COUR DE CASSATION

RAPPORT DE M. BARINCOU, CONSEILLER

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]

Plan

* *assisté de Dimitri Dureux et Sylvie Postel (SDER).*

1. Rappel des faits et de la procédure

Le 12 mai 2018, M. [O] a été interpellé et placé en garde à vue pour infractions à la législation sur les stupéfiants. Il a refusé de communiquer aux enquêteurs les mots de passe permettant de déverrouiller deux téléphones portables, iPhone 4s et iPhone 10, découverts dans son véhicule.

Il a été poursuivi devant le tribunal correctionnel de Lille, pour détention et offre ou cession de cannabis ainsi que pour refus de remettre la convention secrète de déchiffrement d'un moyen de cryptologie, en refusant de fournir le code de déverrouillage d'un téléphone susceptible d'avoir été utilisé dans le cadre d'un trafic de stupéfiants.

Par jugement du 15 mai 2018, le tribunal correctionnel de Lille l'a condamné à des peines d'emprisonnement et d'amende pour infractions à la législation sur les stupéfiants et l'a relaxé du délit de refus de remettre ou de mettre en oeuvre la convention secrète d'un moyen de cryptologie.

Par arrêt du 11 juillet 2019, la cour d'appel de Douai, statuant dans les limites de l'appel formé par le procureur de la République portant uniquement sur cette relaxe, a confirmé le jugement déféré.

Par arrêt du 13 octobre 2020 (Crim., 13 octobre 2020, pourvoi n° 19-85.984), sur un pourvoi formé par le procureur général, la chambre criminelle a cassé cette décision en toutes ses dispositions.

> *Exposé du moyen*
> *6. Le moyen est pris de la violation de l'article 593 du code de procédure pénale.*
> *7. Il critique l'arrêt attaqué en ce qu'il a relaxé le prévenu du chef de refus de remettre aux autorités judiciaires la convention secrète de déchiffrement d'un moyen de cryptologie, alors :*
> *« 1°/ qu'il ressort des dispositions de l'article 29 de la loi 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 toute autre information permettant la mise au clair de ces données » ;*
> *2°/ qu'en affirmant ainsi qu'un code de déverrouillage d'un téléphone ne peut être qualifié de « convention secrète de déchiffrement », sans effectuer l'analyse des caractéristiques techniques du téléphone concerné, pourtant indispensable à fonder sa décision, la cour d'appel n'a pas justifié celle-ci. »*
> *Réponse de la Cour*
> *Vu les articles 434-15-2 du code pénal, 29 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, L. 871-1 et R. 871-3 du code de la sécurité intérieure :*
> *8. Selon le premier de ces textes, toute personne 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, est tenue de remettre cette convention aux autorités judiciaires, ou de la mettre en oeuvre, sur les réquisitions de ces autorités, délivrées en application des titres II et III du Livre Ier du code de procédure pénale.*
> *9. Selon le deuxième, un moyen de cryptologie est 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.*

10. Selon les textes précités du code de la sécurité intérieure, 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.
11. Pour confirmer la relaxe, la cour d'appel énonce qu'un téléphone portable ne peut être considéré comme un moyen de cryptologie au sens des textes précités, et que le code permettant de déverrouiller l'écran d'accueil d'un téléphone, qu'il s'agisse d'un code chiffré ou d'un ensemble de points à relier dans un sens prédéfini par l'utilisateur, ne peut être qualifié, au sens des mêmes dispositions, de convention secrète de déchiffrement. L'arrêt retient qu'un tel code de déverrouillage de l'écran ne sert pas à décrypter les données contenues dans le téléphone, mais seulement à débloquer l'usage de l'écran, pour accéder aux données contenues dans le téléphone
12. En prononçant ainsi, par un motif général et erroné, alors que le code de déverrouillage d'un téléphone portable constitue une convention de déchiffrement s'il permet de mettre au clair les données qu'il contient, la cour d'appel n'a pas justifié sa décision.
13. Il en résulte que la cassation est encourue de ce chef.
Crim., 13 octobre 2020, pourvoi n° 19-85.984

Par arrêt du 20 avril 2021, statuant sur renvoi après cassation, la cour d'appel de Douai, autrement composée, a confirmé le jugement en ce qu'il a renvoyé le prévenu des fins de la poursuite du chef de refus de remettre aux autorités judiciaires ou de mettre en oeuvre la convention secrète de déchiffrement d'un moyen de cryptologie.

Après avoir relevé qu'il avait été enjoint au prévenu, sur instruction du procureur de la République, de révéler aux enquêteurs le code de déverrouillage de ses téléphones et qu'il avait été informé des conséquences d'un refus de communication de ce code, la cour d'appel a retenu que la clé de déverrouillage d'un smartphone n'est pas une convention secrète de chiffrement pour le motif suivant :

Toutefois, la mise en oeuvre 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.

C'est l'arrêt attaqué, contre lequel le procureur général près la cour d'appel de Douai s'est pourvu en cassation, par une déclaration régulièrement faite au greffe de la cour d'appel, le 23 avril 2021.

Par arrêt du 2 février 2022, la chambre criminelle a renvoyé l'affaire devant l'assemblée plénière de la Cour de cassation**.**

2. Analyse succincte du moyen

Le moyen est pris de la violation de l'article 593 du code de procédure pénale.

Le procureur général près la cour d'appel de Douai fait grief à l'arrêt de relaxer le prévenu du chef de refus de remettre aux autorités judiciaires la convention secrète de déchiffrement d'un moyen de cryptologie, faits prévus et réprimés par les articles 434-15-2 et 434-44 du code

pénal, alors « 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 R. 871-3 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 I-phone 4,[1] pourtant indispensable pour fonder sa décision, la cour d'appel a insuffisamment motivé sa décision ».

3. Identification du ou des points de droit faisant difficulté à juger

L'assemblée plénière devra déterminer si le code permettant de déverrouiller l'écran d'accueil d'un téléphone est ou non une convention secrète de déchiffrement d'un moyen de cryptologie, au sens de l'article 434-15-2 du code pénal.

4. Discussion citant les références de jurisprudence et de doctrine

4.1 Textes

L'article 434-15-2 du code pénal figure dans la section intitulée « Des entraves à l'exercice de la justice » et dispose :

> *Est puni de trois ans d'emprisonnement et de 270 000 € d'amende 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 oeuvre, 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 oeuvre 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.*

Cette disposition a été introduite dans le code pénal par l'article 31 de la loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne.

L'adoption de la loi du 15 novembre 2001

L'article 434-15-2 résulte de l'adoption d'un amendement gouvernemental, présenté après l'échec d'une commission paritaire, au cours d'une discussion parlementaire marquée par les attentats commis aux Etats-Unis, le 11 septembre précédent. Il fait partie d'une série de mesures destinées à renforcer l'efficacité de la lutte contre le terrorisme qui ont été insérées, en urgence, dans un texte relatif à la sécurité quotidienne de sorte que les travaux parlementaires ne sont que de peu d'utilité pour en comprendre la portée, comme l'explique le rapporteur de la commission des lois au Sénat :

[1] Si le pourvoi ne vise qu'un seul téléphone, I-phone 4s, le mémoire présenté par le procureur général à l'appui de celui-ci envisage aussi le second téléphone, I-phone 10, saisi en même temps que le premier.

La discussion au Sénat intervient dans un contexte profondément différent de ce qu'il était lors des étapes précédentes de la procédure législative. Le 11 septembre dernier, les Etats-Unis d'Amérique ont en effet été victimes d'attentats terroristes particulièrement effroyables. Tout indique que notre pays pourrait également être frappé. La France a fait part de sa solidarité au peuple américain et a clairement manifesté sa volonté de s'engager aux côtés des Etats-Unis dans la lutte contre le terrorisme.

Ces dramatiques événements ont mis en lumière que certains instruments manquaient dans l'arsenal législatif français pour combattre avec une pleine efficacité le terrorisme.

Le Gouvernement a fait part de son intention de soumettre au Parlement plusieurs propositions destinées à renforcer l'efficacité du dispositif de lutte contre le terrorisme et a choisi, soucieux de voir ces mesures rapidement adoptées, de proposer des amendements au présent projet de loi.

Ces amendements tendent notamment à permettre, sur réquisitions du procureur de la République, la fouille des véhicules, à autoriser certaines perquisitions au cours d'enquêtes préliminaires, à permettre aux agents des entreprises privées de sécurité de procéder dans certaines circonstances à des fouilles de bagages ainsi qu'à des palpations de sécurité. Le Gouvernement souhaite également insérer dans le projet de loi des dispositions relatives à la conservation des données par les opérateurs de télécommunications et prévoir la possibilité pour les juridictions de faire appel à des services dont l'activité est couverte par le secret de la défense nationale pour décrypter des données recueillies au cours d'enquêtes ou d'informations judiciaires et ayant subi des transformations en vue de les rendre indéchiffrables. Le Gouvernement propose enfin de prévoir, dans le code de procédure pénale, la possibilité de procéder à des auditions, interrogatoires et confrontations à distance, par l'intermédiaire d'équipements de télécommunications adaptés. (...)

Compte tenu de la nécessité pour la France de compléter dans l'urgence son dispositif de lutte contre le terrorisme, votre commission accueille favorablement les propositions présentées par le Gouvernement malgré leur caractère tardif dans la procédure législative en cours. Elle considère en effet que la gravité de la situation actuelle justifie le recours à des procédés exceptionnels. »[2]

Le rapporteur de la commission des lois de l'Assemblée nationale reprend ces explications s'agissant plus particulièrement de l'article 434-15-2 du code pénal :

Selon certaines informations d'ores et déjà révélées par les enquêteurs, les responsables des attentats terroristes commis le 11 septembre dernier auraient eu recours à des techniques destinées à rendre illisibles certains de leurs messages électroniques. Il semble donc nécessaire et impérieux d'offrir les moyens, tant aux magistrats dirigeant les enquêtes, qu'il s'agisse du procureur de la République ou du juge d'instruction, qu'à la juridiction de jugement saisie, d'accéder en clair au contenu des ces messages.

En conséquence, les autorités précitées sont autorisées, lorsqu'elles sont confrontées à un message crypté, à recourir à « toute personne physique ou morale qualifiée » en vue d'effectuer les opérations techniques permettant d'obtenir sa version en clair. (...)

