© LEXISNEXIS SA - DROIT PÉNAL - N° 12 - DÉCEMBRE 2022

25

Le saviez-vous ? Chaque jour, vous cryptez vos correspondances !

D'une volonté législative de déchiffrer les communications conspiratives cryptées à la pénalisation prétorienne du simple refus de communiquer le code de déverrouillage de son téléphone portable, dérive de l'article 434-15-2 du Code pénal

Margaux DURAND-POINCLOUX,
avocate associée, cabinet ABPA

Jane PEISSEL,
avocate, cabinet ABPA

et Michael BENDAVID,
avocat associé, cabinet ABPA

Adopté il y a plus de 20 ans, l'article 434-15-2 du Code pénal qui incrimine le refus de révéler la clé de déchiffrement d'un outil de cryptologie a donné lieu ces dernières années à une jurisprudence abondante. Celle-ci est la conséquence, d'une part, de la pratique de nombreux parquets consistant à poursuivre des personnes ayant refusé de dévoiler, durant leur garde à vue, le code de déverrouillage de leur smartphone ; et, d'autre part, de la résistance des juges du fond face au positionnement sévère de la Cour de cassation, au point qu'il est possible aujourd'hui pour chacun d'entre nous de dire, en bons Jourdain : *« il y a plus de cinq ans que je fais de la cryptologie sans que j'en susse rien »*.

1 - Après la chambre criminelle et le Conseil constitutionnel, c'est donc l'assemblée plénière de la Cour de cassation qui livre le 7 novembre 2022 sa solution, en l'occurrence pour un champ d'application extrêmement large du délit [1]. La lente dérive de la portée de ce texte suppose, pour être bien comprise, que l'on se souvienne des circonstances de son adoption et que l'on se remémore les conditions et garde-fous qui ont été posés à sa mise en œuvre. Le caractère extensif de la lecture qu'en fait aujourd'hui la Cour de cassation apparaît alors clairement – ainsi que les difficultés pratiques et d'ordre constitutionnel qui en résultent.

1. Contexte de l'adoption du texte et esprit de la loi

2 - En réaction aux soupçons des enquêteurs sur l'utilisation par les terroristes des attentats du 11 septembre 2001 de techniques de chiffrement de leurs messages électroniques, le législateur français a souhaité donner les moyens à l'État de réagir en cas d'utilisation par des organisations criminelles ou terroristes de moyens de cryptologie. C'est, ainsi, dans le cadre de la loi n° 2001-1062 du 15 novembre 2001 pour la sécurité quotidienne qu'a été adopté l'article 434-15-2 du Code pénal, sur amendement [2].

3 - L'article 434-15-2 du Code pénal sanctionne, donc, *« le fait, pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de remettre ladite convention aux autorités judiciaires ou de la mettre en œuvre, sur les réquisitions de ces autorités délivrées en application des titres II et III du livre I^er^ du code de procédure pénale »*. La peine encourue est aggravée si *« le refus est opposé alors que la remise ou la mise en œuvre de la convention aurait permis d'éviter la commission d'un crime ou d'un délit ou d'en limiter les effets »*.

4 - L'objectif était d'imposer aux fournisseurs – et non aux utilisateurs – de moyens de cryptologie de remettre les conventions permettant le déchiffrement des données transformées au moyen des prestations qu'elles ont fournies [3].

5 - Ce délit était en conséquence intégré dans la section relative aux *« entraves à l'exercice de la justice »*.

6 - Pendant plusieurs années, l'infraction sanctionnée par l'article 434-15-2 du Code pénal n'a, d'ailleurs, quasiment pas été poursuivie. Ce n'est qu'assez récemment, alors que le chiffrement des données devient un outil au service de la confiance des citoyens dans le développement du numérique et que la commercialisation de téléphones utilisant des moyens de cryptologie se banalise, que l'article 434-15-2 du Code pénal a commencé à être utilisé par le ministère public pour poursuivre les suspects refusant de communiquer le code de déverrouillage de leur téléphone [4].

