriminalité[142]. Dans ce cas, les Etats seront amenés à devoir communiquer rapidement. Et généralement, des moyens de communication électroniques sont utilisés « *pour autant que ces moyens offrent des conditions suffisantes de sécurité et d'authentification (y compris le cryptage si nécessaire)* »[143]. Le cryptage est donc un outil essentiel pour les Etats eux-mêmes.

Le Conseil de l'Europe a publié une stratégie pour les années 2016 à 2019 concernant l'utilisation d'internet. Cette stratégie insiste sur le respect des droits de l'homme également au niveau virtuel. L'utilisation du cryptage est reconnue, elle permet d'assurer une protection

---

[136] Convention sur la cybercriminalité faite à Budapest le 23 novembre 2001 approuvée par la loi 3 août 2012, considérants, *M.B.*, 21 novembre 2012.

[137] Convention sur la cybercriminalité faite à Budapest le 23 novembre 2001 approuvée par la loi 3 août 2012, art. 1 c, *M.B.*, 21 novembre 2012.

[138] Convention sur le cybercriminalité, rapport explicatif, p.1, disponible sur www.europarl.europa.eu.

[139] Art. 88*quater* du Code d'instruction criminelle belge.

[140] Convention sur la cybercriminalité faite à Budapest le 23 novembre 2001 approuvée par la loi 3 août 2012, art. 4, *M.B.*, 21 novembre 2012.

[141] Convention sur le cybercriminalité, rapport explicatif, p.1, disponible sur www.europarl.europa.eu.

[142] Convention sur la cybercriminalité faite à Budapest le 23 novembre 2001 approuvée par la loi 3 août 2012, art. 25, *M.B.*, 21 novembre 2012.

[143] Convention sur la cybercriminalité faite à Budapest le 23 novembre 2001 approuvée par la loi 3 août 2012, art. 25 §3, *M.B.*, 21 novembre 2012.

sur internet, notamment contre les atteintes à la vie privée. Cependant, il ne faudrait pas aboutir à un résultat qui empêcherait les états membres à poursuivre les actes criminels[144].

Par conséquent, il existe un besoin contradictoire. D'une part, il faut maintenir le cryptage qui est une forme de sécurité et de protection contre la cyber-criminalité et d'autres ingérences. Alors que, d'autre part, pour l'efficacité des enquêtes pénales, il faudrait contourner le cryptage[145].

D. UNION EUROPÉENNE

L'Union européenne s'est dotée de plusieurs instruments concernant les communications électroniques, la loi belge du 13 juin 2005 relative aux communications électroniques en fait la transposition[146].

La directive « vie privée et communications électroniques » requiert des fournisseurs de services d'assurer la sécurité de leurs services, d'informer les utilisateurs des risques pour la sécurité mais également que les utilisateurs soient avertis qu'en recourant à des techniques de cryptage, ils peuvent protéger leurs communications. Comme le texte le précise, les fournisseurs peuvent faire plus qu'informer, ils peuvent également mettre en place les techniques de sécurité[147].

Le règlement 2016/679, appelé « règlement général sur la protection des données »[148], devrait entrer en vigueur le 25 mai 2018[149]. Ce règlement traite notamment du cryptage dans le cadre de la protection des données. Les personnes responsables du traitement de données à caractère personnel seront tenues de garantir la sécurité de celles-ci, afin d'éviter qu'elles ne

---

[144] Gouvernance de l'internet - Stratégie du Conseil de l'Europe 2016-2019 - Démocratie, droits de l'homme et Etat de droit dans le monde numérique adoptée à la 1252e réunion des Délégués des Ministres le 30 mars 2016, p. 12-13.

[145] Voir à ce propos le commentaire de M. Kerkhofs qui souhaite que soit supprimée cette source de contradiction: Projet de loi relatif à l'amélioration des méthodes particulières de recherche et de certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications. Rapport de la première lecture fait au nom de la Commission de la justice par M. Gautier Calomne et Mme Goedele Uyttersprot, *Doc. parl.*, Ch. Repr., sess. ord. 2015-2016, n°1966/006 du 28 novembre 2016, p. 39.

[146] Loi du 13 juin 2005 relative aux communications électroniques, *M.B.*, 29 juin 2005, p. 28070.

[147] 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 (directive " Vie privée et communications électroniques «), considérant n°20, *J.O.U.E.*, L 201/37 du 31 juillet 2002, p. 39.

[148] 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), considérant n°83, *J.O.U.E.*, L 119 du 4 mai 2016, p.1-88.

[149] 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), art. 99, *J.O.U.E.*, L 119 du 4 mai 2016, p. 87-88.

soient détruites, perdues ou encore, divulguées. Afin de prévenir les risques, les responsables devront notamment utiliser le chiffrement[150].

Les articles 6, 32 et 34 du même règlement envisagent le rôle du chiffrement comme étant une garantie pour la sécurité des données personnelles. D'ailleurs, la mise en place de cette technique par le responsable du traitement permet ce que l'on pourrait qualifier d'« atténuation de sa responsabilité ». Il n'y a pas d'obligation d'utilisation du cryptage par les responsables du traitement. Cependant, son utilisation lui permet de se protéger dans le cas où les données personnelles d'un individu ont été affectées[151].

En 2017, l'Union européenne s'est prononcée à plusieurs reprises à propos du recours au chiffrement.

Premièrement, le Conseil de l'Union européenne a publié un rapport concernant la cybercriminalité. Un fois de plus, ce rapport a mis en avant le caractère contradictoire du chiffrement. Le recours au chiffrement est fréquent et protège les données privées des citoyens dans le monde numérique. Cependant, l'accès à ces données dans le cadre d'enquête pénale est compliqué, parfois même impossible[152].

Diverses raisons complexifient le déchiffrement: il faut en connaître les techniques. Plus le cryptage prend des formes complexes, plus il sera difficile à décrypter et plus cela prendra du temps,…[153] Afin de réduire les problèmes liés au cryptage, plusieurs recommandations ont été faites aux Etats dans ce domaine. Une coopération entre états membres mais également avec le secteur privé est nécessaire pour contourner la problématique du cryptage dans les enquêtes pénales[154]. La coopération des entreprises et fournisseurs sera analysée dans une section ultérieure.

A son tour, la Commission européenne a publié une communication à propos des progrès en matière de sécurité[155]. Elle envisage le chiffrement de la même manière que le Conseil. C'est-à-dire comme une arme à double tranchant. La protection des données complique considérablement la tâche des autorités judiciaires et des enquêteurs dans

---

[150] 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), considérant n°83, *J.O.U.E.*, L 119 du 4 mai 2016, pp. 16.

[151] 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), art. 34, *J.O.U.E.*, L 119 du 4 mai 2016, pp. 52-53.

[152] Conseil de l'Union européenne, Rapport final sur la septième série d'évaluations mutuelle sur la mise en oeuvre pratique et le fonctionnement des politiques européennes en matière de prévention de la cybercriminalité et de lutte contre celle-ci - informations communiquées au Conseil, 12711/17 du 2 octobre 2017, p. 47.

[153] Conseil de l'Union européenne,Rapport final sur la septième série d'évaluations mutuelle sur la mise en oeuvre pratique et le fonctionnement des politiques européennes en matière de prévention de la cybercriminalité et de lutte contre celle-ci - informations communiquées au Conseil, 12711/17 du 2 octobre 2017, pp. 47-51.

[154] Conseil de l'Union européenne, Rapport final sur la septième série d'évaluations mutuelle sur la mise en oeuvre pratique et le fonctionnement des politiques européennes en matière de prévention de la cybercriminalité et de lutte contre celle-ci - informations communiquées au Conseil, 12711/17 du 2 octobre 2017, p.52.

[155] Commission européenne, Communication au Parlement européen, au Conseil européen et au Conseil concernant le onzième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective, COM(2017) 608 final du 18.10.2017.

l'obtention de preuves dans le cadre d'infractions pénales[156]. Par conséquent, divers acteurs ont discuté pour trouver une solution. Finalement, la Commission en est arrivée à la conclusion qu'il faudrait mettre en place les mesures suivantes: « *(a) de mesures juridiques visant à faciliter l'accès à des éléments de preuve chiffrés, ainsi que (b) de mesures techniques visant à renforcer les capacités de déchiffrement* »[157]. Il convient d'aider les autorités sans porter atteinte au cryptage, celui-ci étant essentiel pour la sécurité des données et dans la lutte contre la cybercriminalité[158]. La Commission soutient la mise en place de mesures, présentées en six points[159].

Que faut-il retenir dans ce chapitre qui concerne l'Union européenne? Premièrement, il n'existe pas un cadre légal qui définit clairement le chiffrement. Cette technique est abordée au travers de dispositions éparses et de divers documents. Il existe tout de même des obligations qui pèsent sur les fournisseurs de services[160] ainsi que les personnes responsables du traitement des données à caractère personnel[161]. Dans le cadre des services relatifs aux communications électroniques, il faudra que des autorités réglementaires nationales vérifient les services fournis pour assurer une harmonisation au niveau européen[162].

Ensuite, le caractère ambivalent du cryptage est constamment remis en avant. Comment concilier d'une part, le rôle important du cryptage dans la protection des données et d'autre part, le besoin des autorités d'accéder à ces informations cryptées dans le cadre des enquêtes pénales? Comment garantir l'un sans affecter l'autre[163]? Cette problématique est accentuée par l'accroissement du phénomène terroriste et la volonté de l'Union européenne de le combattre[164].

---

[156] Commission européenne, Communication au Parlement européen, au Conseil européen et au Conseil concernant le onzième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective, COM(2017) 608 final du 18.10.2017, p.10.

[157] Commission européenne, *ibidem,* p.10.

[158] Commission européenne, *ibidem*, p.11.

[159] Commission européenne, *ibidem*, p.11-12.

[160] 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 (directive " Vie privée et communications électroniques «), considérant n°20, *J.O.U.E.*, L 201/37 du 31 juillet 2002, p.39.

[161] 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), art.32, *J.O.U.E.*, L 119 du 4 mai 2016, p.51.

[162] Directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques (directive « cadre »), art. 1.1, *J.O.U.E.*, L108/33 du 24 avril 2002, p.38.

[163] Voir à ce propos le commentaire de M. Kerkhofs qui veut que soit supprimée cette source de contradiction: Projet de loi relatif à l'amélioration des méthodes particulières de recherche et de certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications. Rapport de la première lecture fait au nom de la Commission de la justice par M. Gautier Calomne et Mme Goedele Uyttersprot, *Doc. parl.*, Ch. Repr., sess. ord. 2015-2016, n°1966/006 du 28 novembre 2016, p.39.

