COUR DE CASSATION

AVIS DE M. VALAT ,
AVOCAT GÉNÉRAL

Arrêt n° 659 du 7 novembre 2022 – Assemblée plénière

Pourvoi n° 21-83.146

Décision attaquée : Cour d'appel de Douai, 20 avril 2021

Le Procureur général près la cour d'appel de Douai
C/
M. [O]

Pourvoi formé par le procureur général près la cour d'appel de Douai contre l'arrêt de ladite cour d'appel, 6e chambre, en date du 20 avril 2021, qui, sur renvoi après cassation *(Crim.,* 13 octobre *2020, pourvoi n° 19-85.984)*, a renvoyé M. [C][O] des fins de la poursuite du chef de refus de remettre ou de mettre en œuvre la convention de déchiffrement d'un moyen de cryptologie.

RAPPEL DES FAITS ET DE LA PROCÉDURE

M. [O], interpellé par les services de police le 12 mai 2018 à Roubaix et placé en garde à vue pour infractions à la législation sur les stupéfiants, a refusé de communiquer aux enquêteurs les codes permettant de déverrouiller deux téléphones portables IPhone 4 et IPhone X trouvés en sa possession.

Le tribunal correctionnel de Lille, devant lequel il a été poursuivi pour offre ou cession de cannabis et pour refus de fournir le code de déverrouillage d'un téléphone susceptible d'avoir été utilisé dans le cadre d'un trafic de stupéfiants, constituant une

convention secrète de déchiffrement d'un moyen de cryptologie, l'a condamné du premier chef et relaxé du second.

La cour d'appel, saisie d'un appel du procureur de la République sur la relaxe, a confirmé le jugement déféré.

La chambre criminelle de votre Cour, saisie d'un pourvoi formé par le procureur général près la cour d'appel de Douai *(n°19-85.984 du 13 octobre 2020)*, a censuré l'arrêt de relaxe en toutes ses dispositions, en considérant que le code de déverrouillage d'un téléphone mobile constitue une convention de déchiffrement au sens des articles L. 871-1 et R. 871-3 du code de la sécurité intérieure s'il permet de mettre au clair les données contenues dans ce téléphone, lorsque celui-ci est équipé d'un logiciel permettant de transformer ces données.

Le refus de remettre ce code ou convention de déchiffrement aux autorités judiciaires ou de le mettre en œuvre sur la réquisition de ces autorités constitue alors l'infraction prévue et réprimée par l'article 434-15-2 du code pénal.

Par l'arrêt attaqué, rendu le 20 avril 2021, la cour d'appel de Douai, autrement composée, devant laquelle l'affaire a été renvoyée, a prononcé à nouveau la relaxe de M. [C][O] du chef du délit de refus de remettre ou de mettre en œuvre la convention de déchiffrement d'un moyen de cryptologie.

Le procureur général près la cour d'appel de Douai a formé un nouveau pourvoi en cassation qui est recevable.

ANALYSE SUCCINCTE DES MOYENS

A l'appui de son pourvoi, le procureur général soutient, par un mémoire recevable, qu'il ressort des dispositions de l'article 29 de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique et des articles 132-79 du code pénal et R871-3 du code de la sécurité intérieure que l'on entend comme «conventions permettant le déchiffrement des données transformées au moyen des prestations de cryptologie» les «clés cryptographiques ainsi que tout moyen logiciel ou de toute information permettant la mise au clair de ces données» ; qu'en affirmant de manière générale que le code de déverrouillage d'un smartphone n'est pas une convention secrète de chiffrement sans effectuer l'analyse des caractéristiques techniques du téléphone concerné IPhone 4, pourtant indispensable pour fonder sa décision, la cour d'appel a insuffisamment motivé sa décision.

DISCUSSION

I. Observation liminaire

Bien que le moyen, tel qu'il vient d'être énoncé, ne vise expressément que l'IPhone 4, il ressort du mémoire que l'IPhone X[1] trouvé en possession de M. [O] est également concerné par le moyen.

II. Historique du texte d'incrimination

Après les attentats ayant touché les Etats-Unis d'Amérique le 11 septembre 2001, le législateur français a voté plusieurs dispositions destinées à faciliter la mise au clair de données chiffrées. Ces textes étaient toutefois en gestation avant ces attentats puisque le projet de loi sur la société de l'information déposé en juin 2001 les prévoyait déjà. Une recommandation du Conseil de l'Europe préconisait dès 1995 de « minimiser les effets négatifs de l'utilisation du chiffrement sur les enquêtes des infractions pénales »[2].

Ont donc été votées des dispositions

- autorisant les magistrats à recourir aux moyens techniques de l'Etat soumis au secret de la défense nationale pour déchiffrer un message crypté ;

- obligeant les personnes physiques ou morales fournissant des prestations de cryptologie à remettre aux agents habilités de l'Etat, en charge d'une mission d'interception des correspondances, les conventions permettant de déchiffrer les messages cryptés ;

- incriminant le fait pour quiconque a connaissance de la convention secrète de déchiffrement susceptible d'avoir été utilisée pour préparer, faciliter ou commettre un crime ou un délit, de refuser de la remettre aux autorités judiciaires.

Initialement votées pour une durée limitée, ces trois dispositions ont été pérennisées par la loi du 18 mars 2003 et elles sont toujours en vigueur.

Celles autorisant le recours aux moyens de l'Etat couverts par le secret de la défense nationale figurent aux articles 230-1 et suivants du code de procédure pénale. Le Conseil constitutionnel vient d'ailleurs d'écarter le grief fait à ces dispositions de priver la personne mise en cause de la possibilité de contester la régularité de

[1] Mémoire page 6

[2] Recommandation R (95)13 du 11 septembre 1995 du comité des ministres aux Etats-membres

l'opération, en méconnaissance des droits de la défense, des principes de l'égalité des armes et du contradictoire et du droit à un recours juridictionnel effectif[3].

Celles obligeant les personnes physiques ou morales fournissant des prestations de cryptologie à remettre aux agents habilités de l'Etat, en charge d'une mission d'interception des correspondances, les conventions permettant de déchiffrer les messages cryptés figurent actuellement à l'article L871-1 du code de la sécurité intérieure.