7 - Le *quantum* des peines prévues à l'article 434-15-2 du Code pénal a, parallèlement, été augmenté en 2016 dans le cadre d'une loi renforçant la lutte contre le crime organisé, le terrorisme et leur financement [5].

1. *Cass. ass. plén., 7 nov. 2022, n° 21-83.146 : JurisData n° 2022-018406. – V. dans ce numéro : R. Ollard, Un an de droit pénal numérique : Dr. pén. 2022, chron. 12 ; Dr. pén. 2022, comm. 195, obs. Ph. Conte ; JCP G 2022, 1258, J.-Y. Maréchal ; JCP G 2022, 1320, C. Ribeyre.*
2. *Dalloz actualité, 7 avr. 2021, Garde à vue : ne dites rien, votre téléphone parlera pour vous. – C. Simon-Provo, Peut-on refuser de communiquer le code de déverrouillage d'un téléphone ? : Callalawyer.fr, 15 oct. 2020.*
3. *Dalloz actualité, 7 avr. 2021, Garde à vue : ne dites rien, votre téléphone parlera pour vous. – Compte-rendu des débats de la séance du Sénat du 30 mars 2016 – www.senat.fr.*
4. *Avis de M. Valat, av. gén., arrêt n° 659, 7 nov. 2022, assemblée plénière. – Compte-rendu des débats de la séance du Sénat du 30 mars 2016 – www.senat.fr.*
5. *L. n° 2016-731, 3 juin 2016, art. 16 : JO 4 juin 2016.*

8 - Bien qu'il ait été adopté dans des circonstances exceptionnelles et dans l'objectif qui vient d'être rappelé, ce texte est rédigé dans des termes particulièrement larges, puisqu'il vise :

- « *quiconque ayant connaissance de la convention secrète de chiffrement* », c'est-à-dire aussi bien la personne commercialisant le moyen de cryptologie que la personne suspectée d'avoir commis une infraction à l'aide de ce moyen, et ;
- tout « *moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit* », de sorte qu'il s'applique à toutes les infractions non contraventionnelles, quelle que soit leur gravité.

9 - Ainsi rédigé, le texte permet à l'autorité judiciaire d'en faire une application éloignée de l'esprit de la loi et bien plus fréquente qu'initialement imaginé, sans pour autant, en apparence, déroger au principe d'application stricte de la loi pénale.

10 - Ce nouvel usage du texte instaure une véritable « *obligation de coopérer avec les autorités* » [6] pour la personne suspectée d'avoir commis une infraction. La question de la conformité de ce nouveau délit avec le droit à ne pas s'auto-incriminer et le droit au respect de sa vie privée se pose donc très naturellement, et il y a été partiellement répondu.

2. La conformité du texte avec le droit de ne pas s'incriminer soi-même et le droit au respect de sa vie privée

11 - Cela a été dit, et bien dit : « *L'articulation du droit de se taire en garde à vue et de la demande de communication du code de déverrouillage relève de l'équation insoluble. Rappelons en effet que la personne placée en garde à vue bénéficie du droit, « lors des auditions, après avoir décliné son identité, de faire des déclarations, de répondre aux questions qui lui sont posées ou de se taire ». Dès lors, de deux choses l'une : soit le gardé à vue fait usage de son droit de se taire, auquel cas il est automatiquement en infraction au titre de l'article 434-15-2 du Code pénal ; soit il communique son code secret, et alors son droit de demeurer muet est réduit à néant* » [7].

12 - Aussi, « *sauf à le réduire au droit de ne pas avouer, on perçoit mal, cependant, comment une obligation positive de faire une déclaration pourrait ne pas affecter le droit de se taire.* » [8]. En effet, « *l'obligation faite à la personne suspecte de fournir la convention de chiffrement qu'elle a utilisée équivaut à lui demander d'ouvrir la porte du local où elle a caché le moyen ou le produit de l'infraction en s'auto-incriminant au mépris de la présomption d'innocence* » [9].

