

**Cour de cassation (2^e ch., N.),
4 février 2020,
P.19.1086.N.**

(traduction libre)

Président : M. Van Volsem, conseiller ff. de président,
Rapporteur : M. Francis, conseiller,
Ministère public : M. De Smet, avocat général.

INSTRUCTION – saisie d’un système informatique – cryptage des messages – recherche dans les systèmes informatiques – ordonnance du juge d’instruction – suspect – refus de collaboration – sanction pénale – Convention de sauvegarde des droits de l’homme et des libertés fondamentales – article 6 – article 6.1 – droit au silence – droit de ne pas s’auto-accuser – présomption d’innocence

Le droit de ne pas s’auto-incriminer et la présomption d’innocence ne sont pas absolus. Ils doivent être mis en balance avec d’autres droits comme le droit à la liberté et à la sécurité garanti par l’article 5 de la Convention de sauvegarde des droits de l’homme et des libertés fondamentales et l’interdiction de l’abus de droit mentionnée à l’article 17 de cette Convention. Le droit de ne pas s’auto-incriminer sert en premier lieu à garantir le droit à un procès équitable en excluant les déclarations inexactes faites sous la contrainte. Aucune disposition conventionnelle ni aucun principe général de droit n’empêchent l’incrimination et la sanction d’un suspect qui refuse de donner suite à l’ordonnance du juge d’instruction de fournir des informations sur le fonctionnement d’un système informatique 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, en application de l’article 88quater, §§ 1^{er} et 3, du Code d’instruction criminelle. Il est requis qu’au moment où l’information est demandée, l’appareil ait déjà été examiné sans recours à la contrainte à l’égard de la personne suspectée et que le ministère public démontre qu’au-delà de tout doute raisonnable, cette personne connaît les codes d’accès et que l’information demandée réponde au critère de proportionnalité. (Conv. eur. D.H., art. 6 ; C. i. cr., art. 88ter et 88quater)

(PROC. GÉN. PRÈS LA COUR D’APPEL DE GAND C. M.A.)

1 Voy. la note, ci-après, de Mme C. FORGET, intitulée « La compatibilité entre le droit au silence et le fait de contraindre un suspect à dévoiler un ‘mot de passe’ ». Voy. également, au sujet de la même problématique, l’arrêt, publié ci-avant, de la Cour constitutionnelle, du 20 février 2020, n° 28/2020, également commenté par l’auteur précité.

ARRÊT

I. La procédure devant la Cour

Le pourvoi en cassation est dirigé contre l'arrêt rendu le 15 octobre 2019 par la cour d'appel de Gand, chambre correctionnelle.

(...)

II. La décision de la Cour

Sur le moyen :

1. Le moyen invoque la violation de l'article 88^{quater}, §§ 1^{er} et 3, du Code d'instruction criminelle : l'arrêt acquitte le défendeur de la prévention B, pour laquelle ce dernier a été poursuivi pour avoir refusé de donner suite à l'ordonnance du juge d'instruction de fournir le code d'accès aux GSM trouvés en sa possession, et considère qu'une telle obligation est incompatible avec le droit au silence du défendeur et avec l'interdiction de s'accuser sous la contrainte, déduits notamment de la présomption d'innocence énoncée à l'article 6.2 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales et des articles 14.1 et 14.3.g du Pacte international relatif aux droits civils et politiques, et précisés aux articles 6 et 7 de la directive (UE) 2016/343 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, ainsi qu'aux considérants 25 et 27 du préambule de cette directive ; le droit de garder le silence et le droit de ne pas s'accuser soi-même, comme précisé par la Cour européenne des droits de l'homme, n'interdisent toutefois pas d'imposer à un suspect une obligation d'information pénalement sanctionnée en vue d'obtenir des éléments de preuve matériels qui, comme en l'espèce, sont statiques, existent indépendamment de sa volonté, et ne sont, en tant que tels, pas de nature à l'incriminer ; cette situation est comparable à l'obtention de données biométriques sur la base desquelles des éléments de preuve peuvent être trouvés.

2. L'article 88^{quater}, § 1^{er}, du Code d'instruction criminelle dispose que le juge d'instruction peut ordonner à toute personne dont il présume qu'elle a une connaissance particulière :

- du système informatique qui fait l'objet de la recherche ou de l'extension de celle-ci visée à l'article 88^{ter} ou
- des services qui permettent de protéger ou de crypter des données qui sont stockées, 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 paragraphe 3 de cet article sanctionne celui qui refuse de fournir cette collaboration.

3. En vertu de ces dispositions, est entre autres punissable un suspect qui, bien qu'il connaisse le code d'accès à un système informatique à explorer, tel un GSM, refuse de le communiquer malgré une ordonnance délivrée dans ce sens par le juge d'instruction. Il est requis qu'au moment où l'information est demandée, l'autorité de recherche ou d'instruction ait déjà examiné l'appareil sans recours à la contrainte sur la personne et que l'instance poursuivante démontre alors qu'au-delà de tout doute raisonnable, la personne visée connaît le code.

4. L'article 6.2 de la Convention dispose que toute personne accusée d'une infraction est présumée innocente jusqu'à ce que sa culpabilité ait été légalement établie.

5. L'article 14.2 du Pacte international a la même portée. L'article 14.3.g du Pacte ajoute que toute personne accusée d'une infraction pénale a le droit de ne pas être forcée de témoigner contre elle-même ou de s'avouer coupable.

6. La directive (UE) 2016/343 dispose ce qui suit :

- à l'article 6.1 :

« Les États membres veillent à ce que l'accusation supporte la charge de la preuve visant à établir la culpabilité des suspects et des personnes poursuivies. Cette disposition s'entend sans préjudice de toute obligation incombant au juge ou à la juridiction compétente de rechercher des éléments de preuve tant à charge qu'à décharge, et sans préjudice du droit de la défense de présenter des éléments de preuve conformément au droit national applicable » ;

- à l'article 7 :

« 1. Les États membres veillent à ce que les suspects et les personnes poursuivies aient le droit de garder le silence en ce qui concerne l'infraction pénale qu'ils sont soupçonnés d'avoir commise ou au titre de laquelle ils sont poursuivis.

2. Les États membres veillent à ce que les suspects et les personnes poursuivies aient le droit de ne pas s'incriminer eux-mêmes.

3. L'exercice du droit de ne pas s'incriminer soi-même n'empêche pas les autorités compétentes de recueillir les preuves qui peuvent être obtenues légalement au moyen de pouvoirs de contrainte licites et qui existent indépendamment de la volonté des suspects ou des personnes poursuivies.

4. Les États membres peuvent autoriser leurs autorités judiciaires à tenir compte, lorsqu'elles rendent leur jugement, de l'attitude coopérative des suspects et des personnes poursuivies.

5. L'exercice par les suspects et les personnes poursuivies du droit de garder le silence ou du droit de ne pas s'incriminer soi-même ne saurait être retenu contre eux ni considéré comme une preuve qu'ils ont commis l'infraction pénale concernée ».