Le onzième amendement prévoit que les personnes physiques ou morales fournissant des prestations de cryptologie devront remettre aux agents habilités en charge d'une mission d'interception des correspondances échangées par la voie des télécommunications, les conventions permettant de lire en clair les messages. (...) Par ailleurs, le dispositif proposé par cet amendement insère dans le code pénal un nouvel article 434-15-2, qui punit de trois ans d'emprisonnement et 45 000 euros d'amende le fait, pour quiconque ayant connaissance de la convention secrète de déchiffrement susceptible d'avoir été utilisée pour préparer, faciliter ou commettre un crime ou un

[2] Rapport n° 7, M. Schosteck, commission des lois du Sénat, déposé le 10 octobre 2001

> *délit, de refuser de la remettre aux autorités judiciaires. Cette nouvelle incrimination était également prévue par l'article 46 du projet de loi sur la société de l'information.*[3]

Cette même loi a aussi introduit une nouvelle disposition dans la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications afin de contraindre les fournisseurs de prestations de cryptologie à remettre leurs conventions de déchiffrement aux autorités administratives mettant en oeuvre une interception administrative.

Cette disposition figure désormais à l'article L. 871-1 du code de la sécurité intérieure, issu de la loi n° 2015-912 du 24 juillet 2015, relative au renseignement, qui dispose :

> *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.*

L'article R. 871-3 du même code précise 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 ». L'article L. 881-2 du même code sanctionne le non respect de cette obligation de remise d'une clé de déchiffrement d'une peine de deux ans d'emprisonnement et de 150 000 euros d'amende.

Enfin, cette même loi du 15 novembre 2001 a inséré dans le livre premier du code de procédure pénale, relatif à l'action publique et à l'instruction, un titre IV dont le chapitre unique est intitulé : « De la mise au clair des données chiffrées nécessaires à la manifestation de la vérité ». Les articles 230-1 à 230-5 qui le composent autorisent la réquisition d'une personne qualifiée, voire même dans certains cas le recours à des moyens d'Etat couverts par le secret de la défense nationale, pour effectuer la transcription en clair d'informations cryptées découvertes au cours d'une enquête ou d'une instruction.

Ces diverses dispositions avaient été adoptées pour une durée limitée, allant jusqu'au 31 décembre 2003. Sous l'intitulé « dispositions relatives à la lutte contre le terrorisme », elles ont été pérennisées par la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure, certaines pour une nouvelle durée limitée, les autres, dont l'infraction prévue par l'article 434-15-2 du code pénal, sans limitation de temps. Les travaux parlementaires de ce nouveau texte n'apportent pas d'éléments utiles au sujet de l'incrimination intéressant le présent rapport.

Par la suite, l'article 434-15-2 du code pénal a été modifié par l'article 16 de la loi n° 2016-731 du 3 juin 2016, renforçant la lutte contre le crime organisé, le terrorisme et leur financement et améliorant l'efficacité et les garanties de la procédure pénale, mais uniquement pour aggraver les peines d'amende encourues.

Même adopté en urgence dans cette situation si particulière, l'article 434-15-2 du code pénal ne résulte pas d'un texte de circonstance rédigé à la hâte : les amendements proposés par le gouvernement, et adoptés sans modification par le parlement, avaient été extraits d'un projet de loi sur la société de l'information, déposé au parlement en juin 2001 mais devenu caduc à la fin de la onzième législature, faute d'avoir jamais été inscrit à l'ordre du jour.[4]

---

[3] Rapport n° 3352, M. Le Roux, Commission des lois de l'Assemblée nationale

[4] Projet de loi n° 3143 sur la société de l'information du 14 juin 2001

Ce projet de loi déposé en juin 2001 était lui-même le fruit d'une évolution amorcée au cours des dix années précédentes.

L'origine du texte

Les moyens de cryptologie ont longtemps été réservés aux seuls domaines militaire, diplomatique et gouvernemental comme l'illustre leur classement, par la législation française, en armes de guerre de deuxième catégorie jusqu'en 1996. Ils ne sont devenus progressivement accessibles à l'entreprise privée qu'au cours de la dernière décennie du vingtième siècle.

La loi n° 90-1170 du 29 décembre 1990 sur la réglementation des télécommunications, continuait à soumettre l'utilisation et la fourniture de moyens ou de prestations de cryptologie à des procédures d'autorisation ou de déclaration très restrictives, réservant à l'État l'utilisation des techniques de chiffrement de haut niveau.

L'inéluctable évolution en la matière s'est poursuivie parallèlement au développement des technologies de l'information et, dès 1995, le Conseil de l'Europe a incité les États membres à prendre des mesures « pour minimiser les effets négatifs du chiffrement sur les enquêtes des infractions pénales » : le Comité des ministres s'était dit préoccupé par le risque que les systèmes électroniques d'information puissent être utilisés pour commettre des infractions sans que les lois des Etats membres prévoient déjà les pouvoirs appropriés pour perquisitionner dans ces systèmes et y recueillir des preuves au cours des enquêtes pénales. Il avait alors soumis aux gouvernements diverses recommandations visant à l'adoption de règles spécifiques aux perquisitions des systèmes informatiques et aux saisies des données qu'ils renferment ou à la surveillance technique des données échangées. Il soulignait aussi la nécessité d'instaurer une obligation de coopération avec les autorités chargées de l'enquête ou d'adopter des mesures pour « minimiser les effets négatifs de l'utilisation du chiffrement sur les enquêtes des infractions pénales sans toutefois avoir des conséquences plus que strictement nécessaires sur son utilisation légale ».[5]

La loi n° 96-659 du 26 juillet 1996 réglementant les télécommunications a assoupli le régime de la cryptologie. Elle a prévu une totale liberté d'utilisation des techniques de chiffrement ayant pour seule fonction l'authentification des parties ou le contrôle de l'intégrité du message. Elle a autorisé le recours à des moyens ou prestations de cryptologie assurant aussi des fonctions de confidentialité, selon des modalités variant en fonction de la complexité de la clé de chiffrement utilisée.

Le système français ainsi mis en place, très vite décrié, subordonnait l'utilisation d'une clé supérieure à 128 bits à sa remise à un tiers de confiance, lequel pouvait être tenu de la révéler aux autorités administratives en cas de nécessité.

Le Conseil d'Etat a publié peu après un rapport dont le chapitre consacré aux enjeux de la cryptologie concluait que, à défaut de pouvoir conserver ce dispositif de « tiers de séquestre », que la France avait été la seule à mettre en place et qui était très contraignant pour les entreprises, « il faudra se borner à exiger que les moyens de cryptologie utilisés en France permettent le recouvrement des clés à l'initiative de l'émetteur ou du destinataire du message, qui sera alors tenu de les remettre lui-même à la justice ou aux services de sécurité sous peine de sanctions pénales sévères ».[6]

En 1999, afin notamment d'harmoniser les conditions d'utilisation des moyens de cryptologie avec celles des autres pays européens, les règles ont été assouplies : l'obligation de recourir

---

[5] Recommandation n° R(95)13 du Comité des Ministres aux Etats membres relative aux problèmes de procédure pénale liés à la technologie de l'information

[6] Internet et les réseaux numériques, Rapport du Conseil d'Etat, 1998

au tiers de confiance a été supprimée, les moyens de cryptologie ont été rendus libre d'utilisation, seule leur fourniture restant soumise à diverses procédures simplifiées.[7]

L'adoption de ces mesures a précédé celle de la Convention sur la cybercriminalité, de Budapest en novembre 2001, présentée comme l'accord international le plus pertinent sur la cybercriminalité et la preuve électronique.[8] Cette Convention poursuit trois objectifs : l'harmonisation des législations nationales en ce qui concerne les incriminations relatives à la cybercriminalité, l'adaptation des moyens procéduraux afin de permettre la poursuite de ce type d'infractions et la mise en place d'un régime de coopération internationale en la matière. Elle impose aux Etats parties de se mettre en mesure de disposer de divers moyens pour enquêter sur les infractions informatiques ou sur les infractions classiques commises par informatique et notamment de prévoir la possibilité d'enjoindre à tout utilisateur de communiquer des données informatiques en sa possession (article 18) ou le droit de perquisitionner et d'accéder à tout système informatique et de saisir ou copier les données y figurant (article 19).

4.2 La cryptologie

L'évolution législative retracée ci-dessus a abouti à l'adoption de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) qui encadre les moyens de cryptologie tout en disposant que « l'utilisation d'un moyen de cryptologie est libre ».

Son article 29 définit la notion de « moyen de cryptologie », à laquelle renvoie l'article 434-15-2 du code pénal, dans les termes suivants :

> *Article 29.- On entend par moyen de cryptologie 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. 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.*
> *On entend par prestation de cryptologie toute opération visant à la mise en oeuvre, pour le compte d'autrui, de moyens de cryptologie.*

Cette rédaction est très proche de celle du projet de loi du 14 juin 2001 précité, dont avait été extrait l'article 434-15-2 du code pénal, lequel proposait de définir la notion de « moyen de cryptologie » dans les termes suivants :

> *Article 36 : On entend par moyen de cryptologie 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. Ces moyens de cryptologie ont principalement pour objet de sécuriser le stockage ou la transmission de données, en permettant, en particulier, d'assurer la confidentialité des données ou, par exemple à des fins de signature électronique, leur authentification ou le contrôle de leur intégrité.*

Dans son rapport annuel pour 2016, la CNIL a proposé une définition de la cryptologie :

---

[7] Décrets du 17 mars 1999 : n° 99-199 définissant les catégories de moyens et de prestations de cryptologie pour lesquelles la procédure de déclaration préalable est substituée à celle d'autorisation et n° 99-200 définissant les catégories de moyens et de prestations de cryptologie dispensées de toute formalité préalable

[8] Décret n° 2006-580 du 23 mai 2006 portant publication de la Convention sur la cybercriminalité, faite à Budapest le 23 novembre 2001

