

LA VEILLE JURIDIQUE

Centre de Recherche de l'Ecole des Officiers de la Gendarmerie Nationale

N° 94

Mars 2021

EDITO

Cette veille juridique sort au moment où de nouvelles mesures restrictives sont prises devant l'accélération de la pandémie. Le débat est vif entre ceux qui appellent à un renforcement des mesures de contrôle au nom de la sécurité individuelle et collective et ceux qui placent la liberté au-dessus de toute considération sanitaire. En vérité, la responsabilité de chacun est le meilleur garant de l'une et de l'autre. Les rassemblements inconsidérés, sans aucun respect des règles de distanciation sociale, à des fins ludiques ou politiques, ne sont pas acceptables, alors que les personnels hospitaliers luttent chaque jour pour sauver des vies humaines. Je note la grande discipline dans les zones rurales, dans les petites villes et le laisser-aller que l'on observe dans les grandes

(Suite page 2)



CREOGN
CENTRE DE RECHERCHE
DE L'ÉCOLE DES OFFICIERS DE LA GENDARMERIE NATIONALE

Edito

villes. Cette différence est bien perçue par une « France profonde » qui regarde les urbains avec une hostilité croissante. Cette tension pourrait accentuer une fracture sociale déjà trop profonde.

Le télétravail, la formation à distance sont sans doute une alternative permettant de surmonter la crise, mais ces succédanés ne peuvent compenser la perte du relationnel. L'humain est un animal social, comme le soulignait Aristote. L'envie de retrouver ses proches, ses amis, ses relations de travail est sans doute la bonne nouvelle de cette pandémie. Les retrouvailles n'en seront que plus chaleureuses. Mais le retour à la normale n'éliminera pas l'usage de ces moyens. Le télétravail a un avenir et a déjà pour conséquence de remodeler nos territoires avec un déplacement de populations qui s'observe de confinement en confinement. L'enseignement à distance ne remplace pas la présence. J'ai donné récemment 60 heures de cours sans jamais voir mes élèves... inhumain pour eux comme pour moi. Il convient toutefois de repenser la formation du futur. Le webinar permet, où que l'on soit, d'accéder aux meilleurs contenus, avec les meilleurs enseignants. Pourquoi s'en priver ? Il est possible que le métier d'enseignant se transforme profondément, en s'appuyant sur des « coachs » en présentiel ayant recours à la meilleure ressource du moment, aux contenus les plus à jour. Les technologies numériques vont révolutionner les méthodes, notamment avec la virtualité réelle. La crise de la Covid va accélérer des tendances qui se seraient sans doute inscrites dans une plus longue période. Certains n'hésitent pas à dire que la transformation numérique est le grand vainqueur de la pandémie.

Pour l'heure, la lecture de *La veille juridique* reste un exercice bien conventionnel mais qui prend toute sa valeur dans la richesse des contributions et la fidélité de leurs auteurs que je remercie

Edito

vivement. Parfois de « jeunes plumes » s'ajoutent à l'équipe. C'est la preuve qu'aux âmes bien nées la valeur n'attend pas le nombre des années. Ces jeunes sont les « startups » de l'esprit. Merci à eux aussi.

Bonne lecture de cette veille juridique!

Par le général d'armée (2S) Marc WATIN-AUGOUARD, rédacteur en chef de La veille juridique



SOMMAIRE

Déontologie et sécurité	<u>5</u>
Droit de l'espace numérique	<u>16</u>
Actualité pénale	<u>61</u>
Police administrative	<u>80</u>
Droit des collectivités territoriales et de la sécurité privée	<u>87</u>



Violences policières ou violences procédurières ?

Dans un remarquable ouvrage collectif publié aux éditions Litec en 2008 (*La société au risque de la judiciarisation*), Frédéric Rouvillois nous décrit avec force détails l'irruption du Tiers Pouvoir dans nos sociétés contemporaines. Souvent traduit par le néologisme barbare de « judiciarisation », le recours de plus en plus frénétique au droit et à des instances juridictionnelles pour le traitement de questions qui naguère encore y échappaient presque totalement, est aujourd'hui devenu une réalité tangible et incontournable.

Autrefois l'apanage des pays de la Common Law – et singulièrement des États-Unis –, le phénomène de judiciarisation affecte aujourd'hui la société française dans toutes ses composantes publiques comme privées. Désormais, c'est la société dans son ensemble qui se trouve confrontée à cet envahissement par le procès ou la menace de procès : c'est elle qui vit désormais avec cette épée de Damoclès qui, selon les cas, pourra s'avérer salutaire ou paralysante, coûteuse et déstructurante.

Dans une société victimaire en quête perpétuelle de précaution, de transparence et de coupables, il eût été surprenant – pour ne pas dire miraculeux – que la déferlante des actions judiciaires épargnât les institutions régaliennes comme la police et ceux qui l'incarnent. En même temps qu'elle apparaît parfois comme la forme endimanchée d'une certaine agressivité sociale, la mobilisation croissante du droit et de la justice à l'encontre des forces de l'ordre

Déontologie et sécurité

n'est pas sans lien avec la perte de confiance des administrés dans celles et ceux qui sont dépositaires du monopole de la violence légitime. Arme de déstabilisation massive à la portée de tout citoyen, le recours effréné au droit et à la justice peut conduire certains justiciables à ériger leurs malheurs personnels en source sonnante et trébuchante d'un procès indu. Dans ce nouveau marché des chicanes judiciaires, toutes les causes, même les plus douteuses et invraisemblables, deviennent plaidables. Toutefois, entre l'injustice proclamée et la réalité constatée, il y a fort heureusement un fossé. Certaines revendications victimaires ne sont que supercheries ou affabulations, comme en témoigne le récent **arrêt P. M. et F. F. contre France en date du 18 février 2021 (requêtes n° 60324/15 et 60335/15)**.

Quand l'activisme juridique fabrique des victimes potentielles

Rendu par la cinquième section de la Cour européenne des droits de l'Homme, l'arrêt *P.M. et F. F. contre France* trouve son origine dans les circonstances suivantes : dans la matinée du 1^{er} janvier 2007, après s'être rendus coupables de dégradations de biens en état d'ébriété, deux individus majeurs – deux frères – étaient interpellés par un équipage de la police. Dans le prolongement d'un premier transport vers le commissariat, les deux individus interpellés étaient conduits à l'hôpital aux fins de délivrance d'un certificat de non-admission. De retour au commissariat, les deux frères étaient placés en chambre de sûreté le temps d'un dégrisement (les taux d'imprégnation alcoolique s'élevant respectivement à 0,39 mg/l et

Déontologie et sécurité

0,49 mg/l d'air expiré). À l'issue de ce dégrisement, les individus étaient placés en garde à vue et les droits afférents à cette mesure de contrainte leur étaient régulièrement notifiés. Alors même qu'ils n'en avaient pas exprimé le souhait, les deux suspects étaient soumis pendant le temps de leur garde à vue à un examen médical à l'initiative de l'officier de police judiciaire. À l'occasion de cet examen, des lésions – compatibles avec des allégations de violences policières – étaient constatées sur la personne des deux requérants tant au niveau du visage (hématome périorbitaire, ainsi que diverses éraflures et ecchymoses) que sur le reste du corps (hématomes autour du genou, entorse de la cheville, plaques ecchymotiques au niveau des poignets, etc.). En considération de ces diverses blessures, une ITT de six jours était attribuée à chacun des deux frères quand bien même leur état de santé était par ailleurs jugé compatible avec le maintien en garde à vue. Postérieurement à cette mesure de contrainte, un nouvel examen médical pratiqué à l'initiative des deux suspects révélait l'existence de lésions supplémentaires, tant au niveau du visage que sur le reste du corps des intéressés.

Une semaine après les faits litigieux, attribuant toutes ces lésions aux violences qu'ils auraient subies à différents moments de l'opération de police (lors de l'interpellation, lors du transport aller-retour vers l'hôpital, dans le fourgon de police mais aussi à l'occasion de leur interrogatoire dans le commissariat de police), les deux frères déposaient plainte auprès du procureur de la République de Paris pour violences par personnes dépositaires de l'autorité publique, traitements cruels, inhumains et dégradants.