La directive dispose également ce qui suit dans le préambule :

- au considérant 24 :

« Le droit de garder le silence constitue un aspect important de la présomption d'innocence et devrait servir de rempart contre l'auto-incrimination » ;

- au considérant 25 :

« Le droit de ne pas s'incriminer soi-même constitue également un aspect important de la présomption d'innocence. Les suspects et les personnes poursuivies ne devraient pas être forcés, lorsqu'il leur est demandé de faire des déclarations ou de répondre à des questions, de produire des preuves ou des documents ou de fournir des informations pouvant conduire à leur propre incrimination » ;

- au considérant 27 :

« Le droit de garder le silence et le droit de ne pas s'incriminer soi-même impliquent que les autorités compétentes ne devraient pas contraindre les suspects ou les personnes poursuivies à fournir des informations si ces personnes ne souhaitent pas le faire. Afin de déterminer si le droit de garder le silence ou le droit de ne pas s'incriminer soi-même a été violé, il convient de tenir compte de l'interprétation donnée par la Cour européenne des droits de l'homme du droit à un procès équitable en vertu de la Convention européenne des droits de l'homme » ;

- au considérant 29 :

« L'exercice du droit de ne pas s'incriminer soi-même ne devrait pas empêcher les autorités compétentes de réunir les preuves que l'on peut obtenir légalement d'un suspect ou de la personne poursuivie en recourant à des pouvoirs de contrainte licites et qui existent indépendamment de la volonté du suspect ou de la personne poursuivie, tels que des documents recueillis en vertu d'un mandat, des documents pour lesquels est prévue une obligation légale de conservation et de production sur demande, les échantillons d'air expiré, de sang et d'urine ainsi que les tissus corporels en vue d'une analyse de l'ADN ».

7. Ni ces dispositions conventionnelles et considérants, ni aucun principe général de droit reposant sur ceux-ci n'empêchent l'incrimination et la sanction d'un suspect en application de l'article 88*quater*, §§ 1^{er} et 3, du Code d'instruction criminelle, tel qu'interprété ci-dessus.

8. À cet égard, il convient de tenir compte entre autres de ce qui suit :

- il ressort des motifs que l'arrêt reprend du jugement entrepris qu'il y avait des indices que le défendeur était venu acheter des stupéfiants en Belgique. Il disposait de deux GSM dont il a refusé de donner le code d'accès ;
- des pièces auxquelles la Cour peut avoir égard, il n'apparaît pas que, devant les juges d'appel, il ait été contesté que la police a trouvé les GSM sans recours à la contrainte à l'égard du défendeur, que celui-ci connaissait les codes d'accès visés ou que l'information demandée était proportionnée à l'enquête sur les faits mentionnés ;
- le droit de ne pas s'auto-incriminer et la présomption d'innocence ne sont pas absolus et doivent être mis en balance avec d'autres droits comme le

droit à la liberté et à la sécurité garanti par l'article 5 de la Convention et l'interdiction de l'abus de droit mentionnée à l'article 17 de la Convention ;

- le droit de ne pas s'auto-incriminer sert en premier lieu à garantir le droit à un procès équitable en excluant les déclarations inexactes faites sous la contrainte ;
- le code d'accès à un système informatique existe indépendamment de la volonté de la personne qui a connaissance de ce code. Ce dernier reste inchangé qu'il soit communiqué ou non et entre en ligne de compte pour un contrôle immédiat. Il n'existe aucun risque pour la fiabilité des éléments de preuve ;
- le code d'accès est neutre et il est à distinguer des données éventuellement incriminantes qui sont à retrouver au moyen du système informatique ;
- l'information demandée, bien que la (non-)communication de celle-ci soit sanctionnée d'importantes peines d'emprisonnement, et l'utilisation qui en est faite, sont limitées. Cette information ne porte que sur le code d'accès à un système informatique déjà découvert et illisible sans elle. Il doit en être démontré que le prévenu connaissait ce code. Le droit de celui-ci de présenter complètement sa défense à propos des données retrouvées demeure inchangé ;
- l'état actuel de la technologie rend très difficile voire impossible d'accéder à un système informatique protégé par une application de cryptage, alors que de telles applications sont aisément disponibles. Par conséquent, l'information demandée est nécessaire pour la manifestation de la vérité.

9. En statuant ainsi que le moyen l'énonce, l'arrêt ne justifie dès lors pas légalement sa décision.

Le moyen est fondé.

PAR CES MOTIFS,

LA COUR

Casse l'arrêt attaqué ;

(...)



Note

La compatibilité entre le droit au silence et le fait de contraindre un suspect à dévoiler un « mot de passe »

Introduction

Le chiffrement des données complexifie les poursuites pénales et prive souvent les enquêteurs d'un accès à de précieuses informations¹. Il n'en demeure pas moins que ces techniques de sécurité informatique s'avèrent essentielles en vue d'assurer la protection des données à caractère personnel et, en ce sens, contribuent à protéger le droit au respect de la vie privée². À ce titre, elles sont prônées par différents instruments internationaux tels la Convention 108 modernisée³ ou encore, le Règlement général sur la protection des données⁴. En dépit de ce besoin légitime d'assurer un haut niveau de sécurité des données, selon la Convention de Budapest⁵, les autorités répressives se heurtant à des données chiffrées peuvent imposer la collaboration de tiers afin d'obtenir en « texte clair »⁶ c'est-à-dire déchiffrer les données qui sont en leur possession ou sous leur contrôle⁷. Considérant qu'il s'agit d'une méthode d'enquête, elle exige le respect du critère de proportionnalité mais aussi la prise en considération de l'intérêt légitime de tiers⁸. La Convention de Budapest ne précise toutefois pas si cette obligation de collaboration peut être imposée au suspect ou si ce dernier bénéficie en ce cas du droit au silence garanti par l'article 6, § 2, de la Convention européenne des droits de l'homme (ci-après

- 1 Dans son dernier rapport, Europol affirme à nouveau que le chiffrement des données ralentit considérablement la poursuite des enquêtes pénales (Europol, *Second report of the observatory function of encryption*, 18 février 2020, p. 13).
- 2 Ce lien de dépendance a été illustré dans l'arrêt *I. c. Finlande* où la Cour eur. D.H. estima que le défaut de garanties relatives à la sécurisation des données contre des usages non autorisés constitue une violation de l'obligation positive d'assurer le respect du droit à la vie privée consacré à l'article 8 de la CEDH (Cour eur. D.H., *I. c. Finlande*, 17 juillet 2008, n° 20511/03).
- 3 Rapport explicatif de la Convention modernisée, § 56. La Convention 108 constitue le seul instrument contraignant en matière de protection de données aspirant à constituer un socle minimum en matière de protection des données de portée potentiellement mondiale (Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, STCE n° 108, 1981). Elle fait actuellement l'objet d'une modernisation par le biais de la Convention 108+ ou Convention modernisée.
- 4 Art. 31, § 1 du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données).
- 5 Cette Convention offre un cadre contraignant aux États membres en procédure pénale et en droit pénal matériel dans le domaine de la cybercriminalité. (Convention sur la cybercriminalité, signée à Budapest, le 23 novembre 2001, S.T.C.E., n° 185).
- 6 Rapport explicatif de la Convention sur la cybercriminalité, Conseil de l'Europe, Budapest, 23 novembre 2001, § 176.
- 7 L'expression « en sa possession » ou « sous son contrôle » fait référence d'une part, à la possession matérielle des données et d'autre part, à des situations dans lesquelles l'intéressé ne possède pas matériellement les données à produire mais peut en contrôler librement la production, par exemple si les données sont stockées sur un cloud qu'il met librement à disposition. Le rapport explicatif précise toutefois qu'un accès aux données par une liaison du réseau ne constitue pas nécessairement un « contrôle » au sens de la présente disposition (Rapport explicatif de la Convention sur la cybercriminalité, Conseil de l'Europe, Budapest, 23 novembre 2001, § 173).
- 8 Art. 18, § 2 de la Convention de Budapest.