La 3e disposition est celle qui vous occupe et qui a inséré dans le code pénal un article 434-15-2, qui punit de trois ans d'emprisonnement et de 270 000 € d'amende (45 000 € dans le texte d'origine) 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 Ier du code de procédure pénale.

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, la peine est portée à cinq ans d'emprisonnement et à 450 000 € d'amende.

La loi du 21 juin 2004 a en outre aggravé les peines d'un degré lorsqu'un moyen de cryptologie a été utilisé pour préparer ou commettre un crime ou un délit, ou pour en faciliter la préparation ou la commission. Cette disposition, prévue à l'article 132-79 du code pénal, est toujours en vigueur. Ainsi le trafic de stupéfiants qui fait normalement encourir 10 ans d'emprisonnement à ses auteurs est passible d'une peine de 15 ans de réclusion criminelle quand un moyen de cryptologie a été utilisé. La cour d'assises ou la cour criminelle devrait donc être saisie à chaque fois. Ce n'est évidemment pas la pratique suivie par les parquets et les juges d'instruction.

Cet article 132-79 du code pénal incite les personnes poursuivies à remettre la clé de déchiffrement puisqu'il prévoit que ses dispositions ne sont pas applicables si l'auteur ou le complice de l'infraction a remis aux autorités judiciaires ou administratives à leur demande, la version en clair des messages chiffrés ainsi que les conventions secrètes nécessaires au déchiffrement.

Pendant plusieurs années, l'infraction sanctionnée par l'article 434-15-2 du code pénal n'a quasiment pas été poursuivie, si l'on en croit les bases de données juridiques et ce qu'ont dit les parlementaires lors du vote de la loi du 3 juin 2016 qui a aggravé la peine d'amende encourue. Ce n'est qu'assez récemment que plusieurs parquets ont pris l'initiative de poursuivre de ce chef des suspects refusant de communiquer le code de déverrouillage de leur téléphone portable avec lequel ils

[3] Cons. Cons. Décision n° 2022-987 Qpc du 8 avril 2022

avaient souvent entretenu les relations nécessaires à leur trafic, voire avaient pris en photo avec leur téléphone la drogue ou l'argent tiré de leur activité.

S'il est patent qu'en 2001 le législateur ne pouvait pas avoir à l'esprit que ce texte pourrait être utilisé à l'encontre des dealers en possession de smartphones - pour la bonne raison que les smartphones ne sont arrivés sur le marché qu'en 2007, notamment le tout premier IPhone-, ce n'est pas une raison pour considérer que le texte ne pourrait pas s'appliquer à cette hypothèse.

Il faut, mais il suffit, pour respecter le principe d'interprétation stricte de la loi pénale posé par l'article 111-4 du code pénal, que le comportement en cause corresponde aux prévisions du texte.

Le texte sanctionne quiconque ayant connaissance de la convention susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, refuse 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 Ier du code de procédure pénale secrète de déchiffrement d'un moyen de cryptologie.

Quelques indications doivent être données sur les divers éléments constitutifs de l'infraction avant d'insister sur les éléments que sont : "le moyen de cryptologie" et la "convention secrète de déchiffrement" qui constituent le coeur de la question qui se pose à vous.

III. Eléments constitutifs "périphériques"

A. Quiconque

La 1ère question qui se pose eu égard au fait que le législateur a, semble-t-il, pensé aux fournisseurs de moyens de cryptologie en édictant le texte est de savoir s'il peut être appliqué à des suspects et non à des tiers à la procédure, ce que sont, habituellement, les personnes requises au sens du code de procédure pénale.

La lettre du texte ne semble pas l'interdire puisque c'est « quiconque » qui y est visé. Le Conseil constitutionnel, saisi d'une question prioritaire de constitutionnalité concernant l'application du texte à un suspect, s'est référé au fait que l'article 434-15-2 visait « quiconque »[4]. La question dont il a été saisi soutenait que les dispositions

[4] Décision 2018-696 QPC du 30 mars 2018

contestées, en ce qu'elles sanctionnaient le refus pour une personne suspectée d'une infraction de remettre aux autorités judiciaires, ou de mettre en œuvre à leur demande, une clé de déchiffrement susceptible d'avoir été utilisée pour commettre cette infraction :

- porteraient atteinte au droit au silence et au droit de ne pas contribuer sa propre incrimination ;
- seraient ainsi contraires au droit une procédure juste et équitable garanti par l'article 16 de la Déclaration des droits de l'homme et du citoyen de 1789 et au principe de présomption d'innocence garanti par l'article 9 de cette m me déclaration ;
- violeraient le droit au respect de la vie privée et, selon l'une des parties intervenantes, le secret des correspondances, les droits de la défense, le principe de proportionnalité des peines et la liberté d'expression.

Le représentant du premier ministre aurait invité le Conseil à formuler une réserve d'interprétation pour exclure la personne suspectée du champ d'application du délit[5].

Le Conseil a, selon le commentaire officiel de la décision, pris acte de l'interprétation de la Cour de cassation selon laquelle l'infraction contestée s'appliquait non seulement aux personnes fournissant un moyen de cryptologie susceptible d'aider à la commission d'une infraction, mais aussi à toute personne utilisant un tel moyen de cryptologie, y compris la personne suspectée d'être l'auteur de l'infraction commise à l'aide de celui-ci.

Il a ensuite estimé que les dispositions contestées ne portaient pas atteinte au droit de ne pas s'accuser ni au droit au respect de la vie privée et au secret des correspondances car, en imposant à la personne ayant connaissance d'une convention secrète de déchiffrement d'un moyen de cryptologie de la remettre aux autorités judiciaires uniquement si ce moyen de cryptologie est susceptible d'avoir été utilisé pour préparer, faciliter ou commettre l'infraction et uniquement si la demande émane d'une autorité judiciaire, le législateur avait 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. Le Conseil a également pris en compte le fait que les dispositions critiquées n'imposaient à la personne suspectée de révéler la convention que si elle en avait connaissance, de sorte qu'elles n'avaient pas pour objet d'obtenir des aveux et n'emportaient ni reconnaissance ni présomption de culpabilité mais permettaient seulement le déchiffrement des données cryptées. Il a encore retenu que l'enquête ou l'instruction devaient 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 et il a fait sienne une raison retenue parfois par la Cour EDH (edh) pour valider une contrainte, à savoir que les données, déjà fixées sur un support, existaient indépendamment de la volonté de la personne suspectée.