13 - Pour autant, ce texte a été déclaré conforme à la Constitution sous certaines réserves, et la question de sa conventionnalité n'a pas encore été tranchée.

A. - Un texte conforme à la constitution sous d'importantes réserves

14 - Le 30 mars 2018, le Conseil constitutionnel a estimé qu'« *en imposant à la personne ayant connaissance d'une convention secrète de déchiffrement d'un moyen de cryptologie de remettre ladite convention aux autorités judiciaires ou de la mettre en œuvre uniquement si ce moyen de cryptologie est susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit et uniquement si la demande émane d'une autorité judiciaire , le législateur a poursuivi les objectifs de valeur constitutionnelle de prévention des infractions et de recherche des auteurs d'infractions, tous deux nécessaires à la sauvegarde de droits et de principes de valeur constitutionnelle* » [10].

15 - Le Conseil constitutionnel conclut que les dispositions contestées ne portent atteinte ni au droit de ne pas s'accuser ni au droit au respect de la vie privée ou au secret des correspondances, dès lors que, selon lui :

- « *Elles 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* », exigence qui peut légitimement paraître superflue, pour se confondre avec l'élément moral de l'infraction : on voit mal comment une personne matériellement incapable de déférer à une réquisition pourrait se voir reprocher un manque de coopération ;
- « *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.* » ;
- « *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.* » ;
- « *ces données, déjà fixées sur un support, existent indépendamment de la volonté de la personne suspectée* » [11].

16 - Ce dernier argument paraît puisé dans la jurisprudence de la Cour européenne des droits de l'homme en matière de prélèvements biologiques ainsi que son application par la chambre criminelle de la Cour de cassation. Cela ressort notamment du fameux arrêt Saunders c/ Royaume-Uni [12], dont la solution trouve écho dans plusieurs arrêts récents de la chambre criminelle.

17 - Ainsi celle-ci a-t-elle estimé, s'agissant d'un prévenu refusant de se soumettre aux vérifications tendant à établir la preuve de son état alcoolique, que « *le droit au silence et celui de ne pas contribuer à sa propre incrimination ne s'étendent pas au recueil de données qu'il convient d'obtenir indépendamment de la volonté de la personne concernée* » [13].

B. - Un texte dont la conventionnalité n'est pas encore confirmée

18 - On l'a dit, en cohérence avec la jurisprudence *Saunders* précitée, le Conseil constitutionnel estime que l'article 434-15-2 du Code pénal est conforme aux droits et libertés garantis par la Constitution.

19 - Ce raisonnement paraît, pourtant, critiquable.

20 - En effet, la Cour européenne des droits de l'homme précise, dans cet arrêt, que « *le droit de ne pas s'incriminer soi-même concerne en premier lieu le respect de la détermination d'un accusé de garder le silence. Tel qu'il s'entend communément dans les systèmes juridiques des Parties contractantes à la Convention et ailleurs, il ne s'étend pas à l'usage, dans une procédure pénale, de données que l'on peut obtenir de l'accusé en recourant à des pouvoirs coercitifs mais qui existent indépendamment de la volonté du suspect, par exemple les documents recueillis en vertu d'un mandat, les prélèvements d'haleine, de sang et d'urine ainsi que de tissus corporels en vue d'une analyse de l'ADN* ».

21 - Or, si l'action de l'intéressé ne change, effectivement, rien à la nature des données telles que son ADN, son sang ou ses empreintes papillaires, tel n'est évidemment pas le cas s'agissant des données se trouvant sur son téléphone, et composées de messages qu'il aura rédigés, d'appels qu'il aura passés, etc.