« CEDH ») ainsi que par l'article 14, 3.g, dudit du Pacte international relatif aux droits civils et politiques (ci-après « PIDCP »). Au niveau national, cette question faisait l'objet d'une jurisprudence partagée, le Code d'instruction criminelle permettant au juge d'instruction d'exiger de « toute personne » de fournir certaines informations tels une clé de chiffrement ou un mot de passe sous peine de sanctions pénales. L'arrêt de la Cour de cassation du 4 février 2020⁹ fut l'occasion pour celle-ci de trancher la question d'autant que son approche ne fut pas remise en cause par l'arrêt du 20 février 2020 de la Cour constitutionnelle¹⁰.

1. Le droit au silence : principes généraux

Le droit de ne pas contribuer à sa propre incrimination et le droit de garder le silence sont des normes internationales généralement reconnues au cœur de la notion de procès équitable¹¹. Ainsi, l'article 14, 3.g du PIDCP énonce que « toute personne accusée d'une infraction pénale a le droit de ne pas être forcée de témoigner contre elle-même ou de s'avouer coupable ». Sans être explicitement créé par la CEDH, dès 1993, la Cour européenne des droits de l'homme (ci-après Cour EDH) déduisit de son article 6, § 2, garantissant le droit à la présomption d'innocence¹², le « droit de se taire et de ne pas contribuer à sa propre incrimination »¹³. Sur base de ce fondement, un accusé¹⁴ ne peut être contraint de collaborer à la production de preuves ou être sanctionné pour avoir refusé de communiquer certains documents susceptibles de l'incriminer¹⁵. En outre, l'accusation ne peut chercher à fonder son argumentation en se basant sur des éléments de preuves « obtenus par la contrainte ou les pressions, au mépris de la volonté de l'accusé »¹⁶. De manière similaire, au niveau du droit de l'Union européenne (ci-après UE), la directive 2016/343 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 impose aux États membres de veiller à ce que toute personne poursuivie ait le droit de garder le silence et de ne pas s'incriminer soi-même¹⁷. En

⁹ Cass., 4 février 2020, P.19.1086.N, www.cass.be, publié ci-avant.

¹⁰ C.C., arrêt n° 28/2020 du 20 février 2020, publié ci-avant.

¹¹ Cour eur. D.H., *Brusco c. France*, n° 1466/07, 14 octobre 2010, § 44.

¹² Voy. entre autres : Cour eur. D.H., *Funke c. France*, 25 février 1993, § 44 ; Cour eur. D.H., *Saunders c. Royaume-Uni*, n° 19187/91, CEDH 1996-VI, § 65 ; Cour eur. D.H., *John Murray c. Royaume-Uni*, 8 février 1996, n° 18731/91, § 45, 47 et 50 ; Cour eur. D.H., *Heaney et McGuinness c. Irlande*, 2 mai 2000, n° 34720/97). Ainsi, selon la Cour européenne des droits de l'homme, « Le droit de ne pas contribuer à sa propre incrimination présuppose que, dans une affaire pénale, l'accusation cherche à fonder son argumentation sans recourir à des éléments de preuve obtenus par la contrainte ou les pressions, au mépris de la volonté de l'accusé. En ce sens, ce droit est étroitement lié au principe de la présomption d'innocence (...) ». (M.-A. BEERNAERT, H. D. BOSLY et D. VANDERMEERSCH, *Droit de la procédure pénale*, la Charte, Bruxelles, 2010, pp. 28 et 30 spéc. les notes n° 103 et 115).

¹³ Voy. entre autres Cour eur. D.H., *Funke c. France*, 25 février 1993 (série A n° 256-A, p. 22, par. 44).

¹⁴ Une personne est dite « accusée » dès le moment où elle fait l'objet d'une accusation pénale autrement dit, qu'il y ait une procédure pénale ouverte à son égard voire, envisagée (Cour eur. D.H., *Web c. Autriche*, 8 avril 2004, n° 38544/97).

¹⁵ Cour eur. D.H., *Funke c. France*, 25 février 1993, § 44.

¹⁶ *Ibid.*

¹⁷ Art. 6, 1 et 7 de 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



droit interne, le droit au silence constitue l'une des facettes des droits de la défense et est, à ce titre, érigé en principe général de droit¹⁸. De manière plus spécifique, l'article 47bis, § 2, 2°, du Code d'instruction criminelle (ci-après « C. i. cr. ») confère au suspect faisant l'objet d'une audition le droit d'être informé succinctement des faits à propos desquels il sera entendu mais aussi, de la circonstance qu'il dispose du choix de faire une déclaration, de répondre aux questions qui lui sont posées ou de se taire¹⁹.

2. Un champ d'application limité

Le droit au silence n'est pas absolu et son champ d'application connaît certaines limites. Ainsi, dans le cadre de l'arrêt *Saunders*, la Cour EDH a considéré que n'étaient pas couvertes par le droit au silence, les données que l'on peut obtenir de l'accusé en recourant à des pouvoirs coercitifs et qui existent indépendamment de sa volonté, tels des documents recueillis sur base d'un mandat, des empreintes ADN, son haleine, son sang ou encore son urine²⁰. S'inspirant de cette jurisprudence, la directive 2016/343 exclut elle aussi du champ d'application du droit au silence les preuves obtenues légalement au moyen de pouvoirs de contrainte licites et « qui existent indépendamment de la volonté des suspects ou des personnes poursuivies »²¹. En guise d'exemples, le considérant 29 de la directive précitée indique qu'il peut s'agir de documents recueillis en vertu d'un mandat d'échantillon d'air expiré, de sang et d'urine, des tissus corporels en vue d'une analyse de l'ADN mais aussi des documents pour lesquels est prévue une obligation légale de conservation et de production sur demande²². Dans la même lignée, le C. i. cr. permet aux autorités répressives de collecter certaines données sous la contrainte en vue de procéder à une analyse d'haleine, de sang, d'urine, ou d'ADN par exemple²³ ou encore, d'exiger des documents comptables²⁴ ou sociaux²⁵ dont la loi impose la tenue. Il n'est toutefois pas précisé si un mot de passe ou une clé de chiffrement « existent indépendamment de la volonté du suspect » de sorte que, dans l'affirmative, ils sont en principe exclus du champ d'application du droit au silence garanti par l'article 6, § 2, de la CEDH et peuvent être obtenus auprès de l'accusé par les autorités poursuivantes.

procès dans le cadre des procédures pénales, *O.J.*, L. 65, 11 mars 2016, pp. 1-11 (ci-après directive 2016/343).

