COUR DE CASSATION

Notice au rapport relative à l'arrêt n°659 du 7 novembre 2022
Pourvoi n° 21-83.146 – Assemblée plénière

Par le présent arrêt, l'assemblée plénière de la Cour de cassation confirme l'interprétation déjà donnée aux dispositions de l'article 434-15-2 du code pénal par la chambre criminelle (Crim., 13 octobre 2020, pourvoi n° 19-85.984) mais que la cour d'appel de Douai, saisie sur renvoi après cassation, avait refusé de suivre.

L'article 434-15-2 a été introduit dans le code pénal par la loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne dont l'adoption a été consécutive aux attentats commis aux États-Unis le 11 septembre précédent. Il s'agit toutefois de dispositions préparées de longue date pour tenter de trouver un équilibre entre, d'une part, le développement des moyens de cryptologie, qui favorisent un meilleur respect de la vie privée, de la liberté d'expression et de la sécurité des affaires, et, d'autre part, la lutte contre la cybercriminalité ou la préservation des pouvoirs d'enquête des autorités publiques, compromis par la large diffusion de ces nouveaux outils.

L'utilisation de ce texte pour obtenir la remise du code d'accès à un téléphone portable n'avait certainement pas été envisagée par le législateur en 2001 et pose plusieurs questions qui n'ont toutefois pas été toutes soumises par le pourvoi à l'assemblée plénière de la Cour de cassation.

Saisi en 2018 d'une question prioritaire de constitutionnalité par la chambre criminelle[1], le Conseil constitutionnel a jugé que les dispositions de ce texte, même appliquées à la personne suspectée d'avoir commis une infraction, ne portent pas atteinte à son droit de ne pas faire de déclaration et à celui de ne pas contribuer à sa propre incrimination[2].

La chambre criminelle de la Cour de cassation a ensuite eu l'occasion, notamment par trois arrêts publiés en 2019, 2020 et 2021, de juger que ces dispositions sont applicables au refus de communiquer le code d'accès à un téléphone portable, opposé

[1] Crim., 10 janvier 2018, QPC n° 17-90.019.

[2] Cons. const., 30 mars 2018, décision n° 2018-696 QPC, M. Malek B. [Pénalisation du refus de remettre aux autorités judiciaires la convention secrète de déchiffrement d'un moyen de cryptologie].

à une demande des autorités judiciaires, lorsque cet appareil est susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, quel qu'il soit. Elle a précisé qu'il appartient aux juges du fond 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 donc pas à permettre l'accès aux données qu'il contient mais constitue bien une convention de déchiffrement permettant aussi de les mettre au clair[3].

Une grande partie de la doctrine a critiqué ces solutions en considérant que l'interprétation donnée au texte était trop large, compte tenu de son champ d'application et de l'ingérence ainsi permise dans la vie privée des utilisateurs de smartphones, et en affirmant que le code d'accès à un téléphone portable n'est pas une convention de déchiffrement d'un moyen de cryptologie mais un simple mécanisme d'authentification.

L'assemblée plénière de la Cour de cassation confirme donc ici que le code permettant de déverrouiller l'écran d'accueil d'un téléphone peut être, lorsque cet appareil est équipé d'un moyen de cryptologie, une convention secrète de déchiffrement au sens de l'article 434-15-2 du code pénal.

D'un simple point de vue technique, il est acquis que l'immense majorité des smartphones récents (depuis 2011 pour Apple et 2015 pour Android) « implémentent de série et par conception un mécanisme de chiffrement des données » enregistrées dans la mémoire de l'appareil, qu'il s'agisse des messages échangés, des listes des contacts, des enregistrements sonores, des photographies, des textes ou des fichiers les plus divers. Ceci ressort notamment d'un rapport de la division technique du commandement de la gendarmerie dans le cyberespace, établi à la demande de l'avocat général pour le traitement de cette affaire. Ce système de chiffrement est désormais installé par défaut sur les appareils et s'impose le plus souvent aux utilisateurs même s'il peut exister quelques rares exceptions, liées soit à une intervention délibérée de l'utilisateur, soit à l'utilisation d'un modèle ancien ou particulier.