Déontologie et sécurité

Dans un temps très voisin de cette plainte pénale (13 jours après), l'Inspection générale des services (IGS) – devenue depuis lors la délégation parisienne de l'Inspection générale de la police nationale (IGPN) – était saisie aux fins d'enquête par le Parquet de Paris. Après auditions des différents protagonistes de l'affaire considérée (plaignants, fonctionnaires de police, médecin, infirmière), l'IGS allait conclure « qu'aucun élément de l'enquête ne permettait d'accréditer les dires des requérants, selon lesquels ils auraient été brutalisés à plusieurs reprises par les policiers ». Bien mieux, le rapport de l'IGS pointait du doigt les exagérations des réclamants, leurs mensonges, leur agressivité verbale et leur agitation physique tout au long de l'opération de police. À la lumière des conclusions de ce rapport, et en l'absence de toute infraction suffisamment caractérisée, le Parquet de Paris classait la plainte pénale des deux frères au printemps 2007. Afin de surmonter cette décision de classement, une plainte avec constitution de partie civile était déposée, de sorte qu'une information judiciaire était ouverte (juillet 2009) des chefs de violences aggravées par dépositaires de l'autorité publique. En mai 2012, une ordonnance de non-lieu était rendue faute de charges suffisantes contre quiconque d'avoir commis les faits dénoncés. Par un arrêt en date du 19 septembre 2013, la chambre de l'instruction de la Cour d'appel de Paris confirmait ce non-lieu en considérant « qu'il ne résulte pas des éléments réunis par l'information judiciaire que des policiers se soient volontairement livrés à des violences ni à quelque acte illégitime ». Par un arrêt du 27 mai 2015, le pourvoi en cassation formé par les deux requérants était rejeté par la Chambre criminelle de la Cour de Cassation. Tout en attribuant un caractère définitif à

Déontologie et sécurité

l'arrêt de non-lieu des juges parisiens, cette ultime décision laissait déjà entrevoir une éventuelle saisine de la Cour européenne des droits de l'Homme...

Parallèlement à cette plainte pénale, les deux frères – par ailleurs condamnés dans la même affaire pour dégradations, outrage et rébellion commis en réunion – saisissaient la Commission nationale de déontologie de la sécurité (CNDS, autorité administrative indépendante instituée par une loi du 6 juin 2000, depuis lors absorbée par le Défenseur des droits à la faveur de la réforme constitutionnelle du 23 juillet 2008) par le truchement d'un parlementaire de Seine-Saint-Denis. Après de nombreuses auditions et sur la base d'un examen minutieux de l'intégralité de la procédure, la CNDS (avis du 18 novembre 2008) parvenait à une conclusion sensiblement identique à celle de l'IGS : « si des blessures étaient constatées, rien ne permettait d'établir avec certitude qu'elles étaient imputables à des violences policières illégitimes ». Tout en concluant à l'absence de manquement à la déontologie de la sécurité, la CNDS relevait néanmoins que « le maintien prolongé d'une personne interpellée en position de "décubitus ventral" était de nature à provoquer en certaines circonstances un arrêt cardio-respiratoire et, partant, que l'utilisation d'une telle technique devrait être strictement encadrée ».

Déontologie et sécurité

L'action en responsabilité de l'État, préalable obligatoire à la saisine de la Cour européenne des droits de l'Homme (CEDH) ?

Après épuisement des voies de recours internes (et peut-être même des magistrats eux-mêmes !), les deux frères saisissaient la Cour de Strasbourg d'une requête fondée sur une violation de l'article 3 de la Convention prohibant la torture ainsi que les traitements inhumains et dégradants. En soutien de leur démarche, les requérants prétendaient que leur interpellation et leur garde à vue subséquente comme les investigations menées à la suite de leur plainte caractérisaient des manquements aux obligations matérielles et procédurales résultant de l'article 3 précité de la Convention.

Avant même de statuer sur le fond des prétentions des requérants, la Cour européenne des droits de l'Homme était appelée à trancher une question de droit à la fois délicate et de première importance compte tenu des enjeux pratiques qui en résultent. Toute saisine de la Cour suppose, on le sait, un épuisement des voies de recours interne (art. 35 §1 CEDH). Or, peut-on légitimement considérer qu'un requérant satisfait cette condition en se constituant partie civile dans une instance pénale sans engager par ailleurs une action en responsabilité de l'État à raison du fonctionnement défectueux du service public de la justice, sur le fondement de l'article L. 141-1 du Code de l'organisation judiciaire ?

Contrairement aux requérants, le Gouvernement français voyait

Déontologie et sécurité

dans cette action en responsabilité un préalable obligatoire à la saisine des juges de Strasbourg (§43). Telle n'est pas la position adoptée par la Cour. Au soutien de leur solution, les juges européens énoncent tout d'abord « qu'en matière d'allégation de recours illégal à la force par les agents de l'État, des procédures civiles ou administratives visant uniquement à l'allocation de dommages et intérêts et non à l'identification et à la punition des responsables – telle que l'action en responsabilité de l'article L. 141-1 du Code de l'organisation judiciaire – ne sont pas en règle générale des recours adéquats et effectifs propres à remédier à des griefs fondés sur le volet matériel des articles 2 et 3 de la Convention ». La Cour précise ensuite que « la constitution de partie civile devant les juridictions répressives (d'instruction ou de jugement) est une voie adéquate et efficace pour dénoncer un recours illégal à la force par des agents de l'État ». Adéquate, car l'article 3 – CEDH au même titre que l'article 2 – impose aux États de mener d'office une enquête officielle effective, de nature à permettre d'établir les causes des blessures, d'identifier les éventuels responsables de celles-ci et d'aboutir à leur punition. Efficace, car la plainte avec constitution de partie civile devant le juge d'instruction déclenche l'ouverture d'une instruction ; la recherche des éléments relatifs aux faits dénoncés est alors confiée à un magistrat investigateur qui dispose pour ce faire de moyens bien plus efficaces que ceux auxquels un individu peut avoir accès. Ce mécanisme permet ainsi aux victimes de faits constitutifs d'un crime ou d'un délit d'augmenter leurs chances d'obtenir réparation de leurs préjudices. En conséquence, dès lors que les requérants s'étaient constitués partie civile et que leur action avait donné lieu à

Déontologie et sécurité

plusieurs décisions de justice (en première instance, en appel et en cassation) épuisant ainsi les recours auxquels ces plaintes pouvaient donner lieu, le Gouvernement français ne saurait – dans les circonstances de l'espèce – leur reprocher de ne pas avoir en plus intenté l'action en responsabilité de l'article L. 141-1 du Code de l'organisation judiciaire. En statuant ainsi, la Cour de Strasbourg inscrit sa décision dans le sillon d'une jurisprudence désormais bien éprouvée (V. notamment, CEDH, 21 juin 2018, *Sémache c/ France* ; CEDH, 5 décembre 2019, *J. M. c/ France*).

Quand la posture de victime confine à l'imposture

La requête jugée recevable, il appartenait ensuite à la Cour de Strasbourg d'en apprécier le bien-fondé sous son double aspect procédural et matériel, étant observé que les thèses des parties étaient là encore radicalement discordantes ou, si l'on préfère, irréconciliables, pour reprendre un terme politiquement en vogue. En substance, les requérants prétendaient que l'enquête menée à la suite de leurs accusations était lacunaire, rudimentaire et partielle tandis que l'État défendeur la jugeait parfaitement effective et prompte. Pareillement, alors que les requérants considéraient avoir été victimes de violences policières illégitimes, le Gouvernement français concluait à un usage de la force conforme à l'article 3 CEDH, eu égard à l'état d'excitation, d'agressivité et de violence des requérants.

