



**HAL**  
open science

## Code de déverrouillage d'un téléphone portable

Matthieu Audibert

► **To cite this version:**

Matthieu Audibert. Code de déverrouillage d'un téléphone portable. Veille juridique, 2020. hal-02991975

**HAL Id: hal-02991975**

**<https://hal.science/hal-02991975v1>**

Submitted on 19 Nov 2020

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

*Capitaine Matthieu AUDIBERT*

## JURISPRUDENCE JUDICIAIRE

### Code de déverrouillage d'un téléphone portable

*Cour de cassation – Chambre criminelle – Arrêt n° 1804 du 13 octobre 2020 n° 20-80.150*

Le code de déverrouillage d'un téléphone portable peut constituer « *une convention secrète de déchiffrement d'un moyen de cryptologie* » au sens de l'article 434-15-2 du Code pénal. Le fait de refuser de communiquer le code de déverrouillage de son téléphone à la demande officielle d'un officier de police judiciaire est une infraction au sens de l'article susvisé, dès lors qu'il est démontré que ce code a un impact sur le chiffrement des données du téléphone et que ce téléphone est susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit.

L'article 434-15-2 du Code pénal sanctionne 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 œuvre, sur les réquisitions de ces autorités délivrées en application des titres II et III du livre Ier du code de procédure pénale (...)* ».

Le « moyen de cryptologie » est défini par l'article 29 de la loi

**Droit de l'espace numérique**

[n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique \(LCEN\)](#).

*Ainsi, « 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 ».*

Le 8 mars 2017, Malek B. est interpellé par des fonctionnaires de police pour avoir acquis, détenu et transporté sans autorisation des produits stupéfiants. Placé en garde à vue, il refuse de communiquer le code de déverrouillage de l'un de ses téléphones et argue de son droit au silence. Dès lors, il est renvoyé devant le tribunal correctionnel de Créteil le 10 mars 2017 pour avoir acquis, détenu et transporté sans autorisation des produits stupéfiants et pour avoir refusé de communiquer le code de déverrouillage de son téléphone.

Le prévenu a alors soulevé une question prioritaire de constitutionnalité (QPC) devant le tribunal correctionnel en arguant notamment que l'article 434-15-2 précité ne permettrait pas au mis en cause de faire usage de son droit au silence et serait contraire au droit de ne pas s'auto-incriminer. Dans un arrêt du 10 janvier 2018<sup>5</sup>, la Chambre criminelle de la Cour de cassation a jugé que cette

---

<sup>5</sup>. Criminelle, 10 janvier 2018 n° 17-90.019.

**Droit de l'espace numérique**

question n'avait pas été examinée par le Conseil constitutionnel et présentait dès lors un caractère sérieux justifiant sa saisine.

Dans sa [décision n° 2018-696 QPC du 30 mars 2018](#), le Conseil constitutionnel rejette les arguments soulevés par la défense de Malek B. En effet, le fondement juridique de cette infraction s'attache, d'une part, à la poursuite par le législateur d'une volonté de protéger la prévention des infractions et, d'autre part, à la recherche de leurs auteurs, ces deux objectifs étant nécessaires à la sauvegarde de droits et de principes à valeur constitutionnelle.

Ainsi, cette infraction ne méconnaît pas le droit ne pas contribuer à sa propre incrimination, ni le droit au respect de la vie privée, les droits de la défense, le principe de proportionnalité des peines ou encore la liberté d'expression. Cette infraction est donc conforme à la Constitution. Toutefois, le Conseil constitutionnel pose deux conditions : d'une part, la demande doit émaner de l'autorité judiciaire, garante du procès équitable, d'autre part, ce moyen de cryptologie doit être susceptible d'avoir été utilisé pour « *préparer, faciliter ou commettre une infraction* ».

Cette seconde condition exige que les investigations préalablement réalisées dans le cadre d'une enquête ou d'une information judiciaire aient mis en évidence un lien entre ces données et la préparation, la facilitation ou la commission d'une infraction.

En outre, le Conseil constitutionnel rappelle que cette disposition n'a ni pour objet d'obtenir des aveux de la part du mis en cause, ni de reconnaître ou poser une présomption de culpabilité, mais simplement de permettre le déchiffrement de données chiffrées par la personne ayant connaissance de cette convention<sup>6</sup>.

<sup>6</sup>. LACAZE M., Constitutionnalité du refus de remise d'une convention secrète de déchiffrement, AJ Pénal 2018, p. 257.

## **Droit de l'espace numérique**

Sur ce point, il convient de souligner que la Chambre criminelle a adopté la même position que le Conseil constitutionnel au regard de l'article 6 de la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales, par un arrêt du 10 décembre 2019<sup>7</sup>.