Étymologiquement, la cryptologie est la science du secret. Elle réunit la cryptographie (écriture secrète) et la cryptanalyse (étude des attaques contre les mécanismes de cryptographie)
La cryptologie ne se limite plus aujourd'hui à assurer la confidentialité des secrets. Elle s'est élargie au fait d'assurer mathématiquement d'autres notions : assurer l'authenticité d'un message (qui a envoyé ce message ?) ou encore assurer son intégrité (ce message a-t-il été modifié ?).
Pour assurer ces usages, la cryptologie regroupe quatre principales fonctions : le hachage avec ou sans clé, la signature numérique et le chiffrement.
Le chiffrement (parfois improprement appelé « cryptage ») est la partie de la cryptologie qui a pour objectif de rendre impossible la compréhension d'un message à toute personne n'ayant pas la clé de déchiffrement. Ce principe permet ainsi d'assurer la confidentialité du message mais, par défaut, il n'assure ni son authenticité ni son intégrité. Ainsi, le chiffrement d'un message permet de garantir que seuls l'émetteur et les destinataires légitimes d'un message en connaissent le contenu. C'est une sorte d'enveloppe scellée numérique. Une fois chiffré et sans détenir une clé spécifique, un message est inaccessible et illisible, que ce soit par les humains ou les machines.
Plus précisément, il existe deux grandes familles de chiffrement : le chiffrement symétrique et le chiffrement asymétrique. Le chiffrement symétrique permet de chiffrer et de déchiffrer un contenu avec la même clé, appelée alors la « clé secrète ». Le chiffrement symétrique est particulièrement rapide mais nécessite que l'émetteur et le destinataire se mettent d'accord sur une clé secrète commune ou se la transmettent par un autre canal. Celui-ci doit alors être choisi avec précaution, afin que la clé ne puisse être récupérée par des tiers, ce qui n'assurerait plus la confidentialité du message.
Le chiffrement asymétrique suppose que le (futur) destinataire soit muni d'une paire de clés (clé privée, clé publique) et qu'il ait fait en sorte que les émetteurs potentiels aient préalablement accès à sa clé publique. Dans ce cas, l'émetteur utilise la clé publique du destinataire pour chiffrer le message, tandis que le destinataire utilise sa clé privée pour le déchiffrer.
Parmi les avantages de cette option :
- la clé publique peut être connue de tous et publiée : mais il est nécessaire que les émetteurs aient confiance en l'origine de la clé publique, qu'ils soient sûrs qu'il s'agit bien de celle du destinataire ;
- plus besoin de partager une même clé secrète : le chiffrement asymétrique permet de s'en dispenser.
Ce mode de chiffrement est en revanche plus lent que le chiffrement symétrique. C'est pourquoi est dans certains cas mise en œuvre une technique combinant chiffrements « symétrique » et « asymétrique », mieux connue sous le nom de « chiffrement hybride ».
Cette fois, une clé secrète est déterminée par une des deux parties souhaitant communiquer et celle-ci est envoyée chiffrée par un chiffrement asymétrique. Une fois connue des deux parties, celles-ci communiquent en chiffrant symétriquement leurs échanges. Cette technique est notamment appliquée lorsque l'on visite un site dont l'adresse débute par « https ».[9]

La CNIL a consacré un chapitre de ce même rapport aux « risques liés à la remise en cause du chiffrement ». Pour elle, la cryptologie garantit la confidentialité et la sécurité des

[9] CNIL, rapport d'activité 2016, p. 43

échanges et lui parait de nature à favoriser tant la vie des affaires que la liberté d'expression ou le respect de la vie privée. Elle s'est donc opposée à la mise en place de « portes dérobées » ou de « clés de maître »[10], craignant qu'elles créent « un risque collectif tendant à affaiblir le niveau de sécurité des personnes physiques comme morales face à l'ampleur du phénomène cybercriminel, alors même que la protection des systèmes d'information des entreprises et des États devient de plus en plus impérieuse, au vu des graves préjudices que peuvent causer les atteintes à ces systèmes, du point de vue économique, politique ou de la sécurité publique » :

> *Or, un défaut de chiffrement fait peser plusieurs risques substantiels sur la cybersécurité, qui est vecteur de confiance pour les utilisateurs, particuliers ou professionnels, et d'innovation pour les industriels. Un défaut de chiffrement peut en effet mettre en péril la sécurité des individus. (...) Dans un contexte de cybercriminalité grandissante, qui touche tous les secteurs d'activité, tous les publics (entreprises, autorités) et tous les domaines de la vie quotidienne des particuliers (données bancaires, données de santé, téléphonie, etc.), il ne peut être envisagé d'affaiblir la sécurité des solutions informatiques aujourd'hui déployées, sans que cela devienne préjudiciable au patrimoine informationnel des entreprises et à la protection de la vie privée des individus*.[11]

En 2015, le rapporteur spécial du Conseil des droits de l'homme a conclu que l'utilisation du cryptage et de l'anonymat dans les communications numériques permettent l'exercice des droits à la liberté d'opinion et d'expression à l'ère numérique et méritent donc une protection forte. Il note dans son rapport que la divulgation obligatoire des clés de déchiffrement, prévue par les lois de plusieurs pays européens, pourrait aboutir à exposer des données privées bien au-delà de ce qui est nécessaire et préconise de limiter la portée d'une telle obligation, laquelle ne devrait être prévue que lorsqu'aucun moyen d'enquête moins intrusif n'est disponible.[12]

Le règlement général sur la protection des données préconise expressément le recours au chiffrement comme un des moyens permettant de garantir un niveau de sécurité élevé du traitement des données à caractère personnel.[13] Dans cet esprit, la loi Informatique et Libertés a été modifiée par la loi n° 2016-1321 du 7 octobre 2016 pour confier à la CNIL la

---

[10] *Le principe de la mise en oeuvre d'une « porte dérobée » correspond à prévoir un accès tenu secret vis-à-vis de l'utilisateur légitime aux données contenues dans un logiciel ou sur un matériel. Le principe de la mise en oeuvre d'une « clé maître » correspond à prévoir ouvertement un tel accès, mis en oeuvre via cette clé, aux données chiffrées contenues dans un logiciel ou sur un matériel.*

[11] CNIL, rapport d'activité 2016 p. 48

[12] Rapport sur la promotion et la protection du droit à la liberté d'opinion et d'expression sur le chiffrement et l'anonymat, Conseil des droits de l'Homme des Nations Unies, mai 2015

[13] 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 - § 83 de l'exposé des motifs : *« Afin de garantir la sécurité et de prévenir tout traitement effectué en violation du présent règlement, il importe que le responsable du traitement ou le sous-traitant évalue les risques inhérents au traitement et mette en œuvre des mesures pour les atténuer, telles que le chiffrement. Ces mesures devraient assurer un niveau de sécurité approprié, y compris la confidentialité, compte tenu de l'état des connaissances et des coûts de mise en œuvre par rapport aux risques et à la nature des données à caractère personnel à protéger. »*

mission de promouvoir « l'utilisation des technologies protectrices de la vie privée, notamment les technologies de chiffrement des données »[14].

La législation tente ainsi de trouver un équilibre entre le libre développement des moyens de cryptologie pour tous et la lutte contre la cybercriminalité ou la préservation des pouvoirs d'enquête des autorités publiques, compromis par une diffusion de plus en plus large des moyens de cryptologie.

Cette tension entre des intérêts et objectifs divergents est parfaitement illustrée par l'ordonnance du 16 février 2016 par laquelle un juge de Californie a enjoint, en vain, à la société Apple de déverrouiller un iPhone utilisé par un des auteurs de la tuerie de San Bernardo afin de permettre au FBI d'accéder à son contenu.[15]

Cette même tension peut être aussi illustrée par un article, publié dans le New York Times en 2015, signé par les procureurs de Manhattan ou de Paris ainsi que par le procureur général de la Haute Cour d'Espagne et le chef de la police de Londres, signalant les difficultés résultant de l'encodage des téléphones qui pourraient être une mine d'informations pour les enquêteurs.[16]

Le développement des moyens de cryptologie a en effet permis aux fabricants de smartphones d'équiper la plupart des nouveaux modèles d'un logiciel de chiffrement qui crypte les messages échangés comme les données sauvegardées sur l'appareil.

Deux acteurs se partagent désormais le marché des systèmes d'exploitation pour téléphones portables : Apple et Android, conçu par Google, équipent de l'ordre de 99% des téléphones dans le monde.[17]

Tous les smartphones de marque Apple, depuis le modèle « iPhone 4s »[18], disposent d'un système de chiffrement des données stockées dans la mémoire de l'appareil qui s'impose à l'utilisateur, sans pouvoir être désactivé.

Le chiffrement des données est désormais aussi activé par défaut sur les appareils fonctionnant sous Android, ceci depuis 2015 (avec les versions n° 5, dite Lolippop, puis 6, dite Marshmallow).[19] Un tel cryptage des données pouvant entraver les performances du téléphone et ralentir son fonctionnement, Android le proposait auparavant uniquement en option, notamment pour ce qui concerne les appareils les moins performants.

---

[14] Article 8 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

[15] D. Rebut, JCP, n° 13, 28 Mars 2016, p. 352, FBI vs Apple, les leçons de légalité, de proportionnalité et de transparence de la justice américaine, Libres propos

[16] C.R. Vance, F. Molins, A. Leppard et J. Zaragoza, When phone encryption blocks justice, New York Times, 11 août 2015

[17] Parts de marché des systèmes d'exploitation sur mobile dans le monde en juin 2022 : Android : 71,7% (France : 66,82%) ; iOS Apple : 27,57 % (France :32,63%) autres systèmes (0,57%)

[18] Commercialisé à partir de fin 2011

[19] Comment fonctionne le chiffrement des smartphones sous Android, numérama, mars 2016

Enfin, il est toujours possible de chiffrer les données avec une version antérieure mais ceci suppose une action volontaire de l'utilisateur.
Un tel chiffrement des données rend impossible la lecture du contenu des fichiers enregistrés dans la mémoire de l'appareil, qu'il s'agisse, par exemple, de messages échangés, par SMS ou mail, de photographies, d'une liste des contacts, d'enregistrements sonores ou de tout autre document.

Si les opérateurs de téléphonie mobile peuvent fournir aux enquêteurs les « données de connexion »,[20] seule la clé de déchiffrement permet d'accéder, en clair, aux « données de contenu » sauvegardées dans l'appareil.

D'une manière extrêmement simplifiée, il peut être retenu que cette clé de déchiffrement est générée aléatoirement par le système puis est mise en oeuvre par l'utilisateur au moyen d'un code d'accès, défini par lui, associé à un appareil déterminé, ce qui en garantit la sécurité. Le système peut en outre interdire tout accès après un certain nombre de tentatives au moyen de codes erronés voire même, dans certains cas, programmer alors l'effacement des données contenues dans l'appareil.

Par ailleurs, les smartphones utilisent diverses applications, dont de nombreuses applications de messagerie qui sont, pour la plupart désormais, cryptées indépendamment du matériel utilisé pour communiquer avec elles (téléphone, tablette, ordinateur ...). Le « chiffrement de bout en bout » utilisé par ces messageries crypte les données lors de leur envoi et n'autorise leur déchiffrement qu'à leur arrivée de sorte que personne ne peut y accéder au cours de leur transmission. Tel est notamment le cas des messageries proposées par Apple, Google, Facebook ou encore de Signal, Telegram, WhatsApp ...