Cette dernière raison a été reprise par la chambre criminelle dans un arrêt du 10 décembre 2019 où le demandeur soulevait l'inconventionalité de l'article 434-15-2 du code pénal notamment au regard du droit à ne pas s'auto-incriminer. La chambre criminelle a retenu que « le droit de ne pas s'incriminer soi-même ne s'étend pas aux données que l'on peut obtenir de la personne concernée en recourant à des pouvoirs coercitifs mais qui existent indépendamment de la volonté de l'intéressé »[6]. La personne dont le pourvoi a alors été rejeté a saisi la Cour EDH (edh) qui a interrogé le Gouvernement français le 31 mai 2021 sur les griefs relatifs au droit de garder le

[5] Selon Imane Bello et Emmanuel Mercinier, Avocats, cabinet VIGO AJ Pénal 2020 p.33, La Cour de cassation n'a pas dit que le code de déverrouillage d'un téléphone constitue une convention de cryptologie. Confirmé la revue de presse de la DSJ, citant le quotidien Le Monde, évoquée par votre rapporteur

[6] Crim., 10 décembre 2019, pourvoi n° 18-86.878

silence et de ne pas contribuer à sa propre incrimination, au respect de la vie privée et de la correspondance. L'affaire pourrait être tranchée par la Cour européenne au cours de l'année 2023.

B. Moyen susceptible d'avoir été utilisé pour préparer, faciliter ou commettre l'infraction

Dans la même affaire, la chambre criminelle a été saisie d'un moyen soutenant que les motifs retenus par la décision de condamnation étaient insuffisants à démontrer qu'un téléphone trouvé en possession d'une personne suspectée de se livrer au trafic de stupéfiants avait effectivement pu être utilisé pour préparer, faciliter ou commettre un crime ou un délit. Relevant que l'arrêt attaqué énonçait notamment que la culpabilité du prévenu découlait des éléments découverts en sa possession, soit la somme de 6 680 euros en numéraire, la présence d'une plaquette de résine de cannabis sur le sol du véhicule qu'il conduisait ainsi qu'un téléphone portable, des analyses effectuées sur les billets de banque trouvés sur le prévenu lors de son interpellation qui avaient révélé la présence d'un taux de cannabis et de cocaïne supérieurs à ceux habituellement rencontrés sur les billets en circulation normale, de la découverte de sommes en numéraire et de trois autres téléphones portables lors de la perquisition effectuée à son domicile et de l'absence d'explications cohérentes du prévenu pour justifier la possession de ces sommes d'argent, la chambre criminelle a estimé que ces motifs étaient dénués d'insuffisance et relevaient de l'appréciation souveraine des juges du fond[7].

Une première approche du texte d'incrimination pourrait donner le sentiment que la décision de la cour d'appel qui a été approuvée était peu diserte quant à la preuve que le téléphone saisi avait effectivement été utilisé pour commettre l'infraction.

Le professeur Conte, commentant cet aspect de la décision[8], tout en relevant que la formule de l'article 434-15-4 exige seulement que l'utilisation du moyen de cryptologie ait été possible (« susceptible »), sans qu'il soit requis une vraisemblance, a fortiori une certitude en ce sens, note qu'il faut toutefois que cette possibilité soit inférée des faits de la cause et estime qu'il n'est pas certain que les constatations des juges du fond, qui s'attachent exclusivement aux infractions commises, soient suffisantes, n'évoquant aucune circonstance concrète établissant

[7] Crim., 10 décembre 2019, pourvoi n° 18-86.878

[8] REFUS DE REMETTRE UNE CONVENTION SECRÈTE DE DÉCHIFFREMENT D'UN MOYEN DE CRYPTOLOGIE - Commentaire par Philippe CONTE, Droit pénal n° 2, Février 2020, comm. 27

un lien, serait-il seulement possible, entre l'infraction et l'usage des téléphones. Il se demande si en définitive, ce n'est pas le seul refus, opposé par le prévenu, de révéler les codes de déverrouillage de ces instruments qui a été pris en compte par les juges du fond, pour en conclure qu'ils avaient un contenu compromettant et que, partant, ils avaient bien dû être utilisés pour lui permettre d'exercer son activité délictueuse.

La décision apparait toutefois parfaitement conforme au texte qui n'exige pas une utilisation effective du téléphone mais qu'il soit susceptible d'être utilisé.

Comme le relève le professeur Ribeyre au Jurisclasseur[9] , *« … la preuve de son utilisation effective n'a donc pas besoin d'être rapportée, il suffit que le moyen de cryptologie ait été susceptible d'être utilisé. L'infraction est donc une infraction de prévention. .. »*

La plupart des commentateurs de cette décision n'ont pas abordé cet aspect dans leurs commentaires[10], certains se focalisant sur le fait que la Cour de cassation n'avait pas dit, à cette occasion, que le code de déverrouillage d'un téléphone portable était une convention secrète de déchiffrement d'un moyen de cryptologie et n'émettant aucune critique sur le caractère souverain reconnu aux juges du fond pour juger de la possible utilisation du téléphone pour commettre l'infraction[11].

Madame Lepage a, quant à elle, relevé que *« le terme « susceptible », moins exigeant qu'une probabilité, exprime simplement « la modalité du possible » (cnrtl.fr/définition/susceptible, A). Conformément à l'esprit du texte, la Cour de cassation s'est montrée elle-même peu exigeante envers les juges du fond, dont elle a considéré que les motifs précités étaient suffisants et relevaient de leur appréciation souveraine »*[12]*.*

[9] J-CL Pénal code, Art. 434-15-2

[10] François Fourment, professeur à l'université de Tours, GP 12 mai 2020, n° 18, p. 61 - Rodolphe Mésa, GP, 4 février 2020, n° 5, p. 19 – Les données contenues dans un téléphone n'entrent pas dans le champ d'application du droit de ne pas s'auto-incriminer, JCP, G, n° 52, 23 déc. 2019, p. 1369

[11] AJ Pénal 2020 p.33, La Cour de cassation n'a pas dit que le code de déverrouillage d'un téléphone constitue une convention de cryptologie, Imane Bello, Avocat, cabinet VIGO Avocats, Emmanuel Mercinier, Avocat, cabinet VIGO Avocats

[12] Un an de droit pénal du numérique (Octobre 2019 – Octobre 2020) - Chronique par Agathe LEPAGE

A. - Refus de remise

La façon dont la personne invitée à communiquer la convention secrète de déchiffrement oppose un refus n'a pas donné lieu à contentieux.