S'agissant du volet procédural de l'article 3 de la Convention, la Cour commence par rappeler les qualités usuellement requises de toute enquête se rapportant à des allégations de mauvais traitements

Déontologie et sécurité

infligés à une personne se trouvant entre les mains des forces de l'ordre. À défaut d'être érigée en obligation de résultat, l'enquête doit être officielle, effective, indépendante, menée d'office, prompte, et approfondie. À travers l'identification et le châtiment des éventuels coupables, il s'agit ici non seulement de préserver la confiance du public mais aussi d'éviter toute apparence de complicité ou de tolérance relativement à des actes illégaux. Transposées au cas de l'espèce, ces exigences conduisent les juges strasbourgeois à accorder leur onction aux investigations menées par les autorités nationales. La Cour relève d'abord la diligence avec laquelle les premières investigations ont été menées à la suite de la plainte pénale des deux requérants. La Cour estime ensuite que l'enquête, menée avec minutie, s'est véritablement efforcée d'établir, de manière contradictoire, la réalité des faits litigieux, dont l'examen a donné lieu à des décisions circonstanciées et dûment motivées de juridictions nationales parfaitement indépendantes (indépendance au demeurant non contestée par les requérants).

En même temps qu'elle ne relève aucune carence de l'enquête menée sur les allégations de mauvais traitements subis par les requérants, la Cour de Strasbourg – à l'unanimité – absout l'État français en jugeant que les faits de l'espèce ne caractérisent pas davantage une violation de l'article 3 CEDH sous son volet matériel. Là encore, après un crochet obligé par les principes généraux, les juges européens relèvent tout d'abord que les blessures dont souffraient les requérants au moment des faits apparaissent d'une gravité suffisante pour tomber sous le coup de l'article 3 CEDH. Les événements litigieux s'étant produits alors que les requérants se trouvaient sous le contrôle des forces de l'ordre, la Cour observe

Déontologie et sécurité

ensuite « qu'il revient au Gouvernement de fournir des explications suffisamment convaincantes pour renverser la présomption de fait (au profit des requérants) en démontrant l'absence de crédibilité du récit des requérants et en justifiant soit que leurs blessures ne sont pas imputables aux forces de l'ordre soit qu'elles résultent d'un usage de la force rendu strictement nécessaire par le comportement des personnes en cause ». À ce moment de son raisonnement, la Cour stigmatise le manque de constance des déclarations des requérants, lesquelles sont, de surcroît, largement entachées de contradictions, d'imprécisions et d'incompatibilités avec les constatations médicales (l'un des requérants prétendait ainsi avoir été amené sans connaissance à l'hôpital tandis que l'autre alléguait avoir souffert d'une hémorragie du nez, autant d'affirmations formellement contredites par les examens médicaux). La Cour observe également que la plupart des blessures constatées peuvent s'expliquer par le recours aux techniques de contention et de maintien au sol utilisées par les policiers et dont le Gouvernement ne cherche nullement à nier la mise en œuvre. En considération de l'agressivité des requérants, unanimement constatée par les témoins des faits litigieux, la Cour concède que « le recours à ces techniques ne traduit pas, au cas d'espèce, un usage de la force autre que celui qui était strictement nécessaire pour éviter que les requérants ne blessent des tiers ou ne se blessent eux-mêmes ». Alors même que l'entorse à la cheville et l'hématome périorbitaire revêtent indiscutablement un caractère de gravité plus importante que les autres blessures, la Cour estime *in fine* « qu'elle n'est pas en position, au vu des éléments dont elle dispose, de se départir des appréciations factuelles des juridictions nationales selon lesquelles

Déontologie et sécurité

les requérants n'ont pas été victimes, lors de leur interpellation et de leur garde à vue, d'un usage de la force non strictement nécessaire ».

Droit de l'espace numérique

JURISPRUDENCE JUDICIAIRE

Par le capitaine Matthieu Audibert

La conservation et l'accès aux données techniques de connexion. Vers un nouveau paradigme pour les enquêtes judiciaires ?

Cour de justice de l'Union européenne (CJUE), affaire C-746/18, arrêt du 2 mars 2021 H.K/Prokuratuur

Dans la continuité de sa jurisprudence établie depuis 2014¹, la CJUE poursuit l'encadrement des dispositions juridiques liées à la conservation² et maintenant à l'accès, à des fins pénales, aux données techniques de connexion. Dans le même temps, la CJUE pose un certain nombre de garanties liées à cet accès qui mettent à mal les prérogatives du procureur de la République et certaines prérogatives du juge d'instruction au regard de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 lue à la lumière de la charte des droits fondamentaux de l'Union européenne (UE).

S'agissant des faits, un individu (H.K) a été condamné en première

1. Arrêt du 8 avril 2014, Digital Rights Ireland et Seitlinger e.a., C-293/12 et C-594/12 ; arrêt du 21 décembre 2016, Tele2 Sverige, C-203/15 et C-698/15 ; arrêt du 6 octobre 2020, La Quadrature du Net e.a. contre Premier ministre e.a., C-511/18, C-512/18 et C-520/18.

2. LASSALLE, Maxime, Protection des données, renseignements, procédure pénale et enquêtes administratives : l'approche française remise en cause par la CJUE, *Recueil Dalloz*, 2021, p. 406.

Droit de l'espace numérique

instance à une peine privative de liberté de deux ans pour avoir commis plusieurs vols, escroqueries et exercé des actes de violences. Pour déclarer coupable cet individu, la juridiction de première instance s'est fondée sur différents actes réalisés par les services d'enquête et notamment l'obtention de données relatives aux communications électroniques. Ces données peuvent être récupérées par les enquêteurs suite à l'autorisation délivrée par le procureur territorialement compétent. Plus précisément, ces données concernent plusieurs numéros de téléphones de l'individu et les différentes identités associées.

Condamné en première instance, il fait appel et celui-ci est rejeté par la cour d'appel estonienne. Il introduit alors un pourvoi en cassation contre cette décision auprès de la Cour suprême de son pays et conteste notamment la recevabilité des procès-verbaux établis à partir des données techniques de connexion récupérées par les enquêteurs sur autorisation du procureur.

Saisie de ce pourvoi, la juridiction suprême estonienne va sursoir à statuer et va adresser trois questions préjudicielles à la CJUE :

« Convient-il d'interpréter l'article 15, paragraphe 1, de la directive [2002/58], lu conjointement avec les articles 7, 8, 11 et 52, paragraphe 1, de la [Charte], en ce sens que l'accès des autorités nationales, dans le cadre d'une procédure pénale, à des données permettant de retrouver et d'identifier la source et la destination d'une communication téléphonique à partir du téléphone fixe ou mobile du suspect, d'en déterminer la date, l'heure, la durée et la nature, d'identifier le matériel de communication utilisé ainsi que de localiser le matériel de communication mobile utilisé constitue une ingérence tellement grave dans les droits fondamentaux garantis par les articles

Droit de l'espace numérique

précités de la Charte que, lors de la prévention, de la recherche, de la détection et de la poursuite d'infractions pénales, cet accès doit être limité à la lutte contre la criminalité grave, indépendamment de la période pour laquelle les autorités nationales ont accès aux données conservées ?

Convient-il d'interpréter l'article 15, paragraphe 1, de la directive [2002/58] à partir du principe de proportionnalité tel que formulé aux points 55 à 57 de [l'arrêt du 2 octobre 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788),] en ce sens que, si la quantité des données visées à la première question, auxquelles les autorités nationales ont accès, n'est pas très importante (tant du point de vue de la nature des données que du point de vue de la longueur de la période concernée), l'ingérence dans les droits fondamentaux qui en découle peut être justifiée de manière générale par l'objectif de la prévention, de la recherche, de la détection et de la poursuite d'infractions pénales et que, plus la quantité des données auxquelles les autorités nationales ont accès est importante, plus les infractions pénales contre lesquelles l'ingérence est destinée à lutter doivent être graves ?