6. *Praxis Cyberdroit, Dalloz 2022, C. Féral-Schuhl.*
7. *Dalloz actualité, 7 avr. 2021, Garde à vue : ne dites rien, votre téléphone parlera pour vous.*
8. *AJ pénal 2018, p. 257, Constitutionnalité du refus de remise d'une convention secrète de déchiffrement.*
9. *E. Dreyer, L'OPJ gardien de la liberté individuelle ? : JCP G 2020, 1417.*
10. *Cons. const., 30 mars 2018, n° 2018-696 QPC.*
11. *Cons. const., 30 mars 2018, n° 2018-696 QPC.*
12. *CEDH, 17 déc. 1996, n° 19187/91, Saunders c/ Royaume-Uni, pour une revue exhaustive, se rapporter au dossier documentaire de la décision n° 2018-696 QPC.*
13. *Cass. crim., 6 janv. 2015, n° 13-87.652 : JurisData n° 2015-000055. – Confirmé par Cass. crim., 10 déc. 2019, n° 18-86.878 : JurisData n° 2019-022224.*

22 - Dès lors, alors que la question de la communication du code de déverrouillage du téléphone n'est pas encore tranchée par la Cour européenne des droits de l'homme qui a été saisie d'une requête à cet égard, toujours pendante depuis le 31 mai 2021 [14], les doutes quant à la teneur de la décision à intervenir sont permis.

23 - À titre de comparaison, la jurisprudence américaine [15], après quelques atermoiements, considère aujourd'hui que :

- non seulement la personne mise en cause ne peut être contrainte de fournir ses codes sans que cela porte atteinte au cinquième amendement, c'est-à-dire au droit constitutionnel au silence et au droit ne pas s'auto-incriminer [16] ;
- mais encore que celle-ci ne peut pas davantage être forcée à mettre son doigt ou présenter son visage pour déverrouiller son téléphone [17].

24 - Un tel raisonnement pourrait être adopté par la Cour européenne des droits de l'homme.

25 - En attendant sa décision, il convient de se reporter à celles de la chambre criminelle de la Cour de cassation, dont la plume a sensiblement moins tremblé à l'idée de fragiliser le droit de ne pas s'auto-incriminer.

3. Une lecture extensive du texte par la chambre criminelle de la Cour de cassation

26 - Avec l'arrêt rendu le 7 novembre 2022, l'assemblée plénière apporte une réponse claire à trois des questions qui se posent au sujet du délit prévu par l'article 434-15-2 du Code pénal. Elle indique ainsi que l'infraction peut être constituée même si la réquisition émane d'un officier de police judiciaire, que la preuve de l'usage d'une convention de chiffrement par le suspect n'est pas nécessaire, et enfin qu'un téléphone portable moderne peut constituer un moyen de cryptologie entrant dans le champ d'application du texte.

27 - Comme on le verra, chacune de ces trois solutions pose des difficultés pratiques et d'ordre constitutionnel et conventionnel, au regard en particulier de la gravité de la peine encourue.

A. - L'infraction est constituée par le simple refus d'exécuter la réquisition délivrée par un officier de police judiciaire

28 - Selon la lettre de l'article 434-15-2 du Code pénal, l'infraction est caractérisée par le refus de communiquer les codes de téléphones *« aux autorités judiciaires »* ou de les mettre en œuvre *« sur les réquisitions de ces autorités délivrées en application des titres II et III du livre Ier du Code de procédure pénale »*. Le Conseil constitutionnel a jugé que ce texte s'applique *« **uniquement** si la demande émane **d'une autorité judiciaire** »* [18]. Il a expressément tenu compte de cette considération pour dire que l'article 434-15-2 était conforme aux droits et libertés garantis par la Constitution.

29 - Or, la chambre criminelle a décidé dès 2019 que le texte s'appliquait même dans l'hypothèse où la réquisition émanait d'un officier de police judiciaire [19]. Cette solution a été confirmée par un arrêt du 13 octobre 2020, qui précise que la réquisition peut valablement être délivrée sur le fondement des articles 60-1, 77-1-1 et 99-3 du Code de procédure pénale, à la seule condition que le fonctionnaire de police avertisse la personne placée en garde à vue que le refus d'y déférer est susceptible de constituer une infraction pénale [20].