[164] Commission européenne, Communication au Parlement européen, au Conseil européen et au Conseil concernant le onzième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective, COM(2017) 608 final du 18.10.2017, p. 1-18.

Finalement, tout l'enjeu sera de trouver un juste équilibre entre d'une part, la protection des données et d'autre part, la nécessité de récolter des preuves et de faciliter le travail des enquêteurs.

E. BELGIQUE

La Belgique a adopté la loi du 13 juin 2005 relative aux communications électroniques, celle-ci transpose les directives européennes[165]. Cependant, le champ d'application est plus restreint que celui des directives, cette loi s'applique au secteur des télécommunications[166].

La cryptographie est définie comme « *l'ensemble des services mettant en oeuvre les principes, moyens et méthodes de transformation de données dans le but de cacher leur contenu sémantique, d'établir leur authenticité, d'empêcher que leur modification passe inaperçue, de prévenir leur répudiation et d'empêcher leur utilisation non autorisée* »[167]. Les caractéristiques énoncées précédemment se retrouvent dans cette définition, c'est-à-dire la confidentialité, l'intégrité et l'authenticité.

En principe, fournir des services peut se faire librement. Toutefois, dans certaines circonstances, les fournisseurs de services devront respecter des conditions[168]. L'article 48 de la même loi prescrit: « *L'emploi de la cryptographie est libre. La fourniture au public de services de cryptographie que le Roi détermine, après avis de l'Institut, est soumise à une déclaration préalable auprès de l'Institut. Le Roi arrête, après avis de l'Institut, le contenu et la forme de cette déclaration* »[169]. Cette disposition autorise toute personne à utiliser la cryptographie. Par contre, les fournisseurs de services sont soumis à des obligations. Ils doivent rendre une déclaration préalable à l'Institut belge des services postaux et des télécommunications et l'Institut est tenu de donner son avis sur le service de cryptographie.

Le Code d'instruction criminelle mentionne également le cryptage. Notamment, aux articles 39*bis* et 88*quater* du code qui seront particulièrement intéressants pour la suite de l'exposé et seront approfondis ultérieurement.

5. LE CRYPTAGE ET LE DROIT AU SILENCE: PROBLÉMATIQUE

Il convient maintenant de répondre à la question posée en début d'exposé. Il arrive que, dans le cadre d'une affaire pénale, les autorités judiciaires aient besoin d'avoir accès aux données cryptées d'un suspect. Celui-ci peut-il se retrancher derrière le droit au silence ou devra-t-il fournir la clé de cryptage ou même ses codes pour accéder aux données et par conséquent, aux preuves pouvant l'incriminer?

Il convient de remarquer que cette question avait déjà traversé l'esprit des juges en 1996. Selon certains juges, le critère « indépendant de la volonté du suspect » pouvait poser

---

[165] Loi du 13 juin 2005 relative aux communications électroniques, art.1, *M.B.*, 29 juin 2005, p. 28070.

[166] Projet de loi relatif aux communications électroniques, *Doc. parl.*, Ch. Repr., sess. ord. 2004-2005, n° 1425/001 du 4 novembre 2004, p.3.

[167] Loi du 13 juin 2005 relative aux communications électroniques, art. 2,40°, *M.B.*, 29 juin 2005, p. 28070.

[168] Loi du 13 juin 2005 relative aux communications électroniques, art.3, *M.B.*, 29 juin 2005, p. 28070.

[169] Loi du 13 juin 2005 relative aux communications électroniques, art. 48, *M.B.*, 29 juin 2005, p. 28070.

des problèmes. Ils se demandaient comment il faudrait considérer un code PIN ou une clé de cryptage[170]?

A. L'ARTICLE 39*BIS* DU CODE D'INSTRUCTION CRIMINELLE

Tout d'abord, l'article 39*bis* du Code d'instruction criminelle concerne la recherche non secrète dans les systèmes informatiques[171]. Pour saisir le support en lui-même, il faudra utiliser l'article 35 du Code d'instruction criminelle. Cependant, si ce support est saisi, c'est généralement pour avoir accès aux données stockées dans le système. Il s'agira d'une saisie de données « immatérielles » et l'article 39*bis* s'appliquera[172].

> Le 5ème paragraphe prescrit:
>
> « *[e]n vue de permettre les mesures visées à cet article, le procureur du Roi ou le juge d'instruction peut également, sans le consentement du propriétaire ou de son ayant droit, ou de l'utilisateur, ordonner, à tout moment:*
> *- la suppression temporaire de toute protection des systèmes informatiques concernés, le cas échéant à l'aide de moyens techniques, de faux signaux, de fausses clés ou de fausses qualités;*
> *- l'installation de dispositifs techniques dans les systèmes informatiques concernés en vue du décryptage et du décodage de données stockées, traitées ou transmises par ce système.*
> *Toutefois, seul le juge d'instruction peut ordonner cette suppression temporaire de protection ou cette installation de dispositifs techniques lorsque ceci est spécifiquement nécessaire pour l'application du paragraphe 3* ».

Les enquêteurs sont généralement confrontés à un problème: l'accès aux données saisies. En effet, elles peuvent être cryptées ou encore protégées par un code. Afin de pouvoir rechercher des éléments de preuve, le procureur du Roi ou le juge d'instruction peuvent autoriser la suppression temporaire des protections et l'installation de dispositifs pour décrypter les données. L'autorisation ne nécessite aucun consentement du propriétaire, de l'ayant droit ou de l'utilisateur. L'article 88*ter* a été inclus dans cet article et concerne l'extension de la recherche[173].

Existe-t-il une contradiction avec le droit au silence dans ce cas? Tout d'abord, il ne semble pas que les juridictions belges et, a fortiori, les juridictions européennes et internationales aient eu à connaître de cet article.

---

[170] Cour eur. D.H., arrêt *Saunders c. Royaume-Uni*, 17 décembre 1996, Opinion dissidente de M. le juge Martens, à laquelle M. le juge Kuris déclare se rallier, §12.

[171] Projet de loi portant des modifications diverses au Code d'instruction criminelle et au Code pénal, en vue d'améliorer les méthodes particulières de recherche et certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications et créant une banque de données des empreintes, *Doc. parl.*, Ch. Repr., sess. ord. 2015-2016, n° 1966/001 du 8 juillet 2016, p. 8.

[172] A. MASSET, « Le régime des nullités en procédure pénale » *in* A. JACOBS et A. MASSET (sous la direction de), *Actualités de droit pénal et de procédure pénale*, CUP, 148, Larcier, Bruxelles, 2014, p.252.

[173] Projet de loi portant des modifications diverses au Code d'instruction criminelle et au Code pénal, en vue d'améliorer les méthodes particulières de recherche et certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications et créant une banque de données des empreintes, *Doc. parl.*, Ch. Repr., sess. ord. 2015-2016, n° 1966/001 du 8 juillet 2016, p. 8.

Le décryptage par les autorités ne porte pas atteinte au droit au silence. Pour quelles raisons? Dans le cas de l'article 39*bis* §5, le suspect n'intervient pas dans la procédure. On ne lui demande pas de communiquer des informations. Ici, il s'agit d'une procédure visant à déchiffrer les données sans l'accord de la personne, il ne collabore pas. Les autorités ne cherchent pas à obtenir des éléments de preuve en usant de la coercition au mépris de la volonté de l'accusé[174], elles ne cherchent pas à utiliser des subterfuges pour faire parler l'accusé[175]. La jurisprudence de la Cour européenne des droits de l'homme est donc respectée. Dans ce cas de figure, il n'est même pas demandé au suspect de parler.

Il ne faudrait pas arriver à un raisonnement qui empêcherait totalement les autorités d'obtenir les éléments de preuve nécessaires à la manifestation de la vérité.

Cet article doit plutôt être envisagé comme un palliatif à l'absence de coopération du suspect, ce qu'on ne peut lui reprocher. Il sera analysé dans une section suivante. En effet, si un suspect fait usage de son droit au silence en ce qui concerne les données cryptées et la clé de cryptage qui s'y rapporte, les enquêteurs vont tout de même vouloir accéder aux données[176].

Dans un autre registre, cet article pourrait cependant se révéler critiquable du point de vue de l'article 8 de la Convention européenne des droits de l'homme qui protège la vie privée. En effet, les autorités auront accès à des preuves mais également à des éléments très privés qui n'auront aucun rapport avec l'affaire en cours. Ne faudrait-il pas prévoir des limites? Le juge d'instruction ne devrait-il pas être le seul à pouvoir autoriser cette mesure qu'il s'agisse aussi bien de la recherche en elle-même que de l'extension? Il semble que oui. Cependant, cela ne concerne pas le droit au silence, sujet du présent exposé, nous n'allons donc pas l'aborder.

B. L'ARTICLE 88*QUATER* DU CODE D'INSTRUCTION CRIMINELLE

L'article 88*quater* du Code d'instruction criminelle a été introduit par la loi du 28 novembre 2000[177]. Son champ d'application matériel est plus large que celui de l'article 39*bis*. En effet cette disposition concerne le « *système informatique qui fait l'objet de la recherche ou de son extension visée à l'article 39bis, § 3 ou des services qui permettent de protéger ou de crypter des données qui sont stockées, traitées ou transmises par un système informatique* »[178].

L'article 88*quater* porte-t-il atteinte au droit au silence?

---

[174] Cour eur. D.H., arrêt *Saunders c. Royaume-Uni*, 17 décembre 1996, §68.

[175] Conseil de l'Europe/Cour européenne des droits de l'homme, Guide sur l'article 6 de la Convention européenne des droits de l'homme - Droit à un procès équitable (volet pénal), 2014, p. 25, disponible sur www.echr.coe.int (consulté le 18/04/2018).

[176] Projet de loi portant des modifications diverses au Code d'instruction criminelle et au Code pénal, en vue d'améliorer les méthodes particulières de recherche et certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications et créant une banque de données des empreintes, *Doc. parl.*, Ch. Repr., sess. ord. 2015-2016, n° 1966/001 du 8 juillet 2016, p. 22.

[177] Loi du 28 novembre 2000 relative à la criminalité informatique, art. 9, *M.B.*, 03 février 2001, p.02909.

[178] Art. 88*quater* §1 du Code d'instruction criminelle belge.