La notion de « convention secrète » de déchiffrement remonte à la loi n° 90-1170 du 29 décembre 1990 sur la réglementation des télécommunications qui avait amorcé le mouvement de libéralisation des moyens de cryptologie et entendait trouver un équilibre entre les intérêts de la sécurité de l'État, la protection des informations et le développement des communications ou des transactions sécurisées. Cette loi avait libéralisé l'utilisation des moyens de cryptologie mais uniquement lorsque les fonctions de confidentialité étaient assurées par des prestataires agréés conservant une « convention secrète de déchiffrement » pouvant être remise aux autorités en cas de réquisition. Pour tenir compte de l'évolution très rapide en la matière, la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, qui entendait lever les restrictions encore imposées au développement de la cryptologie, a notamment étendu la définition des moyens de cryptologie et supprimé les organismes agréés devant détenir des conventions secrètes de déchiffrement.

De telles conventions de déchiffrement restent toutefois visées par les articles L. 871-1 et R. 871-3 du code de la sécurité intérieure et ce dernier texte définit très largement les conventions de déchiffrement comme les « clés cryptographiques [ou] tout moyen logiciel ou toute autre information permettant la mise au clair de ces données ». Ces

[3] Crim., 10 décembre 2019, pourvoi n° 18-86.878, publié au *Bulletin* ; Crim., 13 octobre 2020, pourvoi n° 20-80.150, publié au *Bulletin* ; Crim., 13 octobre 2020, pourvoi n° 19-85.984 ; Crim., 12 janvier 2021, pourvoi n° 20-84.045, publié au *Bulletin*.

textes s’appliquent, en matière d’interceptions administratives, aux seuls prestataires des moyens de cryptologie. Ils ont donc un champ d’application différent de l’article 434-15-2 du code pénal, ce qui explique que les arrêts ne les visent pas même s’ils reprennent cette définition en indiquant que « la convention de déchiffrement, visée par ce texte, 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 ».

Pour tenir compte de la diversité des appareils en circulation, des possibles exceptions au principe d’un chiffrement des smartphones par défaut et de l’évolution des technologies, l’assemblée plénière n’a pas retenu que tout téléphone portable est équipé d’un moyen de cryptologie mais a jugé qu’il appartient au juge, en cas de poursuites sur le fondement de l’article 434-15-2 du code pénal, de le rechercher et de vérifier alors si le code de déverrouillage permet de mettre au clair tout ou partie des données cryptées, qui sont stockées dans sa mémoire ou auxquelles il peut donner accès à distance.

L’assemblée plénière de la Cour de cassation a donc cassé l’arrêt de la cour d’appel de Douai qui avait limité, à tort, l’utilisation d’un moyen de cryptologie au seul envoi des données à l’occasion d’une communication alors que le chiffrement concerne aussi la sauvegarde des données stockées dans la mémoire d’un appareil. En effet, l’article 29 de la loi n° 2004-575 du 21 juin 2004 précitée prévoit expressément que les « moyens de cryptologie ont principalement pour objet de garantir la sécurité du stockage ou de la transmission de données ».

La cour d’appel avait en outre retenu que le code de déverrouillage d’un téléphone portable ne vise pas à rendre compréhensibles des données mais tend seulement à permettre d'accéder aux données et aux applications d'un téléphone alors qu’il lui appartenait de rechercher si les codes de déverrouillage des téléphones en cause permettaient ou non de traduire en clair des données qui étaient cryptées. La chambre criminelle de la Cour de cassation avait précisé à ce sujet que la présence d’un tel moyen de cryptologie sur l’appareil peut se déduire de ses caractéristiques ou des logiciels qui l'équipent ou être déterminée au moyen d’une expertise ordonnée à cette fin[4].

[4] Crim., 13 octobre 2020, pourvoi n° 20-80.150, publié au *Bulletin*.