Le parquet général a interrogé le commandement de la gendarmerie du cyberespace sur les questions techniques posées par le présent pourvoi puis a communiqué le rapport rédigé en réponse par le colonel Duvinage.

Ce dernier conclut que, quel que soit le mécanisme utilisé à cette fin (hachage cryptographique, stockage dans un composant sécurisé, stockage de façon chiffrée), le système de déverrouillage de tout téléphone portable est un moyen de cryptologie en ce qu'il « donne accès à l'affichage des données du téléphone en clair à l'utilisateur, et qu'en l'absence de connaissance dudit code de déverrouillage aucun autre utilisateur doté de connaissances techniques « normales » et ne disposant d'aucun équipement matériel ou logiciel spécifique ne peut accéder à cet affichage des données du téléphone en clair ».[21]
Il ajoute que « le code de déverrouillage d'un iPhone (versions iPhone 4 et suivantes) est bien une convention secrète de déchiffrement d'un moyen de cryptologie, portant sur le déchiffrement des données stockées » dans l'appareil, de même que les systèmes ayant

[20] Définies par l'article L. 34-1 du code des postes et des communications électroniques comme étant celles qui « portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation des équipements terminaux »

[21] Rapport du colonel Duvinage, code de déverrouillage d'un téléphone portable et convention secrète de déchiffrement d'un moyen de cryptologie, pièce diverse n° 00, page 16

recours à une empreinte digitale ou à la reconnaissance faciale.[22] Il précise enfin qu'il en va de même des téléphones fonctionnant sous Android (à partir de la version 6.0).[23]

4.3 L'application de l'article 434-15-2 du code pénal

La décision du Conseil constitutionnel

La nouvelle infraction, introduite dans le code pénal en 2001, ne parait pas avoir été très utilisée dans les années suivantes et la Cour de cassation ne s'est prononcée, pour la première fois, à son sujet qu'en 2018 à l'occasion de l'examen d'une question prioritaire de constitutionnalité.

La chambre criminelle a renvoyé cette QPC au Conseil constitutionnel en considérant que les dispositions de l'article 434-15-2 du code pénal, appliquées à une personne suspectée d'avoir commis une infraction, pourrait porter atteinte à son droit de ne pas faire de déclaration et à celui de ne pas contribuer à sa propre incrimination qui résultent des articles 9 et 16 de la Déclaration des Droits de l'homme et du Citoyen du 26 août 1789.

> *Attendu que la question prioritaire de constitutionnalité est ainsi rédigée :*
> *« Les dispositions de l'article 434-15-2 du code pénal, en ce qu'elles ne permettent pas au mis en cause, auquel il est demandé 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 faire usage de son droit au silence et du droit de ne pas s'auto-incriminer, sont-elles contraires au principe du droit au procès équitable prévu par l'article 16 de la Déclaration des Droits de l'homme et du Citoyen du 26 août 1789, au principe de la présomption d'innocence, duquel découle droit de ne pas s'auto-incriminer et le droit de se taire, prévu à l'article 9 de la Déclaration des Droits de l'Homme et du Citoyen du 26 août 1789 ? » ;*
> *Attendu que la disposition législative contestée est applicable à la procédure et n'a pas été déjà déclarée conforme à la Constitution dans les motifs et le dispositif d'une décision du Conseil constitutionnel ;*
> *Attendu que la question posée présente un caractère sérieux en ce que l'article 434-15-2 du code pénal qui contraint, sous menace de sanctions pénales, une personne suspectée dans le cadre d'une procédure pénale, à remettre aux enquêteurs 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, pourrait porter atteinte au droit de ne pas faire de déclaration et à celui de ne pas contribuer à sa propre incrimination qui résultent des articles 9 et 16 de la Déclaration des Droits de l'homme et du Citoyen du 26 août 1789 ;*
> ***Crim. 10 janvier 2018, pourvoi n° 17-90.019***

Par une décision n° 2018-696 du 30 mars 2018, le Conseil constitutionnel a déclaré le premier alinéa de l'article 434-15-2 du code pénal conforme à la Constitution :

---

[22] Rapport précitéhttp://srv-cassation.cour-de-cassation.justice.fr/rpvjcc/Jurinet/Ged.asp?ID_GED=1370875&Domaine=P, page 21

[23] Rapport précité, page 24

(...) *7. En premier lieu, 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.*
8. En second lieu, aux termes de la première phrase de l'article 29 de la loi du 21 juin 2004 mentionnée ci-dessus constitue un moyen de cryptologie « 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 ». Les dispositions 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.
9. Il résulte de ce qui précède que les dispositions contestées ne portent pas atteinte au droit de ne pas s'accuser ni au droit au respect de la vie privée et au secret des correspondances.
10. Le premier alinéa de l'article 434-15-2 du code pénal, qui ne méconnaît pas non plus les droits de la défense, le principe de proportionnalité des peines et la liberté d'expression, ni aucun autre droit ou liberté que la Constitution garantit, doit être déclaré conforme à la Constitution.
Cons. Const., Décision n° 2018-696 QPC du 30 mars 2018

Le Conseil Constitutionnel relève ainsi que le refus de révéler une convention secrète de déchiffrement d'un moyen de cryptologie n'est punissable qu'aux conditions suivantes :

- L'enquête doit avoir permis d'identifier l'existence de données traitées par le moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit ;
- La demande de révélation doit émaner d'une autorité judiciaire ;
- Il doit être établi que la personne poursuivie en avait connaissance.

Le commentaire qui accompagne cette décision note que le Conseil constitutionnel « a ainsi pris acte de l'interprétation de la Cour de cassation selon laquelle l'infraction contestée s'applique 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 ».

Cette décision a fait l'objet de plusieurs commentaires critiques de la doctrine :

Mme Lacaze regrette l'absence de toute réserve d'interprétation excluant l'application de l'incrimination à la personne mise en cause ou, tout au moins, réservant l'application de ce texte à la recherche des infractions les plus graves :

Le large champ d'application du texte - qui couvre les investigations relatives à tout crime ou délit et non pas aux seules infractions en matière de terrorisme et de délinquance organisée, comme pourrait le laisser penser l'objet des lois qui l'ont institué et en ont renforcé la pénalité - faisait espérer une analyse minutieuse de proportionnalité. La décision déçoit pourtant fortement. Le Conseil constitutionnel laisse en effet plusieurs questions sans réponse explicite et, pour juger sans réserve le texte conforme à la Constitution, n'opère pas de véritable conciliation entre les droits et principes invoqués et les objectifs à valeur constitutionnelle de prévention des infractions et de recherche de leurs auteurs. (...)

Après avoir rappelé que la demande doit émaner d'une « autorité judiciaire », le Conseil commence par poser que l'obligation contestée ne s'impose qu'à la personne dont il est établi « qu'elle en a connaissance », et seulement si l'enquête ou l'instruction ont « permis d'identifier l'existence de données traitées par le moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit ». La demande ne peut alors pas être systématique et, s'il peut bien trouver à s'exercer au cours d'une garde à vue, le texte n'est pas applicable au refus opposé à l'injonction d'un OPJ agissant d'initiative. Pour utiles qu'ils puissent être face aux pratiques qui semblent s'être instaurées en certains endroits, ces rappels des conditions textuelles ne constituent pas une réserve d'interprétation.

Sur le second aspect, si le Conseil constitutionnel a déjà jugé plusieurs fois que le droit invoqué n'interdit pas d'instituer des obligations pénalement sanctionnées de fournir des documents utiles à l'enquête, de telles obligations ont déjà emporté condamnation de la France sur le fondement de l'article 6 § 3 de la Conv. EDH. Le Conseil en a du reste conscience, et semble chercher à se prémunir d'une telle issue en soulignant que les données, « déjà fixées dans un support, existent indépendamment de la volonté de la personne suspectée ». La référence à la jurisprudence européenne est, là encore, assez évidente. Celle-ci a en effet admis le recours à certains moyens coercitifs ayant pour objet d'obtenir des preuves, au motif que le droit de ne pas contribuer à sa propre accusation n'est pas absolu et « ne s'étend pas à l'usage dans une procédure pénale des données [...] qui existent indépendamment de la volonté du suspect ». L'extension de la notion à l'incrimination contestée paraît cependant hasardeuse car la jurisprudence européenne ne l'a, jusqu'ici, utilisée que pour des « éléments produits par le fonctionnement organique normal », ce qui n'est aucunement le cas de l'article 434-15-2. La Cour européenne exige en outre, en toute hypothèse, qu'il soit procédé à une balance des intérêts n'emportant pas un anéantissement du droit. Elle a ainsi plusieurs fois constaté une violation de l'article 6 § 3 en cas d'infliction d'une sanction pénale consécutive au refus d'apporter des renseignements aux autorités.

S'agissant des autres griefs, la motivation paraît inexistante. On peut s'en étonner au vu des développements récents de la jurisprudence constitutionnelle en matière d'atteinte à la liberté d'expression, et le regretter tant il semble difficile d'écarter toute atteinte au droit au respect de la vie privée, même dans la conception « très restrictive » revendiquée par le commentaire. Surtout, dès lors que l'obligation instituée peut bien avoir pour objet d'accéder au contenu de conversations dont la nature privée, voire confidentielle, est attestée par le recours au procédé de cryptologie, l'atteinte au secret des correspondances paraît indéniable.