Convient-il de considérer que l'exigence figurant au deuxième point du dispositif de [l'arrêt du 21 décembre 2016, Tele2 (C-203/15 et C-698/15, EU:C:2016:970)], selon laquelle l'accès des autorités nationales compétentes aux données doit être soumis à un contrôle préalable par une juridiction ou une autorité administrative indépendante, signifie que l'article 15, paragraphe 1, de la directive [2002/58] doit être interprété en ce sens que l'on peut considérer comme une autorité administrative indépendante le ministère public

Droit de l'espace numérique

qui dirige la procédure d'instruction et qui, ce faisant, est, en vertu de la loi, tenu d'agir de manière indépendante, en étant uniquement soumis à la loi et en examinant, dans le cadre de la procédure d'instruction, à la fois les éléments à charge et les éléments à décharge concernant la personne poursuivie, mais qui représente l'action publique au cours de la procédure judiciaire ultérieure ? »

Saisie de ces questions préjudicielles, la CJUE va, tout en rappelant sa jurisprudence antérieure sur l'interdiction faite aux États membres de procéder à une conservation généralisée et indifférenciée des données techniques de connexion, préciser que cet accès doit être « circonscrit à des procédures visant à la lutte contre la criminalité grave ou à la prévention des menaces graves contre la sécurité publique »³ (I).

En outre, la CJUE va indiquer que le droit de l'UE s'oppose à ce que le ministère public, en charge de diriger l'enquête pénale et, le cas échéant, d'engager l'action publique, puisse autoriser l'accès aux enquêteurs aux données techniques de connexion. Ce dernier point implique de nombreuses conséquences pour le Parquet français mais également pour le juge d'instruction (II).

3. Point 60 1).

Droit de l'espace numérique

I. La notion de criminalité grave ou de menace grave contre la sécurité publique comme seul critère autorisant l'accès aux autorités publiques aux données techniques de connexion

Ce nouvel arrêt de la CJUE rappelle une solution qui n'est pas nouvelle (A). Toutefois, combiné à l'arrêt *Quadrature du Net*, ce nouvel arrêt relatif aux données de connexion est susceptible d'entraîner de lourdes conséquences dans le succès de nombreuses enquêtes judiciaires (B).

A) Une solution non nouvelle dégagée par la CJUE s'agissant de la conservation des données de connexion

Dans ses questions préjudicielles, la Cour suprême estonienne s'interroge sur les modalités d'accès à ces données au regard de l'article 15 §1 de la directive 2002/58. L'accès par les autorités nationales, dans le cadre d'une enquête judiciaire, à ces données constitue-t-il une ingérence tellement grave dans les droits fondamentaux garantis par la Charte que cet accès doit faire l'objet d'une limitation à la lutte contre la criminalité, nonobstant la période pendant les enquêteurs ont eu accès à ces données ?⁴

En outre, la Cour suprême estonienne s'interroge au regard du volume de données concernées. L'argumentation sous-jacente de l'Estonie étant que si le volume de données n'est pas très important,

4. Point 26 1).

Droit de l'espace numérique

aussi bien s'agissant de la nature de celles-ci que de la période de collecte, cela peut-il justifier que l'ingérence qui en découle dans les droits fondamentaux puisse être justifiée par l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales ?⁵ En outre, de manière implicite, la juridiction estonienne tente de soumettre un accès proportionné à la gravité de l'infraction. Autrement dit, plus l'infraction est grave, plus la qualité de données accessibles serait importante⁶.

Dans l'argumentaire du gouvernement estonien, il est intéressant de souligner que l'accès aux données conservées en vertu du droit national estonien peut être sollicité pour tout type d'infraction pénale⁷, ce qui est également le cas du droit français⁸.

Pour répondre à ces questions préjudicielles, la CJUE rappelle sa jurisprudence antérieure. Tout d'abord, elle subordonne l'accès à ces données à leur conservation de manière conforme au droit de l'Union⁹. Elle rappelle le principe dégagé dans l'arrêt *Quadrature du Net* du 6 octobre 2020, à savoir que le droit de l'Union s'oppose à des législations nationales prévoyant à des fins pénales, à titre préventif, la conservation généralisée et indifférenciée des données

5. Point 26 2).

6. *Ibid.*

7. Point 28.

8. Articles L. 34-1 et R. 10-13 du Code des postes et des communications électroniques et dispositions du Code de procédure pénale, voir par exemple l'article 60-1.

9. Point 29. Voir aussi arrêt du 6 octobre 2020, *La Quadrature du Net e.a.*, c-511/18, C-512/18 et c-520/18, point 167).

Droit de l'espace numérique

techniques de connexion (de localisation et de trafic)¹⁰¹¹.

Ensuite, la CJUE va se livrer à un contrôle de proportionnalité dans l'accès à ces données entre, d'une part, la gravité de l'ingérence dans les droits fondamentaux et, d'autre part, l'objectif d'intérêt général poursuivi¹². Il s'agit là encore d'un rappel de sa position exprimée dans l'arrêt *Quadrature du Net*¹³. La CJUE poursuit en indiquant que « seule la lutte contre la criminalité et la prévention des menaces graves contre la sécurité publique sont de nature à justifier des ingérences graves dans les droits fondamentaux consacrés [par la Charte]¹⁴ ». Ces ingérences sont notamment celles qui « impliquent la conservation des données relatives au trafic et des données de localisation, qu'elle soit généralisée et indifférenciée ou ciblée¹⁵ ».

Sur ce point, la CJUE conclut que « seules des ingérences ne présentant pas un caractère grave peuvent être justifiées par l'objectif (...) de prévention, de recherche, de détection et de poursuite d'infractions pénales en général¹⁶ ».

Sur les données, la CJUE fait ensuite la distinction avec les données

10. Point 30. Voir aussi arrêt du 6 octobre 2021, *La Quadrature du Net e.a.*, c-1/18, C-512/18 et c-520/18, point 168.

11. LASSALLE, Maxime, Protection des données, renseignements, procédure pénale et enquêtes administratives : l'approche française remise en cause par la CJUE, *Recueil Dalloz*, 2021, p. 406.

12. Points 31 et 32.

13. Arrêt du 6 octobre 2020, *La Quadrature du Net e.a.*, c-511/18, C-512/18 et c-520/18, point 131.

14. Points 33.

15. *Ibid.*

16. *Ibid.* Voir aussi arrêt du 6 octobre 2020, *La Quadrature du Net e.a.*, c-511/18, C-512/18 et c-520/18, points 140 et 146.

Droit de l'espace numérique

relatives à l'identité civile des utilisateurs non associées aux données de communication. Pour les premières, considérant que celles-ci ne permettent pas, à elles seules, de connaître les usages de l'utilisateur ou encore sa localisation, la CJUE considère que leur conservation n'est pas en contradiction avec le droit de l'Union¹⁷. Il convient de souligner que la Cour européenne des droits de l'Homme adopte la même solution s'agissant des données relatives à l'identité civile des utilisateurs¹⁸¹⁹.

Dans la suite de son raisonnement, la CJUE considère l'accès limité à une quantité limitée de données de connexion comme étant un critère inopérant pour justifier une telle ingérence²⁰ et rappelle, comme dans l'arrêt *Quadrature du Net*²¹, que le juge pénal est tenu d'écarter « des informations et des éléments de preuve qui ont été obtenus au moyen d'une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation incompatible avec le droit de l'Union ou encore au moyen d'un accès de l'autorité compétente à ces données en violation de ce droit, dans le cadre d'une procédure pénale ouverte à l'encontre de personnes soupçonnées d'actes de criminalité, si ces personnes ne sont pas en mesure de commenter efficacement ces informations et ces éléments de preuve, provenant d'un domaine échappant à la

17. Point 34. Voir aussi arrêt du 6 octobre 2020, *La Quadrature du Net e.a.*, c-511/18, C-512/18 et c-520/18, points 157 et 158.