- Deuxième paragraphe

L'analyse commercera par le deuxième paragraphe car il ne semble pas être problématique. Il dispose que:

> « *Le juge d'instruction ou un officier de police judiciaire auxiliaire du procureur du Roi et de l'auditeur du travail délégué par lui, peut ordonner à toute personne appropriée de mettre en fonctionnement elle-même le système informatique ou, selon le cas, de rechercher, rendre accessibles, copier, rendre inaccessibles ou retirer les données pertinentes qui sont stockées, traitées ou transmises par ce système, dans la forme qu'il aura demandée. Ces personnes sont tenues d'y donner suite, dans la mesure de leurs moyens.*
> *L'ordonnance vises à l'alinéa 1er, ne peut être prise à l'égard de l'inculpé et à l'égard des personnes visées à l'article 156* »[179].

Il s'agit d'ordonner aux personnes, aptes à le faire, de mettre en fonctionnement le système auquel les autorités veulent accéder. Ces personnes doivent intervenir activement[180].

Ce paragraphe exclut expressément de son champ d'application l'inculpé et les personnes visées par l'article 156 du Code d'instruction criminelle, c'est-à-dire la famille du prévenu, au sens large. Les membres de la famille sont exclus car il serait « *difficilement acceptable que ces personnes soient obligées à rassembler des éléments de preuve contre leur proche, sous la contrainte de sanctions pénales* »[181]. Le prévenu est exclu du champ d'application du deuxième paragraphe afin que la disposition n'entre pas en contrariété avec le droit au silence[182]. Toutefois, l'exclusion du suspect pourrait, à mon sens, se justifier autrement. Il ne faudrait pas que le suspect profite de mettre en fonctionnement l'appareil pour supprimer les données compromettantes[183].

- Premier paragraphe

Le premier paragraphe se révèle être plus problématique du point de vue du droit au silence. Il dispose que:

> « *§1er. Le juge d'instruction ou un officier de police judiciaire auxiliaire du procureur du Roi et de l'auditeur du travail délégué par lui, peut ordonner à quiconque dont il présume qu'il a connaissance particulière du système informatique qui fait l'objet de la recherche ou de son extension visée à l'article 39bis, § 3 ou des services qui permettent de protéger ou de crypter des données qui sont stockées,*

---

[179] art. 88*quater* §2 du Code d'instruction criminelle belge.

[180] 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*, p. 28 (disponible sur www.crid.be).

[181] Projet de loi relatif à la criminalité informatique, *Doc. parl.*, Ch. Repr., sess. ord. 1999-2000, n° 213/1 et n° 214/1 du 3 novembre 1999, p. 28.

[182] Projet de loi relatif à la criminalité informatique, *Doc. parl.*, Ch. Repr., sess. ord. 1999-2000, n° 213/1 et n° 214/1 du 3 novembre 1999, p. 27.

[183] Cette justification concerne l'article 39*bis* du C.I.Cr. mais pourrait également, me semble-t-il, se justifier dans le cadre de l'article 88*quater*: « *Le ne doit pas se voir d'abord offrir la possibilité d'introduire lui-même ce code d'accès. En effet, cela impliquerait le risque de voir le suspect effacer les données dans le système informatique par une manipulation rapide ou l'introduction d'un code erroné* » - Projet de loi relatif à l'amélioration des méthodes particulières de recherche et de certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications, *Doc. parl*., Ch. Repr., sess. ord. 2015-2016, n°1966/001 du 8 juillet 2016, p. 22-23.

traitées ou transmises par un système informatique, de fournir des informations sur le fonctionnement de ce système et sur la manière d'y accéder ou d'accéder aux données qui sont stockées, traitées ou transmises par un tel système, dans une forme compréhensible. Le juge d'instruction mentionne les circonstances propres à l'affaire justifiant la mesure dans une ordonnance motivée qu'il transmet au procureur du Roi ou à l'auditeur du travail »[184].

Il est fait obligation à quiconque, sans distinction, de fournir les informations concernant le support. Il s'agit d'une obligation d'information qui peut consister en des explications verbales à propos du fonctionnement, du mot de passe ou encore de clé de chiffrement[185]. Le suspect n'est pas exclu dans cette hypothèse. Cela pose-t-il un problème au niveau du droit au silence et du privilège contre l'auto-incrimination?

Les juridictions belges se sont très peu prononcées à propos de l'article 88*quater* et l'ont fait de manière contradictoire. A présent, il s'agira de dresser les deux visions.

- Violation du droit au silence et du privilège de non-incrimination

La première position est défendue par le Tribunal Correctionnel de Termonde dans un jugement du 17 novembre 2014 et, en appel de ce jugement, par la Cour d'appel de Gand le 23 juin 2015. Les décisions ont conclu à une violation du droit au silence et celui de ne pas s'auto-incriminer.

En 2012, une ordonnance du juge d'instruction avait obligé des suspects à communiquer leur clé de cryptage[186]. Le Tribunal Correctionnel se demandait si cette ordonnance n'était pas contraire au droit au procès équitable, auquel cas, il aurait fallu écarter la preuve obtenue irrégulièrement en vertu de l'article 32 du Titre préliminaire du Code de procédure pénale[187]. Le Tribunal a considéré que cette obligation de fournir la clé de cryptage était contraire au droit du suspect de ne pas s'auto-incriminer[188]. Pour quelles raisons? L'ordonnance du juge d'instruction a obligé à fournir les informations concernant le cryptage, sous contrainte et au mépris de la volonté des prévenus. Les prévenus ont collaboré activement aux preuves à charge qui seront retenues contre eux. Il y a eu une violation des droits de la défense et de l'autonomie procédurale et partant, cet ordonnance était contraire à l'interdiction d'auto-incrimination et le droit à un procès équitable reconnu par la Cour européenne des droits de l'homme[189]. Par conséquent, les preuves obtenues à l'aide de la clé ont été annulées[190].

Ensuite, l'arrêt de 2015 a confirmé la décision du premier juge et a également ajouté de la doctrine pour appuyer ses arguments. Dans de la doctrine concernant l'article 88*quater* du Code d'instruction criminelle, des auteurs avaient reconnu que l'article ne s'appliquait pas

---

[184] art. 88*quater* §1er du Code d'instruction criminelle belge.

[185] 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.*, n°7, 2001, p. 684.

[186] Corr. Termonde, 17 novembre 2014, *T.Strafr.*, 2016/3, p. 256.

[187] Corr. Termonde, *Op. cit.*, p. 257.

[188] Corr. Termonde, *op.cit.*, pp. 255-259.

[189] Corr. Termonde, *op.cit.*, p. 255 et 258.

[190] Corr. Termonde. *op. cit.,* p. 258.

aux suspects mais uniquement aux tiers. Sinon, cela consisterait à dire que les inculpés devraient témoigner ou fournir des preuves à leur encontre[191].

Des auteurs de doctrine ont soutenu la « thèse de la violation » et divers arguments ont été avancés.

Pour certains, la non-exclusion des suspects du champ d'application *ratione personae* de cet article, serait une erreur de la part du législateur et serait en contradiction avec la jurisprudence de la Cour européenne des droits de l'homme[192]. Mais également que la différence de traitement du suspect dans les deux paragraphes n'est pas très claire[193].

D'autres ont considéré qu'il est vrai que la clé de chiffrement pouvait être obtenue avec la volonté du suspect même si l'existence de la clé, après sa création, est indépendante de sa volonté[194].

- Non-violation du droit au silence et du privilège de non-incrimination

La deuxième position est celle défendue par la chambre des mises en accusation d'Anvers dans un arrêt prononcé le 21 décembre 2017. Les faits concernaient une dame soupçonnée de traite d'être humains. Le juge d'instruction avait ordonné à l'inculpée de donner ses codes de sécurité conformément à l'article 88*quater*, premier paragraphe. Cependant, il se ravise et décide qu'un tel ordre ne peut être ordonné à un suspect. Le bureau du procureur du Roi a fait appel de la seconde ordonnance[195].

Selon la Cour, le suspect est exclu du champ d'application personnel du deuxième paragraphe mais pas du premier paragraphe. La Cour renvoie aux travaux préparatoires affirmant que cette obligation de collaboration du suspect ne viole pas le droit au procès équitable[196]. Plus précisément, la Cour considère que fournir une clé de cryptage n'est pas protégé par le droit au silence car il s'agit d'une donnée qui existe indépendamment de la volonté du suspect[197]. La chambre des mises en accusation a conclu en le respect du droit au procès équitable essentiellement parce que la clé de cryptage ne dépend pas de la volonté de l'accusé, elle doit simplement être correcte. De plus, une clé de cryptage n'est pas un élément à charge en elle-même, ce sont les données stockées qui peuvent être incriminantes[198].

---

[191] Gent, 23 juni 2015, *T. Strafr.*, 2016/3, p.241 concernant J. KERKHOFS et Ph. VAN LINTHOUT, « Cybercriminaliteit doorgelicht », *T.Strafr*., n°4, 2010, pp. 192-193.

[192] C. VAN DE HEYNING et J. COPPENS, « Noot - Het bevel tot medewerking van artikel 88*quater* Sv., het zwijgrecht en het verbod op zelfincriminatie », *T. Strafr.*, 2016/3, p. 262; voir à ce propos note de bas de page n° 19: P. DE HERT en G. LICHTENSTEIN, "De wet van 28 november 2000 inzake informaticacriminaliteit en het formeel strafrecht" in CENTRUM VOOR BEROEPSVERVOLMAKING IN DE RECHTEN (ed.), *Jaarboek 2002-2003*, Antwerpen, Maklu, 408-410. Zij verwijzen daarbij ook naar een analyse van de Nederlandse situatie door B. KOOPS, *Verdachte en ontsleutelplicht: hoe verreikt nemo tenetur?*, Kluwer, Deventer, 2000, 125p.

[193] D. DEWANDELEER, « Computermisdrijven en strafonderzoek in een ICT-context », *Themis 57- Straf-en strafprocesrecht*, Brugge, La Charte, 2017, p. 159.

[194] C. VAN DE HEYNING et J. COPPENS, « Noot - Het bevel tot medewerking van artikel 88*quater* Sv., het zwijgrecht en het verbod op zelfincriminatie », *T. Strafr.*, 2016/3, p. 264; voir à ce propos note de bas de page n° 31: B.J. KOOPS, "Het decryptiebevel en het nemo-teneturbeginsel: Nopen ontwikkelingen sinds 2000 tot invoering van een ontsleutelplicht voor verdachten?", Universiteit van Tilburg, 2012, 85.

[195] Antwerpen (Kamer van Inbeschuldigingstelling), K/2895/2017, 21 december 2017, inédit, p. 2.

[196] Antwerpen (Kamer van Inbeschuldigingstelling), *op. cit.,* p. 3.