L'article 434-15-2 du Code pénal a fait donc l'objet d'un contrôle de constitutionnalité et d'un contrôle de conventionnalité favorables.

Fort de l'analyse du Conseil constitutionnel, le tribunal correctionnel condamna Malek B. pour cette infraction. Celui-ci fit appel et la Cour d'appel de Paris a alors examiné si le fait pour Malik B. de refuser de communiquer le code de déverrouillage de son téléphone au fonctionnaire de police était constitutif ou non de l'infraction prévue par l'article 434-15-2 du Code pénal.

S'agissant de la réquisition délivrée par les autorités judiciaires, la Cour d'appel relève qu'aucun élément ne ressort de la procédure tendant à démontrer qu'une réquisition avait été adressée par une autorité judiciaire à Malek B. afin qu'il communique le code de déverrouillage de son téléphone, ce dernier n'ayant opposé son refus qu'à un fonctionnaire de police. Ainsi, pour la Cour d'appel de Paris, les officiers de police judiciaire ne font pas partie de l'autorité judiciaire qui comprend les magistrats du Parquet et ceux du siège<sup>8</sup>.

Concernant le « moyen de cryptologie », la Cour d'appel s'appuie

---

<sup>7</sup>. Criminelle, 10 décembre 2019, n° 18-86.878.

<sup>8</sup>. Conseil constitutionnel, 11 août 1993, n° 93-326 DC, §5.

## Droit de l'espace numérique

sur l'article 29 de la LCEN précité pour juger que, concernant les téléphones portables d'usage courant, le code de déverrouillage permet d'accéder aux données qu'il contient, et donc à ses messages, mais ne permet pas en revanche de déchiffrer les données contenues. Le code de déverrouillage n'est pas donc pas, pour la Cour d'appel, une convention secrète de chiffrement d'un moyen de cryptologie.

Pour ces deux motifs, la Cour d'appel de Paris a prononcé la relaxe de Malek B. s'agissant de l'infraction prévue par l'article 434-15-2 du Code pénal par arrêt du 16 avril 2019<sup>9</sup>.

Cet arrêt de la Cour d'appel de Paris était très critiquable. En effet, qu'il s'agisse des téléphones fonctionnant sous Android ou iOS, les données sont automatiquement chiffrées, soit par un système AES-128 bits (Android), soit par AES-256 bits (Apple). Ces systèmes sont directement implémentés dans le smartphone de manière physique via une puce intégrée (Soc « system on a chip » fonctionnant comme un microprocesseur) qui génère elle-même la clé, intrinsèquement inaccessible au constructeur comme à l'utilisateur. Elle est en effet située dans un environnement sécurisé nommé « TEH » (Trusted Execution Environment).

Toutefois, considérer qu'un code de téléphone n'est pas une convention secrète de déchiffrement n'est pas évident, ce code ne pouvant être réduit à une simple fonction d'authentification. Pour reprendre les termes de la professeure Agate LEPAGE, « *certaines*

---

<sup>9</sup>. Paris, 16 avril 2019, n° 18/09267.

## Droit de l'espace numérique

*portables (...) associent le code de déverrouillage à une fonction automatique de protection des données »<sup>10</sup>.*

Pour abonder en ce sens, la documentation technique des constructeurs, notamment Apple, apporte des précisions. Le guide de sécurité du système d'exploitation iOS, dans sa version de mai 2019 que la société a rendu publique, expose qu'à chaque fois qu'un fichier est créé, le système de protection des données crée une nouvelle clé permettant de le chiffrer (p. 16).

S'agissant du code de déverrouillage, il est indiqué (p. 20) que, par la configuration d'un code sur l'appareil, l'utilisateur active la protection des données de façon automatique. Il est par ailleurs précisé (p. 21) que plus le code est complexe et long, plus la clé de chiffrement l'est. Nous pouvons donc en conclure que, pour ce type d'appareils, la typologie et la dureté du code de déverrouillage ont un impact sur la clé de chiffrement des données contenues dans le terminal. Dès lors, la fonction du code de déverrouillage dépasse le simple mécanisme d'authentification et a un rôle sur le chiffrement et donc le déchiffrement des données présentes dans le téléphone.

Pour les téléphones fonctionnant sous Android, il est possible de chiffrer l'intégralité d'une mémoire de stockage. Cette fonction est nommée « Full Disk Encryption » et existe depuis la version 5.0 d'Android. Le système utilise une clé de chiffrement de 128 bits dénommée clé DEK. Celle-ci est elle-même chiffrée par une clé dite clé KEK. La clé KEK est créée à partir du code de déverrouillage de l'utilisateur. Depuis la version 7 d'Android, il est possible de chiffrer

---

<sup>10</sup>. LEPAGE A., Un an de droit pénal du numérique, Dr. Pén. 2019, n° 12.