Pour convaincre de la conformité de l'article 434-15-2 à la Constitution et limiter les risques de violation de l'article 6 § 3, le Conseil constitutionnel aurait alors plus sûrement dû opérer une réserve d'interprétation excluant l'application de l'incrimination à la personne mise en cause. À tout le moins, aurait-il dû mener une analyse véritable de la conciliation opérée par le texte tel qu'il est interprété. Que certaines des atteintes invoquées soient considérées comme justifiées aurait pu être compris, du moins s'agissant de la recherche des infractions les plus graves. La négation de toute atteinte, en revanche, semble nier l'évidence.[24]

[24] M. Lacaze, Constitutionnalité du refus de remise d'une convention secrète de déchiffrement, AJ pénal 2018. 257

M. A. Caprioli conclut son commentaire, critique lui aussi, de la manière suivante :

> *6. La motivation de cette décision nous semble relativement pauvre et elle nous éclaire finalement que très faiblement quant au périmètre d'application de l'article 434-15-2 du Code pénal. En effet, qu'est-ce qu'une « convention secrète de déchiffrement d'un moyen de cryptologie » ? Conformément à l'article 29, alinéa 1er de la LCEN, ce sont des informations qui sont transformées au moyen d'une « convention secrète » (une clé de cryptographie asymétrique ou la clé publique d'un bi-clé asymétrique, le déchiffrement étant réalisé avec la clé privée) dans le but d'en assurer la confidentialité. Cette convention sécrète permet de déchiffrer les informations, de les rendre intelligibles. Une telle précision a son importance étant rappelé que les textes de droit pénal sont d'interprétation stricte. En l'espèce, c'est le code de déverrouillage du téléphone portable du gardé à vue qui était initialement concerné. Dans cette perspective, certains commentaires dans la presse spécialisée en sécurité ont estimé qu'à la suite de la décision du Conseil constitutionnel, le code d'accès à son (ou ses) téléphone portable pouvait être demandé à un prévenu. Or, 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 vocation première de l'article 434-15-2 du Code pénal était de viser les informations chiffrées et non leur accessibilité. Sur ce plan, la décision du Conseil ne peut être approuvée dans la mesure où elle est particulièrement préjudiciable aux libertés individuelles si l'on considère que les deux notions se confondent à la fois sur les plans technique et juridique. En revanche, il aurait été souhaitable que le Conseil constitutionnel déclare le premier alinéa de l'article 434-15-2 du Code pénal conforme à la Constitution, mais entendu de façon stricte, c'est-à-dire uniquement pour la « convention secrète de déchiffrement d'un moyen de cryptologie ».*[25]

Le professeur Conte critique essentiellement la motivation de la décision du Conseil constitutionnel qu'il juge trop pauvre.[26] Partageant cet avis, Mme Quémener approuve toutefois la décision sur le fond :

> *Il apparaît que la décision du Conseil constitutionnel est peu motivée et aurait pu répondre plus clairement aux arguments soulevés, à savoir l'éventualité d'une atteinte au droit au silence ou droit de se taire et à celui de ne pas contribuer à sa propre incrimination qui résultent des articles 9 et 16 de la Déclaration des droits de l'homme et du citoyen du 26 août 1789.*
> *S'agissant de ce dernier principe, le Conseil aurait pu s'appuyer en particulier sur la décision (CEDH 17 déc. 1996, Saunders c/ Royaume-Uni, n° 19187/91, RSC 1997. 476, obs. R. Koering-Joulin ; Rev. UE 2015. 353, étude M. Mezaguer) qui souligne clairement que ce droit « 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 ».*

[25] E. A. Caprioli, Communication Commerce électronique n° 9, Septembre 2018, comm. 69

[26] P. Conte, Droit pénal n° 7-8, Juillet 2018, comm. 123

La jurisprudence judiciaire (Crim. 6 janv. 2015, n° 13-87.652, D. 2015. 1738, obs. J. Pradel) a d'ailleurs repris également cette motivation en affirmant 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, la cour d'appel n'a méconnu aucune des dispositions légales et conventionnelles visées au moyen ».
Enfin, un parallèle aurait pu être fait avec d'autres infractions de refus de collaborer, comme l'obligation pénalement sanctionnée de se soumettre au prélèvement (C. pr. pén., art. 706-56). Dans une décision, le Conseil constitutionnel avait précisé que cette infraction de refus n'implique pas davantage de reconnaissance de culpabilité et n'est pas contraire à la règle selon laquelle nul n'est tenu de s'accuser, et qu'en conséquence, cette incrimination ne porte pas atteinte à la présomption d'innocence (Cons. const. 16 sept. 2010, n° 2010-25 QPC, D. 2012. 308, obs. J.-C. Galloux et H. Gaumont-Prat ; AJ pénal 2010. 545, étude J. Danet).

IV - Une décision critiquée mais favorable aux enquêtes : La décision que vient de rendre le Conseil constitutionnel est au coeur d'enjeux et d'équilibre fragile entre la protection des droits et des données numériques et personnelles, et la recherche et l'établissement d'infractions pénales qui nécessitent impérativement le recours à des investigations numériques indispensables, mais qui doivent être strictement encadrées par le législateur.
Ainsi, pour l'association La Quadrature du Net, cette décision remet en cause le droit au chiffrement et l'intérêt de son usage, mais également la vie privée, la confidentialité des communications, le secret des sources journalistiques et la liberté de communication.[27]
Cette analyse apparaît cependant erronée dans la mesure où le Conseil précise les éléments de l'infraction de façon stricte et ne permet pas par voie de conséquence le chiffrement.
L'accès aux données numériques est aujourd'hui l'un des enjeux essentiels pour les services d'enquêtes. À travers cette décision, le Conseil constitutionnel entend aussi rappeler que le refus de remettre les clés de chiffrement doit être sanctionné, car il constitue une entrave préjudiciable aux enquêtes pénales, ce qui peut être lourd de conséquence, et ce particulièrement dans un contexte de menaces terroristes durables.[28]

Il est intéressant de noter que la direction des services judiciaires souligne, dans une revue de presse, que « le Conseil constitutionnel a eu (...) une interprétation de la loi plus sécuritaire que ne le souhaitait le gouvernement » :

L'institution présidée par Laurent Fabius et le Premier ministre se sont retrouvés à front renversé lors de l'examen d'une question prioritaire de constitutionnalité (QPC). Celle-ci portait sur l'article 434-15-2 du code pénal (...) Philippe Blanc, représentant du Premier ministre à l'audience, avait reconnu le problème. Selon lui, « la seule interprétation qui permette de rendre cet article conforme à la Constitution est de dire qu'elle exclut son application à des personnes suspectées d'avoir elles-mêmes commis une infraction ». Autrement dit, la justice peut demander ces « conventions de déchiffrement » à un témoin ou à un tiers à l'enquête. Le gouvernement reconnaît donc que l'application que les procureurs de la République font de ce texte est inconstitutionnelle. Malgré cette position officielle, le Conseil constitutionnel a décidé de déclarer cet article du code pénal conforme, en précisant qu'il s'applique à tous, y compris à une personne suspectée, même si l'objet n'est pas d'« obtenir des aveux de sa part ». Il précise néanmoins que l'enquête aura dû identifier que des données contenues dans le terminal

[27] https://www.numerama.com/tech/340941-la-quadrature-du-net-denonce-une-restriction-du-droit-au-chiffrement.html

[28] M. Quéméner, Le refus de déchiffrement à l'épreuve des droits fondamentaux, Dalloz IP/IT 2018.514

en question « sont susceptibles d'avoir été utilisées pour préparer, faciliter ou commettre un crime ou un délit ». (...) Selon l'association La Quadrature du Net, qui s'est jointe à la procédure, la décision du 30 mars « remet en cause le droit au chiffrement et l'intérêt de son usage ». Reste un point juridique qui n'a pas été tranché (...) : le code PIN d'un téléphone ou le code déverrouillage d'une carte SIM sont-ils un « moyen de cryptologie » ? Il reviendra sans doute à la Cour de cassation de trancher cette question.[29]

La jurisprudence de la chambre criminelle

Alors qu'elle n'avait examiné aucun pourvoi relatif à l'application de ce texte entre 2001 et 2018, la chambre criminelle a été amenée à se prononcer récemment à son sujet à plusieurs reprises dans des affaires au cours desquelles les services de police, enquêtant principalement sur des infractions à la législation sur les stupéfiants, avaient demandé à des personnes placées en garde à vue de leur communiquer le code de leur téléphone portable.

La jurisprudence de la chambre criminelle en la matière se limite à sept arrêts de sorte qu'il semble possible de les citer de manière exhaustive :

Par un arrêt du 10 décembre 2019 *(pourvoi n° 18-86.878)*, la chambre criminelle a tiré les conséquences de la décision rendue par le Conseil constitutionnel en jugeant 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.

Elle a donc approuvé une cour d'appel qui avait énoncé que l'article 434-15-2 du code pénal, en ce qu'il incrimine le refus, par l'utilisateur d'un téléphone crypté, de remettre aux autorités judiciaires ou de mettre en oeuvre la convention secrète de déchiffrement d'un moyen de cryptologie, n'est pas contraire aux articles 6 et 8 de la Convention européenne des droits de l'homme.

Sur le premier moyen pris en ses trois premières branches ;
Attendu que pour écarter le moyen pris de l'inconventionnalité de l'article 434-15-2 du code pénal, l'arrêt énonce que l'atteinte au droit de se taire et au droit de ne pas s'auto-incriminer est constituée dès lors que les données ne peuvent exister indépendamment de la volonté du suspect, ce qui n'est pas le cas des données contenues dans les téléphones, qui peuvent être obtenues par des moyens techniques ;
Attendu qu'en statuant ainsi, et dès lors 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, la cour d'appel n'a méconnu aucune des dispositions légales et conventionnelles visées au moyen ;
D'où il suit que les griefs ne peuvent être admis ;
Sur le premier moyen pris en sa quatrième branche ;
Attendu que pour déclarer le prévenu coupable de refus de remettre aux autorités judiciaires ou de mettre en oeuvre la convention secrète de déchiffrement d'un moyen de cryptologie, l'arrêt relève que M. [X] a refusé de communiquer aux enquêteurs les codes de ses téléphones, rendant ainsi impossible leur exploitation ; que les juges ajoutent que les éléments découverts en sa possession au moment de son interpellation, soit 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

[29] J.B. Jacquin, Le Monde, 16 avril 2018

normale, laissent présumer un usage du téléphone portable en lien avec des infractions à la législation sur les stupéfiants ;
Attendu qu'en l'état de ses motifs, dépourvus d'insuffisance comme de contradiction et résultant de son appréciation souveraine des circonstances de fait contradictoirement débattues, la cour d'appel a justifié sa décision ;
Qu'ainsi, le moyen n'est pas fondé ;
Crim., 10 décembre 2019, pourvoi n° 18-86.878, publié

Il convient de noter que, à la suite de cette décision, l'intéressé a introduit un recours devant la Cour européenne des droits de l'homme en invoquant une atteinte à son droit de garder le silence et de ne pas contribuer à sa propre incrimination ainsi qu'une atteinte à sa vie privée et à l'intimité de sa correspondance. Cette affaire a été communiquée, le 31 mai 2021, au gouvernement français sous l'angle des articles 6 § 1 et 8 de la Convention afin de recueillir ses observations en réponse aux deux questions suivantes :

1. La condamnation pénale du requérant, sur le fondement de l'article 434-15-2 du code pénal, pour avoir refusé de communiquer le code de déverrouillage de son téléphone portable aux policiers durant sa garde à vue, a-t-elle porté atteinte à son droit de garder le silence et de ne pas contribuer à sa propre incrimination tel que garanti par l'article 6 de la Convention ?
2. Y a-t-il eu violation du droit du requérant au respect de sa vie privée et de sa correspondance, au sens de l'article 8 de la Convention ? [30]

La chambre criminelle a ensuite, le 13 octobre 2020, rendu deux arrêts publiés, relatifs à la question de savoir si le code d'accès à un téléphone portable constitue la convention de déchiffrement d'un moyen de cryptologie visée par l'article 434-15-2 du code pénal.