30 - Ces décisions ont conduit récemment certains parquets à faire délivrer aux suspects placés en garde à vue des réquisitions écrites – qui leur sont donc directement adressées et remises par officiers de police judiciaire – d'avoir à remettre le code de déverrouillage de leur téléphone.

31 - Au-delà de l'étonnement que peut susciter une telle pratique, la logique de la Cour de cassation qui la sous-tend nous paraît doublement critiquable.

32 - D'une part, elle s'éloigne de la lettre du texte et de la volonté du législateur. L'article 434-15-2 vise en effet *« l'autorité judiciaire »*, à laquelle il paraît pour le moins délicat d'intégrer l'officier de police judiciaire, dans la mesure où le second est censé agir sous l'autorité et le contrôle de la première. Ainsi, de nombreux auteurs, cités par les Cahiers du Conseil constitutionnels qui paraissent donc les approuver, rappellent que *« le renvoi à la notion de réquisition et d'autorités judiciaires exclurait donc du champ d'application de l'infraction les autorités de jugement et les officiers de police judiciaire »* [21].

33 - Quant à la volonté du législateur, c'est bien simple : lors de l'adoption de la loi en 2001, les officiers de police ne disposaient pas encore d'un pouvoir autonome de réquisition. Celui-ci a été introduit dans notre droit en 2003.

34 - Dans ces conditions, la jurisprudence de la chambre criminelle paraît, pour beaucoup, dont les auteurs de ces lignes, contraire au principe d'interprétation stricte de la loi pénale, puisqu'elle *« élude une des conditions constitutives de l'infraction »* [22].

35 - D'autre part, la position de la Cour de cassation est critiquable en ce qu'elle entame fortement les garanties dont le texte est entouré, puisque le contrôle assuré par l'autorité judiciaire n'intervient possiblement qu'*a posteriori*. Peut-être est-ce la raison pour laquelle la haute juridiction a cru devoir, parallèlement, ajouter à la loi une condition qu'elle ne prévoit pas, pour exiger que la personne soit informée de la circonstance que son refus l'exposerait à une sanction pénale.

36 - Cette information paraît pourtant superflue, puisque nul n'est censé ignorer la loi. Surtout, en pratique, loin d'offrir une protection pour les personnes poursuivies, elle nous paraît constituer plutôt une menace et une pression supplémentaire d'avoir à déférer à la réquisition.

37 - En l'état, il existe donc selon nous un doute sérieux quant à la conformité de la jurisprudence de la Cour de cassation aux droits et libertés garantis par la Constitution, au regard de la jurisprudence du Conseil constitutionnel.

B. - La preuve de l'usage du moyen de cryptologie pour préparer, faciliter ou commettre l'infraction suspectée n'est pas nécessaire

38 - Trois observations méritent d'être formulées ici.

39 - En premier lieu, selon la lettre du texte, pour que l'infraction soit constituée, il faut que le *« moyen de cryptologie [soit] susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit »*. Le Conseil constitutionnel reprend expressément cette exigence pour rappeler que le délit est constitué *« **uniquement** si ce moyen de cryptologie est susceptible d'avoir*