## Droit de l'espace numérique

individuellement les fichiers (File Based Encryption ou FBE). Avec cette fonction, un fichier est chiffré par AES avec une clé DEK de 512 bits. La clé DEK est ensuite chiffrée par une autre clé de 256 bits (clé KEK). La clé KEK est stockée dans une zone sécurisée du téléphone qui est isolée et indépendante du système Android (zone TEE).

Pour obtenir cette clé KEK afin de déchiffrer les données, il faut trois éléments cumulatifs : le code d'authentification créé lors de la connexion de l'utilisateur, une somme de contrôle (*hash*) calculée à partir d'un fichier stocké dans l'espace de l'utilisateur, un code nommé Stretched Credential calculé par une fonction de dérivation de clé qui utilise le code de déverrouillage de l'utilisateur. Ainsi, ce code de déverrouillage créé par l'utilisateur est indispensable pour récupérer la clé KEK afin de déchiffrer les données. Il a donc un rôle sur le chiffrement des données présentes dans le téléphone<sup>11</sup>.

Suite à l'arrêt de la Cour d'appel de Paris, il convient de relever que le Parquet général près la cour d'appel ne s'est pas pourvu en cassation. Toutefois, cet arrêt était susceptible d'engendrer des conséquences fâcheuses pour les enquêteurs. Depuis les révélations d'Edward Snowden, le grand public a largement adopté les applications de communication chiffrées. En outre, les fabricants de téléphones et les concepteurs des systèmes d'exploitation et d'applications ont largement renforcé la sécurité des terminaux. Ainsi, comme le notent Benoist Hurel et Vincent Lemonier, « *aujourd'hui, il n'est malheureusement pas exagéré d'affirmer que*

---

<sup>11</sup>. *Connection between PIN/password and encryption keys in Android*. Disponible sur : <https://security.stackexchange.com/questions/196230/connection-between-pin-password-and-encryption-keys-in-android>



## Droit de l'espace numérique

*des enquêtes portant sur des structures criminelles majeures sont rendues impossibles, ou sont extrêmement ralenties, par l'utilisation de messageries cryptées que les enquêteurs ne peuvent pas intercepter en temps réel »<sup>12</sup>.*

Ainsi, comme le prévoit l'article 620 du Code de procédure pénale et suite à l'ordre formel donné par le ministre de la Justice, le procureur général près la Cour de cassation s'est pourvu en cassation dans l'intérêt de la loi. Ce pourvoi particulier permet au procureur général près la Cour de cassation de dénoncer à la Chambre criminelle des « *actes judiciaires, arrêts ou jugements contraires à la loi, ces actes, arrêts ou jugements peuvent être annulés* ». Si l'arrêt est rendu en dernier ressort, ce qui est le cas en l'espèce de l'arrêt de la Cour d'appel de Paris, et que le pourvoi est accueilli, « *la cassation est prononcée, sans que les parties puissent s'en prévaloir et s'opposer à l'exécution de la décision annulée* »<sup>13</sup>.

Dans ce pourvoi, deux questions étaient posées à la Chambre criminelle :

- Un officier de police judiciaire peut-il demander à un mis en cause de communiquer le code de déverrouillage d'un téléphone portable et, si la réponse est affirmative, sous quelle forme ?
- Le code de déverrouillage d'un téléphone portable peut-il constituer une convention secrète de déchiffrement d'un moyen

---

**12.** HUREL B., LEMONIER V., L'enquête pénale à l'épreuve du chiffrement, *Délibérée*, vol. 4, n° 2, 2018, p. 53-57.

**13.** Article 621 du Code de procédure pénale.

**Droit de l'espace numérique**

de cryptologie ?

Concernant la première question, la Cour d'appel a noté qu'aucune réquisition n'a été adressée par une autorité judiciaire à Malek B. de communiquer son code de déverrouillage, celui-ci ayant seulement refusé de communiquer ce code à la suite d'une demande qui lui a été faite au cours de son audition par un fonctionnaire de police. Sur ce point, la Chambre criminelle considère que la Cour d'appel a justifié sa décision.

Toutefois elle précise que « *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* ». Elle indique également 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* ».

Autrement dit, l'officier de police judiciaire qui demande le code de déverrouillage d'un téléphone doit matérialiser sa demande et avertir le mis en cause que son éventuel refus constituerait l'infraction prévue par l'article 434-15-2 du Code pénal.

À ce titre, la motivation de la Chambre criminelle est parfaitement logique.