18 Cass., 13 mai 1986, *R.D.P.*, 1986, p. 905.

19 À ce propos voy. C. DE VALKENNEER, *Manuel de l'enquête pénale*, Bruxelles, Larcier, 2018, pp. 221-260.

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

21 Art. 7, 3 de la directive 2016/343.

22 Considérant 29 de la directive 2016/343.

23 Art. 90undecies C. i. cr.

24 F. KUTY, « Le droit au silence, les investigations de l'administration fiscale et l'enquête pénale », *J.T.*, 2008/22, n° 6314, pp. 386-389.

25 H. D. BOSLY, « Le droit au silence pendant la phase administrative de la surveillance du respect des lois sociales », in *L'auditorat du travail : compétences civiles et pénales*, Bruxelles, Larcier, 2012, pp. 417-443.

3. L'obligation du suspect de fournir certaines informations sous la contrainte : quid du mot de passe et d'une clé de chiffrement ?

a) L'obligation de collaboration visée par l'article 88^{quater}, § 1 C. i. cr.

Dans le cadre d'une enquête pénale, à l'occasion d'une audition, il arrive fréquemment que l'enquêteur sollicite le mot de passe du téléphone portable de la personne auditionnée²⁶ afin de pouvoir exploiter le système informatique saisi²⁷. En cas de refus, l'enquêteur peut s'adresser au juge d'instruction, ce dernier étant compétent pour ordonner à toute personne « dont on présume qu'elle dispose de connaissances particulières » du système visé, de fournir certaines informations sur le fonctionnement de ce système et la manière d'y accéder²⁸. Le défaut de collaboration ou le fait de faire obstacle à la recherche, voire à l'extension de recherche dans un système informatique, est passible de sanctions pénales, à savoir une peine d'emprisonnement de six mois à trois ans et d'une amende de vingt mille euros à vingt mille euros ou d'une de ces peines seulement²⁹. Cette sanction peut être portée à un emprisonnement d'un à cinq ans avec une amende de cinquante mille euros à cinquante mille euros dans le cas où la collaboration aurait eu pour effet d'empêcher la commission d'un crime ou d'un délit ou d'en limiter les effets³⁰. Malheureusement, la loi ne précise pas si cette ordonnance peut être adressée à un suspect compte tenu du fait qu'il bénéficie du droit au silence³¹. Cette question faisait jusqu'ici l'objet d'une jurisprudence très partagée auprès des juridictions essentiellement néerlandophones³², controversée à présent tranchée suite à l'arrêt de la Cour de cassation faisant l'objet de notre propos.

26 En pratique, des formulaires sont parfois présentés au suspect afin qu'il note le code d'accès de son téléphone portable et autorise les enquêteurs à exploiter le système informatique et ce, même s'il ne bénéficie pas de l'assistance d'un avocat. Même si cette pratique n'a, à notre connaissance, fait l'objet d'aucun recours devant les cours et tribunaux, on peut supposer qu'à l'instar d'une visite domiciliaire sur consentement, il ne s'agit pas d'un acte d'enquête de sorte que la présence d'un avocat n'est pas requise (*Doc. parl.*, Chambre, session 2010-2011, n° 53 1279/005, pp. 51-54).

27 Art. 39^{bis} et 88^{ter}, § 1 C. i. cr.

28 L'article 88^{quater}, § 1 C. i. cr. stipule en effet : « 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 88^{ter} ou des services qui permettent de protéger ou de crypter des données qui sont stockées, 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 ».

29 Art. 88^{quater}, § 3, al. 1^{er}, C. i. cr.

30 Art. 88^{quater}, § 3, al. 2, C. i. cr.

31 Cour eur. D.H., *Funke c. France*, 25 février 1993, § 44.

32 Ainsi, certaines décisions considèrent qu'une telle obligation viole le droit au silence : voy. Corr., Anvers, section Malines, 11 janvier 2018, *N.C.*, 2018/5, pp. 515-519 ; Anvers (chambre des mises en accusation), 7 juillet 2017, *N.C.*, 2018/5, pp. 503-505 ; Gand (4 ch.), 14 mai 2019, *R.A.B.G.*, 2019/13, pp. 1159-1167 ; Corr. Flandre orientale (section Veurne), 23 octobre 2018, *N.C.*, 2018/6, p. 606-607. D'autres considèrent qu'une telle obligation ne viole pas le droit au silence : voy. Anvers (chambre des mises en accusation), 28 juin 2018, *N.C.*, 2018/5, pp. 511-515 ; Anvers (chambre des mises en accusation), 21 décembre 2017, *N.C.*, 2018/5, pp. 505-509 ; Gand (10 ch.), 7 juin 2019,



b) L'arrêt de la cour de cassation du 4 février 2020

Dans le cadre de l'arrêt du 4 février 2020, la Cour de cassation saisit l'occasion de dire pour droit que l'obligation imposée à un suspect de fournir un mot de passe sous peine de sanctions pénales n'est pas contraire au droit au silence. En l'espèce, l'inculpé, poursuivi pour des faits de trafic de stupéfiants, fut contraint de fournir les codes d'accès des deux téléphones portables trouvés en sa possession. N'ayant pas obtempéré aux injonctions du juge d'instruction prises sur pied de l'article 88quater, § 1^{er} C. i. cr., il fut poursuivi devant les juridictions pénales. En second degré de juridiction, la cour d'appel de Gand estima qu'une telle obligation est incompatible avec le droit de ne pas contribuer à sa propre incrimination et de garder le silence de sorte qu'elle ne pouvait pas être imposée au prévenu³³.

La Cour de cassation ne suivit pas cette analyse pour différents motifs. Tout d'abord, bien que la loi ne l'exige pas expressément, elle souligne que l'ordonnance du juge d'instruction suppose le respect du critère de proportionnalité raison de la nécessité de disposer d'indices sérieux de culpabilité – en l'occurrence d'achat de stupéfiants – et la saisie sans recours à la contrainte des deux téléphones portables. Rappelant ensuite que le droit au silence n'est pas absolu et qu'il trouve sa raison d'être dans la volonté d'exclure les déclarations inexactes et faites sous la contrainte, la Cour pointe le fait qu'un code d'accès à un système informatique « existe indépendamment de la volonté de la personne qui a connaissance de ce code ». En effet, d'après la Cour, « ce dernier reste inchangé qu'il soit communiqué ou non et entre en ligne de compte pour un contrôle immédiat ». Elle ajoute que ce code est « neutre » à la différence des données éventuellement incriminantes que l'on peut retrouver dans le système informatique. Puis, tout en admettant la possibilité d'user de la contrainte à l'égard du suspect, le non-respect de l'ordonnance étant passible de sanctions pénales, elle précise d'une part, que l'utilisation de l'information est limitée, celle-ci ne portant que sur le code d'accès et d'autre part, qu'il doit être démontré que le prévenu connaissait ce code. Enfin, elle fait valoir qu'en l'état actuel de la technologie, il est « très difficile voire impossible d'accéder à un système informatique protégé par une application de cryptage, alors que de telles applications sont aisément disponibles » de sorte que cette mesure est nécessaire à la manifestation de la vérité. Elle conclut dès lors à la non-violation du droit au silence garanti par l'article 6, § 2, de la CEDH.