14. *CEDH, 31 mai 2021, n° 23624/20, Minteh c/ France.*
15. *Comparaison issue de S. Vergnolle, Clair-obscur autour de la qualification des codes de déverrouillage des téléphones et des personnes pouvant les requérir : D. 2021, p. 609.*
16. *Dictrict court du Michigan, United States c/ Kirschner, 30 mars 2010, 823 F. Supp. 2d 665.*
17. *District court de Californie, In the matter of a search of a residence in Oakland California, 10 janv. 2019.*
18. *Cons. const., 30 mars 2018, n° 2018-696 QPC : JurisData n° 2018-004904.*
19. *Cass. crim., 10 déc. 2019, n° 18-86.878 : JurisData n° 2019-022224. – Cass. crim., 13 oct. 2020, n° 19-85.984 : JurisData n° 2020-016478. – Cass. crim., 13 oct. 2020, n° 20-80.150 : JurisData n° 2020-015967. – Cass. crim., 3 mars 2021, n° 19-86.757 : JurisData n° 2021-002926.*
20. *Cass. crim., 13 oct. 2020, n° 20-80.150 : JurisData n° 2020-015967.*
21. *Commentaire de la décision n° 2018-696 QPC du 21 mars 2018 : Cah. Cons. const.*
22. *Eric A. Caprioli, Quand le refus de communiquer le code du téléphone est un délit : Comm. com. électr. 2021, comm. 8.*

été utilisé pour préparer, faciliter ou commettre un crime ou un délit » [23].

40 - Le terme « *susceptible* » signifie évidemment que la preuve d'une utilisation effective n'a pas besoin d'être rapportée. La question demeure toutefois de savoir quel degré d'exigence pèse sur la partie poursuivante, pour administrer la preuve d'une utilisation conspirative – fût-elle potentielle – d'un moyen de cryptologie. À l'extrême, peut-on établir une sorte de présomption générale et absolue d'utilisation d'un tel téléphone pour commettre, préparer ou faciliter tout délit soupçonné ? Ou faut-il au contraire qu'il ressorte de l'enquête des éléments précis et circonstanciés de cet usage ?

41 - On opte évidemment pour la seconde solution, tant la présomption générale de commission d'une infraction heurterait nombre de nos principes. Pourtant, la Cour de cassation a validé un arrêt d'une cour d'appel ayant jugé que « *les éléments découverts en possession* » du suspect « *laissent présumer un usage du téléphone portable en lien avec des infractions à la législation sur les stupéfiants* », alors que ces éléments se résumaient en l'occurrence à des indices de l'existence d'un trafic de stupéfiants (« *la plaquette de résine de cannabis et les sommes d'argent très importantes, dont l'analyse des billets a démontré la présence d'un taux de cannabis et de cocaïne supérieurs à ceux habituellement rencontrés sur les billets en circulation normale* »), et au refus de l'intéressé de livrer le code d'accès de son téléphone [24].

42 - Si l'on conçoit que la chambre criminelle laisse aux juges du fond le soin de caractériser souverainement si le moyen de cryptologie est « *susceptible* » d'avoir été utilisé par le suspect, une telle motivation nous paraît critiquable et porteuse d'une dérive supplémentaire préoccupante, et aurait pu justifier une censure pour manque de base légale. En particulier, déduire du simple refus de l'intéressé de dévoiler son code d'accès, que le téléphone a été utilisé pour commettre l'infraction reprochée, revient *in fine* à réduire à néant le premier élément constitutif du délit.

43 - En deuxième lieu, ce qui précède vaut *a fortiori* dans la mesure où la lettre du texte exige que ce soit le « *moyen de cryptologie* » lui-même qui soit utilisé pour la commission de l'infraction, et non le téléphone portable sur lequel ce moyen de cryptologie serait, par ailleurs, installé. Rappelons à cet égard que le moyen de cryptologie est défini par l'article 29 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique, comme « *tout matériel ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'informations ou de signaux, à l'aide de conventions secrètes ou pour réaliser l'opération inverse avec ou sans convention secrète* ». Dans cette optique, un trafiquant de stupéfiants qui converse avec ses complices *via* son smartphone n'utilise pas spécifiquement l'outil de chiffrement pour commettre le délit, mais seulement son appareil de communication, par ailleurs doté d'un système de chiffrement. Ce moyen n'a, à notre connaissance, jamais été invoqué, de sorte que la jurisprudence n'y a pas encore répondu.