Dans la plupart des espèces, l'intéressé a tenté de justifier son refus par le fait qu'il ne voulait pas que les enquêteurs puissent prendre connaissance d'éléments relatifs à sa vie privée en affirmant que cela n'avait aucun lien avec la commission d'une infraction.

Précision est ici apportée que la chambre criminelle juge que lorsque la personne gardée à vue communique son code de déverrouillage, elle n'est pas soumise à une audition à laquelle son avocat pourrait être présent[13].

Une question n'a pas encore été posée à la chambre criminelle : le refus de communication du code de déverrouillage qui serait opposé au cours d'une enquête préliminaire pourrait-il être sanctionné ? On sait que dans ce type d'enquête une perquisition (et l'exploitation du contenu d'un téléphone y est assimilée) ne peut être effectuée qu'avec le consentement du titulaire des lieux ou, à certaines conditions, avec l'autorisation du juge des libertés et de la détention. Si, au cours d'une enquête préliminaire, une personne refuse de communiquer son code, faut-il considérer qu'elle ne fait qu'exercer, en quelque sorte, son droit de ne pas consentir à la fouille du téléphone ou, le consentement à la perquisition étant distinct de la communication du code, commet-elle l'infraction ? [14] Ce n'est toutefois pas une question qui se pose dans l'espèce qui vous est soumise.

B. - Réquisitions

Le texte prévoit que la personne qui connaît la convention secrète de déchiffrement doit être requise par les autorités judiciaires de la leur remettre.

Il a été soutenu, par une partie de la doctrine, que les officiers de police judiciaire n'étaient pas des autorités judiciaires.

Il a, en sens contraire, été relevé que les réquisitions prévues aux titres II et III du livre Ier du code de procédure pénale étaient celles prévues aux articles 60-1 et 60-2, dans le cadre de l'enquête de flagrance, 77-1-1 et 77-1-2 dans celui de l'enquête

---

[13] Crim., 12 janvier 2021, pourvoi n° 20-84.045, J-Y. Maréchal, Lexis360, 11 février 2021

[14] Sur cette question : Eloi Clément, AJ Pénal 2021, p. 214 – J-Y. Maréchal, Lexis360, 11 février 2021

préliminaire et 99-3 et 99-4 dans celui de l'instruction, qui pouvaient être délivrées, selon le cas, par le procureur de la République ou le juge d'instruction, mais également par les officiers de police judiciaire voire, depuis la loi n° 2019-222 du 23 mars 2019, par les agents de police judiciaire soit sur autorisation, soit sur délégation soit encore sous le contrôle des magistrats.

Sur ce point, la chambre criminelle a jugé que contrairement à ce qu'avait jugé la cour d'appel la réquisition pouvait être délivrée par un fonctionnaire de police, la réquisition délivrée par un officier de police judiciaire agissant en vertu des articles 60-1, 77-1-1 et 99-3 du code de procédure pénale sous le contrôle de l'autorité judiciaire, entrant dans les prévisions de l'article 434-15-2 du code pénal.

Elle a également jugé qu'une simple demande formulée au cours d'une audition, sans avertissement que le refus d'y déférer était susceptible de constituer une infraction pénale, ne constituait pas une réquisition au sens du texte précité.

Cette précision a conduit la DACG à adresser aux parquets une dépêche précisant qu'il est nécessaire que :

- une demande de remise du code soit formulée en procédure dans le cadre de l'enquête, par le procureur de la République, l'officier de police judiciaire ou, sous le contrôle de ce dernier, par l'agent de police judiciaire ;

- dans le cadre de l'instruction préparatoire, par le juge d'instruction ou l'officier de police judiciaire ;

- il soit rappelé à la personne que le refus de répondre à la réquisition est constitutif d'une infraction pénale.

C. - Connaissance de la convention secrète de déchiffrement

Le délit n'est constitué que si la personne qui refuse de remettre la conventions secrète de déchiffrement en a connaissance. La plupart du temps, s'agissant d'un téléphone trouvé en possession d'une personne suspectée de se livrer au trafic de stupéfiants, la question ne se pose pas. Comme indiqué plus haut, la plupart des suspects ne soutiennent pas qu'ils ignorent le code de déverrouillage Ils refusent de le communiquer en avançant d'autres raisons plus ou moins convaincantes.

M. [O], pour sa part, a purement et simplement refusé de communiquer aux enquêteurs le code de déverrouillage des deux téléphones en arguant de la protection de sa vie privée[15], le téléphone (sans que l'arrêt précise lequel des deux) contenant des photographies à caractère intime qu'il ne souhaitait pas divulguer [16].

II. - Les éléments constitutifs sur lesquels votre Assemblée devra se prononcer

A. Moyen de cryptologie

L'article 29 de la loi du 21 juin 2004 définit le moyen de cryptologie comme un matériel ou un 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. Ces 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.

Le commentaire de la décision du Conseil constitutionnel du 30 mars 2018 précitée relevait que : « La cryptologie, « science du secret », peut être définie comme le procédé consistant à transformer, notamment à l'aide d'un algorithme, des données en vue de les rendre inintelligibles aux yeux des tiers » et qu'elle a « pour fonction de garantir la confidentialité des échanges (le chiffrement), d'authentifier de manière certaine l'auteur du message et, enfin, d'assurer l'intégrité de ce dernier, c'est-à-dire de garantir que son contenu n'a pas été modifié (hachage) ».