Le premier arrêt, reproduit ci-dessous, (*pourvoi n° 20-80.150*) est intervenu dans l'affaire qui avait donné lieu à la QPC du 10 janvier 2018. La chambre criminelle y juge que le refus de remettre la convention de déchiffrement est punissable lorsqu'il est opposé à une réquisition délivrée par un officier de police judiciaire en précisant que tel ne serait pas le cas s'il s'agissait d'une simple demande formulée au cours d'une audition, sans avertissement que le refus d'y déférer est susceptible de constituer une infraction pénale.

Ce même arrêt précise que « le code de déverrouillage d'un téléphone portable peut constituer une convention secrète de déchiffrement d'un moyen de cryptologie lorsque ledit téléphone est équipé d'un tel moyen, ce qui 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 ».

Le second arrêt *(pourvoi n° 19-85.984*) concerne l'affaire soumise à l'assemblée plénière. La chambre criminelle y précise 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. »

Exposé du moyen
5. Le moyen est pris de la violation de l'article 434-15-2 du code pénal.
6. Le moyen critique l'arrêt attaqué en ce qu'il a relaxé M.[W]du chef de refus de remettre une convention secrète de déchiffrement d'un moyen de cryptologie, alors :

[30] Requête n° 23624/20, communiquée le 31 mai 2021

« 1°/ que la cour d'appel a imposé une exigence non expressément prévue par l'article 434-15-2 du code pénal, en énonçant qu'il ne ressort d'aucun élément de la procédure qu'une réquisition ait été adressée par une autorité judiciaire à [P][W]de communiquer ce code de déverrouillage ou de le mettre en oeuvre, cependant qu'elle constatait que le prévenu a refusé de communiquer ce code à la suite d'une demande qui lui été faite au cours de son audition par un fonctionnaire de police ;
2°/ 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 des données contenues dans l'appareil grâce à un algorithme défini de manière à les rendre inintelligibles.»

Réponse de la Cour
Sur le moyen pris en sa première branche
7. Pour relaxer le prévenu, l'arrêt énonce que M.[W]a refusé de communiquer le code de déverrouillage de son téléphone portable, sur la demande d'un fonctionnaire de police, faite au cours de son audition, et non en vertu d'une réquisition émanant d'une autorité judiciaire de le communiquer ou de le mettre en oeuvre.
8. En prononçant ainsi, la cour d'appel a justifié sa décision.
9. C'est à tort qu'elle a énoncé que cette réquisition ne pouvait être délivrée par un fonctionnaire de police, alors que 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, dans leur rédaction applicable au litige, sous le contrôle de l'autorité judiciaire, entre dans les prévisions de l'article 434-15-2 du code pénal.
10. L'arrêt n'encourt pour autant pas la censure, dès lors qu'une simple demande formulée au cours d'une audition, sans avertissement que le refus d'y déférer est susceptible de constituer une infraction pénale, ne constitue pas une réquisition au sens du texte précité.
11. Dès lors, le moyen n'est pas fondé.
Mais sur le moyen pris en sa seconde branche
Vu les articles 434-15-2 du code pénal, 29 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, L.871-1 et R. 871-3 du code de la sécurité intérieure :
12. Selon le premier de ces textes, toute personne 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, est tenue de remettre ladite convention aux autorités judiciaires ou de la mettre en oeuvre, sur les réquisitions de ces autorités délivrées en application des titres II et III du livre Ier du code de procédure pénale.
13. Il résulte de la combinaison des autres textes 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.
14. 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.
15. Pour relaxer le prévenu, l'arrêt énonce 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.
16. En se référant ainsi à la notion inopérante de téléphone d'usage courant, la cour d'appel a méconnu les textes susvisés et les principes ci-dessus rappelés.
17. Par conséquent, la cassation est encourue.

Portée et conséquences de la cassation
18. La cassation aura lieu sans renvoi, dans les conditions fixées par l'article 621 du code de procédure pénale, les parties ne pouvant s'en prévaloir, ni s'opposer à l'exécution de la décision annulée.

Crim., 13 octobre 2020, pourvoi n° 20-80.150, publié[31]

Exposé du moyen
6. Le moyen est pris de la violation de l'article 593 du code de procédure pénale.
7. Il critique l'arrêt attaqué en ce qu'il a relaxé le prévenu du chef de refus de remettre aux autorités judiciaires la convention secrète de déchiffrement d'un moyen de cryptologie, alors :
1°/ qu'il ressort des dispositions de l'article 29 de la loi 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 toute autre information permettant la mise au clair de ces données » ;
2°/ qu'en affirmant ainsi qu'un code de déverrouillage d'un téléphone ne peut être qualifié de « convention secrète de déchiffrement », sans effectuer l'analyse des caractéristiques techniques du téléphone concerné, pourtant indispensable à fonder sa décision, la cour d'appel n'a pas justifié celle-ci. »
Réponse de la Cour
Vu les articles 434-15-2 du code pénal, 29 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, L. 871-1 et R. 871-3 du code de la sécurité intérieure :
8. Selon le premier de ces textes, toute personne 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, est tenue de remettre cette convention aux autorités judiciaires, ou de la mettre en oeuvre, sur les réquisitions de ces autorités, délivrées en application des titres II et III du Livre Ier du code de procédure pénale.
9. Selon le deuxième, un moyen de cryptologie est 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.
10. Selon les textes précités du code de la sécurité intérieure, 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.
11. Pour confirmer la relaxe, la cour d'appel énonce qu'un téléphone portable ne peut être considéré comme un moyen de cryptologie au sens des textes précités, et que le code permettant de déverrouiller l'écran d'accueil d'un téléphone, qu'il s'agisse d'un code chiffré ou d'un ensemble de points à relier dans un sens prédéfini par l'utilisateur, ne peut être qualifié, au sens des mêmes dispositions, de convention secrète de déchiffrement. L'arrêt retient qu'un tel code de déverrouillage de l'écran ne sert pas à décrypter les données contenues dans le téléphone, mais seulement à débloquer l'usage de l'écran, pour accéder aux données contenues dans le téléphone
12. En prononçant ainsi, par un motif général et erroné, alors que le code de déverrouillage d'un téléphone portable constitue une convention de déchiffrement s'il permet de mettre au clair les données qu'il contient, la cour d'appel n'a pas justifié sa décision.

[31] Commenté par : E. Dreyer, JCP 2020.1417 ; S. Vergnolle, D. 2021.609 ; C. Ribeyre, Dr. pen., 2021. Comm. 1

13. Il en résulte que la cassation est encourue de ce chef.
Crim., 13 octobre 2020, pourvoi n° 19-85.984, publié

Deux arrêts plus récents n'ont pas été publiés : ils confirment les solutions antérieures et reprochent aux cours d'appel de ne pas avoir recherché si les téléphones portables en cause étaient équipés d'un moyen de cryptologie de sorte que leur code de déverrouillage permettait de mettre au clair les données qu'ils contiennent.
Le second souligne en outre l'exigence, déjà rappelée par le Conseil constitutionnel, selon laquelle il convient de déterminer si le prévenu avait connaissance de l'existence d'un tel moyen de cryptologie.

Vu les articles 434-15-2 du code pénal, 29 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, L. 871-1 et R. 871-3 du code de la sécurité intérieure, et 593 du code de procédure pénale :
8. Selon le premier de ces textes, toute personne 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, est tenue de remettre cette convention aux autorités judiciaires, ou de la mettre en oeuvre, sur les réquisitions de ces autorités, délivrées en application des titres II et III du Livre Ier du code de procédure pénale.
9. Selon le deuxième, un moyen de cryptologie est 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.
10. Selon les textes précités du code de la sécurité intérieure, 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.
11. Selon le texte susvisé du code de procédure pénale, tout jugement ou arrêt doit être motivé, et l'insuffisance ou la contradiction dans les motifs équivaut à leur absence.
12. Pour déclarer le demandeur coupable du chef de refus de remettre ou de mettre en oeuvre la convention secrète de déchiffrement d'un moyen de cryptologie, la cour d'appel retient qu'il a refusé de communiquer aux enquêteurs le code secret permettant de déverrouiller son téléphone portable et ajoute qu'un tel code, qui a pour objet de garantir la sécurité du stockage ou de la transmission des données contenues dans le téléphone et d'assurer leur confidentialité est un moyen de cryptologie au sens de l'article 434-15-2 du code pénal, les enquêteurs, lorsqu'ils conduisent une enquête pénale, sous l'autorité du procureur de la République, étant compris dans les autorités judiciaires visées par ce texte.
13. Si la cour d'appel a exactement considéré que 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, entre dans les prévisions de l'article 434-15-2 du code pénal, elle n'a toutefois pas justifié sa décision, en déclarant le demandeur coupable par un motif d'ordre général, sans avoir constaté que le téléphone du prévenu était équipé d'un moyen de cryptologie et que le code de déverrouillage permettait de mettre au clair les données qu'il contient.
14. Il en résulte que la cassation est encourue.
Crim., 3 mars 2021, pourvoi n° 19-86.757

Vu les articles 434-15-2 du code pénal, 29 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, L. 871-1 et R. 871-3 du code de la sécurité intérieure :
9. Selon le premier de ces textes, toute personne 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, est tenue de remettre cette convention aux autorités judiciaires, ou de la mettre en oeuvre, sur les réquisitions de ces autorités, délivrées en application des titres II et III du Livre Ier du code de procédure pénale.

10. Selon le deuxième, un moyen de cryptologie est 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.

11. Selon les textes précités du code de la sécurité intérieure, 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.

12. Pour déclarer le prévenu coupable, la cour d'appel a rappelé que le prévenu avait refusé de déverrouiller le téléphone découvert dans la chambre qu'il occupait.

13. Elle conclut que le refus du prévenu de remettre les codes de son téléphone portable et de son ordinateur portable, utilisés pour commettre les délits est constitutif de l'infraction prévue et réprimée par l'article 434-15-2 du code pénal, ces appareils ayant été utilisés pour commettre les délits reprochés sur le fondement de l'article 222-16 du code pénal.

14. En se déterminant ainsi, sans rechercher si les appareils en cause étaient équipés d'un moyen de cryptologie dont le prévenu avait connaissance, la cour d'appel a méconnu les textes et principes susvisés.

