7 novembre 2022

Cour de cassation

Pourvoi n° 21-83.146

Le téléphone personnel est un antre de données intimes. Celles-ci sont trop nombreuse et trop importantes pour permettre dans le cadre d'une enquête l'accès à des policiers pour pouvoir obtenir des informations spécifiques dans le cadre de l'enquête poursuivie. C'est pourquoi la Cour de cassation en son assemblée plénière a enfin tranché sur la question : Est-ce qu'un code de sécurité de téléphone doit être donné dans le cadre d'une enquête de police ? En effet la question a été soulevé après les refus multiple des Cours d'appel de condamner un suspect dans un trafic de stupéfiants pour avoir refusé de donner les codes des 2 portables trouvé en sa possession lors de son arrestation. Il fallait donc pour la Cour de cassation de fermement mettre en place cette obligation de donner le code de téléphone malgré la possibilité d'atteinte aux données personnelles.

Faits : A la suite d'une arrestation dans le cadre d'une enquête pour infractions à la législation sur les stupéfiants, le suspect a refusé de communique aux enquêteurs les mots de passe des deux smartphones découverts en sa possession lors de son interpellation. Cette personne fût poursuivi pour détention et offre ou cession de cannabis ainsi que pour le refus de remettre le code de ces smartphones susceptible d'avoir été utilisé pour les besoins d'un trafic de stupéfiants.

Procédure : Par jugement du 15 mai 2018 le tribunal correctionnel l'a condamné pour infraction à la législation sur les stupéfiants, mais l'a relaxé sur le terrain du délit de refus de remettre ou de mettre en œuvre la convention secrète d'un moyen de cryptologie. Cette relaxe a été confirmé par la Cour d'appel de Douai dans un arrêt du 11 juillet 2019. Celui-ci a été cassé et annulé par la Cour de cassation en sa chambre criminelle le 13 octobre 2020 puis renvoyé devant la cour d'appel de Douai qui a confirmé la relaxe du suspect le 20 avril 2021. Cela a résulté en un pourvoi en cassation par le procureur général à la cour d'appel qui a amené la chambre criminelle de la Cour de cassation à renvoyer l'affaire devant l'assemblée

plénière.

Problème de droit : Cela pose le problème suivant à la Cour de cassation : peut-on considérer le code d'un téléphone comme étant l'équivalent d'une convention secrète de déchiffrage d'un moyen de cryptologie et donc obliger dans le cadre d'une enquête pour stupéfiants de le donner pour les besoins de l'enquête.

Solution de la Cour : La Cour de cassation, en vertu des articles 434-15-2 du code pénal et de 29 de la loi n°2004-57 du 21 juin 2004 pour la confiance dans l'économie numérique, a considéré que selon le premier texte, la connaissance ou possession d'un moyen de cryptologie doit être remis dans le cadre de réquisitions s'il a été susceptible d'avoir été utilisé pour préparer faciliter ou commettre un crime ou un délit. Sur le second texte, un moyen de cryptologie s'entend être tout matériel ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'information ou de signaux, à l'aide de conventions secrètes ou pour réaliser l'opération inverse avec ou sans convention secrète. Les moyens de cryptologie ont principalement pour objet de garantir la sécurité du stockage ou de la transmission de données. La Cour a déterminé que la cour d'appel a violé les textes susvisés en ne considérant pas le code de verrouillage des smartphones comme étant des moyens de cryptologie au sens du second texte pour l'application du premier texte.

Note :

La question du déverrouillage d'un téléphone dans le cadre d'une enquête amène une plus grande difficulté que l'on ne pourrait penser. En effet, qu'est-ce qu'un téléphone de nos jours ? Un outil que chaque personne (ou presque) transporte sur soi-même où qu'ils aillent ou font. Ces bijoux de technologie sont dotés de capacités permettant de retracer la vie entière d'une personne depuis l'obtention de l'objet. Que ce soit un accès à un réseau social, des messages personnels ou encore, le type d'application que la personne possède, tous ces éléments de données personnelles vont bien au-delà d'une quelconque enquête et touche un trop grand nombre d'information portant atteinte directement non seulement à la protection des données personnelles (RGPD, *Loi n° 78-17* du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.) mais aussi au droit à la vie privée (DUDH, article 9 Code civil).