44 - En troisième lieu enfin, ces questions font écho à l'exigence du Conseil constitutionnel selon laquelle « *l'enquête ou l'instruction doivent avoir permis d'identifier l'existence des données traitées par le moyen de cryptologie* ». Il semble, en effet, qu'il en découle une interdiction pour les autorités de poursuite d'aller « *à la pêche* » aux informations. Le texte n'est pas conçu pour permettre de s'assurer qu'il n'existe pas de preuves de l'infraction sur tel ou tel support ; mais pour faciliter l'accès à des preuves dont on peut déjà raisonnablement supposer, sinon démontrer, l'existence.

45 - En l'état, sur ce plan également, la jurisprudence de la Cour de cassation pose question quant à sa conformité à la décision du Conseil constitutionnel.

C. - Le code de déverrouillage d'un téléphone portable peut être un moyen de cryptologie

46 - Comme évoqué *supra*, la notion de « *moyen de cryptologie* » est définie par l'article 29 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique. Ce texte précise en outre que les « *moyens de cryptologie ont principalement pour objet de garantir la sécurité du stockage ou de la transmission de données, en permettant d'assurer leur confidentialité, leur authentification ou le contrôle de leur intégrité* ». La convention de déchiffrement est quant à elle définie par l'article R. 871-3 du Code de la sécurité intérieure, comme correspondant à « *des clés cryptographiques ainsi que de tout moyen logiciel ou de toute autre information permettant la mise au clair de ces données* ».

47 - Concrètement, il s'agit d'outils utilisant des algorithmes de chiffrement qui permettent de rendre inintelligibles des données, sauf à disposer d'une clé mathématique, par construction secrète. La question fondamentale posée à la Cour de cassation dans l'arrêt commenté était alors : le code de déverrouillage d'un téléphone est-il une clé mathématique permettant le déchiffrement de données cryptées, ou bien constitue-t-il « *seulement* » un code indispensable pour utiliser le téléphone et donc accéder aux données qu'il contient – sans que celles-ci ne fassent l'objet d'un (dé)cryptage ?

48 - La réponse est évidemment autant technique que juridique, et n'admet aucune réponse générale. Certains outils tels que les téléphones cryptés (« PGP ») relèvent manifestement de la première catégorie, tandis que les téléphones de générations plus anciennes disposaient d'un simple code d'accès, limitant l'accès au système, mais sans le moindre chiffrement des données. Qu'en est-il des smartphones les plus récents ?

49 - La Cour de cassation et les juges du fond ont apporté des réponses très différentes, aboutissant *in fine* à la décision de l'assemblée plénière du 7 novembre 2022. Par un premier arrêt remarqué du 16 avril 2019, la cour d'appel de Paris jugeait qu'« *un code de déverrouillage d'un téléphone portable d'usage courant, qui ouvre l'accès aux données qui y sont contenues, ne constitue pas une convention secrète d'un moyen de cryptologie, en ce qu'il ne permet pas de déchiffrer des données ou messages cryptés* » [25].

50 - Cette solution avait été censurée sur pourvoi du ministère public, la chambre criminelle jugeant « *inopérante* » la notion de « *téléphone d'usage courant* » pour écarter la qualification de moyen de cryptologie. Elle affirmait ainsi que « ***le code de déverrouillage d'un téléphone portable peut constituer une telle convention lorsque ledit téléphone est équipé d'un moyen de cryptologie*** », et ajoutait que « *l'existence d'un tel moyen peut se déduire des caractéristiques de l'appareil ou des logiciels qui l'équipent ainsi que par les résultats d'exploitation des téléphones au moyen d'outils techniques, utilisés notamment par les personnes qualifiées requises ou experts désignés à cette fin, portés, le cas échéant, à la connaissance de la personne concernée* [26] ».