R.A.B.G., 2019/13, pp. 1167-1174 ; Gand (chambre des mises en accusation), 8 février 2018, *N.C.*, 2018/5, pp. 509-511 ; Corr. Anvers, 13 juillet 2018, *N.C.*, 2018/5, pp. 519-521.

33 Une approche similaire avait été retenue par le tribunal correctionnel de Termonde et confirmée par la cour d'appel de Gand. Le tribunal avait jugé qu'en ordonnant aux prévenus de rendre accessibles les supports de données, ils avaient été contraints, moyennant une prestation intellectuelle propre, de contribuer activement à l'administration de la preuve de sorte que les éléments de preuve fournis par les supports de données cryptées étaient frappés de nullité (Corr. Termonde, 17 novembre 2014, *T. Straft.*, 2016/3, pp. 255-260 et Gand 23 juin 2015, *NjW*, 2016, liv. 336, p. 134, note C. CONINGS).

c) Commentaires

Sans le mentionner expressément, dans l'arrêt commenté, la Cour de cassation se réfère à la jurisprudence *Saunders* de la Cour EDH considérant qu'un mot de passe, à l'instar d'autres données – telles que des documents recueillis sur base d'un mandat, des empreintes ADN, l'haleine, le sang, ou encore l'urine – existe « indépendamment de la volonté du suspect »³⁴ dans la mesure où il resterait inchangé, qu'il soit communiqué ou non. Il est donc, sur cette base, exclu du champ d'application du droit au silence. Cette interprétation mérite toutefois d'être nuancée. Eu égard à la diversité de mots de passe, il conviendrait par exemple de distinguer le « mot de passe » protégeant l'accès aux données stockées sur la carte SIM de celui protégeant l'accès à la mémoire du téléphone lui-même.

Dans le premier cas, l'accès aux données suppose l'introduction d'un code 'PIN'³⁵ voire, dans certains cas, d'un code 'PUK'³⁶. En principe, le code 'PUK' existe indépendamment du choix opéré par l'utilisateur, celui-ci étant déterminé par le fabricant pour protéger le système informatique des accès illicites³⁷. Par contre, le code 'PIN' est créé initialement par l'opérateur et est ensuite modifiable par l'utilisateur du système informatique, il est alors le fruit de sa propre décision et peut être renouvelé à tout moment, parfois même à distance. Dès lors, *a contrario* de ce qu'affirme la Cour de cassation, un code d'accès « ne reste pas inchangé » une fois communiqué ou, à tout le moins, pas nécessairement.

Dans le second cas, lorsque la méthode de verrouillage vise à protéger l'accès au téléphone lui-même, la présence d'un élément de choix dans le chef de l'utilisateur est d'autant plus claire. En effet, il n'est pas inutile de rappeler que les méthodes de verrouillage disponibles varient selon le modèle de smartphone et le système d'exploitation choisis et peuvent consister en de nombreuses mesures alternatives potentiellement cumulables. Un utilisateur peut décider de n'utiliser aucune méthode de verrouillage ou choisir un mot de passe classique. Il peut également opter pour une méthode graphique tel le simple glissement du doigt sur l'écran ou faire le choix d'un motif personnel à dessiner. L'utilisateur peut enfin décider

34 Cour eur. D.H., *Saunders c. Royaume-Uni*, 17 décembre 1996, n° 1187/91, § 69. Dans une opinion dissidente de l'arrêt *Saunders* précité, le juge Martens critique néanmoins la validité de la distinction opérée entre les données « qui existent indépendamment de la volonté du suspect », des autres types de données. Il estime que dans les deux cas la volonté du suspect n'est pas respectée. Il illustre son propos en indiquant « Peut-on vraiment dire que le contenu d'un ballon d'alcootest dans lequel une personne soupçonnée de conduite en état d'ivresse a été contrainte de souffler a une existence indépendante de la volonté du suspect ? Que dire d'un code PIN ou de la clé d'un système de chiffrement, enfouis dans la mémoire du suspect ? » (Cour eur. D.H., *Saunders c. Royaume-Uni*, 17 décembre 1996, n° 1187/91, opinion dissidente du juge Martens à laquelle le juge Kuris déclare se rallier, I. C.12).

35 Le code 'PIN' pour « Personal Identification Number » est composé de quatre chiffres et permet l'accès au téléphone portable.

36 Le code 'PUK' pour « PIN Unlock Key » est composé de huit chiffres et sert à débloquent le téléphone portable en cas d'oubli du code 'PIN'.

37 ENISA, *Mobile threats incident handling* (part. II), septembre 2015, p. 38, disponible sur <https://www.enisa.europa.eu/>.



d'activer ou de désactiver des méthodes de verrouillage biométriques telles qu'un scanner d'iris, la reconnaissance faciale ou encore un lecteur d'empreintes digitales. Compte tenu de ce large panel mis à disposition des personnes concernées, il est difficile d'affirmer qu'un code d'accès existe nécessairement « indépendamment de la volonté du suspect ».

En outre, si ce code est « neutre », comme le souligne la Cour de cassation, et en ce sens, « non incriminant », il n'en demeure pas moins qu'il donne accès à des informations susceptibles de se muer en éléments de preuve. On pourrait donc considérer qu'indirectement, dévoiler une telle donnée peut comporter un caractère incriminant³⁸. À cela s'ajoute le fait que même si, comme le met en exergue la Cour, le droit au silence vise à exclure les déclarations inexactes et faites sous la contrainte³⁹ et dès lors, les erreurs judiciaires⁴⁰, on tend à reconnaître à l'accusé le droit de s'abstenir de répondre aux questions qui lui sont posées⁴¹ et de « se cantonner dans un rôle de contestation purement passive »⁴². Certains auteurs affirment ainsi que le droit au silence permet de « laisser l'accusé libre et maître de ses réponses »⁴³ assurant ainsi « le respect de la dignité et de la liberté de l'homme » ce qui « exige que tout suspect soit totalement libre de décider de l'attitude à adopter face aux accusations portées contre lui »⁴⁴. Or, dévoiler un mot de passe implique la participation du suspect à la solution d'une question qui lui est posée suscitant dès lors un doute quant à la compatibilité d'une telle obligation avec l'article 6, § 2, de la CEDH.

De plus, on peut s'interroger sur la manière dont les autorités répressives appliqueront la présomption de connaissance du mot de passe, par exemple, lorsque le téléphone a été bloqué à distance ou encore, lorsque l'utilisateur ne dispose plus de la clé de chiffrement. On notera que, pour contourner cet écueil, la directive 2016/343 limite la possibilité de collecter certaines données sous la contrainte à celles pour lesquelles « une obligation légale de conservation et de production sur demande » est prévue⁴⁵. En ce sens, en droit national, seuls les documents

38 Cette analyse a été retenue par l'Avocat général dans le cadre de son avis rendu dans l'arrêt de la cour d'appel d'Anvers (Anvers, 21 décembre 2017, chambre des mises en accusation, K/2895/2017, inédit).