Dans son pourvoi dans l'intérêt de la loi, le procureur général reprenant les développements techniques de la DACG, a relevé qu'il doit :

---

[15] Jugement page 4

[16] Arrêt page 4

« ... être considéré que le code de verrouillage d'un téléphone constitue une convention secrète de déchiffrement dès lors qu'il est utilisé dans le mécanisme de chiffrement.
Le verrouillage est un dispositif qui interdit l'accès à l'utilisation de l'appareil. Ce système de sécurité est configuré par l'utilisateur. Il s'agit en général d'un verrouillage par code (4 ou 6 chiffres), dessin (pattern) ou biométrie (empreinte digitale ou reconnaissance faciale). Cette technique, à elle seule, ne permet pas de chiffrer le contenu de la mémoire de l'appareil. Dans ce cas, les données restent intelligibles pour un expert qui accéderait directement à la mémoire de l'appareil sans passer par l'interface.
Le chiffrement permet de transformer les données contenues dans l'appareil grâce à un algorithme défini de manière à les rendre inintelligibles. Ce système peut être mis en place volontairement par l'utilisateur, mais il peut également être installé de manière systématique par le fabriquant au moment de la production de l'appareil, et reste transparent pour l'utilisateur.
Les sociétés Apple et Google, dont les systèmes d'exploitation respectifs iOS et Android équipent 96% des smartphones dans le monde, ont renforcé leur offre de produits inviolables, dont seul l'utilisateur détient la clef.
Dans le cas d'un smartphone fonctionnant sous iOS (Apple iPhone)[17], tous les fichiers sont chiffrés (algorithme Advanced Encryption Standard - AES) par une clé de chiffrement[18] aléatoire de 256 bits dénommée clé DEK (Disk Encryption Key). Cette clé est stockée dans les métadonnées du fichier. Les métadonnées sont chiffrées par une clé iOS créée à l'installation du système initiale d'iOS et à chaque effacement total du téléphone par l'utilisateur.

La clé de classe KEK est elle-même chiffrée par une clé unique matérielle ainsi que par une clé créée à partir du code verrou dénommée clé de code (pour la classe Complète Protection). Ainsi, pour tous les fichiers appartenant à cette classe, le code verrou est indispensable au chiffrement et au déchiffrement.
Dans le cas d'un smartphone fonctionnant sous Android, il est possible de chiffrer l'intégralité d'une mémoire de stockage (par exemple la mémoire du téléphone ou la carte additionnelle). Cette fonction est nommée Full Disk Encryption et existe depuis la version 5.0 d'Android. Le système utilise une clé de chiffrement de 128 bits (clé DEK). Celle-ci est elle-même chiffrée par une autre clé (clé KEK). La clé KEK est créée à partir du code verrou de l'utilisateur. Plus précisément, la clé KEK est créée par une fonction de dérivation de clé (Key Derivation Function - KDF) nommée scrypt qui utilise, en entrée, le code verrou de l'utilisateur.
Depuis la version 7[19] d'Android, il est possible de chiffrer individuellement les fichiers (fonction FBE pour File Based Encryption). Dans le mode FBE, un fichier est chiffré

[17] Document de référence :
https://www.apple.com/business/docs/site/iOS_Seturity_Guide.pdf

[18] Il s'agit d'un grand nombre utilisé pour chiffrer (ou crypter) des données. Cette clé est utilisée par un algorithme de chiffrement qui combine la clé avec les données pour produire des données cryptées. L'opération est réversible : c'est le déchiffrement. L'algorithme de chiffrement le plus utilisé est l'algorithme AES (utilisé par iOS et Android). Les clés de chiffrement utilisés par AES sont des clés d'une longueur de 128 bits, 256 bits ou 512 bits
[19] Ronan Lotus, Marwin Bauman, « Android 7 File Based Encryption and the Attacks against it » University of Amsterdam, janvier 2017, https:/ » delaat.net/rp/2016-2017/p45/report.pdf

par AES avec une clé (clé DEK) de 512 bits. La clé DEK est ensuite cryptée par une autre clé de 256 bits (clé KEK). La clé KEK est stockée dans une zone sécurisée du téléphone, isolée et indépendante du système Android (zone TEE).
Pour obtenir cette clé KEK dans le but de déchiffrer le fichier, il faut trois éléments cumulatifs :
• un code d'authentification créé lors de la connexion de l'utilisateur,
• une somme de contrôle (hash) calculée à partir d'un fichier stocké dans l'espace de l'utilisateur,
• un code nommé Stretched Credential calculé par une fonction de dérivation de clé qui utilise en entrée le code verrou de l'utilisateur.
Ce dernier élément signifie que sans code verrou de l'utilisateur, la clé KEK ne pourra être récupérée et aucune opération de déchiffrement ne peut être réalisée.

Le conseiller rapporteur de l'arrêt rendu sur pourvoi d'ordre du Garde des sceaux a exposé, dans son rapport, que la société Apple, dans le guide de sécurité qu'elle éditait, faisait valoir que le système d'exploitation iOS protégeait non seulement l'appareil et ses données mais également l'ensemble de l'écosystème, notamment tout ce que les utilisateurs font localement, sur les réseaux et avec des services Internet clés. (...) En outre, les fonctionnalités de sécurité clés comme le chiffrement de l'appareil ne sont pas configurables et ne peuvent donc pas être désactivées par mégarde par l'utilisateur. (...) (Apple, IOS, guide de sécurité, p.5)

La chaîne de démarrage sécurisée, la signature du code et la sécurité des processus exécutés permettent de garantir que seuls le code et les apps fiables peuvent s'exécuter sur un appareil. iOS offre des fonctionnalités de chiffrement et de protection des données supplémentaires pour protéger les données utilisateur, même lorsque d'autres parties de l'infrastructure de sécurité ont été compromises (sur un appareil comportant des modifications non autorisées, par exemple). (...) En plus des fonctionnalités de chiffrement matériel intégrées aux appareils iOS, Apple utilise une technologie appelée Data Protection pour accroître la protection des données stockées dans la mémoire Flash de l'appareil. La protection des données permet à l'appareil de répondre à des événements courants comme les appels téléphoniques entrants, tout en assurant un niveau de chiffrement élevé des données utilisateur. Les apps clés du système, comme Messages, Mail, Calendrier, Contacts, Photos et les données Santé, utilisent par défaut la protection des données, et les apps tierces installées sur iOS 7 ou ultérieur bénéficient automatiquement de cette protection » (Apple, IOS, guide de sécurité, p.18- 19) ».

Il a encore relevé que certains téléphones étaient commercialisés précisément en raison de leur chiffrement, tel que le Hoom x2 (Atos) ou le Teorem (Thalès), que l'ANSSI décrivait comme : "conçu pour un usage au quotidien comme en situation de crise, le téléphone chiffrant Teorem est utilisable comme un téléphone de bureau ou comme un téléphone mobile. Les communications sont chiffrées par défaut et permettent des échanges d'informations classifiées jusqu'au niveau Secret Défense".