[197] Antwerpen (Kamer van Inbeschuldigingstelling), *op. cit.,* p. 3.

[198] Antwerpen (Kamer van Inbeschuldigingstelling), *op. cit.,* p. 3.

La Cour d'appel va raisonner en trois étapes. Tout d'abord, elle analyse le *principe nemo tenetur* et il y a bien une coercition puisqu'on criminalise la non-coopération[199]. Le suspect pourrait tout de même considérer qu'il s'incrimine indirectement[200]. Ensuite, l'obligation de décryptage ne peut pas, selon elle, être considérée comme une ingérence grave qui porterait atteinte à l'essence même du privilège contre l'auto-incrimination[201]. Et finalement, cette ingérence serait justifiée par l'intérêt public[202].

Plus récemment encore, le 8 février 2018, la chambre des mises en accusation de Gand a elle aussi déclaré que l'article 88*quater*, premier paragraphe ne violait pas la droit au procès équitable. En ce sens qu'il s'agit d'une obligation de coopération passive[203].

La doctrine s'est également prononcée en ce sens. L'argument principal est de se référer aux travaux préparatoires pour justifier que le premier paragraphe puisse s'appliquer à l'égard d'un suspect. Mais également parce que les preuves obtenues sont fiables et qu'il ne s'agit pas de renverser la charge de la preuve[204].

- Appréciation

Les deux visions défendues par les Cours et tribunaux belges ainsi que par la doctrine étant dressées, il convient maintenant de prendre position.

Tout d'abord, le droit au silence et le droit à ne pas être obligé de s'incriminer soi-même interdisent à l'accusation de recourir à des éléments de preuve en utilisant la coercition abusive, au mépris de la volonté de l'accusé[205]. Cependant, cela n'est pas interdit s'il s'agit de preuves indépendantes de la volonté de l'accusé[206].

La question essentielle à se poser est de savoir si cette clé de cryptage, voire le cryptage en lui-même, est une donné dépendante de la volonté du suspect ou non. Si les données sont indépendantes de la volonté du suspect, alors le droit au silence ne les protégera pas. La volonté peut se définir comme la « *faculté de déterminer librement ses actes en fonction de motifs rationnels; pouvoir de faire ou de ne pas faire quelque chose* »[207].

Il semble que le cryptage soit dépendant de la volonté du suspect. Dans le cas d'un simple code ou d'un mot de passe sur un téléphone portable, il émane clairement de notre volonté. Et ce, contrairement à des éléments comme l'ADN ou des prélèvements qui sont

---

[199] Antwerpen (Kamer van Inbeschuldigingstelling), *op. cit.,* p. 4.

[200] Antwerpen (Kamer van Inbeschuldigingstelling), *op. cit.,* p. 5.

[201] Antwerpen (Kamer van Inbeschuldigingstelling), *op. cit.,* p. 5.

[202] Antwerpen (Kamer van Inbeschuldigingstelling), *op. cit.,* pp.5-6.

[203] F. SCHUERMANS, « Verdachte heeft passieve medewerkingsplicht bij zoekingen in zijn smartphone », *De Juristenkrant*, nr 364, 28 février 2018, pp. 2-3.

[204] C. CONINGS, « Ontsleutelplicht van verdachte en verbod op zelfincriminatie », *N.J.W.*, 17 février 2016, pp. 135-136.

[205] Conseil de l'Europe/Cour européenne des droits de l'homme, Guide sur l'article 6 de la Convention européenne des droits de l'homme - Droit à un procès équitable (volet pénal), 2014, p. 25, disponible sur www.echr.coe.int (consulté le 18/04/2018).

[206] Conseil de l'Europe/Cour européenne des droits de l'homme, Guide sur l'article 6 de la Convention européenne des droits de l'homme - Droit à un procès équitable (volet pénal), 2014, p. 25, disponible sur www.echr.coe.int (consulté le 18/04/2018).

[207] Définition du mot volonté disponible sur www.larousse.fr.

vraiment indépendants de la volonté du suspect. En effet, personne ne choisit sa naissance, ni ses gênes.

Selon KOOPS, il est vrai qu'après avoir été créée, l'existence de la clé ne dépend plus du suspect mais sa communication dépend bien de sa volonté[208]. Le cryptage asymétrique suppose que les personnes qui veulent communiquer partagent une clé commune[209] et en cas de cryptage asymétrique, l'utilisateur a une clé secrète et peut distribuer une clé publique[210]. Il y a donc une volonté de partager cette clé ou non. Ajoutons également qu'en Belgique l'utilisation du chiffrement est libre[211]. Les personnes pourront décider librement d'utiliser le cryptage ce qui signifie encore une fois qu'il s'agit d'une volonté. L'utilisation du cryptage ainsi que la communication de la clé de cryptage sont totalement dépendants de la volonté de l'utilisateur. Dès lors, le droit au silence couvre de tels éléments de preuve.

Il faudra cependant vérifier s'il est porté atteinte à l'essence même du droit au silence. En effet, selon la jurisprudence Jalloh, « *Pour rechercher si une procédure a anéanti la substance même du droit de ne pas contribuer à sa propre incrimination, la Cour doit examiner en particulier les éléments suivants : la nature et le degré de la coercition, l'existence de garanties appropriées dans la procédure et l'utilisation qui est faite des éléments ainsi obtenus* »[212]. La Cour européenne des droits de l'homme n'a pas eu à connaître d'un tel cas, il apparaît donc opportun de réaliser le test dans cet exposé afin de pouvoir trancher la question.

En premier lieu, il faut constater que le premier paragraphe oblige le suspect à fournir des informations sur le système et notamment sa clé de cryptage. Cette obligation est appelée par certains auteurs une obligation passive[213]. Tandis que le deuxième paragraphe oblige à mettre un système en fonctionnement, ce qui est parfois qualifié d'obligation de collaboration active[214]. Il y aurait donc une différence de nature dans l'obligation qui justifierait une différence de traitement de l'accusé[215]. Cependant, même s'il ne s'agit pas matériellement de la même action, les conséquences s'avèrent être les mêmes: l'accès des autorités aux données, pouvant être incriminantes, stockées sur le support informatique.

---

[208] C. VAN DE HEYNING et J. COPPENS, « Noot - Het bevel tot medewerking van artikel 88*quater* Sv., het zwijgrecht en het verbod op zelfincriminatie », *T. Strafr.*, 2016/3, p. 264; voir à ce propos note de bas de page n° 31: B.J. KOOPS, "Het decryptiebevel en het nemo-teneturbeginsel: Nopen ontwikkelingen sinds 2000 tot invoering van een ontsleutelplicht voor verdachten?", Universiteit van Tilburg, 2012, 85.

[209] J.-N. COLIN, « Du secret à la confiance… quelques éléments de cryptographie » *in* H. JACQUEMIN (sous la direction de), *L'identification électronique et les services de confiance depuis le règlement eIDAS*, CRIDS, 39, Bruxelles, Larcier, 2016, p. 10.

[210] J.-N. COLIN, *op. cit.*, p. 11.

[211] Loi du 13 juin 2005 relative aux communications électroniques, art. 48, *M.B.*, 29 juin 2005, p. 28070.

[212] Cour eur. D.H., arrêt *Jalloh c. Allemagne*, 11 juillet 2006, §101.

[213] F. SCHUERMANS, « Verdachte heeft passieve medewerkingsplicht bij zoekingen in zijn smartphone », *De Juristenkrant*, nr 364, 28 février 2018, pp. 2-3.

[214] F. SCHUERMANS, *op. cit.*, p.3; C. CONINGS, « Ontsleutelplicht van verdachte en verbod op zelfincriminatie », *N.J.W.*, 17 février 2016, p.135; D. DEWANDELEER, « Computermisdrijven en strafonderzoek in een ICT-context », *Themis 57- Straf-en strafprocesrecht*, Brugge, La Charte, 2017, p.160.

[215] Projet de loi relatif à la criminalité informatique, *Doc. parl.*, Ch. Repr., sess. ord. 1999-2000, n° 213/1 et n° 214/1 du 3 novembre 1999, p. 27.

De plus, il existe des sanctions, particulièrement élevées, en cas de refus de collaboration. Par conséquent, soit le suspect ne coopère pas et se voit infliger une sanction, soit il coopère et risque également de se voir infliger une sanction. Il existe une coercition abusive de la part des autorités. Le degré de la coercition semble être élevé car peu importe le choix qui sera fait, il aboutira à une sanction élevée.

L'article 88*quater*, premier paragraphe, in fine prévoit que l'ordonnance du juge d'instruction devra être motivée en fonction des circonstances propres à l'espèce. Est-ce une garantie appropriée? Il semble qu'on ne puisse pas répondre à cette réponse de manière abstraite. Il conviendra d'analyser si, *in casu*, l'ordonnance se justifie. Il faudra également analyser que la motivation n'est pas stéréotypée[216].

Il convient d'analyser le critère de l'utilisation faite des preuves. En ce qui concerne l'affirmation de la Chambre des mises en accusation selon laquelle fournir la clé n'est pas en soi incriminant[217]. C'est vrai, cependant, elle donne accès à des éléments qui peuvent être incriminants. En réalité, il ne s'agit pas d'une simple information anodine qui viendrait uniquement appuyer ce que les enquêteurs savent déjà. C'est bien plus que cela, la clé donne accès aux infractions dans la plupart des cas et de nouvelles infractions peuvent même être découverte. Les autorités judiciaires ont donc accès à des données potentiellement illimitées.

> En effet, « *la clé est susceptible de donner accès à de nombreuses données, dont certaines seulement constituent des éléments de preuves recherchés par l'instruction. Le juge ne jouit pas pour autant d'un accès légitime ou nécessaire à toutes les autres données. Il lui est cependant difficile de distinguer dans le contenu crypté les données auxquelles il lui est indispensable d'avoir accès et les autres. Le munir d'une clé de décryptage l'autorise à accéder à des données de manière disproportionnée (…) La remise des clés de cryptage doit par conséquent être limitée aux cas dans lesquels une telle mesure se révèle indispensable* »[218].

Il est possible de considérer qu'il n'y a pas de violation de l'article 6 si la pièce obtenue a un caractère limité dans l'ensemble des documents et ne permet d'établir à elle seule la culpabilité du prévenu[219]. Cependant, l'article 88*quater*, paragraphe premier, va plus loin que le caractère limité qu'autorise la Cour européenne des droits de l'homme, à titre d'exemple, fournir l'identité d'un conducteur lorsqu'on connaît déjà l'infraction[220]. Par conséquent, il faudra analyser, *in casu*, quelle utilisation sera faite des preuves et également s'il existait d'autres preuves.