18. CEDH, *Brayer contre Allemagne*, 30 janvier 2020, n° 50001/12.

19. DE MONTECLER Marie-Christine. Protection des données : la CJUE infléchit sa jurisprudence. *AJDA*, 2020, p. 1880.

20. Point 40.

21. Arrêt du 6 octobre 2020, *La Quadrature du Net e.a.*, c-511/18, C-512/18 et c-520/18, points 226 et 227.

Droit de l'espace numérique

connaissance des juges et qui sont susceptibles d'influencer de manière prépondérante l'appréciation des faits²²».

Pour conclure sur ces deux questions, la CJUE écarte les critères liés à la durée de l'accès aux données et à la nature des données disponibles pour conclure que le droit de l'Union²³ n'autorise l'accès, dans le cadre des enquêtes judiciaires, aux données de connexion permettant de tirer des conclusions sur la vie privée des personnes visées par les investigations, que dans le cadre de la lutte contre la criminalité grave ou pour prévenir des menaces graves contre la sécurité publique²⁴.

B) Quelles conséquences pour les enquêtes judiciaires ?

Pour commencer, il peut être intéressant de comparer l'appréhension juridique des données techniques de connexion et les données de contenu par les services d'enquête.

D'un point de vue technique, s'agissant des correspondances émises par la voie des communications électroniques, on distingue traditionnellement les données relatives aux contenus et les données techniques de connexion. Les premières contiennent les paroles prononcées ou écrites et les secondes les informations relatives à la connexion des appareils aux réseaux téléphoniques ou à Internet.

²². Point 44.

²³. Article 15 §1 de la directive 2002/58, articles 7, 8, 11 et 52 de la Charte des droits fondamentaux.

²⁴. Point 45.

Droit de l'espace numérique

Les interceptions de correspondances (donc les données de contenu) sont possibles en matière criminelle et en matière correctionnelle si la peine encourue est égale ou supérieure à trois ans d'emprisonnement²⁵ dans le cadre d'une information judiciaire. S'agissant de l'enquête de flagrance et de l'enquête préliminaire, les interceptions de correspondances émises par la voie des communications électroniques sont possibles pour l'une des infractions entrant dans le champ d'application des articles 706-73 et 706-73-1 du Code de procédure pénale²⁶.

En revanche, que ce soit en enquête de flagrance²⁷, en enquête préliminaire²⁸ ou dans le cadre d'une information judiciaire²⁹, aucun seuil n'est exigé s'agissant de la possibilité de requérir les opérateurs de communication électroniques aux fins de récupérer des données techniques de connexion. Autrement dit, en droit français, il est possible de récupérer ces données aussi bien pour une contravention que pour un délit ou un crime. Cette différence de traitement entre ces deux types de données se comprend aisément, les premières portant sur les propos ou écrits échangés et les secondes sur les informations techniques relatives à la connexion des appareils aux différents réseaux. Le degré d'intrusion dans la vie privée est donc sensiblement différent.

Avec son arrêt H.K/Prokuratuur, la CJUE reprend ses solutions déjà dégagées dans les arrêts Tele2 Sverige et Quadrature du Net,

²⁵. Article 100 du Code de procédure pénale.

²⁶. Infractions relatives à la criminalité et à la délinquance organisées.

²⁷. Article 60-1 du Code de procédure pénale.

²⁸. Article 77-1-1 du Code de procédure pénale.

²⁹. Article 99-3 du Code de procédure pénale.

Droit de l'espace numérique

s'agissant de la non-conformité au droit de l'Union de législations nationales prévoyant une conservation généralisée et indifférenciée des données techniques de connexion. L'apport de cet arrêt réside, comme nous l'avons vu précédemment, dans un accès autorisé, à des fins pénales, aux données techniques de connexion uniquement en vue de lutter contre la criminalité grave ou de prévenir des menaces graves contre la sécurité publique.

Or, réduire les données accessibles aux seules infractions pénales graves n'est pas concevable pour les services d'enquête, notamment parce que la notion « d'infraction grave » exclut de nombreuses possibilités d'investigations. Une réduction drastique du champ de conservation des données et des données accessibles méconnaît les processus d'investigations dont la vocation est aussi de garantir le droit des victimes d'obtenir un jugement et réparation pour le préjudice subi. En outre, au début d'une enquête, il est impossible de déterminer une zone délimitée qui pourrait être celle de l'auteur et de ses éventuels complices. Il est impossible pour les magistrats et les enquêteurs de connaître à l'avance les données dont ils auront besoin pour élucider les enquêtes qu'ils mènent. Enfin, il est impossible de déterminer à l'avance quelles personnes feront l'objet d'investigations³⁰, à charge comme à décharge. Ainsi, « plus que le dispositif national, ce sera peut-être la méthodologie d'enquête qui devra être revue³¹ ».

Par ailleurs, cette possibilité d'accéder aux données de connexion

30. MOLINS, François. La protection des citoyens européens dans un monde ultra-connecté. Fondation Robert Schuman, *Question d'Europe*, n° 510, avril 2019.

31. NICAUD, Baptiste. CJUE : un équilibre – trop ? – rigoureux entre droit au respect de la vie privée et conservation des données. *AJ Pénal*, 2020, p. 531.

Droit de l'espace numérique

permet d'identifier les auteurs mais aussi et surtout de matérialiser des infractions, de démontrer des liens de complicité ou des coactions³², de déterminer si les faits ont été commis avec des circonstances aggravantes.

En outre, comme nous venons de le voir, la CJUE n'envisage l'accès aux données de connexion conservées que dans le cadre de la lutte contre la criminalité grave. Or, cette notion de gravité n'est pas explicitée dans l'arrêt et la jurisprudence antérieure de la CJUE relative aux données de connexion. En droit français, cette notion de gravité est déterminée en fonction de l'échelle des peines. Ainsi, un crime est par essence nécessairement grave. Or, s'agissant des délits, la liste des infractions potentiellement concernées par un accès prohibé aux données de connexion est extrêmement longue.

C'est le cas, par exemple, des infractions pouvant être exclusivement commises par la voie des communications électroniques : infractions relatives à la vie privée³³, cyberharcèlement³⁴, provocation à la discrimination, à la haine ou à la violence à l'égard d'une personne ou d'un groupe de personnes à raison de leur origine ou de leur appartenance à une ethnie, une nation, une race ou à une religion déterminée³⁵, la provocation à la haine ou à la violence à raison du sexe ou de l'orientation sexuelle, de l'identité de genre ou du handicap et provocation à des

³². *op.cit.* note 30, p. 26.

³³. Articles 226-1 et suivants du Code pénal.

³⁴. Article 222-33-2-2 du Code pénal.

³⁵. Article 24 de la loi du 29 juillet 1881 relative à la liberté de la presse.

Droit de l'espace numérique

discriminations les concernant³⁶.

Ces infractions sont-elles graves ? La sanction prévue pour celles-ci varie entre un an et deux d'emprisonnement. L'application stricte de cet arrêt de la CJUE empêcherait donc le recours aux données de connexion pour enquêter sur des infractions de haine en ligne. Or, ces données sont absolument essentielles pour élucider de tels faits. Ainsi, « l'inquiétude pèse tant sur les procédures en cours que sur l'avenir des moyens d'enquêtes³⁷ » pour élucider ces infractions.

Enfin, l'arrêt de la CJUE faisant suite à une question préjudicielle³⁸, il appartient à la juridiction nationale qui a saisi la CJUE de résoudre l'affaire, conformément à la décision de la CJUE. En outre, cette décision lie les autres juridictions nationales des pays de l'Union européenne qui seraient saisies d'un problème similaire. La combinaison des arrêts *Quadrature du Net* et *H.K./Prokuratuur* est donc susceptible de remettre profondément en cause les méthodes actuelles d'enquêtes judiciaires^{39,40}.

Nonobstant les questions de la conservation et de l'accès à des fins pénales aux données de connexion, la CJUE vient préciser les modalités d'accès à ces données et, notamment, s'agissant du

³⁶. *Ibid.*

³⁷. *op.cit.* note 31, p. 26.

³⁸. Article 267 du Traité sur l'Union européenne.