39 En ce sens, selon la Cour eur. D.H., le droit de ne pas contribuer à sa propre incrimination présuppose que, dans une affaire pénale, l'accusation cherche à fonder son argumentation sans recourir à des éléments de preuve obtenus par la contrainte ou les pressions, au mépris de la volonté de l'accusé. Voy. Cour eur. D.H., *Saunders c. Royaume-Uni*, 17 décembre 1996, n° 1187/91, § 68.

40 Cour eur. D.H., *Murray c. Royaume-Uni*, 8 février 1996, Recueil 1996-I, p. 49, § 45.

41 M. ESSAÏD, *La présomption d'innocence*, Rabat, La Porte, 1971, p. 275, cité par F. KUTY, « L'étendue du droit au silence en procédure pénale », *R.D.P.C.*, 2000, n° 3, pp. 309-334.

42 R. ERGEC, *Convention européenne des droits de l'homme*, Bruxelles, Bruylant, 2014, p. 577.

43 R. GARRAUD, *Traité théorique et pratique d'instruction criminelle et de procédure pénale*, t. II, Paris, Sirey, 1909, n° 467, 232, cité par F. KUTY, « L'étendue du droit au silence en procédure pénale », *R.D.P.C.*, 2000, n° 3, pp. 309-334.

44 T. WERQUIN, « Droit pénal social : le droit de ne pas contribuer à sa propre incrimination, le droit au silence et l'obstacle à la surveillance », *J.T.T.*, 2000, p. 82.

45 Considérant 29 de la directive 2016/343.

comptables⁴⁶ ou sociaux⁴⁷, c'est-à-dire des documents dont la loi impose la tenue, peuvent entraîner des sanctions pénales lorsqu'ils ne sont pas remis sur demande des autorités. Par analogie, on pourrait soutenir que le fait de ne pas divulguer un mot de passe ou une clé de chiffrement ne peut faire l'objet d'une incrimination spécifique, ceux-ci n'étant soumis à aucune obligation de conservation, le chiffrement étant libre⁴⁸.

Par ailleurs, dans l'arrêt commenté, la Cour de cassation affirme que « le droit de ne pas s'auto-incriminer et la présomption d'innocence ne sont pas absolus et doivent être mis en balance avec d'autres droits comme le droit à la liberté et à la sécurité garanti par l'article 5 de la CEDH et l'interdiction de l'abus de droit mentionnée à l'article 17 de la CEDH ». On peut s'étonner d'une telle assertion. En effet, *a contrario* de ce qu'affirme la Cour, le droit à la liberté et à la sécurité garanti par l'article 5 de la CEDH ne concerne pas la répression des infractions pénales mais vise en principe, le droit à la liberté d'une personne et les conditions permettant de procéder à une privation de liberté⁴⁹. En outre, cette disposition doit pas être confondue avec les obligations positives ou obligations « d'actions » à charge des États, qui ont été dégagées au fil de la jurisprudence de la Cour de l'UE par le biais notamment des articles 2 et 3 de la CEDH⁵⁰. Ainsi, parallèlement aux obligations de s'abstenir d'ingérences dans les droits fondamentaux, les États sont tenus de mettre en place et d'appliquer un cadre juridique adapté offrant, par exemple, une protection de l'intégrité physique et morale d'un individu contre les actes de violence pouvant être commis par des particuliers⁵¹. Affirmer qu'une méthode d'enquête prescrivant la communication aux autorités, par le suspect d'une information comme un code d'accès à un système informatique s'inscrirait dans le droit à la sûreté dont bénéficieraient les individus au titre de l'article 5 de la CEDH, est un dérapage dangereux d'autant que, même si l'article 6, § 2, de la CEDH n'est pas absolu, des préoccupations d'intérêt général ne sauraient avoir pour conséquence de mettre à mal la substance même des droits de la défense de la personne concernée⁵². Enfin, s'agissant de l'article 17 de la CEDH, visant « l'interdiction de l'abus de droit »⁵³, la référence à cette disposition dans l'arrêt

46 F. KUTY, « Le droit au silence, les investigations de l'administration fiscale et l'enquête pénale », *J.T.*, 2008/22, n° 6314, pp. 386-389.

47 H. D. BOSLY, « Le droit au silence pendant la phase administrative de la surveillance du respect des lois sociales », in *L'auditorat du travail : compétences civiles et pénales*, Bruxelles, Larcier, 2012, pp. 417-443.

48 Art. 48 de la loi du 13 juin 2005 sur les communications électroniques, *M.B.*, 30 juin 2005.

49 R. ERGEC, *Convention européenne des droits de l'homme*, Bruxelles, Bruylant, 2014, p. 302.

50 À ce propos, voy. J.-F. AKANDJI-KOMBE, *Les obligations positives en vertu de la Convention européenne des droits de l'homme*, Précis des droits de l'homme, Éditions du Conseil de l'Europe, 2006 ; C. MADELAINE, *La technique des obligations positives en droit de la Convention européenne des droits de l'homme*, Paris Dalloz, coll. « Nouvelle bibliothèque de thèses », 2014.

51 Voir, parmi d'autres, Cour eur. D.H., *Bevacqua et S. c. Bulgarie*, n°71127/01, 12 juin 2008, § 65.

52 Voy. en ce sens Cour eur. D.H., *Ibrahim et autres c. Royaume-Uni*, n° 50541/08, 50571/08, 50573/08, 40351/09, 13 septembre 2016, § 252.

53 Selon l'article 17 de la CEDH, « Aucune des dispositions de la (...) Convention ne peut être interprétée comme impliquant pour un État, un groupement ou un individu, un droit quelconque de se livrer à une activité ou d'accomplir un acte visant à la destruction des droits ou libertés reconnus



commenté est tout aussi énigmatique. Cet article a notamment pour but d'empêcher les individus de tirer de la CEDH un droit qui leur permette de se livrer à une activité ou d'accomplir une action visant à la destruction des droits garantis par la Convention⁵⁴. Il s'agit par exemple, sous couvert de la liberté d'expression, d'incitation à la violence⁵⁵ ou encore de promouvoir des thèses totalitaires⁵⁶. Cette disposition connaît également une portée négative à charge des États puisque la Convention ne saurait être interprétée comme permettant de priver les individus de leurs droits fondamentaux, en ce inclus l'article 6 de la CEDH⁵⁷. Compte tenu de ce qui précède, ni le penchant positif de l'article 17 de la CEDH ni son penchant négatif ne peuvent nous éclairer sur l'interprétation retenue par la Cour de cassation *in casu*. Tout au plus, la Cour a probablement voulu souligner qu'un individu ne pourrait tirer du droit au respect de la vie privée garanti par l'article 8 de la CEDH, un droit inconditionnel au chiffrement qui lui permettrait par ailleurs de faciliter la commission d'infractions pénales. En ce cas, il aurait été préférable de s'inspirer de la jurisprudence relative à l'article 17 de la CEDH pour examiner la proportionnalité de l'ingérence dans les articles 6 et 8 de la CEDH comme la Cour de cassation l'a fait déjà pour les articles 10 et 11 par exemple. Cette dernière estime en effet que cet article 17 ne trouve à s'appliquer qu'à titre exceptionnel et dans des hypothèses extrêmes⁵⁸, ce qui n'est pas le cas en l'espèce.

d) L'approche de la Cour de cassation confirmée par la Cour constitutionnelle

Parallèlement au pourvoi introduit par l'avocat général près la cour d'appel de Gand dans le cadre de l'arrêt commenté, la Cour constitutionnelle fut saisie d'une question préjudicielle de la cour d'appel d'Anvers. Celle-ci s'interrogeait quant à la constitutionnalité de la différence de traitement entre l'inculpé contraint de fournir certaines informations tel un mot de passe et celui qui ne peut être contraint d'agir directement dans un système informatique. En effet, outre la possibilité laissée au juge d'instruction d'imposer à toute personne appropriée de fournir certaines informations sur base de l'article 88quater, § 1 C. i. cr., l'article 88quater, § 2 C. i. cr. permet au magistrat instructeur d'imposer aux mêmes personnes de

dans la (...) Convention ou à des limitations plus amples de ces droits et libertés que celles prévues à [la] Convention ».