Il a rappelé que des applications de messageries cryptées, tel que Télégram, pouvaient être installées par l'utilisateur d'un téléphone, leur accès étant conditionné à son déverrouillage.

M. Buisson, dans un article analysant la problématique des téléphones portables, a signalé que les IPhone de chez Apple, depuis le modèle 4S, étaient tous équipés d'un dispositif de chiffrement des données qui ne peut être désactivé par l'utilisateur[20].

Dans le cadre de l'instruction du pourvoi qui vous est soumis, j'ai sollicité le concours de la division technique du Commandement de la Gendarmerie dans le Cyberespace qui a établi un rapport dont il résulte bien que l'immense majorité des téléphones portables actuellement en circulation implémentent de série et par conception un mécanisme de chiffrement des données, activé soit par défaut, soit par paramétrage de l'utilisateur[21]. S'agissant des IPhone, c'est depuis le modèle 4 que le chiffrement est implémenté par défaut[22]. Ce chiffrement ne peut être désactivé par l'utilisateur qui ne peut désactiver que le code de déverrouillage, les données restant néanmoins chiffrées[23].

Il résulte des développements qui précèdent que si certains smartphones sont équipés de moyen de cryptologie, ce n'est pas le cas de tous. Comment dans ces conditions, les enquêteurs peuvent-ils déterminer si le téléphone saisi est équipé d'un tel moyen ?

La chambre criminelle a tout d'abord jugé que l'existence d'un moyen de cryptologie équipant un téléphone portable pouvait se déduire des caractéristiques de l'appareil ou des logiciels qui l'équipaient. C'est effectivement ce qui résulte des indications qui viennent d'être données. Le téléphone peut être équipé d'origine d'un moyen de cryptologie mais un tel moyen peut également être ajouté au téléphone par voie logicielle.

La chambre criminelle a ajouté que la présence d'un moyen de cryptologie pouvait aussi être déterminée par les résultats d'exploitation des téléphones au moyen d'outils techniques. Et elle a apporté une précision d'importance pour les juges du fond en ajoutant que les outils techniques en question étaient ceux utilisés notamment par les personnes qualifiées requises ou experts désignés à cette fin, portés, le cas échéant, à la connaissance de la personne concernée. Dès lors soit le téléphone saisi est d'une marque et d'un modèle dont les documents techniques accessibles à tous permettent de savoir avec certitude qu'il est équipé d'un moyen de cryptologie (c'est le cas pour les IPhone à partir du modèle 4) ou il y a lieu de recourir à une personne qualifiée ou à un expert selon le cadre juridique de la saisie et les investigations techniques effectuées par ce spécialiste permettront de déterminer si le téléphone est équipé d'un moyen de cryptologie.

[20] Procédures, n° 1, janvier 2021
[21] Rapport p. 17
[22] Rapport p. 18
[23] Rapport p. 19

A cet égard, il peut être signalé que plusieurs sociétés fabriquent et commercialisent des dispositifs qui permettent une exploitation des téléphones portables saisis au cours des enquêtes judiciaires.

Certains, comme la société Cellebrite, affirment même pouvoir « *Contourner tout type de verrouillage par modèle, mot de passe ou code PIN et surmonter rapidement les défis de chiffrement sur les appareils Android et iOS les plus courants* »[24].

La solution retenue par la chambre criminelle est parfaitement exacte au plan technique. Elle est en outre d'une grande clarté et nous ne pouvons que vous inviter à la faire votre.

A. - Convention secrète de déchiffrement

L'article L871-1 du CSI dispose que « Les personnes physiques ou morales qui fournissent des prestations de cryptologie visant à assurer une fonction de confidentialité sont tenues de remettre dans un délai de soixante-douze heures aux agents autorisés dans les conditions prévues à l'article L. 821-4, sur leur demande, les conventions permettant le déchiffrement des données transformées au moyen des prestations qu'elles ont fournies. Les agents autorisés peuvent demander aux fournisseurs de prestations susmentionnés de mettre eux-mêmes en œuvre dans un délai de soixante-douze heures ces conventions, sauf si ceux-ci démontrent qu'ils ne sont pas en mesure de satisfaire à ces réquisitions» tandis que l'article R871-3 du même code prévoit que « Les conventions mentionnées à l'article L. 871-1 s'entendent des clés cryptographiques ainsi que de tout moyen logiciel ou de toute autre information permettant la mise au clair de ces données ».

La chambre criminelle en a déduit qu'une convention de déchiffrement s'entend de tout moyen logiciel ou de toute autre information permettant la mise au clair d'une donnée transformée par un moyen de cryptologie.

Il en résulte que le code de déverrouillage d'un téléphone mobile peut constituer une clé de déchiffrement, si ce téléphone est équipé d'un moyen de cryptologie.

Des auteurs considèrent que le code de déverrouillage d'un téléphone portable ne peut être considéré comme une convention secrète de déchiffrement.

Ainsi M. Caprioli écrivait en 2018 : *« selon nous, le code de déverrouillage du portable n'entre pas dans cette définition étant donné qu'il est uniquement question de « convention secrète de déchiffrement d'un moyen de cryptologie ». En effet, ce dernier permet simplement de déverrouiller le téléphone afin d'accéder à son contenu, les messages potentiellement litigieux n'ayant pas fait l'objet d'un chiffrement. Ainsi, l'utilisation d'un code secret permet uniquement de créer une protection de l'accès aux données et non de procéder à leur chiffrement. Il existe une véritable différence technique fondamentale entre ces deux notions puisque la*

[24] https://cellebrite.com/fr/cellebrite-ufed-fr/

vocation première de l'article 434-15-2 du Code pénal était de viser les informations chiffrées et non leur accessibilité »[25].

Il persistait après que la chambre criminelle eut statué le 13 octobre 2020 en écrivant : *« Comment estimer qu'un code de déverrouillage de téléphone portable constitue une convention secrète de déchiffrement s'il ne remplit aucun des critères de celle-ci ? Ce code permet de bloquer l'accès aux données du téléphone, soit ; mais il ne les modifie en aucune façon et il garantit encore moins une confidentialité et une sécurité générales. Ainsi, le problème de cette solution est que le postulat initial des juges est erroné. D'un point de vue juridique, le code du téléphone portable ne peut et ne doit pas être confondu avec une convention secrète de déchiffrement qui présente des caractéristiques bien plus complexes »*.