Crim., 9 mars 2022, pourvoi n° 21-83.557

Il faut ajouter que la chambre criminelle a considéré que l'exploitation d'un téléphone portable pendant une garde à vue est assimilable à une perquisition de sorte que l'officier de police judiciaire peut solliciter la communication du code d'accès à ce téléphone en dehors de la présence de l'avocat, tout comme il aurait pu solliciter toute autre information permettant l'accès à un espace privé préalablement identifié, qu'il soit ou non dématérialisé, pour les besoins d'une perquisition.

Réponse de la Cour

7. Pour écarter le moyen de nullité, selon lequel Mme L. a été entendue hors la présence de son avocat, l'arrêt attaqué énonce que le procès verbal d'exploitation du téléphone de l'intéressée n'a pas le caractère d'une audition dès lors que celle-ci n'a fait aucune déclaration et qu'aucune question sur les faits pour lesquels elle est placée en garde à vue ne lui a été posée.

8. Les juges ajoutent, par ailleurs, qu'il n'est pas rapporté la preuve d'une atteinte au droit de ne pas contribuer à sa propre incrimination, dès lors que ce droit ne s'étend pas à l'usage de données que l'on peut obtenir de la personne en recourant à des pouvoirs coercitifs, mais qui existent indépendamment de la volonté du suspect.

9. En l'état de ces énonciations, la chambre de l'instruction n'a méconnu aucun des textes visés au moyen.

10. En premier lieu, aucune disposition légale ne prévoit la présence de l'avocat lors de l'exploitation d'un téléphone portable, assimilable à une perquisition.

11. En second lieu, la communication à un officier de police judiciaire, sur sa sollicitation, d'une information permettant l'accès à un espace privé préalablement identifié, qu'il soit ou non dématérialisé, pour les besoins d'une perquisition, ne constitue pas une audition au sens de l'article 63-4-2 du code de procédure pénale.

12. Dès lors, le moyen doit être écarté.

Crim., 12 janvier 2021, pourvoi n° 20-84.045 [32]

[32] Commenté par : R. Parizot, RSC 2021.128 ; J.-B. Perrier, D. 2021.1564 ; E. Clément, AJ pénal 2021.214

***

Selon cette jurisprudence, les dispositions de l'article 434-15-2 du code pénal sont donc applicables au refus de communiquer le code d'accès à un téléphone portable, opposé à une demande des autorités judiciaires, et notamment à une réquisition d'un officier de police judiciaire, dès lors que des indices permettent de penser que ce téléphone est susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, quel qu'il soit. Afin de caractériser l'élément moral de cette infraction intentionnelle, il doit être établi que la personne concernée avait connaissance de l'existence du moyen de cryptologie équipant son téléphone avant de refuser d'en communiquer le code d'accès. Il convient enfin de s'assurer que le téléphone en cause est effectivement équipé d'un moyen de cryptologie et que son code de déverrouillage ne se limite pas à donner accès aux données qu'il contient mais constitue aussi une convention de déchiffrement permettant de les mettre au clair. Ceci peut nécessiter des investigations techniques, révélant que le téléphone est doté d'un tel moyen de cryptologie, mais peut aussi se déduire des seules caractéristiques techniques de l'appareil ou des applications qui l'équipent.

Les positions de la doctrine

D'une manière générale, la doctrine a été assez critique vis-à-vis des solutions adoptées tant par le Conseil constitutionnel en 2018 que par la chambre criminelle en 2020.

La rédactrice de l'article du Jurisclasseur de procédure pénale consacré à l'article 434-15-2 du code pénal indiquait, avant la publication des arrêts d'octobre 2020, que le code d'accès à un téléphone n'est pas un moyen de cryptologie mais un mécanisme d'authentification.

> ***92. c) Le refus d'accès érigé en infraction pénale**. – Le législateur, conscient des difficultés d'accès à la preuve et des refus des personnes interpellées à communiquer leurs clés de déchiffrement en a tiré les conséquences en créant une infraction spécifique. Ainsi, l'article 434-15-2 du Code pénal sanctionne de 3 ans d'emprisonnement et de 270 000 € d'amende "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 la remettre 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.*
> *93. – Suite à une question prioritaire de constitutionnalité (QPC) transmise par la Cour de cassation (Cass. crim., 10 janv. 2018, n° 17-90.019), le Conseil constitutionnel (Cons. const., 30 mars 2018, n° 2018-696 QPC) a jugé conforme à la constitution l'incrimination de refus de remettre aux autorités judiciaires une convention secrète de déchiffrement d'un moyen de cryptologie. Même appliquée à la personne mise en cause, elle ne méconnaît pas le droit de ne pas contribuer à sa propre accusation, ni aucun autre droit ou liberté constitutionnellement garantis.*
> *En pratique, il s'avère que cette infraction est parfois retenue en cas de refus des personnes interpellées de donner le code d'accès de leur téléphone portable. Cette interprétation de l'article 434-15-2 du Code pénal apparaît en l'état erronée et a conduit à l'annulation de plusieurs procédures. En effet, l'infraction vise les moyens de cryptologie comme certaines applications (signal ou telegram par ex., L. n° 2004-575, 21 juin 2004, art. 29) ce que n'est pas un code d'accès à un téléphone qui correspond à un mécanisme d'authentification et non de cryptologie. On voit donc là que le droit se heurte en ce domaine à la technique particulièrement évolutive et donc source d'insécurité juridique. Une modification de l'article 434-15-2 du Code pénal visant non pas les moyens de cryptologie mais tous les dispositifs de blocage ou de verrouillage de*

téléphone permettrait aux enquêteurs d'accéder à des indices numériques souvent pertinents. »[33]

Ce point de vue était partagé par M. de Combles de Nayves, commentant l'arrêt de la cour d'appel de Paris du 16 avril 2019, ultérieurement censuré par la chambre criminelle[34], en ces termes :

> *2.2. Le code de déverrouillage n'est pas une convention secrète de déchiffrement :*
> *En second lieu, 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 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.*[35]

A l'inverse, le professeur Lepage retient que la cour d'appel de Paris a, dans ce même arrêt, sans doute donné au texte une interprétation plus restrictive que stricte alors que la frontière entre déverrouillage et déchiffrement ne lui parait pas si nette :

> *11. - Un autre point était plus délicat, qui avait trait à l'interprétation des termes « convention secrète de déchiffrement d'un moyen de cryptologie ». Précisément, le code de déverrouillage d'un téléphone portable constitue-t-il une telle convention ? (...)*
> *La cour d'appel de Paris, se référant à la définition du moyen de cryptologie que pose l'article 29 de la loi n° 2004-515 du 21 juin 2004, a considéré qu'« 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 ». La décision établit un lien logique entre code et accès qu'elle fait reposer implicitement sur une nette dissociation entre elles de deux acceptions de la notion d'accès. Si le code de déverrouillage permet, selon la cour d'appel de Paris, d'accéder aux données, c'est au sens de pénétration dans le système rendant possible l'utilisation des fonctionnalités du téléphone – au sens où un code permet l'accès à un système de traitement automatisé*

---

[33] JurisClasseur Procédure pénale, App. Art. 427 à 457 Fasc. 20 : la preuve numérique, Date de la dernière mise à jour : 18 Avril 2019, Mme Quéméner

[34] Crim., 13 octobre 2020, n° 20-80.150, précité

[35] AJ pénal 2019. 439

de données ou l'accès à un lieu physique tel un immeuble d'habitation. Celui qui, grâce au code de déverrouillage, moyen d'authentification, peut pénétrer dans le téléphone a accès à son contenu (contacts, messages, images, etc.) – au passage, on remarquera que la portée de la solution, circonscrite aux téléphones portables « d'usage courant », n'est pas très claire. Les données sont matériellement accessibles à l'utilisateur au sens où il peut les consulter. Pour autant cet accès matériel n'est pas nécessairement gage d'accès intellectuel, c'est-à-dire de compréhension. L'emploi d'une langue étrangère constitue un obstacle à un tel accès aisément surmontable par une traduction.

À une toute autre échelle, le déchiffrement permet de surmonter l'obstacle redoutable que la cryptologie oppose à la compréhension des données. Déchiffrées, les données se laissent pénétrer intellectuellement. Pour la cour d'appel, l'accès au contenu du téléphone, que permet le code de déverrouillage, ne doit donc pas être confondu avec l'accès intellectuel aux données cryptées qui, lui, est du ressort de la convention secrète de cryptologie. La solution procède à tout le moins d'une interprétation stricte. En distinguant nettement le code qui permet d'entrer de celui qui permet de déchiffrer, elle a pour elle le mérite d'une apparente simplicité qui ne déroute guère le profane en sécurité informatique. C'est peut-être ce qui en fait aussi sa limite, à telle enseigne qu'il est permis de se demander si cette interprétation n'est pas, somme toute, plus restrictive que stricte. La question se pose au regard de certains portables, tels ceux d'une des plus grandes marques de ce marché, qui associent le code de déverrouillage à une fonction automatique de protection des données. La création d'un fichier donne lieu à la création d'une clé permettant de le chiffrer et c'est le code de déverrouillage qui livre également des clés de déchiffrement (V. en ce sens W. Azoulay, obs. préc.). La frontière entre déverrouillage et déchiffrement n'est donc sans doute pas toujours aussi nette que celle que trace la présente décision. À telle enseigne qu'il faut souligner que même si le code de déverrouillage peut permettre de déchiffrer des données contenues dans le téléphone, il n'est pas certain qu'il constitue à proprement parler une convention de déchiffrement d'un moyen de cryptologie (V. en ce sens P. de Combles de Nayves, note préc.). En tout cas, dès lors que la présente décision les distingue en laissant le code de déverrouillage hors du champ de l'article 434-15-2 du Code pénal, demeure intacte en pratique l'immense difficulté du déverrouillage d'un téléphone portable quand son propriétaire ne veut pas en révéler le code ou que, celui-ci mort, personne d'autre que lui ne le connaît.[36]

Commentant les deux arrêts rendus par la chambre criminelle le 13 octobre 2020, le professeur Ribeyre retient que ce qu'il considère être une extension du champ d'application de l'article 434-15-2 du code pénal à la plupart des smartphones, pouvant s'appliquer à n'importe quel crime ou délit préparé ou facilité par un tel outil, paraît totalement disproportionnée alors qu'elle constitue une ingérence dans la vie privée de l'utilisateur du téléphone qui contient des données personnelles :