C’est bien sûr l’un des éléments qui amène les droits à rentrer en conflit entre eux. L’enquêteur et la Police, dans le cadre d’une enquête où des enjeux justifient l’atteinte à la vie privée il est difficile de juger si l’action de donner l’accès à un téléphone est réellement proportionnel aux besoins de l’enquête. Le téléphone étant un élément extrêmement lié à la vie privée est définitivement dans une différente magnitude qu’une simple base de données. Le téléphone est un outil qui joue dans chaque instant de la vie que ce soit l’agenda ou les contacts téléphonique. Un accès à celui-ci ne peut être considéré qu’avec la prise en compte de l’atteinte grave à la vie privée du propriétaire au point de pouvoir le considérer plus grave encore qu’une fouille d’un appartement, et ce n’est pas quelque chose qui va diminuer dans le futur au vu du développement technologique et societal qui tourne toujours plus autour du téléphone.

C’est pourquoi d’un côté, la cour d’appel à assurément tort dans le sens d’aide à l’enquête de refuser une obligation d’ouverture du téléphone, dans ce cas précis, cela permettrait de retrouver les acheteurs ou vendeurs de stupéfiants et peut être de démanteler toute l’opération. En revanche, d’un autre côté, la Cour de cassation n’a pas fait preuve de précision dans sa décision, en considérant que l’article 434-15-2 du code pénal devait s’appliquer de la même manière que pour un simple logiciel ou base de données, ceux-ci ne contenant pas une quantité pour certaines personnes presque incalculable de données personnelles.

Il faut néanmoins reconnaitre que la logique de la Cour de cassation se tient, l’article 29 de la loi n°2004-57 du 21 juin 2004 pour la confiance dans l’économie numérique détermine en effet la définition du moyen de cryptologie qui vise ici un grand nombre de système électroniques et numériques. Et son application textuelle ne pose pas réellement de problème non plus, le texte du code pénal énonçant le terme clair de moyen de cryptologie, cela signifie qu’il n’y a aucun problème en termes de texte.

Le problème est beaucoup plus présent dans le fait que son application donne une portée beaucoup plus vaste que l’on ne pouvait considérer lors de l’écriture de l’article en 2004, car l’atteinte au droit à la vie privée et la sécurité des données personnelles est beaucoup trop vaste grâce à ce texte. La définition est trop large et combinée avec l’article du code pénal, donne une liberté d’accès à un très grand nombre d’appareils ce qui va au-delà et en deçà de ce que le texte prévoyait.

Il faut de plus noter que l'avocat général, dans son rapport à fait remarque le nombre extrêmement bas d'utilisation de l'article du code pénal depuis sa création du fait que celui-ci se supposait limité à des outils spécifiques. Mais grâce au texte de 2004, le texte soudainement possède une portée bien trop grande et une atteinte particulièrement problématique aux droits des personnes.

Il faut espérer qu'une précision sur ce sujet viendra au plus tôt afin de séparer les bases de données, des téléphones ou autre ordinateurs protégés d'un mot de passe afin de renforcer la protection des données personnelles et faciliter le travail des enquêteurs pour qu'ils n'aient pas à porter une atteinte disproportionnée à ces droits.

Arrêt :

7 novembre 2022
Cour de cassation
Pourvoi n° 21-83.146
Assemblée plénière

Vu les articles 434-15-2 du code pénal et 29 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique :

10. Selon le premier de ces textes, est punissable toute personne qui, 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, refuse de la remettre 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.

11. Selon le second, un moyen de cryptologie s'entend de 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 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.

12. Pour l'application du premier de ces textes et au sens du second, 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, que ce soit à l'occasion de son stockage ou de sa transmission. 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.

13. Dès lors, il incombe au juge de rechercher si le téléphone en cause est équipé d'un tel moyen et si son code de déverouillage permet de mettre au clair tout ou partie des données cryptées qu'il contient ou auxquelles il donne accès.

14. Pour confirmer la relaxe, l'arrêt retient que la clé de déverrouillage de l'écran d'accueil d'un smartphone n'est pas une convention secrète de déchiffrement, 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.

15. En statuant ainsi, la cour d'appel a violé les textes susvisés.

Sources :

https://www.cnil.fr/fr/reglement-europeen-protection-donnees RGPD

https://www.cnil.fr/fr/la-loi-informatique-et-libertes Loi du 6 janvier 1978