³⁹. DAOUD, Emmanuel, BELLO, Imane, PECRIAUX, Océane. Données de connexion et sauvegarde de la sécurité nationale : l'exception confirme la règle. *Dalloz IP/IT*, 2021, p. 46.

⁴⁰. *op.cit.* note 31, p. 26.

Droit de l'espace numérique

contrôle préalable de cet accès. Ce faisant, elle remet en question les prérogatives du Parquet français et, par extension, certaines prérogatives du juge d'instruction.

II. L'exclusion du ministère public dans le contrôle préalable de certains actes d'enquêtes : vers un nouveau paradigme dans la procédure pénale française ?

Il s'agit ici d'examiner la troisième question posée par la Cour suprême estonienne et la réponse apportée par la CJUE. En effet, au regard de l'article 15, paragraphe 1, de la directive 2002/58 et de l'arrêt Tele2 du 21 décembre 2016, le ministère public est-il compétent pour autoriser cet accès ? Par sa réponse, la CJUE remet en cause certaines prérogatives du ministère public français (A) et, par là même, certaines du juge d'instruction (B).

A) Une remise en cause du Parquet français au travers du ministère public estonien

Pour analyser la possibilité pour le ministère public estonien d'autoriser cet accès, la CJUE va analyser ses caractéristiques. Ainsi, il est « tenu d'agir de manière indépendante », il doit « examiner les éléments à charge et à décharge lors de la procédure d'instruction, l'objectif de cette procédure [étant] la collecte d'éléments de preuve ainsi que la réunion des autres conditions nécessaires à la tenue d'un procès », il « représente l'action publique lors du procès et (...) serait donc également partie à la procédure ». Enfin, il « est organisé de manière hiérarchique »⁴¹.

⁴¹. Point 47. Voir également CRICHTON, Cécile. Précisions sur l'accès aux

Droit de l'espace numérique

Tout d'abord, la CJUE va contrôler le respect de l'exigence de proportionnalité dans l'accès aux données. Elle relève ainsi que la loi estonienne autorise au Parquet estonien un accès général à toutes les données sans préciser l'objectif poursuivi⁴². Elle en conclut ainsi que ces dispositions ne respectent pas l'exigence de proportionnalité⁴³. Ensuite, la CJUE va ajouter un point fondamental qui impactera certainement le Parquet français. Elle indique « que l'accès des autorités nationales compétentes aux données conservées [doit être] subordonné à un contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante et que la décision de cette juridiction ou de cette entité [doit intervenir] à la suite d'une demande motivée de ces autorités présentée, notamment, dans le cadre de procédures de prévention, de détection ou de poursuites pénales⁴⁴ ».

Elle précise que la juridiction ou l'entité de contrôle « [doit disposer] de toutes les attributions et [doit présenter] toutes les garanties nécessaires en vue d'assurer une conciliation des différents intérêts et droits en cause. S'agissant plus particulièrement d'une enquête pénale, un tel contrôle exige que cette juridiction ou cette entité soit en mesure d'assurer un juste équilibre entre, d'une part, les intérêts liés aux besoins de l'enquête dans le cadre de la lutte contre la criminalité et, d'autre part, les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel

métadonnées lors du procès pénal. *Dalloz actualité*, 5 mars 2021.

⁴². Points 49 et 50.

⁴³. *Ibid.*

⁴⁴. Point 51. Voir également arrêt du 6 octobre 2020, *La Quadrature du Net e.a*, c-511/18, C-512/18 et c-520/18, point 189.

Droit de l'espace numérique

des personnes dont les données sont concernées par l'accès⁴⁵ ». Dès lors, cette juridiction ou entité de contrôle doit avoir « une position de neutralité vis-à-vis des parties à la procédure pénale⁴⁶ ».

Dans la mesure où le ministère public estonien dirige l'enquête mais est également susceptible d'exercer l'action publique, la CJUE en conclut que celui-ci ne peut être considéré comme indépendant : il n'a pas la qualité de tiers à la procédure et, notamment, vis-à-vis des enquêteurs qui demandent l'accès aux données et il peut faire l'objet d'une influence extérieure⁴⁷. Enfin, la CJUE insiste pour rappeler qu'un contrôle de l'accès postérieur n'est pas suffisant, car il doit intervenir dans les plus brefs délais, « préalablement à tout accès, sauf cas d'urgence dûment justifié⁴⁸ ».

Forts de ces éléments, examinons la situation du Parquet français. Aux termes de la loi, la police judiciaire est exercée sous la direction du procureur de la République⁴⁹. Il exerce l'action publique dans le respect du principe d'impartialité⁵⁰, il ne prend donc pas parti dans les enquêtes. Toutefois, c'est lui qui dispose du principe de l'opportunité des poursuites⁵¹ et peut, le cas échéant, mettre en œuvre l'action publique et requérir une condamnation⁵². Enfin, le procureur de la République est placé sous l'autorité du procureur

45. Point 52.

46. Point 54.

47. Points 54-57.

48. Point 58.

49. Articles 12 et 41 du Code de procédure pénale.

50. Article 31 du Code de procédure pénale.

51. Article 40 du Code de procédure pénale.

52. Article 40-1 du Code de procédure pénale.

Droit de l'espace numérique

général près la Cour d'appel⁵³.

Or, sur ces points, la CJUE a clairement tranché⁵⁴ : le droit de l'Union s'oppose à une législation nationale qui donne compétence au ministère public, qui dirige l'enquête judiciaire et exerce, le cas échéant, l'action publique ultérieurement, pour autoriser l'accès aux enquêteurs aux données de connexion.

En droit français, dans le cadre de l'enquête de flagrance, le procureur de la République ou l'officier de police judiciaire, et l'agent de police judiciaire sous le contrôle de ce dernier, peuvent, par réquisition, récupérer les données de connexion intéressant une enquête en cours⁵⁵. Au cours de l'enquête préliminaire, le procureur ou l'officier ou l'agent de police judiciaire, peuvent, sur autorisation du procureur de la République également récupérer ces données, toujours par réquisition⁵⁶. Dans la loi, le contrôle préalable n'existe que dans le cadre de l'enquête préliminaire. En pratique, il existe aussi en enquête de flagrance dans la mesure où il s'agit de réquisitions émises sous frais de justice.

Ainsi, aucun tiers à la procédure, tel un juge des libertés et de la détention, n'intervient pour autoriser cet accès. Seul le procureur de la République est susceptible d'exercer un tel contrôle. Or, comme nous l'avons vu, du fait de son positionnement, il y a d'une part un problème de contrôle préalable tel qu'exigé par la CJUE mais

53. Articles 35 à 37 du Code de procédure pénale.

54. Point 60 2).

55. Article 60-1 du Code de procédure pénale.

56. Article 77-1-1 du Code de procédure pénale.

Droit de l'espace numérique

également un problème d'indépendance au sein même de l'enquête, dans la mesure où c'est le procureur qui exerce, le cas échéant, l'action publique à l'issue de l'enquête qu'il dirige.

En conclusion, le Parquet français est clairement menacé par l'arrêt de la CJUE du 2 mars, tant en raison de son positionnement dans la procédure qu'en raison de ses attributions propres.

B) Une remise en cause par ricochet du juge d'instruction ?

À première vue, le juge d'instruction ne semble pas impacté par cet arrêt de la CJUE qui ne traite que du ministère public. Pour autant, certains points de l'arrêt le concernent.

Celui-ci ne représente pas l'action publique. Son rôle est d'instruire à charge et à décharge⁵⁷. Il procède ainsi à tous les actes d'enquête qu'il juge utiles à la manifestation de la vérité. Il peut procéder lui-même à ces actes ou les déléguer aux officiers de police judiciaire par le biais de commissions rogatoires⁵⁸. À cet effet, les officiers de police judiciaire exercent, dans les limites de la commission rogatoire, tous les pouvoirs du juge d'instruction⁵⁹.