---

[216] Exemple en ce qui concerne le refus des motivations stéréotypées par la Cour européenne des droits de l'homme: Cour eur. D.H., arrêt *Buzadji c. République de Moldova*, 5 juillet 2016, §122. Cet arrêt concerne la matière de la détention préventive. A mon sens, la motivation concernant l'ordonnance délivrée en vertu de l'article 88*quater* ne doit pas être stéréotypée.

[217] Antwerpen (Kamer van Inbeschuldigingstelling), *op. cit.,* p.3.

[218] 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*, pp. 28-29 (disponible sur www.crid.be).

[219] Cour eur. D.H., arrêt *Bykov c. Russie*, 10 mars 2009, §104; Cour eur. D.H., arrêt *O'Halloran et Francis c. Royaume-Uni*, 29 juin 2007, §62; Conseil de l'Europe/Cour européenne des droits de l'homme, Guide sur l'article 6 de la Convention européenne des droits de l'homme - Droit à un procès équitable (volet pénal), 2014, p.25-26, disponible sur www.echr.coe.int (consulté le 18/04/2018).

[220] Cour eur. D.H. (gde ch.), arrêt *O'Halloran et Francis c. Royaume-Uni*, 29 juin 2007, §58.

Il est vrai qu'il est de l'intérêt des enquêteurs d'avoir accès aux informations notamment pour des raisons de sécurité. Il faudra mettre cet intérêt en balance avec le fait qu'en principe les preuves doivent être obtenues régulièrement. L'intérêt public ne devra pas aboutir à anéantir le droit au silence[221].

Il convient de conclure qu'ordonner au suspect de communiquer la clé de cryptage sera difficilement compatible avec le droit au silence et le privilège contre l'auto-incrimination. Cependant, tous les éléments relatifs aux faits devront être pris en considération.

- Quid du mot de passe?

Comme précisé précédemment, cet exposé n'a pas vocation à se prononcer sur le mot de passe ou le code d'accès. Cependant, il me semble intéressant d'en dire quelques mots.

Prenant en considération que le mot de passe a pour but de sécuriser un appareil électronique et qu'il a un but similaire au cryptage, dans la plupart des cas. Il me semble qu'il faudra l'assimiler au cryptage et considérer qu'un accusé peut exercer son droit au silence pour ne pas délivrer son code aux autorités[222].

En effet, le code n'est pas, en lui-même, une preuve à charge mais conduira probablement à des éléments pouvant entraîner la condamnation du suspect. Par conséquent, le raisonnement exposé en ce qui concerne les clés de cryptage vaut également à propos des mots de passe.

Comment vont faire les autorités pour avoir accès aux informations sans violer le droit au procès équitable?

6. PALLIATIFS: QUELLES SOLUTIONS POUR LES ENQUÊTEURS?

Compte tenu de la section précédente, il me semble que les autorités de poursuite ne pourront pas se servir de l'article 88*quater* du Code d'instruction criminelle, à l'encontre d'un suspect, pour obtenir la clé de cryptage qui donnera accès à toutes les données contenues sur le support informatique. En effet, cela serait difficilement compatible avec le droit au silence et l'interdiction d'auto-incrimination. De ce fait, le travail des enquêteurs se complique.

L'actualité prouve que le cryptage est remis en question, notamment suite aux attentats terroristes[223]. Cependant, les Etats ne sont pas unanimes sur la façon de faire face aux problèmes concernant le cryptage et les enquêtes. Des Etats comme la France et le Royaume-Uni souhaitent plutôt contourner la cryptographie alors que des Etats, comme les Pays-Bas et

---

[221] Cour eur. D.H., arrêt *Jalloh c. Allemagne*, 11 juillet 2006, §97; Cour eur. D.H., arrêt *Heaney et McGuinness c. Irlande*, 21 décembre 2000, §§57-58; Conseil de l'Europe/Cour européenne des droits de l'homme, Guide sur l'article 6 de la Convention européenne des droits de l'homme - Droit à un procès équitable (volet pénal), 2014, p. 26, disponible sur www.echr.coe.int (consulté le 18/04/2018).

[222] J. LAUSSON, « Non, une garde à vue ne vous oblige pas à déverrouiller votre smartphone », *numerama*, 18 avril 2018, disponible sur numerama.com (consulté le 30/04/2018) et B. FITEN, « Apple vs. het FBI: veel vragen blijven onbeantwoord », *Juristenkrant*, n°327, 2016, pp.12-13.

[223] Commission européenne, Communication au Parlement européen, au Conseil européen et au Conseil concernant le onzième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective, COM(2017) 608 final du 18.10.2017; Y. VAN COUTER et E. ROEGIERS, « Les défis de la cybersécurité », *Journal de droit européen*, Juin 2016, n°230, p.213; E. DENÉCÉ, « La révolution du renseignement », *Sécurité globale*, 2008/2 (N°4), p.41 et J. LAUSSON, « Chiffrement: l'Union européenne en ordre dispersé », *numerama*, 05/12/2016, disponible sur numerama.com (consulté le 22/03/2018).

l'Allemagne sont favorables au chiffrement et considèrent qu'il s'agit d'un droit fondamental qu'il convient de protéger[224]. D'autres Etats sont, quant à eux, en faveur d'une loi européenne qui permettrait d'accéder aux informations privées et au cloud ainsi qu'un partage des données au niveau transfrontalier[225].

Cette section ne se veut pas exhaustive mais envisagera des pistes de réflexion. Elle aura pour but d'analyser les différentes solutions qui s'offrent aux enquêteurs, principalement belges, pour obtenir les informations cryptées sans forcer le suspecter à collaborer à sa propre incrimination.

A. L'ARTICLE 39*BIS* DU CODE D'INSTRUCTION CRIMINELLE

Premièrement, en ce qui concerne la Belgique, il s'agira d'envisager l'article 39*bis* du Code d'instruction criminelle, précédemment mentionné. Le procureur du Roi et le juge d'instruction pourront autoriser que soit installé un moyen permettant de décrypter les données d'un système, et ce, sans avoir besoin de l'accord de la personne concernée[226].

Le cinquième paragraphe de l'article 39*bis* prévoit que les protections peuvent être supprimées à l'aide de fausses clés. Cette notion a été précisée par le projet de loi:

> « *Les notions de 'faux signaux' et de 'fausses clés' se réfèrent à 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. Ainsi, un mot de passe craqué peut notamment être considéré comme une fausse clé. Par 'la suppression de toute protection', il n'est pas entendu l'entrée d'un mot de passe correct* »[227].

Ici, l'autorisation est donnée au gouvernement de craquer le système. Il s'agit d'une sorte de hacking ou de piratage par le gouvernement.

Comme expliqué précédemment, l'avantage de cette technique est qu'elle ne semble pas contrevenir à l'interdiction d'auto-incrimination et au droit au silence. Toutefois, cela pourrait poser des problèmes au niveau de la protection de la vie privée, garantie par l'article 8 de la Convention européenne des droits de l'homme[228]. Il pourrait être reproché qu'il n'y a aucune limite aux informations auxquelles les autorités pourront avoir accès. Il est vrai qu'il pourrait y avoir un accès aux éléments de preuve concernant l'infraction mais également à toute sorte d'informations extrêmement privées: des photos de famille, des données bancaires, des conversations intimes,… Il y aurait donc une certaine forme de comparaison avec la

---

[224] J. LAUSSON, « Chiffrement: l'Union européenne en ordre dispersé », *numerama*, 05/12/2016, disponible sur numerama.com (consulté le 22/03/2018).

[225] J. LAUSSON, « Chiffrement: l'Union européenne en ordre dispersé », *numerama*, 05/12/2016, disponible sur numerama.com (consulté le 22/03/2018).

[226] Art. 39*bis* §5 du Code d'instruction criminelle belge.

[227] Projet de loi relatif à l'amélioration des méthodes particulières de recherche et de certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications, *Doc. parl.*, Ch. Repr., sess. ord. 2015-2016, n°1966/001 du 8 juillet 2016, pp. 21-22.

[228] F. KONING, « Reconnaissance du droit du citoyen de refuser de donner accès à un système informatique nonobstant l'ordre de la loi, et reconnaissance d'un droit de recours contre un refus du parquet de laisser consulter son dossier d'information », *J.L.M.B.*, 2016/16, p. 738.

perquisition d'un domicile, il conviendrait de prévoir des garanties similaires[229]. Cependant, cela n'est pas le sujet du présent exposé.

Les inconvénients sont nombreux. Il conviendra tout d'abord de détecter le type de cryptage utilisé. Et ensuite et principalement, il faudra déchiffrer. Cela impose d'utiliser du matériel très performant et couteux[230]. De plus, cela peut prendre énormément de temps et être très complexe.

> En ce sens, « *casser le chiffrement en lui-même est vraiment compliqué, voire souvent quasi impossible avec les ressources dont on dispose aujourd'hui. Donc les possibilités pour casser du chiffrement évoquées dans le rapport sont plus adaptées pour des chiffrements avec des algorithmes faibles ou des algorithmes forts mais combinées avec des algorithmes faibles* »[231].

Mais justement, le cryptage est de plus en plus complexe et sophistiqué[232]. Par conséquent, le décryptage sera soit impossible ou prendra trop de temps[233].

Il faut également prendre en considération que chaque nouvel accès nécessitera l'accord du juge d'instruction pour utiliser une nouvelle clé[234]. Cela ne facilite pas le travail des enquêteurs qui était déjà très compliqué.

B. Les entreprises et fournisseurs de services

La coopération des entreprises et fournisseurs de services est essentielle dans cette matière. Pour accéder aux données cryptées, les autorités s'adressent aux entreprises.

Si l'article 88*quater* n'existait pas, la recherche dans un système informatique ne serait pas optimale[235]. Cet article oblige ceux qui ont une connaissance particulière d'un système, d'une part, à fournir les informations sur ce système et son fonctionnement et, d'autre part, à faire fonctionner ce système. L'obligation peut être donnée à diverses personnes, le projet de loi en mentionne quelques unes, de manière non-exhaustive: « *il peut s'agir d'importateurs/ de distributeurs d'ordinateurs ou de logiciels, de « trusted third parties », de fournisseurs de*

---

[229] C. Forget, « La collecte de preuves informatiques en matière pénale » *in* J-F Henrotte et F. Jongen (sous la direction de), *Pas de droit sans technologie*, CUP, 158, Bruxelles, Larcier, 2015, pp. 257-260.