54 Cour eur. D.H., *Orban et autres c. France*, n° 20985/05, 15 janvier 2009, § 33.

55 Dans l'affaire *Belkacem c. Belgique* par exemple, celui-ci fut condamné à une amende et à une peine de prison pour avoir posté sur la plateforme YouTube une série de vidéos dans lesquelles il appelait les auditeurs à dominer les non-musulmans, à leur donner une leçon et à les combattre. La Cour a jugé qu'une attaque aussi générale, véhémente et ouvertement haineuse était en contradiction avec les valeurs de tolérance, de paix sociale et de non-discrimination. Elle a de plus estimé que les propos du requérant préconisant le Jihad et défendant la charia tout en appelant à la violence dans le but de l'imposer pouvaient être considérés comme un « discours de haine » (Cour eur. D.H., *Belkacem c. Belgique*, n° 34367/14, 27 juin 2017, §§ 33-36).

56 Cour eur. D.H., *Lawless c. Irlande*, n° 332/57, 1^{er} janvier 1961, § 7.

57 *Ibid.*, § 6.

58 Pour un approfondissement voy. le *Guide sur l'article 17 de la Convention – Interdiction de l'abus de droit*, Conseil de l'Europe/Cour européenne des droits de l'homme, 2019.

mettre ledit système en fonctionnement et d'agir sur les données informatiques qu'il contient, c'est-à-dire de les rechercher, de les copier, de les rendre accessibles ou inaccessibles ou encore de les retirer de l'appareil exploité⁵⁹. Dans le premier cas, la loi ne souffre aucune dérogation alors que dans le second, il est précisé que cette « obligation d'agir » dans le système informatique ne peut être adressée à un inculpé et aux personnes visées par l'article 156 C. i. cr., à savoir, les ascendants ou descendants de la personne prévenue ainsi que ses proches⁶⁰.

La Cour constitutionnelle répond sans ambages à cette question considérant que la différence de traitement entre l'obligation d'« information » et l'obligation de « coopération » repose sur un critère objectif⁶¹. Selon la Cour, la première consiste à fournir une information qui « existe indépendamment de la volonté » du suspect de sorte que le droit de ne pas contribuer à sa propre incrimination ne s'applique pas⁶². La seconde en revanche, suppose une participation active du suspect aux opérations effectuées dans le système et, dès lors, à la collecte de preuves, ce qui pourrait le conduire à contribuer à sa propre incrimination, entraînant de ce fait une violation de l'article 6, § 2, de la CEDH⁶³. Concernant le droit au respect de la vie privée garanti par les articles 8 de la CEDH et 22 de la Constitution, la Cour précise *in fine* qu'en égard à « la nécessité de mettre à la disposition des autorités judiciaires les moyens adéquats en vue de poursuivre et de réprimer les infractions », il paraît justifié « qu'une personne puisse se voir ordonner de fournir les informations dont elle dispose concernant le fonctionnement ou l'accès à un système informatique »⁶⁴. En d'autres termes, la Cour valide de manière sommaire une méthode d'enquête en considérant qu'elle poursuit un but légitime sans toutefois vérifier concrètement si l'ingérence qu'elle entraîne est « nécessaire dans une société démocratique » tel que le requiert pourtant l'article 8, § 2, de la CEDH. À cet égard, la Cour EDH impose d'examiner l'affaire dans son ensemble et de vérifier si les motifs invoqués pour justifier pareille ingérence étaient pertinents et suffisants tout en s'assurant que la mesure soit proportionnée aux buts légitimes poursuivis compte tenu notamment des garanties offertes aux justiciables⁶⁵.

On ajoutera que sur ce point, la jurisprudence récente de la Cour de Justice de l'Union européenne relative aux articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne (ci-après Charte) garantissant respectivement le droit au respect de la vie privée et le droit à la protection des données à caractère personnel n'est pas dénuée d'intérêt. En vertu de l'article 52, § 1^{er}, de la Charte, toute ingérence dans ces droits doit être prévue par loi, respecter le contenu essentiel desdits droits et, dans le respect du principe de proportionnalité, s'avérer nécessaire et

59 Art. 88*quater*, § 2, C. i. cr.

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

61 C.C., arrêt n° 28/2020 du 20 février 2020, point B.6.1 (cet arrêt est publié ci-avant).

62 C.C., arrêt n° 28/2020 du 20 février 2020, point B.7.

63 C.C., arrêt n° 28/2020 du 20 février 2020, point B.6.2.

64 C.C., arrêt n° 28/2020 du 20 février 2020, point B.7.

65 Cour eur. D.H., *Z c. Finlande*, n°22009/93, 25 février 1997, § 94.

répondre effectivement à un objectif d'intérêt général reconnu par l'Union⁶⁶. Selon la CJUE, le critère de proportionnalité suppose une mesure apte à réaliser l'objectif poursuivi, ne dépassant pas les limites de ce qui est approprié et nécessaire à la réalisation de cet objectif⁶⁷. En poussant son analyse, la cour constitutionnelle aurait pu reprocher à l'article 88quater, § 1^{er} C. i. cr., de ne pas exiger le respect du critère de subsidiarité, c'est-à-dire, l'obligation, pour qu'une ordonnance du juge d'instruction puisse être prise sur son fondement, que ce magistrat ait d'abord constaté que d'autres moyens, moins intrusifs, ne permettaient pas d'atteindre l'objectif poursuivi et que cette mesure s'avérait absolument nécessaire pour la manifestation de la vérité. En effet, comme l'a relevé par exemple le Conseil national du numérique français⁶⁸, « le chiffrement des données n'est pas un obstacle insurmontable pour accéder aux informations nécessaires aux enquêtes. Il existe de nombreux moyens de le contourner, même s'il est très robuste, en exploitant des failles techniques ou en s'introduisant directement dans l'équipement de la personne ciblée. En outre, si les contenus sont chiffrés, les métadonnées y afférent restent généralement en clair, dans la mesure où elles sont indispensables au fonctionnement du système. Ces métadonnées sont bien souvent suffisantes pour cartographier un réseau ou localiser des individus, sans qu'il y ait besoin pour cela d'entrer dans le contenu des communications privées »⁶⁹. Or, le C. i. n'impose pas au juge d'instruction de tenir compte de l'existence d'alternatives moins intrusives.

e) Une position divisée au sein des États membres de l'Union européenne

La compatibilité entre l'obligation du suspect de fournir les clés de chiffrement ou un mot de passe et le droit au silence ne fait pas l'objet d'une position unanime au sein des États membres de l'UE. À l'heure actuelle, dans la majorité des États membres, une telle obligation est considérée comme contraire au droit de ne pas contribuer à sa propre incrimination⁷⁰. Cinq États⁷¹ disposent néanmoins d'une réglementation permettant d'obliger un suspect à remettre la clé d'accès ou à faciliter l'accès aux données dans un format non crypté. Au sein de ces États, la jurisprudence n'est toutefois pas tranchée. Ainsi, en France par exemple, une telle obligation a été validée par le Conseil constitutionnel considérant que « les dispo-

⁶⁶ Art. 52, § 1^{er}, de la Charte des droits fondamentaux de l'Union européenne.