51 - Le même scénario s'est produit à Aix-en-Provence, où la relaxe prononcée par la cour d'appel a été cassée par la chambre criminelle [27], puis de nouveau à l'occasion de l'affaire ayant suscité l'arrêt du 7 novembre 2022. Ici, la cour d'appel de Douai avait confirmé une relaxe en énonçant qu'un téléphone portable ne pouvait être considéré comme un moyen de cryptologie et que le code de déverrouillage de l'écran d'accueil d'un téléphone ne pouvait être qualifié de convention secrète de déchiffrement.

52 - Sur renvoi après cassation (au motif que cette motivation était « *générale et erronée, alors que le code de déverrouillage d'un téléphone portable constitue une convention de déchiffrement s'il*

23. *Cons. const., 30 mars 2018, n° 2018-696 QPC : JurisData n° 2018-004904.*
24. *Cass. crim., 10 déc. 2019, n° 18-86.878 : JurisData n° 2019-022224.*
25. *CA Paris, 16 avr. 2019, n° 18/09267.*
26. *Cass. crim., 13 oct. 2020, n° 20-80.150 : JurisData n° 2020-015967.*
27. *Cass. crim., 9 mars 2022, n° 21-83.557 : JurisData n° 2022-003582.*

permet de mettre au clair les données qu'il contient » [28], la cour d'appel résistait et confirmait la relaxe au motif que « *la clé de déverrouillage de l'écran d'accueil d'un smartphone n'est pas une convention secrète de chiffrement, car elle n'intervient pas à l'occasion de l'émission d'un message et ne vise pas à rendre incompréhensibles ou compréhensibles des données, au sens de l'article de la loi du 21 juin 2004, mais tend seulement à permettre d'accéder aux données et aux applications d'un téléphone, lesquelles peuvent être ou non cryptées* ».

53 - C'est cette solution qui est censurée par la formation solennelle de la Cour de cassation. Elle reproche en effet à la cour d'appel d'avoir omis de s'assurer des caractéristiques techniques des smartphones en cause, pour déterminer si, au cas particulier, ceux-ci disposaient d'une solution de chiffrement des données qu'ils contiennent.

54 - Reste à déterminer si tel était le cas en l'espèce. La Cour de cassation n'y répond bien évidemment pas – cela n'entrait pas dans son office. Toutefois, elle livre deux indices éloquents de son opinion.

55 - D'une part, la cassation intervient pour violation de la loi et non manque de base légale, alors que cette voie paraissait pleinement loisible. Elle donne ainsi plus de force à sa jurisprudence. D'autre part, elle précise dans son communiqué qu'« *aujourd'hui la plupart des téléphones portables* » seraient dotés d'une convention de chiffrement des données.

56 - À supposer que ce soit exact, il appartiendra néanmoins aux parquets d'administrer la preuve de cette caractéristique technique, pour chaque appareil donnant lieu à des poursuites, sur la base notamment des notices techniques fournies par les constructeurs. Il nous paraît qu'il leur incombera également de démontrer que le suspect lui-même avait conscience de cette caractéristique technique car, comme la résistance des juges du fond l'illustre parfaitement, ceci n'a rien d'évident.

57 - Vu la teneur des règles établies par la Cour de cassation, les prétoires seront donc prochainement l'objet de débats techniques, au cas par cas. Si l'on ajoute cette difficulté aux autres, d'ordres constitutionnel et conventionnel, évoqués ci-dessus, les débats semblent donc loin d'être clos.■

28. *Cass. crim., 13 oct. 2020, n° 19-85.984 : JurisData n° 2020-015967 ; Dr. pén. 2021, comm. 1 ; JCP G 2020, 1417, E. Dreyer ; Procédures 2020, comm. 229 ; Comm. com. électr. 2021, comm. 8, préc. ; D. 2021, p. 609, note S. Vergnolle.*

Mots-Clés : Numérique - Refus de transmettre une convention secrète de déchiffrement - Code de déverrouillage