S'agissant des données de connexion, le juge d'instruction ou l'officier de police judiciaire commis par lui peuvent, par réquisition, récupérer les données de connexion intéressant une enquête en

⁵⁷. Article 81 du Code de procédure pénale.

⁵⁸. Article 151 du Code de procédure pénale.

⁵⁹. Article 152 du Code de procédure pénale.

Droit de l'espace numérique

cours⁶⁰. Ce pouvoir précis va alors rentrer en contradiction avec l'arrêt de la CJUE. Celle-ci explique en substance que celui qui exerce le contrôle préalable doit être un tiers par rapport à celui qui demande l'accès aux données de connexion. L'autorité de contrôle ne doit donc pas être impliquée dans la conduite de l'enquête pénale⁶¹.

Or, lorsque le juge d'instruction requiert en vertu de l'article 99-3 du Code de procédure pénale, aucune entité ne contrôle préalablement sa réquisition. Seule une nullité nécessairement postérieure peut le cas échéant être soulevée⁶². Surtout, le juge d'instruction est impliqué dans l'enquête, car c'est justement son rôle d'informer à charge et à décharge⁶³. La CJUE indique que le droit de l'Union « s'oppose à une réglementation nationale donnant compétence au ministère public dont la mission est de diriger la procédure d'instruction pénale (...) pour autoriser l'accès d'une autorité publique aux données [de connexion] aux fins d'une instruction pénale⁶⁴ ». Nous pouvons donc en déduire que l'article 99-3 du Code de procédure pénale semble contraire au droit de l'Union.

Le raisonnement pourrait également s'appliquer aux interceptions de correspondances bien que non concernées par cet arrêt. En effet, si en enquête de flagrance et en enquête préliminaire, celles-ci sont

⁶⁰. Article 99-3 du Code de procédure pénale.

⁶¹. Point 54.

⁶². Article 170 du Code de procédure pénale.

⁶³. Article 81 du Code de procédure pénale.

⁶⁴. Point 59.

Droit de l'espace numérique

autorisées par le juge des libertés et de la détention⁶⁵, dans le cadre de l'information, le juge des libertés et de la détention n'intervient pas pour les autoriser⁶⁶. Il serait paradoxal que les données de connexion fassent l'objet d'un traitement plus strict que les données de contenu, objets des interceptions. Pour ces raisons, le juge d'instruction est également menacé par ricochet par cet arrêt de la CJUE.

À cet égard, il convient de s'interroger si la jurisprudence de la CJUE n'incite pas les États membres à tendre vers la création d'un juge de l'enquête : magistrat non impliqué dans la procédure qui serait uniquement chargé, à la demande des enquêteurs ou du procureur de la République ou du juge d'instruction pourtant indépendant, d'autoriser certains actes attentatoires à des droits ou libertés.

65. Article 706-95 du Code de procédure pénale.

66. Article 100 du Code de procédure pénale.

Droit de l'espace numérique

Par le Général d'armée (2S) Marc Watin-Augouard

**Cour de cassation, Chambre criminelle, n° 20-84.004,
arrêt n° 236 du 2 mars 2021, M.A...X ; et autre(s)**

Ne relève pas de la procédure de géolocalisation en temps réel (art. 230-32 du Code de procédure pénale – CPP) la localisation d'une personne en dehors du territoire national qui ne s'appuie pas sur un itinéraire ou un positionnement obtenu en temps réel ou qui résulte de l'exploitation de fadettes.

La PJ de Metz identifie un groupe organisé, impliqué dans l'acheminement et la diffusion d'importantes quantités de produits stupéfiants dans le secteur de la Moselle-Est. Les personnes sont mises en examen des chefs de transport, détention, offre ou cession, acquisition et emploi d'une substance ou plante classée comme stupéfiant, de participation à un groupement formé ou une entente établie en vue de la préparation d'un ou plusieurs délits punis de dix ans d'emprisonnement, et de non-justification de ressources, et placés en détention provisoire. Les mis en examen contestent la régularité des opérations de géolocalisation menées en dehors du territoire national, sur les territoires marocains, espagnols et allemands, sans autorisation préalable ou concomitante de ces États.

La chambre de l'instruction ne donne pas suite à leur demande, considérant qu'une mesure de localisation opérée à l'étranger ne saurait s'analyser en une mesure de géolocalisation, faute pour les procès-verbaux d'exploitation de cette mesure de faire état d'une

Droit de l'espace numérique

indication précise de lieu.

Pour justifier l'arrêt de la chambre de l'instruction, la Cour de cassation relève que :

- même si les heures de franchissement aller-retour des frontières sont mentionnées, il ne saurait être considéré qu'il y a géolocalisation ;
- la plupart des pièces ne comportent aucune indication précise de lieu, dès lors que l'intéressé franchit la frontière, les procès-verbaux se bornant à indiquer qu'il se rend sur le territoire allemand. L'absence de toute indication sur l'itinéraire ou de la localisation en temps réel sur le territoire étranger exclut la qualification de géolocalisation ;
- la seule indication du pays étranger, d'où les appels paraissent avoir été passés ou reçus provisoirement sans plus ample précision de lieu, ne saurait s'analyser en une mesure de géolocalisation. La seule mention de la date et de l'heure d'arrivée au Maroc d'un des protagonistes ne provient pas d'une opération de localisation en temps réel sur son territoire mais de l'exploitation des fadettes de sa ligne ;
- l'indication d'un déplacement en Espagne « effectué visiblement en avion » ne saurait s'analyser en une mesure de géolocalisation, aucune autre précision n'étant apportée.

Note sur la géolocalisation en temps réel

La géolocalisation en temps réel se distingue de la géolocalisation

Droit de l'espace numérique

en temps différé et de la surveillance⁶⁷. Elle a été autorisée par la loi du 28 mars 2014⁶⁸ qui est venue combler le vide juridique consécutif à deux arrêts de la Cour de cassation du 22 octobre 2013⁶⁹ tirant les conclusions de la jurisprudence de la Cour européenne des droits de l'Homme⁷⁰.

Avant la loi du 28 mars 2014, aucun texte spécifique ne venait encadrer son usage. Dans le cadre d'une information judiciaire, le recours à l'article 81 du CPP semblait autoriser le juge d'instruction à procéder à tous les actes d'information qu'il jugeait « utiles à la manifestation de la vérité ». S'agissant des enquêtes préliminaires ou de flagrance, le Parquet s'appuyait sur l'article 41 du CPP, selon lequel « le procureur de la République procède ou fait procéder à tous les actes d'enquête nécessaires à la recherche et à la poursuite des infractions à la loi pénale », et les articles 60-2 et 77-1-1 dudit Code (réquisition judiciaire concernant des données informatiques). Dans une délibération du 19 décembre 2013, la Commission nationale de l'informatique et des libertés (CNIL) a rappelé que « l'utilisation de dispositifs de géolocalisation est particulièrement sensible au regard des libertés individuelles, dans la mesure où ils permettent de suivre de manière permanente et en temps réel des personnes, aussi bien dans l'espace public que dans des lieux privés. Le recours à la géolocalisation en temps réel – poursuit-elle –

67. La surveillance des personnes ou des biens est une technique d'enquête qui est mise en œuvre dans le « monde réel » (art. 706-80 CPP).

68. Loi n° 2014-372 du 28 mars 2014 relative à la géolocalisation.

69. Cass.crim, 22 octobre 2013, bull.crim 2013, n° 196 et 197.

70. CEDH, 2 septembre 2010, n° 35623/05, *Uzun c/Allemagne*.

Droit de l'espace numérique

s'apparente à une interception du contenu des communications électroniques prévues aux articles 100 et suivants du Code de procédure pénale, qui font notamment référence à la transcription des correspondances émises par la voie des communications et imposent d'identifier la liaison à intercepter ».