[230] Conseil de l'Union européenne, Rapport final sur la septième série d'évaluations mutuelles sur la mise en oeuvre pratique et le fonctionnement des politiques européennes en matière de prévention de la cybercriminalité et de la lutte contre celle-ci, 12711/17, 2 octobre 2017, p. 48.

[231] Propos de Jef Mathiot dans P. Hérard, « Cybercriminalité: comment l'Europe veut contourner la confidentialité des communications », *TV5MONDE*, 22 octobre 2017, mise à jour le 11.11.2017 disponible sur information.tv5monde (consulté le 13 avril 2018).

[232] Conseil de l'Union européenne, Rapport final sur la septième série d'évaluations mutuelles sur la mise en oeuvre pratique et le fonctionnement des politiques européennes en matière de prévention de la cybercriminalité et de la lutte contre celle-ci, 12711/17, 2 octobre 2017, p. 47.

[233] M. Wack, N. Cottin, B. Mignot et A. ElMoundi, « Certification et archivage légal de dossiers numériques », *Document numérique*, 2002/1, vol.6, p.148.

[234] Projet de loi relatif à l'amélioration des méthodes particulières de recherche et de certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications, *Doc. parl.*, Ch. Repr., sess. ord. 2015-2016, n°1966/001 du 8 juillet 2016, p. 20.

[235] Projet de loi relatif à la criminalité informatique, *Doc. parl.*, Ch. Repr., sess. ord. 1999-2000, n° 213/1 et n° 214/1 du 3 novembre 1999, p. 26.

service, d'opérateurs, d'ingénieurs d'entreprise ayant élaboré une configuration informatique spécifique, de spécialiste de la sécurité, … »[236].

Cependant, pour diverses raisons, les entreprises ne sont pas toujours enclines à coopérer. La première raison que l'on peut épingler est le caractère transfrontalier des services. Cela complique considérablement le travail des autorités répressives notamment au regard de la loi applicable[237]. En ce qui concerne les obligations de collaboration imposées à certaines entreprises en vertu du Code d'instruction criminelle, il est en principe contraire au droit international qu'un état puisse imposer des mesures contraignantes sur un autre territoire que le sien[238].

On retrouve également une tendance différente à collaborer, selon les entreprises. Certaines coopèrent sans grande difficulté tandis que d'autres refusent catégoriquement, invoquant notamment leurs intérêts commerciaux[239].

En effet, il existe des risques pour l'intérêt commercial. Il peut être reproché qu'après que les clés soient remises, il n'existe pas de règles visant à les protéger. Ces clés pourraient donc être détournées et pourraient tomber entre de mauvaises mains[240]. C'est pour cela que les entreprises préfèrent remettre la clé à l'utilisateur et n'avoir aucune responsabilité dans le processus. Ainsi, en cas d'ordre provenant des autorités, elles peuvent soutenir que les données sont cryptées pour elles aussi[241]. Le risque est également grand pour les sociétés commerciales que la confiance du consommateur soit brisée si l'utilisateur sait que la police peut avoir accès à ses données protégées.

Un autre conflit pourrait également survenir entre d'une part, les pays très protecteur de la vie privée et ceux qui le sont beaucoup moins. Les premiers pourraient interdire les entreprises se trouvant sur leur territoire de collaborer et les autres pourraient obliger leurs entreprises et celles se trouvant sur d'autres états membres à collaborer. Certains pays pourraient également invoquer le principe de souveraineté pour refuser la demande[242].

Finalement, obliger les fournisseurs de services à fournir les clés de cryptage contrevient au principe de chiffrement de bout-en-bout selon lequel seul l'utilisateur devrait

---

[236] Projet de loi relatif à la criminalité informatique, *Doc. parl.*, Ch. Repr., sess. ord. 1999-2000, n° 213/1 et n° 214/1 du 3 novembre 1999, p. 27.

[237] A. GOSSÉ, « Dans quelle mesure les autorités judiciaires belges peuvent-elles contraindre des entreprises de télécommunication étrangères à collaborer à une enquête pénale en Belgique? », *droit pénal de l'entreprise*, 2017/3, p. 180.

[238] A. GOSSÉ, *op.cit.*, p. 196 voir également dans ce texte les notes de bas de page n°195: J. KERKHOFS et P. VAN LINTHOUT, *Cybercrime*, Bruxelles, Politeia, 2013, p. 445 et n°196: K. DE SCHEPPER et F. VERBRUGGEN, « Ontsnappen space invaders aan onze pacmannen? De materiële en formele strafrechtsmacht van België bij strafbare weigering van de medewerking door elektronische dienstverleners », *T. Strafr.*, 2016/3, p. 163.

[239] A. GOSSÉ, *op. cit.*, p. 180.

[240] 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*, p. 29 (disponible sur www.crid.be).

[241] A. GOSSÉ, *op. cit*., p. 192; B. FITEN, « Apple vs. het FBI: veel vragen blijven onbeantwoord », *Juristenkrant*, n°327, 2016, p.12.

[242] A. GOSSÉ, *op.cit.*, pp. 196-197.

être en connaissance de cette clé ainsi que les personnes avec lesquelles il communique, à l'exclusion de tout intermédiaire[243].

C. LA PORTE DÉROBÉE: « *BACK DOOR* »

Pour contrecarrer la problématique du cryptage et l'accès aux données par les autorités, une solution a été envisagée: la *back door*.

De quoi s'agit-il? « *Une porte dérobée se traduit habituellement par l'existence d'un moyen d'accès non autorisé, dissimulé dans un programme, pour faciliter l'intrusion des pirates informatiques et l'installation d'autres malwares* »[244]. Ici, précisément, l'utilisation d'une porte dérobée permettrait aux enquêteurs de s'en servir pour accéder aux données cryptées.

Dans l'affaire des attaques terroristes de San Bernardino, le FBI avait requis l'intervention d'Apple afin de déverrouiller un iPhone bloqué. Apple avait refusé de créer une *back door*. La société considérait que cela créerait un précédent dangereux. Cette porte pourrait être utilisée par les criminels mais également par des pays pour restreindre les libertés[245].

L'utilisation des portes dérobées faciliterait considérablement le travail judiciaire. Les *back doors* sont difficiles à déceler[246], leur utilisation par le gouvernement signifie également que d'autres personnes, ayant des intentions malveillantes, pourront pénétrer dans le support informatique.

En 2004, l'Union européenne a créé le rôle de contrôleur européen de la protection des données, il fait respecter les règles à ce propos[247]. L'article 39 du Traité sur l'Union européenne et l'article 16 du Traité sur le fonctionnement de l'Union européenne imposent la protection des données à caractère personnel et les institutions doivent veiller au respect de ces données. Le contrôleur est garant du bon respect de ces articles. Il avait fermement déconseillé l'usage des *back doors* et encouragé le cryptage de bout en bout[248]. Cette solution envisagée au niveau européen a été abandonnée à cause de questions de liberté et de vie privée[249].

---

243 G. CHAMPEAU, « Lutte contre le chiffrement: le gouvernement dévoile ses pistes », *numerama*, 5/09/2016, numerama.com (consulté le 22/03/2018).

244 X., « Qu'est-ce qu'une porte dérobée », disponible sur http://www.anti-cybercriminalite.fr (consulté le 13 avril 2018).

245 B. FITEN, « Apple vs. het FBI: veel vragen blijven onbeantwoord », *Juristenkrant*, n°327, 2016, p.12.

246 B.-R. RIVIÈRE, « Systèmes informatiques: Portes dérobées, la menace fantôme », *LesEchos*, 22/04/2011, disponible sur archives.lesechos.fr (consulté le 14 avril 2018).

247 Union européenne, « Contrôleur européen de la protection des données » disponible sur europa.eu.

248 J. LAUSSON, « Le chiffrement sans backdoor doit être 'encouragé et, si nécessaire, rendu obligatoire' », *numerama*, 28 juillet 2016, disponible sur numerama.com, (consulté le 22/03/2018); dans le même ordre d'idée: J. VALERO, « Ansip: 'I am strongly against any backdoor to encrypted systems' », *euractiv*, 23 février 2016, disponible sur euractiv.com (consulté le 30/04/2018).

249 P. HÉRARD, « Cybercriminalité: comment l'Europe veut contourner la confidentialité des communications », *TV5MONDE*, 22 octobre 2017, mise à jour le 11.11.2017 disponible sur information.tv5monde (consulté le 13 avril 2018).

A mon sens, la collaboration des fournisseurs de services est la meilleure option qui s'offre aux enquêteurs s'ils veulent avoir accès aux données cryptées. Cette solution ne violerait pas le droit au silence du suspect et serait le choix le plus respectueux du point de vue des droits de l'homme et de la vie privée. Il est vrai que la clé, une fois remise, pourrait tomber entre des mains indélicates. Cependant, cela semble bien plus sécurisé que l'installation de *back doors* par tous les fournisseurs de services. De plus, en Belgique, la non-collaboration entraîne une amende plutôt conséquente ce qui permet de limiter les cas de refus des entreprises. Cependant, ce sujet est controversé et connaît des partisans comme des détracteurs[250].

7. CONCLUSION

Le droit au silence a fait l'objet d'énormément de discussions. La jurisprudence a, à de nombreuses reprises, tenté de cerner les tenants et les aboutissants du droit au procès équitable. L'analyse a permis de mettre en lumière que ce droit n'est pas absolu. Et qu'en principe, beaucoup d'éléments devront être pris en considération pour apprécier s'il y a eu une atteinte au droit au silence.

Le cryptage a connu des développements essentiellement dans des ouvrages de nature plutôt scientifique. Une approche juridique a également été nécessaire. Principalement parce que la cryptographie a mis en évidence un important problème: l'accès, par les autorités judiciaires, aux données stockées sur les supports informatiques.

Cela a poussé les états à prendre des mesures pour contourner la problématique du chiffrement. En ce qui concerne la Belgique, l'analyse s'est portée sur les articles 39*bis* et 88*quater* du Code d'instruction criminelle. Mais est-ce que ces articles sont en conformité avec le droit au silence? Il me semble que l'article 39*bis* n'est pas contraire au droit au silence. Par contre, à ce propos, l'article 88*quater* se révèle plus problématique. Plusieurs éléments permettent d'aboutir à cette conclusion. Cependant, les juridictions belges se sont très peu prononcées. Et à ma connaissance, les juridictions européennes et internationales ne l'ont pas fait. Par conséquent, il convient de rester prudent.

Quelles sont alors les alternatives pour les enquêteurs? Plusieurs pistes de réflexion ont été abordées. L'analyse a mis en évidence que les solutions avaient leurs avantages et inconvénients. A ce sujet, les Etats n'ont pas adopté une voie claire et identique. La question reste assez controversée.