Une telle appréciation ne fait aucune référence aux écrits d'Apple qui précise dans le guide de fonctionnement de l'IPhone que « En configurant un code de verrouillage d'appareil, l'utilisateur active automatiquement la protection des données. iOS prend en charge les codes à six chiffres, à quatre chiffres et alphanumériques de longueur arbitraire. En plus de déverrouiller l'appareil, un code de verrouillage fournit l'entropie pour certaines clés de chiffrement. Cela signifie qu'une personne malintentionnée en possession d'un appareil ne peut pas accéder aux données appartenant a des classes de protection spécifiques sans le code de verrouillage ».

M. Combles de Nayves a une position plus nuancée. Il écrit en effet :

« L'assertion selon laquelle l'usage du code ne permet pas de déchiffrer les données stockées dans le téléphone mais uniquement d'y accéder mérite d'être questionnée. La plupart des smartphones sont en effet cryptés ou offrent au moins la possibilité de l'être et, dans ce cas, l'usage du code de déverrouillage permet à l'utilisateur de décrypter ses données et de pouvoir les lire. Sans l'usage du code ou d'un autre moyen d'identification, il est impossible de le faire.

En revanche, un code de déverrouillage ne semble pas constituer une « convention » de déchiffrement. Il s'agit d'un mécanisme d'authentification, comme peut l'être l'usage de l'empreinte digitale. La convention de déchiffrement n'est en principe détenue que par le concepteur du logiciel du téléphone. Toutefois, s'agissant d'Apple, la société a déjà précisé qu'elle ne peut pas extraire des données d'un téléphone crypté car elle ne possède pas la clé de déchiffrement.
Dans le chapitre intitulé « De la mise au clair des données chiffrées nécessaires à la manifestation de la vérité » du titre IV du code de procédure pénale, le législateur a prévu, aux articles 230-1 à 230-5, les moyens techniques et procéduraux permettant le déchiffrement de données cryptées. L'article 230-1 du code de procédure pénale prévoit ainsi que dans le cas où les données sont protégées par un mécanisme

[25] Infraction pénale en mati re de cryptologie - L'obligation légale de remettre la clé de déchiffrement est conforme la Constitution - Commentaire par Éric A. Caprioli, Communication Commerce électronique n° 9, Septembre 2018, comm. 69

d'authentification, les opérations techniques peuvent permettre la mise au clair des données et, si besoin, de la convention secrète de déchiffrement utilisée. Il existe donc bien une différence technique, entérinée par la loi, entre un moyen d'authentification et une convention secrète de déchiffrement ».

Cette analyse est en opposition directe avec la décision prise par la chambre criminelle sur le pourvoi dans l'intérêt de la loi, d'ordre du garde des sceaux puisque dans cet arrêt il a été jugé que « la convention secrète de déchiffrement d'un moyen de cryptologie contribue à la mise au clair des données qui ont été préalablement transformées, par tout matériel ou logiciel, dans le but de garantir la sécurité de leur stockage, et d'assurer ainsi notamment leur confidentialité. Le code de déverrouillage d'un téléphone portable peut constituer une telle convention lorsque ledit téléphone est équipé d'un moyen de cryptologie » ce qui signifie que la convention de déchiffrement est indissolublement liée au moyen de cryptologie, le déverrouillage du téléphone décryptant les données précédemment transformées pour garantir leur confidentialité[26].

Un commentateur ne s'est pas trompé sur l'analyse de la chambre criminelle puisqu'il a relevé que *« la jurisprudence étend ainsi le champ de l'article 434-15-2 du Code pénal à la plupart des smartphones dont le système d'exploitation est récent, du moins si leur utilisateur a choisi d'avoir un code de déverrouillage qui active la protection des données. Cela peut viser aussi un code informatique. En revanche un téléphone ancien, dont le code PIN permettrait simplement de débloquer l'écran, ne devrait pas tomber sous le coup de cette incrimination. Il faut donc apprécier chaque situation avant d'entrer en condamnation* »[27].

M. Azoulay écrit, pour sa part, dans deux articles différents que :

« De façon pratique, et à titre d'illustration, le guide de sécurité d'iOS nous renseigne de ce qu'un iPhone recourt à un chiffrement de type hybride. À chaque nouveau fichier, une nouvelle clé de chiffrement est créée afin de garantir la protection des données. Celle-ci est alors transmise au moteur AES matériel du terminal, lequel l'utilise pour chiffrer le fichier lors de son écriture dans la mémoire dite « flash » [4]. Le système de fichier étant entouré d'une clé effaçable dont le rôle est de détruire rapidement les données à la demande, entre autres, de l'utilisateur, il s'agira pour les enquêteurs d'éviter cette perte d'informations pour la suite de leurs investigations. La seconde était définie en 1998 comme étant « des clés non publiées nécessaires à la mise en œuvre d'un moyen ou d'une prestation de cryptologie » (Décret n° 98-102 du 24 février 1998 N° Lexbase : O2123BIH). Selon la précédente illustration, la création d'un code sur le terminal par l'utilisateur a pour inévitable effet d'activer la protection de ses données. S'il est exact qu'une multiplication des combinaisons pourrait être entreprise par les enquêteurs afin d'accéder au contenu du terminal, le système prévoit en revanche que « des délais de plus en plus longs sont prévues après la saisi d'un code non valide sur l'écran de verrouillage » [5], étant précisé que ce délai est imposé de façon matérielle, et non logicielle, par un coprocesseur, toute tentative de contournement demeurant infructueuse [6]. Pis, si l'option «effacer les

[26] Solution confirmée par Crim., 3 mars 2021, n° 19-86-757

[27] C. Ribeyre « application du délit au cas du détenteur d'un téléphone portable », Dt pénal, n° 1, Janvier 2021, comm. 8

données» est activée, l'appareil détruira automatiquement les fichiers après dix tentatives consécutives de saisies inexactes, les enquêteurs perdant une nouvelle fois la possibilité d'accéder à d'éventuelles informations »[28]