## Droit de l'espace numérique

En effet, il convient de rappeler que les dispositions citées en référence à ce même article, « *titres II et III du livre 1<sup>er</sup> du code de procédure pénale* », renvoient aux pouvoirs généraux de réquisitions des officiers de police judiciaire, à savoir les articles 60, 60-1, 60-2 dans le cadre de l'enquête de flagrance, 77-1-1, 77-1-2 dans le cadre de l'enquête préliminaire et 99-3 et 99-4 dans le cadre de l'information judiciaire. En outre, « *la police judiciaire est exercée, sous la direction du procureur de la République, par les officiers, fonctionnaires et agents désignés au présent titre* »<sup>14</sup>. De plus, « *le procureur de la République procède ou fait procéder à tous les actes nécessaires à la recherche et à la poursuite des infractions pénales. À cette fin, il dirige l'activité des officiers et agents de la police judiciaire dans le ressort de son tribunal. Il peut, en outre, requérir tout officier de police judiciaire, sur l'ensemble du territoire national, de procéder aux actes d'enquête qu'il estime nécessaires dans les lieux où chacun d'eux est compétent (...)* »<sup>15</sup>.

S'agissant de la seconde question, la Cour d'appel avait écarté la possibilité pour le code de déverrouillage de constituer une convention secrète de déchiffrement d'un moyen de cryptologie. Elle indiquait 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* ».

---

<sup>14</sup>. Article 12 du Code de procédure pénale.

<sup>15</sup>. Article 41 du Code de procédure pénale.

## Droit de l'espace numérique

Sur ce point, la Chambre criminelle adopte une position radicalement différente de celle de la Cour d'appel. Elle rappelle 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* ». Elle conclut, dès lors, par une formule lapidaire : « *le code de déverrouillage d'un téléphone portable peut constituer une telle convention lorsque ledit téléphone est équipé d'un moyen de cryptologie.* »

Faisant œuvre de pédagogie, elle explique le raisonnement *in concreto* que les juges du fond doivent adopter. Ainsi, « *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* » .

Autrement dit, il faut justifier dans la procédure que le code de déverrouillage a un rôle sur le chiffrement du téléphone. Ce qui est le cas, comme nous l'avons démontré, des téléphones fonctionnant sous iOS ou Android. Cela inclut également d'éventuelles applications chiffrées de communication. En outre, la Chambre criminelle précise que ce lien peut être démontré par les résultats d'exploitation des téléphones au moyen d'outils. Il s'agit ici des outils de criminalistique numérique qui équipent les enquêteurs. Connecter le téléphone à ces outils et tenter d'extraire les données

## Droit de l'espace numérique

sans code de déverrouillage caractérise là encore le lien entre code de déverrouillage et chiffrement des données. Les enquêteurs et les juges du fond doivent donc rentrer dans les caractéristiques des téléphones, la Chambre criminelle jugeant « *inopérante* » la notion de téléphone d'usage courant.

La Chambre criminelle casse et annule logiquement l'arrêt de la Cour d'appel et ce, dans le seul intérêt de la loi. Cet arrêt n'est donc pas opposable à Malek B. qui demeure relaxé sur ce fondement.

En conclusion, il résulte de cet arrêt que l'infraction est susceptible d'être caractérisée, dès lors qu'une personne refuse de donner le code de déverrouillage de son téléphone sous réserve des quatre conduites suivantes :

- Une demande de remise du code est formulée en procédure :
  - Dans le cadre de l'enquête, par le procureur de la République, l'officier de police judiciaire ou, sous le contrôle de ce dernier, par l'agent de police judiciaire<sup>16</sup>,
  - Dans le cadre de l'instruction préparatoire, par le juge d'instruction ou l'officier de police judiciaire ;
- Il est rappelé à la personne que le refus de répondre à la réquisition est constitutif d'une infraction pénale ;

---

<sup>16</sup>. Depuis la loi du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice, l'agent de police judiciaire, dans le seul cadre de l'enquête et sous le contrôle de l'officier de police judiciaire, peut également adresser ce type de réquisition.

## **Droit de l'espace numérique**

- Les caractéristiques de l'appareil objet de la réquisition, les logiciels qui l'équipent ou les résultats de son exploitation au moyen d'outils techniques, révèlent qu'il est doté d'un moyen de cryptologie<sup>17</sup>;
- Le téléphone a été utilisé pour préparer, faciliter ou commettre un crime ou un délit.

Si le chiffrement est utile pour protéger la vie privée, un consensus nécessairement raisonnable doit aboutir. Un chiffrement sans aucune limite servirait davantage les intérêts des malfaiteurs que ceux des citoyens. Cette exception prévue par la loi et exercée sous le contrôle de l'autorité judiciaire permet d'y parvenir à la lumière de l'arrêt rendu par la Chambre criminelle.

---

<sup>17</sup>. Ce qui est le cas, comme nous l'avons démontré, de la plupart des téléphones fonctionnant sous iOS ou Android au regard de leurs caractéristiques techniques, le code de déverrouillage du terminal défini par l'utilisateur faisant en effet partie intégrante de la chaîne de chiffrement et de déchiffrement des données qu'il contient.