Le cryptage et le droit au silence connaîtront encore des évolutions. La Cour européenne de justice ainsi que la Cour européenne des droits de l'homme seront probablement amenées, dans un futur proche, à se prononcer sur la question. Cela nous permettra d'avoir une vision plus précise de la place du droit au silence à l'ère numérique.

[250] B. FITEN, « Apple vs. het FBI: veel vragen blijven onbeantwoord », *Juristenkrant*, n°327, 2016, p.12.

BIBLIOGRAPHIE

A. Législation et travaux parlementaires

1. Droit international

- Conventions et Pactes

Convention de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950, approuvée par la loi du 13 mai 1955, *M.B.*, 19 août 1955, *err.*, 29 juin 1961.

Convention sur la cybercriminalité faite à Budapest le 23 novembre 2001 approuvée par la loi 3 août 2012, *M.B.*, 21 novembre 2012.

Convention sur le cybercriminalité, rapport explicatif, http://www.europarl.europa.eu.

Pacte international relatif aux droits civils et politiques, adopté à New-York le 16 décembre 1966 par l'Assemblée générale des Nations unies.

- Autres documents

Conseil de l'Union européenne, Rapport final sur la septième série d'évaluations mutuelle sur la mise en oeuvre pratique et le fonctionnement des politiques européennes en matière de prévention de la cybercriminalité et de lutte contre celle-ci - informations communiquées au Conseil, 12711/17 du 2 octobre 2017, p.1-97.

Conseil de l'Europe, 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, adoptée le 11 septembre 1995 lors de la 543e réunion des Délégués des Ministres.

Gouvernance de l'internet - Stratégie du Conseil de l'Europe 2016-2019 - Démocratie, droits de l'homme et Etat de droit dans le monde numérique adoptée à la 1252e réunion des Délégués des Ministres le 30 mars 2016, 22 p.

2. Droit de l'Union européenne

- Traités

Traité sur le fonctionnement de l'Union européenne

Traité sur l'Union européenne

- Droits fondamentaux

Charte des droits fondamentaux de l'Union européenne

- Droit dérivé

- Règlements

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), *J.O.U.E.*, L 119 du 4 mai 2016, pp.1-88.

- Directives

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 (directive « Vie privée et communications électroniques »), *J.O.U.E.*, L 201/37 du 31 juillet 2002, pp. 37-47.

Directive (UE) 2016/343 du Parlement européen et du Conseil du 9 mars 2016 portant renforcement de certains aspects de la présomption d'innocence et du droit d'assister à son procès dans le cadre des procédures pénales, *J.O.U.E.*, L 65 du 11 mars 2016, p.1-11.

- Communications et autres documents

Commission européenne, Communication au Parlement européen, au Conseil européen et au Conseil concernant le onzième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective, COM(2017) 608 final du 18.10.2017.

Commission européenne, Commission staff working document impact assessment - Accompanying the document Proposal for measures on the strengthening of certain aspects of the presumption of innocence and of the right to be present at trial criminal proceedings, 27 novembre 2013, SWD/2013/0478 final.

Commission européenne, « Livre vert sur la présomption d'innocence », COM(2006) 174 final du 26.4.2006, 18 p.

Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions relative aux avancées dans le programme de l'Union européenne relatifs aux garanties procédurales accordées aux suspects et aux personnes poursuivies - Renforcer les fondements de l'espace européen de justice pénale, Bruxelles, 27 novembre 2013, COM/2013/0820 final, pp. 1-14.

Résolution du Parlement européen sur la proposition de recommandation du Parlement européen au Conseil sur les normes minimales en matière de garanties procédurales accordées aux suspects et aux personnes mises en cause dans des procédures pénales dans l'Union européenne (2003/2179(INI)), P5_TA(2003)0484, 6 novembre 2003, *J.O.U.E.*, C 83 E/180 du 2 avril 2004, pp. 180-185.

3. Droit belge

Code d'instruction criminelle

Loi du 13 juin 2005 relative aux communications électroniques, *M.B.*, 29 juin 2005, p. 28070.

Loi du 24 octobre 2013 modifiant le titre préliminaire du Code de procédure pénale en ce qui concerne les nullités, *M.B.*, 12 novembre 2013, p. 84999.

Loi du 28 novembre 2000 relative à la criminalité informatique, *M.B.*, 03 février 2001, p. 2909.

Titre préliminaire du Code de procédure pénale

Travaux parlementaires

Projet de loi portant des modifications diverses au Code d'instruction criminelle et au Code pénal, en vue d'améliorer les méthodes particulières de recherche et certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications et créant une banque de données des empreintes, *Doc. parl.*, Ch. Repr., sess. ord. 2015-2016, n °1966/001 du 8 juillet 2016.

Projet de loi portant des modifications diverses au Code d'instruction criminelle et au Code pénal, en vue d'améliorer les méthodes particulières de recherche et certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications et créant une banque de données des empreintes, *Doc. parl.*, Ch. Repr., sess. ord. 2015-2016, n °1966/006 du 8 juillet 2016.

Projet de loi relatif à la criminalité informatique, *Doc. parl.*, Ch. Repr., sess. ord. 1999-2000, n° 213/1 et 214/1 du 3 novembre 1999.

Projet de loi relatif aux communications électroniques, *Doc. parl.*, Ch. Repr., sess. ord. 2004-2005, n° 1425/001 du 4 novembre 2004.

Rapport concernant le relevé des lois qui ont posé des difficultés d'application ou d'interprétation pour les cours et tribunaux, *Doc. parl.*, Ch. Repr., sess. ord. 2010-2011, n °1414/006 du 8 février 2012, 383p.

B. Jurisprudence

CEDH

Cour eur. D.H., arrêt *Allan c. Royaume-Uni*, 5 novembre 2002.

Cour eur. D.H., arrêt *Brusco c. France*, 14 octobre 2010.

Cour eur. D.H., arrêt *Buzadji c. République de Moldova*, 5 juillet 2016.

Cour eur. D.H., arrêt *Bykov c. Russie*, 10 mars 2009.

Cour eur. D.H., arrêt *Engel et autres c. Pays-Bas*, 8 juin 1976.

Cour eur. D.H., arrêt *Funke c. France*, 25 février 1993.

Cour eur. D.H., arrêt *Heaney et McGuinness c. Irlande*, 21 décembre 2000.

Cour eur. D.H., arrêt *J.B. c. Suisse*, 3 mai 2001.

Cour eur. D.H., arrêt *Jalloh c. Allemagne*, 11 juillet 2006.

Cour eur. D. H. (gde ch.), arrêt *John Murray c. Royaume-Uni*, 8 février 1996.

Cour eur. D.H., arrêt *Kalnénienė c. Belgique*, 31 janvier 2017.

Cour eur. D.H., arrêt *Navone et autres c. Monaco*, 24 octobre 2013.

Cour eur. D.H., arrêt *O'Halloran et Francis c. Royaume-Uni*, 29 juin 2007.

Cour eur. D.H., arrêt *Öztürk c. Allemagne*, 21 février 1984.

Cour eur. D.H., arrêt *Salabiaku c. France*, 7 octobre 1988.

Cour eur. D.H., arrêt *Salduz c. Turquie*, 27 novembre 2008.

Cour eur. D.H., arrêt *Saunders c. Royaume-Uni*, 17 décembre 1996.

Cour eur. D.H., arrêt *Schenk c. Suisse*, 12 juillet 1988.

Cour eur. D.H., arrêt *Shlychkov v. Russia*, 9 February 2016.

Cour eur. D.H., arrêt *Stojkovic c. France et Belgique*, 27 octobre 2011.

Belgique

Antwerpen (Kamer van Inbeschuldigingstelling), K/2895/2017, 21 december 2017, inédit.

C.A., 25 janvier 2001, n°4/2001;

C.C., 13 mars 2008, n°50/2008.

C.C., 15 juin 2017, n°76/2017.

C.C., 17 décembre 2015, n°178/2015.

C.C., 22 décembre 2016, n°168/2006.

Cass., 13 janvier 1999, P.98.0412.F.

Cass., 13 mai 1986, *Rev. dr. pén. crim.*, 1986.

Cass., 17 novembre 2015, R.G. P.14.1274.N.

Cass. (1ère ch.), 1er octobre 2009, n° D.07.0024.N.

Cass (2e ch.), 5 octobre 2010, P.10.0703.N

Cass. (2e ch.), 7 février 2001, P.00.1532.F.

Cass. (2e ch.), 10 décembre 2002, P.02.1146.N.

Cass. (2e ch.), 14 mars 2017, Larcier Cassation 2018.

Cass. (2e ch.), 15 décembre 2004, P.04.1189.F.

Cass. (2e ch.), 19 juin 2013, P.12.1150.F, concl. M.P.

Cass. (2e Ch.), 22 juin 2010, P.10.0872.N.

Cass. (2e ch.), 28 mai 2013, P. 13.0066.N.

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

Gand, 23 juin 2015, *T. Strafr.*, 2016/3, pp. 232-242.

C. Doctrine

AKDENIZ, Y. et C. WALKER, C., « Whisper who dares: encryption, privacy rights and the new world disorder », *in* Y. AKDENIZ, C. WALKER, et D. WALL, *The internet, Law and Society*, United Kingdom, Pearson Education, 2000, 388p.

BAKER, S., et HURST, P., *The limits of Trust - Cryptography, Governments and Electronic Commerce*, The Hague, Kluwer Law International, 1998, 621p.

BEERNAERT, M.-A., « Antigone: les prémices de l'arrêt du 14 octobre 2003 », *in L'évolution de la jurisprudence Antigone sous le triple axe pénal, social et fiscal*, 2016, 17p (disponible sur dial.uclouvain.be).

BEERNAERT, M.-A., BOSLY, H.-D., et VANDERMEERSCH, D., *Droit de la procédure pénale*, 8ème éd., Brugge, la Charte, 2017, 2067 p.

BEYS, M., *Quels droits face à la police*, Bruxelles, J & D édition, 2014, 596 p.

BLAISE, N. et COLETTE-BASECQZ, N., *Manuel de droit pénal général*, 3e éd., Limal, Anthémis, 2016, 660 p.

BOSLY, H.-D., COLETTE-BASECQZ, N., DELHAISE, E., DE NAUW, A., MANDOUX, P., NEDERLANDT, O. ET VANDERMEERSCH, D., « Chronique semestrielle de jurisprudence », *Rev. dr. pén.*, 2016/12, p.1164-1303.