Reste à savoir enfin si le code de déverrouillage d'un téléphone portable constitue une convention de déchiffrement d'un moyen de cryptologie, ce qu'avait implicitement admis l'arrêt précité du 10 décembre 2019. La cour d'appel de Paris avait cependant répondu par la négative s'agissant d'un « téléphone portable d'usage courant ». Mais c'est précisément cette décision qui fait l'objet d'une cassation sans renvoi par le premier arrêt commenté, affirmant qu'« une convention secrète de déchiffrement 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 ». Cette définition peut s'appliquer au code d'un téléphone portable « lorsque ledit téléphone est équipé d'un moyen de cryptologie ». Si la référence à un « téléphone d'usage courant » manquait certes de précision, la solution presque intuitive des juges du fond n'est pas complètement invalidée par la

[36] A. Lepage, Un an de droit pénal du numérique, Droit pénal, n° 12, décembre 2019, p. 26

Cour de cassation puisque ce n'est que si le téléphone est équipé d'un moyen de cryptologie que son utilisateur récalcitrant pourra être condamné. La seconde espèce confirme cette analyse en indiquant que « le code de déverrouillage d'un téléphone portable constitue une convention de déchiffrement s'il permet de mettre au clair les données qu'il contient ». Ce sont donc uniquement les téléphones qui utilisent un procédé de chiffrement des données qui peuvent donner lieu à l'application de l'article 434-15-2. L'existence d'un moyen de cryptologie pourra « 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 ». Encore faudra-t-il que l'utilisateur du téléphone en soit conscient, ce pourquoi la Cour de cassation ajoute que ces résultats d'analyse seront portés à sa connaissance le cas échéant.

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.

Ne faudrait-il pas revenir à l'esprit initial du texte et le réserver aux appareils spécialement configurés pour les besoins des réseaux criminels – tout en privilégiant l'emploi de moyens de décryptage sans passer par le concours aléatoire des utilisateurs ?

En l'état du droit, l'incrimination, qui peut s'appliquer pour n'importe quel crime ou délit préparé ou facilité par un smartphone, paraît totalement disproportionnée alors qu'elle constitue une ingérence dans la vie privée de l'utilisateur du téléphone qui contient des données personnelles. Rappelons que le refus de répondre à la réquisition d'un enquêteur n'est punissable dans le Code de procédure pénale « que » de 3 750 € d'amende (CPP, art. 60-1) et qu'ici l'auteur du refus encourt 3 ans d'emprisonnement et 270 000 € d'amende. On peut au moins espérer que la jurisprudence écartera le cumul des peines avec celles des infractions qui sont à l'origine de ce délit revisité de l'article 434-15-2 du Code pénal.[37]

Dans un autre commentaire de ces mêmes arrêts, la solution est encore critiquée par M. A. Caprioli :

7 – Nonobstant l'intérêt pratique de cette décision, il serait préjudiciable à la sécurité juridique que la jurisprudence continue dans cette voie. En effet, cela engendre une interprétation trop large de l'article 434-15-2 et donne des contours d'autant plus flous concernant son champ d'application. D'ailleurs, en supposant que la décision aille vers le vrai, les difficultés pratiques apparaissent directement. Comment savoir, préalablement à la demande du code secret, si le téléphone en question est équipé d'un moyen de cryptologie ? L'officier de police judiciaire disposera-t-il d'une liste (mise à jour) des modèles et marques des appareils avec leurs fonctionnalités ? Que se passe-t-il si le code d'ouverture du téléphone se présente sous la forme d'une empreinte digitale ?

L'application de l'article ne peut donc être certaine lors des enquêtes de police. Il existe des conséquences qui vont plus loin que le cadre de l'article 434-15-2. En effet, quid de l'application de l'article 132-79 du Code pénal ? Par déduction, il devrait lui aussi s'appliquer aux codes de téléphones portables. Son champ d'application ne deviendrait-il pas trop large ? Cette hypothèse réduirait le contrôle de son étendue et serait susceptible de générer une perte d'efficacité.

[37] C. Ribeyre, Refus de remettre une convention secrète de déchiffrement, Dr. Pénal, n° 1, janvier 2021

Si le recours à l'article 434-15-2 du Code pénal a été peu utilisé jusqu'à maintenant, il est probable, avec son extension au code de déverrouillage du téléphone portable, que son usage se généralisera.
In fine, il va sans dire qu'une telle insécurité juridique n'était pas prévue par le législateur.[38]

Le professeur Dreyer est encore plus virulent dans sa critique des solutions adoptées tant par le Conseil constitutionnel que par la Cour de cassation en considérant que « l'interprétation extensive de l'incrimination pose problème tant est contestable la légitimité du délit ». Pour lui, « la lourdeur des peines fulminées, associée au lien étroit entre les données que l'autorité judiciaire cherche à décrypter et la culpabilité de l'intéressé, pourraient bien faire apparaître que la solution est excessive en ce qu'elle transforme le suspect en collaborateur du service public de la justice, ce qui constitue une inversion des rôles difficilement défendable ».[39]

4.4 La circonstance aggravante de l'article 132-79 du code pénal

La chambre criminelle ne parait pas avoir encore eu l'occasion de se prononcer sur l'application d'un autre texte dont l'interprétation pourrait être proche de celle donnée à l'article 434-15-2 du code pénal.

L'article 132-79 du code pénal prévoit une circonstance aggravante générale, élevant la peine encourue d'un degré, lorsqu'un moyen de cryptologie a été utilisé pour préparer ou commettre un crime ou un délit.

Art. 132-79 : Lorsqu'un moyen de cryptologie au sens de l'article 29 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique a été utilisé pour préparer ou commettre un crime ou un délit, ou pour en faciliter la préparation ou la commission, le maximum de la peine privative de liberté encourue est relevé ainsi qu'il suit :
1° Il est porté à la réclusion criminelle à perpétuité lorsque l'infraction est punie de trente ans de réclusion criminelle ;
2° Il est porté à trente ans de réclusion criminelle lorsque l'infraction est punie de vingt ans de réclusion criminelle ;
3° Il est porté à vingt ans de réclusion criminelle lorsque l'infraction est punie de quinze ans de réclusion criminelle ;
4° Il est porté à quinze ans de réclusion criminelle lorsque l'infraction est punie de dix ans d'emprisonnement ;
5° Il est porté à dix ans d'emprisonnement lorsque l'infraction est punie de sept ans d'emprisonnement ;
6° Il est porté à sept ans d'emprisonnement lorsque l'infraction est punie de cinq ans d'emprisonnement ;
7° Il est porté au double lorsque l'infraction est punie de trois ans d'emprisonnement au plus.
Les dispositions du présent article ne sont toutefois pas applicables à l'auteur ou au complice de l'infraction qui, à la demande des autorités judiciaires ou administratives, leur a remis la version en clair des messages chiffrés ainsi que les conventions secrètes nécessaires au déchiffrement.

[38] E. A. Caprioli, Cryptologie et communication du code du téléphone, Comm. - Commerce électronique, n° 1, janvier 2021

[39] E. Dreyer, L'OPJ, gardien de la liberté individuelle ? JCP, n° 51, 14 Décembre 2020, 1417

Ce texte est issu de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) et renvoie à son article 29 pour définir les moyens de cryptologie.

Il est visé par le moyen du pourvoi formé par le procureur général près la cour d'appel de Douai.

Plus que la portée générale de cette circonstance aggravante en cas d'utilisation d'un moyen de cryptologie, les travaux parlementaires ont surtout souligné la nouveauté consistant, comme le prévoit le dernier alinéa du texte, à en écarter l'application en cas de remise de la convention secrète nécessaire au déchiffrement des données.[40]

Le président Guérin souligne que, compte tenu de la jurisprudence de la chambre criminelle sur l'article 434-15-2 du code pénal, l'utilisation d'un téléphone équipé d'un logiciel de chiffrement des données pourrait constituer la circonstance aggravante prévue par l'article 132-79 du même code.[41]

4.5 Application en l'espèce

Dans la présente affaire, le prévenu a été relaxé tant par le tribunal correctionnel que par le premier arrêt de la cour d'appel de Douai du 11 juillet 2019. Le tribunal correctionnel avait établi une distinction entre la clé de chiffrement d'une application de messagerie et le code de déverrouillage du téléphone. La cour d'appel avait retenu que le code de déverrouillage d'un téléphone ne pouvait pas être qualifié de « convention secrète de déchiffrement » dès lors qu'il permet uniquement de débloquer l'usage de l'écran tactile pour permettre l'accès à l'ensemble des données contenues dans le téléphone.[42]

Cette motivation a été censurée par l'arrêt de la chambre criminelle précité du 13 octobre 2020 *(pourvoi n° 19-85.984*) qui retient que « le code de déverrouillage d'un téléphone mobile constitue une convention de déchiffrement (...) 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 ».

Statuant sur renvoi après cassation, la cour d'appel de Douai a confirmé la relaxe du prévenu en indiquant que « la mise en oeuvre 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 » puis 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 29 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 ».

La cour d'appel limite ainsi l'utilisation d'un moyen de cryptologie au seul envoi des données alors que, d'un simple point de vue technique, il est acquis, au contraire, que le chiffrement des données peut aussi concerner celles qui sont stockées sur l'appareil. En ce qui concerne l'aspect juridique de cette question, l'article 29 de la loi n° 2004-575 du 21 juin 2004 indique que les moyens de cryptologie ont « principalement pour objet de garantir la sécurité du

---

[40] Rapports de M. Jean Dionis du Séjour (n° 612), Mme Tabarot (n° 608) et M. Türk (n° 351)

41 Jurisclasseur pénal, Art. 132-71 à 132-80, Fasc. 20, n° 267

[42] Rapport de M. de Larosière de Champfeu et conclusions de M. Valleix pour le pourvoi n° 19-85.984

stockage ou de la transmission de données » sans établir de distinction particulière entre ces deux opérations.

Lorsqu'un tel moyen de cryptologie est utilisé, la clé de déchiffrement, permettant de mettre au clair les données sauvegardées, est mise en oeuvre par la composition du code d'accès au téléphone sur cet appareil. Cette technique, désormais généralisée sur l'ensemble des nouveaux smartphones, n'était toutefois pas utilisée sur les appareils les plus anciens.

Il appartiendra donc à l'assemblée plénière de la Cour de cassation de dire si le code permettant d'accéder à un téléphone portable est une convention secrète de déchiffrement d'un moyen de cryptologie, au sens de l'article 434-15-2 du code pénal, à charge pour le juge de fond de rechercher si l'appareil concerné met en oeuvre une telle technologie.