⁶⁷ C.J.U.E., 8 avril 2014, *Digital Rights Ireland Ltd & Michael Seitlinger e.a.*, C-293/12 & C-594/12, §§ 46, 65 et 69.

⁶⁸ Le Conseil national du numérique est commission consultative créée en 2011 par décret du président de la République (décret n° 2011-476). Il est chargé d'étudier les questions relatives au numérique, en particulier les enjeux et les perspectives de la transition numérique de la société, de l'économie, des organisations, de l'action publique et des territoires.

⁶⁹ Conseil national de sécurité du Numérique, « Prédiction, chiffrement et libertés », septembre 2017, p. 12.

⁷⁰ Europol, *Second report of the observatory function of encryption*, 18 février 2020, p. 13.

⁷¹ Il s'agit de la Belgique, de la France, de l'Irlande, du Royaume-Uni et de la Croatie (Europol, *Second report of the observatory function of encryption*, 18 février 2020, p. 13).

sitions critiquées n'imposent à la personne suspectée d'avoir commis une infraction, en utilisant un moyen de cryptologie, de délivrer ou de mettre en œuvre la convention secrète de déchiffrement que s'il est établi qu'elle en a connaissance. Elles n'ont pas pour objet d'obtenir des aveux de sa part et n'emportent ni reconnaissance ni présomption de culpabilité mais permettent seulement le déchiffrement des données cryptées. En outre, l'enquête ou l'instruction doivent avoir permis d'identifier l'existence des données traitées par le moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit. Enfin, ces données, déjà fixées sur un support, existent indépendamment de la volonté de la personne suspectée »⁷². Les conditions sont donc plus strictes qu'en droit belge puisque les autorités judiciaires françaises doivent pouvoir démontrer que le chiffrement des données a été utilisé pour préparer, faciliter ou commettre une infraction. Par ailleurs, selon la cour d'appel de Paris, le champ d'application de cette obligation de collaboration se limite à la clé de chiffrement, laquelle ne s'apparente pas à un mot de passe⁷³. Du côté des Pays-Bas, si s'il n'existe aucune obligation de collaboration imposée au suspect, la jurisprudence admet que celui-ci peut être contraint physiquement de déverrouiller son téléphone portable à l'aide de données biométriques, en l'occurrence l'empreinte digitale de son pouce⁷⁴. Le tribunal précise néanmoins qu'une telle approche ne peut être retenue pour la divulgation d'un mot de passe où le suspect est contraint d'effectuer une déclaration, ce qui entraînerait une violation du droit au silence⁷⁵. Cette jurisprudence contraste avec celle retenue par les plus hautes juridictions belges.

Conclusion

On peut regretter que, par une approche aussi tranchée que celle adoptée dans l'arrêt commenté, la Cour de cassation n'ait pas saisi l'occasion d'effectuer une distinction entre les différents types de codes d'accès, mots de passe, méthodes de verrouillage et moyens de chiffrement des communications. À cela s'ajoute le fait que même si le C. i. cr. suppose le respect de garanties strictes telles que l'intervention d'un juge d'instruction, l'exigence d'une ordonnance motivée et la

72 Conseil constitutionnel, décision n° 2018-696, 30 mars 2018, *J.O.R.F.*, n° 0076 du 31 mars 2018, texte n° 111.

73 Ainsi, en l'espèce, le prévenu était poursuivi pour ne pas avoir révélé le code de déverrouillage de son téléphone portable dans le cadre d'une affaire de stupéfiants. Dans son arrêt, la cour d'appel, après avoir rappelé l'importance des moyens de cryptologie en vue de « garantir la sécurité du stockage ou de la transmission des données, en permettant d'assurer leur confidentialité, leur authentification ou le contrôle de leur intégrité [...] » souligne qu'un « un code de déverrouillage d'un téléphone portable d'usage courant, s'il permet d'accéder aux données de ce téléphone portable et donc aux éventuels messages qui y sont contenus, ne permet pas de déchiffrer des données ou messages cryptés et, en ce sens, ne constitue pas une convention secrète d'un moyen de cryptologie » (C.A. Paris, Pôle 8, 3^e ch., 16 avril 2019, n° 18/09267).

74 Rechtbank Noord-Holland, 14 décembre 2018, n° 15/168454-18.

75 Rechtbank Noord-Holland, 28 février 2019, n° 15/870028-16 et n° 13/032439-13. On indiquera que dans cette affaire, le prévenu fut menotté et a dû ensuite placer son pouce droit sur l'écran de son iPhone en vue de le déverrouiller.

nécessité de pouvoir présumer que la personne concernée connaisse le mot de passe, certaines des garanties pourtant requises en cas d'ingérence dans le droit au respect de la vie privée font défaut. Ainsi, l'article 88^{quater}, § 1, C. i. cr. ne prévoit pas expressément le respect des critères de proportionnalité en limitant, par exemple, cet acte d'enquête aux infractions les plus graves, et/ou de subsidiarité en imposant au juge d'instruction de s'enquérir de l'existence de moyens d'enquête moins intrusifs. Ceci d'autant que certes, un mot de passe n'est pas en soi incriminant, mais exiger du suspect qu'il le dévoile revient à le contraindre à répondre à une question qui lui est posée et à fournir un accès à des informations qui pourraient comporter un caractère incriminant. À ce propos, l'absence de position unanime au sein des États membres de l'Union européenne n'est pas anodine. On peut espérer que la Cour EDH ou la Cour de Justice de l'Union européenne soient amenées à trancher définitivement la question d'autant que tant la Cour constitutionnelle que la Cour de cassation laissent en suspens la question de la compatibilité de l'obligation de fournir certaines informations avec la directive 2016/343. Celle-ci permet, pour rappel, d'obliger le suspect à fournir certaines informations pour lesquelles « une obligation légale de conservation et de production sur demande » est prévue⁷⁶ ce qui n'est pas le cas pour un « mot de passe ou une clé de chiffrement.

Catherine FORGET⁷⁷,

Avocate au Barreau de Bruxelles (JusCogens),

Assistante en droit pénal et procédure pénale à l'Université de Saint-Louis

⁷⁶ Considérant 29 de la directive 2016/343 du 9 mars 2016.

⁷⁷ L'auteure remercie vivement Franck DUMORTIER pour ses précieuses relectures.