CHALUS, D., « La Dialectique Aveu - Droit au silence dans la manifestation de la vérité judiciaire en droit pénal comparé », *R.J.T.*, Volume 43, 2009, pp. 321-366.

COLIN, J.-N., « Du secret à la confiance… quelques éléments de cryptographie » *in* H. JACQUEMIN (sous la direction de), *L'identification électronique et les services de confiance depuis le règlement eIDAS*, CRIDS, 39, Bruxelles, Larcier, 2016, 425 p.

CONINGS, C., « Ontsleutelplicht van verdachte en verbod op zelfincriminatie », *N.J.W.*, 17 février 2016, pp.135-136.

Conseil de l'Europe/Cour européenne des droits de l'homme, Guide sur l'article 6 de la Convention européenne des droits de l'homme - Droit à un procès équitable (volet pénal), 2014, 68 p, disponible sur www.echr.coe.int (consulté le 18/04/2018).

CRAS, S., et ERBEŽNIK, A., « The Directive on the Presumption of Innocence and the Right to Be Present at Trial », *eucrim*, 2016, pp. 25-36.

DE SCHEPPER, K., et VERBRUGGEN, F., « Ontsnappen space invaders aan onze pacmannen? De materiële en formele strafrechtsmacht van België bij strafbare weigering van de medewerking door elektronische dienstverleners », *T. Stafr.*, 2016/3.

DE LA SERNA, I., « Le droit au silence - discours prononcé par le Procureur général I. de la Serna à l'occasion de la rentrée solennelle de la Cour d'appel de Mons le 1er septembre 2014 », *Pli juridique*, n°32, juin 2015, pp. 3-10.

DE VALKENEER, C., *Manuel de l'enquête pénale*, 4ème édition, Bruxelles , Larcier, 2011, 558 p.

DE VILLENFAGNE, F., et DUSOLLIER, S., La Belgique sort enfin ses armes contre la cybercriminalité: à propos de la loi du 28 novembre 2000 sur la criminalité informatique, 35 p. (disponible sur www.crid.be).

DENÉCÉ, E., « La révolution du renseignement », *Sécurité globale*, 2008/2 (N°4), pp. 37-49.

DENNING, D., *Cryptography and data security*, United States, Addison-Wesley Publishing Compagny, 1982, 400p.

DEWANDELEER, D., « Computermisdrijven en strafonderzoek in een ICT-context », *Themis 57- Straf-en strafprocesrecht*, Brugge, La Charte, 2017, pp. 125-163.

DU JARDIN, J., « Les droits de la défense dans la jurisprudence de la Cour de cassation (1990-2003), 61 p., disponible sur www.justice.belgium.be (consulté le 24/04/2018).

FITEN, B., « Apple vs. het FBI: veel vragen blijven onbeantwoord », *Juristenkrant*, n°327, 2016, pp.12-13.

FORGET, C., « La collecte de preuves informatiques en matière pénale » *in* J-F HENROTTE ET F. JONGEN (sous la direction de), *Pas de droit sans technologie*, CUP, 158, Bruxelles, Larcier, 2015, pp. 251-278.

FRANCHIMONT, M., JACOBS, A. ET MASSET, A., *Manuel de procédure pénale*, 4ème éd., Bruxelles, Larcier, 2012, 1603 p.

FRANSSEN, V., et TOSZA, S., « 6. 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* V. FRANSSEN et A. MASSET (sous la direction de), *Les droits du justiciable face à la justice pénale*, CUP, 171, Liège, Anthémis, 2017, p. 205-249.

GOSSÉ, A., « Dans quelle mesure les autorités judiciaires belges peuvent-elles contraindre des entreprises de télécommunication étrangères à collaborer à une enquête pénale en Belgique? », *droit pénal de l'entreprise*, 2017/3, pp. 179-204.

JACKSON, J., « Re-conceptualizing the right of silence as an effective fair trial standard », *I.C.L.Q.*, 2009, vol.58, pp. 835-861.

KENNES, L., *Manuel de la preuve en matière pénale*, 2ème éd., Malines, Kluwer, 2009, 435 p.

KERKHOFS, J., et P. VAN LINTHOUT, P., *Cybercrime*, Bruxelles, Politeia, 2013, 640 p.

KERKHOFS, J., et VAN LINTHOUT, P., « Cybercriminaliteit doorgelicht », *T.Strafr.*, n°4, 2010.

KONING, F., « Reconnaissance du droit du citoyen de refuser de donner accès à un système informatique nonobstant l'ordre de la loi, et reconnaissance d'un droit de recours contre un refus du parquet de laisser consulter son dossier d'information », *J.L.M.B.*, 2016/16, p. 733-742.

KOOPS, B.-J., "Het decryptiebevel en het nemo-teneturbeginsel: Nopen ontwikkelingen sinds 2000 tot invoering van een ontsleutelplicht voor verdachten?", Universiteit van Tilburg, 2012, 85.

KOOPS, B.-J., « The Crypto Controversy - A Key Conflict in the Information Society », *Law and Electronic Commerce*, Vol.6, London, Kluwer Law International, 1999

KUTY, F., « L'étendue du droit au silence en procédure pénale », *Rev. dr. pén.*, 2000/3, pp. 309-334.

LAMBERIGTS, S., « The Privilege against Self-Incrimination: a Chameleon of Criminal Procedure », *NJECL*, 2016, vol. 7, pp. 418-438.

LEROUX, O., « Arnaques, fraudes et escroqueries sur internet: moyens concrets d'investigation - Point sur l'affaire dite Yahoo! à la suite du second arrêt de la Cour de cassation », J.T., 2012/40-41, n°6500, p.839-843.

LEROUX, O., « Chapitre IX - Criminalité informatique» *in* H-D. BOSLY ET C. DE VALKENEER (sous la direction de), *Les infractions,* Volume 1, 2ème éd., Bruxelles, Larcier, 2016, p. 448-508.

LUGENTZ, F., *La preuve en matière pénale - sanction des irrégularités*, Limal, Anthémis, 2017, 296 p.

MASSET, A., « Le régime des nullités en procédure pénale » *in* A. JACOBS et A. MASSET (sous la direction de), *Actualités de droit pénal et de procédure pénale*, CUP, 148, Larcier, Bruxelles, 2014, 452p.

MEESE, J., « The sound of silence. Het zwijgrecht en het nemo tenetur-beginsel in strafzaken. Een historisch en rechtsvergelijkend overzicht » *in* Van Oevelen, A., Rozie, J., Rutten, S. (sous la direction de), *Zwijgrecht versus spreekplicht*, Intersentia, 2013, 258p.

MEUNIER, C., « 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.*, n°7, 2001, pp. 611-690.

MICHIELS, O., *La jurisprudence de la Cour constitutionnelle en procédure pénale: le Code d'instruction criminelle remodelé par le procès équitable?* , Limal, Anthemis, 2015, 700 p.

MICHIELS, O., *Procédure pénale - Notes sommaires et provisoires*, 5ème éd., Presses Universitaires de Liège, 2016-2017, 435 p.

MOLE, N., et HARBY, C., « Le droit à un procès équitable - Un guide sur la mise en oeuvre de l'article 6 de la Convention européenne des droits de l'homme », *Précis n°3 sur les droits de l'homme*, 2002, 69 p.

MONCEAUX, E., *Quel droit au silence en procédure pénale?*, Université Panthéon-Assas, 2011, 93 p. (disponible sur docassas.u-paris2.fr).

PAAR, C., et PELZL, J., *Understanding cryptography (a textbook for Students and Practitioners)*, Berlin, Springer, 2010, 372 p.

PIETTE-COUDOL, T., *Echanges électroniques Certification et sécurité*, Paris, Litec, 2000, 237p.

SCHUERMANS, F., « Verdachte heeft passieve medewerkingsplicht bij zoekingen in zijn smartphone », *De Juristenkrant*, nr 364, 28 février 2018, pp. 2-3.

SEPEC, M., « Digital data encryption - Aspects of criminal law and dilemmas in Slovenia », *Digi (Digital evidence and electronic signature law review)*, vol.10, 2013, pp.147-153.

STALLINGS, W., *Cryptography and Network security - Principles and Practices*, 4e éd., Prentice Hall, 592 p.

VAN COUTER, Y., et ROEGIERS, E., « Les défis de la cybersécurité », *Journal de droit européen*, Juin 2016, n°230

VAN DE HEYNING, C., et COPPENS, J., « Het bevel tot medewerking van artikel 88*quater* Sv., het zwijgrecht en het verbod op zelfincriminatie », *T. Strafr.*, 2016/3, pp. 260-265.

VANDERMEERSCH, D., *Eléments de droit pénal et de procédure pénale*, 5ème éd., Bruxelles, La Charte, 2015, 875 p.

WACK, M., COTTIN, N., MIGNOT, B., et ELMOUNDI, A., « Certification et archivage légal de dossiers numériques », *Document numérique*, 2002/1, vol.6, pp.145-158.

D. Articles provenant de sites internet

CHAMPEAU, G., « Lutte contre le chiffrement: le gouvernement dévoile ses pistes », *numerama*, 5/09/2016, numerama.com (consulté le 22/03/2018).

HÉRARD, P., « Cybercriminalité: comment l'Europe veut contourner la confidentialité des communications », *TV5MONDE*, 22 octobre 2017, mise à jour le 11.11.2017 disponible sur information.tv5monde (consulté le 13 avril 2018).

LAUSSON, J., « Chiffrement: l'Union européenne en ordre dispersé », *numerama*, 05/12/2016, disponible sur numerama.com (consulté le 22/03/2018).

LAUSSON, J., « Le chiffrement sans backdoor doit être 'encouragé et, si nécessaire, rendu obligatoire' », *numerama*, 28 juillet 2016, disponible sur numerama.com (consulté le 22/03/2018).

LAUSSON, J., « Non, une garde à vue ne vous oblige pas à déverrouiller votre smartphone », *numerama*, 18 avril 2018, disponible sur numerama.com (consulté le 30/04/2018).

RIVIÈRE, B.-R., « Systèmes informatiques: Portes dérobées, la menace fantôme », *LesEchos*, 22/04/2011, disponible sur archives.lesechos.fr (consulté le 14 avril 2018).

Union européenne, « Contrôleur européen de la protection des données » disponible sur europa.eu.

VALERO, J., « Ansip: 'I am strongly against any backdoor to encrypted systems' », *euractiv*, 23 février 2016, disponible sur euractiv.com (consulté le 30/04/2018).

X., « Qu'est-ce qu'une porte dérobée », disponible sur http://www.anti-cybercriminalite.fr (consulté le 13 avril 2018).