Et que

« Le système Android, qui équipe près de neuf smartphones sur dix, utilise un algorithme de chiffrement nécessitant la création d'une clé de déchiffrement pour déverrouiller les données existantes. En septembre 2008, date de sortie de la première version, l'utilisateur devait lui-même opérer la démarche de chiffrer ses données et d'en générer la clé par le biais des paramètres de sécurité de son téléphone. Depuis octobre 2015, date de mise à disposition d'une sixième version plus connue sous l'appellation de « Marshmallow », le contenu d'un smartphone est automatiquement chiffré dès lors que son écran est verrouillé. Il en est exactement de même pour iOS, second système du marché développé par Apple, à ceci près que depuis septembre 2015, date de remplacement de la version 8, la firme de Cupertino n'est plus en mesure de communiquer la moindre donnée que contiendrait un terminal eu égard au fait que « les données généralement recherchées par les forces de l'ordre sont cryptées, et Apple ne possède pas la clé de décryptage », rendant toute extraction de leur part impossible. Obtenir le code du téléphone serait alors la solution la plus rapide pour en déchiffrer les données, étant précisé que sa non-communication peut, dans certaines occurrences, constituer un délit pénal ».

Mme Vergnolle souligne, quant à elle, que l'emploi du verbe « contribuer » dans l'attendu définissant la convention de déchiffrement pourrait laisser penser que la convention secrète de déchiffrement ne serait qu'un moyen, parmi d'autres, concourant au déchiffrement des données alors que cette convention permet en réalité à elle seule d'accéder aux données préalablement chiffrées[29]

Le rapport de la division technique du Commandement de la gendarmerie dans le Cyberespace conclut que le code de déverrouillage de l'écran d'un IPhone (à partir du modèle 4) est bien une convention secrète de déchiffrement d'un moyen de cryptologie, portant sur le déchiffrement des données stockées et que les fonctions de déverrouillage par empreinte digitale et par reconnaissance faciale sont également des conventions, secrètes ou non, de déchiffrement[30].

Comme on vient de le voir, les auteurs qui estiment que le code de déverrouillage d'un smartphone ne constitue pas une convention secrète de déchiffrement ne s'appuient sur aucun élément technique documenté alors qu'au contraire, ceux qui affirment, comme la chambre criminelle, que le code déverrouillage de l'écran d'un

[28] W. Azoulay, Vers un encadrement constitutionnel du chiffrement à l'ère cryptolithique, Lexbase, 23 mai 2018

[29] W. Azoulay, ATER - Laboratoire de Droit Privé et de Sciences Criminelles à l'Université d'Aix-Marseille, Présomption d'usage d'un téléphone : l'obligation d'en fournir le code est conventionnelle, Lexbase, 23 janvier 2020

[30] Rapport p. 21

smartphone décrypte les données précédemment rendues inintelligibles par le verrouillage s'appuient sur des constats techniques précis et spécialement sur les spécifications des constructeurs desdits smartphones.

La position de la chambre criminelle mérite donc d'être confirmée.

III. - L'application des principes ci-dessus exposés au cas particulier de M. [O]

Au cas particulier qui nous occupe, la cour d'appel énonce que « la mise en œuvre d'un moyen de cryptologie suppose la transformation, à l'occasion de la communication entre plusieurs personnes, de données claires pour les rendre incompréhensibles, ou de données codées pour les rendre claires. Dès lors, 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 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 ».

On relèvera tout d'abord que la cour d'appel limite le champ de la cryptologie aux communications (elle ajoute : « à l'occasion de l'émission d'un message ») et semble en exclure les données alors que la cryptologie a, selon l'article 29 de la loi du 21 juin 20004 pour la confiance dans l'économie numérique, pour objet de garantir non seulement la sécurité de la transmission de données mais encore celle du stockage, lequel est seul en cause lorsque des enquêteurs demandent à un suspect le code de déverrouillage de son téléphone portable pour avoir accès au contenu de celui-ci.

Au-delà de cette inadéquation du motif à la situation concernée voire à une lecture partielle de l'article 29 de la loi du 21 juin 2004, il ne peut qu'être relevé qu'en énonçant de manière générale que la clé de déverrouillage de l'écran d'accueil d'un téléphone mobile n'est pas une convention secrète de chiffrement[31], sans procéder à aucune vérification technique s'agissant des appareils saisis, la cour d'appel n'a pas justifié sa décision puisque l'on a vu que tout dépendait des logiciels équipant le téléphone concerné. Il suffisait d'ailleurs de se référer aux manuels d'utilisation pour acquérir la certitude qu'ils étaient équipés d'un moyen de cryptographie activé par le verrouillage automatique de l'écran et déverrouillé par l'entrée du code de déverrouillage ou, pour l'IPhone X, l'utilisation de la reconnaissance faciale dont ce modèle est doté[32].

---

[31] Il doit falloir plutôt lire « déchiffrement » car personne n'a jamais soutenu que déverrouiller un téléphone pouvait chiffrer les données : la question est de savoir si le déverrouillage déchiffre les données.

[32] Mme Vergnolle, dans son étude précitée considère que l'infraction s'applique aussi au déverrouillage biométrique, ce que confirme l'étude de la Gendarmerie.

Même si, nous pensons, avec M. Buisson[33] que « *ce délit, prévu pour exercer sur le requis une contrainte psychologique destinée à obtenir la prestation demandée, n'est pas, particulièrement dans le domaine du trafic de stupéfiants, de nature à satisfaire la ratio legis : le suspect préférera une poursuite supplémentaire de ce chef à la révélation d'un code qui va permettre aux enquêteurs d'établir l'ampleur de son trafic... La vraie solution réside dans l'emploi de la contrainte, compatible avec le droit de ne pas s'incriminer soi-même, pour obtenir la révélation des informations cryptées, telle que peut la permettre une opération de décryptage (CPP, art. 230-1 et s.).* » nous vous invitons à censurer l'arrêt attaqué car le refus d'un suspect de communiquer le code de déverrouillage d'un téléphone portable aux enquêteurs tombe légalement sous le coup des dispositions de l'article 434-15-4 du code pénal.

D. PROPOSITION

Avis de cassation

[33] Procédures n° 12, Décembre 2020, comm. 229 Recueil d'indices : téléphone portable et convention de déchiffrement d'un moyen de cryptologie Commentaire par Jacques BUISSON