Si la Cour de cassation a validé la géolocalisation dans le cadre d'une instruction relative à un trafic de stupéfiants, parce qu'elle est mise en œuvre sous le contrôle d'un juge (Cass.crim, 22 novembre 2011, Mohamed X et autres), elle a cependant, à l'occasion des deux arrêts précités, remis en cause cette pratique pour les enquêtes conduites sous la direction du Parquet. Elle était, en effet, contraire à la jurisprudence de la Cour européenne des droits de l'Homme statuant sur la conformité de la géolocalisation à l'article 8 de la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales. La Cour n'a pas contesté le bien-fondé de la géolocalisation, « nécessaire dans une société démocratique », mais, constatant que la géolocalisation est une ingérence dans la vie privée – protégée par l'article 8§1 de ladite Convention – elle a exigé l'intervention d'un juge pour en contrôler la procédure. Or, il est désormais acquis que le procureur de la République n'est pas considéré comme un magistrat indépendant⁷¹.

Les arrêts de la Cour de cassation ont provoqué un véritable « séisme », dans la mesure où toutes les géolocalisations en cours, dans le cadre d'une enquête préliminaire ou d'une enquête de flagrance, ont été interrompues, sans préjudice des nullités pouvant être prononcées.

⁷¹. CEDH, arrêt *Mdevedyev c/ France*, 29 mars 2010 et *Moulin c/France*, 23 novembre 2011.

Droit de l'espace numérique

La loi du 28 mars 2014 a créé les articles 230-32 à 230-44 du CPP qui ont posé le principe d'un recours à la géolocalisation, en temps réel, d'une personne sans son consentement, d'un véhicule ou d'un objet, à l'insu de son propriétaire ou de son possesseur⁷². Pour le Conseil constitutionnel⁷³, « la mise en œuvre de ce procédé n'implique pas d'acte de contrainte sur la personne visée ni d'atteinte à son intégrité corporelle, de saisie, d'interception de correspondance ou d'enregistrement d'image ou de son ; l'atteinte à la vie privée qui résulte de la mise en œuvre de ce dispositif consiste dans la surveillance par localisation continue et en temps réel d'une personne, le suivi de ses déplacements dans tous lieux publics ou privés ainsi que dans l'enregistrement et le traitement des données ainsi obtenues ».

Selon les termes de cette loi (modifiée par la loi n° 2019-222 du 23 mars 2019), la géolocalisation peut être autorisée pour les besoins des procédures relatives aux infractions punies d'au moins trois ans d'emprisonnement au lieu de cinq (art. 230-32 CPP)⁷⁴. Le juge d'instruction peut l'autoriser pour une durée de quatre mois renouvelable. Dans le cadre d'une enquête préliminaire ou de flagrance, la géolocalisation peut être mise en œuvre sur décision du procureur de la République pour une durée de quinze jours (criminalité organisée) ou de huit jours (autres cas). À l'issue, après

72. La géolocalisation en temps réel peut aussi être mise en œuvre dans le cadre d'une recherche des causes de la mort ou de la disparition (art. 74, 74-1 et 80-4 du CPP) ou de la recherche d'une personne en fuite (art. 74-2 du CPP).

73. Décision n° 2014-693 DC du 25 mars 2014.

74. Par similitude, l'article 67 bis-2 du Code des douanes, qui autorise la géolocalisation dans la cadre des enquêtes douanières, prévoit un seuil d'emprisonnement de 3 ans.

Droit de l'espace numérique

autorisation du juge des libertés et de la détention, elle peut être prolongée pour une durée d'un mois renouvelable.

La géolocalisation est aussi possible dans le cadre des enquêtes ou informations judiciaires en recherches des causes de la mort et des blessures (art. 74 et 80-4 du CPP), des enquêtes ou informations judiciaires en recherches des causes de la disparition (art. 74-1 et 80-4 du CPP), des enquêtes en recherches des personnes en fuite (art. 74-2 du CPP).

Le Conseil constitutionnel déclare conformes à la Constitution les dispositions de la loi du 23 mars 2019, en considérant, selon les mêmes termes que sa décision du 23 mars 2014, que « la géolocalisation, mesure de police judiciaire, n'implique pas d'acte de contrainte sur la personne visée, ni d'atteinte à son intégrité corporelle, de saisie, d'interception de correspondance ou d'enregistrement d'image ou de son ». En autorisant le recours à la géolocalisation lorsque les nécessités de l'enquête l'exigent pour un crime ou un délit puni d'une peine d'au moins trois ans d'emprisonnement, le législateur n'a pas porté atteinte aux exigences constitutionnelles.

La circulaire CRIM/2014-7/G-1.04.2014 du 1^{er} avril 2014 précise que deux techniques de géolocalisation en temps réel sont mises en œuvre dans le cadre d'une procédure pénale :

- le suivi dynamique d'un terminal de télécommunications ;
- le suivi dynamique par un système (balise) placé sur un moyen de transport⁷⁵ ou sur tout autre objet, soit par sa propre technologie

⁷⁵. Cass.crim, (n° 15-87755), 7 juin 2016, George sX..., Juan Y... « MM. X... et Y... ne

Droit de l'espace numérique

(par exemple un smartphone, une tablette, un véhicule par son GPS), soit par l'intermédiaire d'une balise.

Toute personne (et pas uniquement la personne soupçonnée) peut être concernée, dès lors que la mesure relève des « nécessités de l'enquête ».

Le territoire national, limite géographique

L'article 230-32 spécifie bien l'application géographique de la géolocalisation à « l'ensemble du territoire national ». Au-delà des frontières, une mesure de coopération est nécessaire. Les données issues d'une géolocalisation mise en œuvre sur le territoire national et s'étant poursuivie sur le territoire d'un autre État ne peuvent, lorsque cette mesure n'a pas fait l'objet d'une acceptation préalable ou concomitante de celui-ci au titre de l'entraide pénale, être exploitées en procédure qu'avec son autorisation. Dans un arrêt du 9 février 2016⁷⁶, la Cour de cassation a statué sur la pose de dispositifs de géolocalisation sur une Renault Clio et une Audi A2, utilisées par les personnes soupçonnées de trafic de stupéfiants, permettant de constater les déplacements de ces véhicules en France, en Belgique et aux Pays-Bas. Ces opérations de

sauraient se faire un grief de ce que la chambre de l'instruction a rejeté leur requête par les motifs repris au moyen, dès lors qu'en dehors du recours, par les autorités publiques, à un procédé déloyal, non démontré, ni même allégué, en l'espèce, un mis en examen est irrecevable à contester la régularité de la géolocalisation en temps réel d'un véhicule volé et faussement immatriculé sur lequel il ne peut se prévaloir d'aucun droit. »

⁷⁶. Cass.crim, (n° 15-85.070), 9 février 2016, M. X.

Droit de l'espace numérique

géolocalisation ne sont pas légales dès lors que « les demandes d'entraide pénale internationales indispensables à l'utilisation et à l'exploitation de ces données en procédure ne se trouvent pas au dossier de l'information ».

Le calendrier commande

Compte tenu de l'atteinte aux libertés individuelles qu'entraîne la géolocalisation en temps réel, les conditions de forme sont rigoureuses, s'agissant notamment de la prise en compte de la chronologie.

Ainsi, le 29 septembre 2020, la Chambre criminelle de la Cour de cassation⁷⁷ considère que la pose d'une balise de géolocalisation par un enquêteur agissant en urgence doit faire l'objet d'une information immédiate du procureur de la République ou du juge d'instruction. Dans le cadre d'une information judiciaire, des enquêteurs procèdent un matin, à 3H20, à la pose d'un dispositif de géolocalisation sur un véhicule. Ils agissent en vertu des dispositions de l'article 230-35 du CPP. Ils avisent le juge d'instruction à 9h30. Le véhicule fait également l'objet de mesures de sonorisation. Ces dispositifs combinés permettent l'interpellation et la mise en examen de l'auteur. Celui-ci demande à la Cour l'annulation de la mesure de géolocalisation jugée conforme par la chambre de l'instruction.

La Cour considère qu'en cas d'urgence résultant d'un risque imminent de déperissement des preuves ou d'atteinte grave aux

⁷⁷. Cour de cassation – Chambre criminelle – (20-80.915) - Arrêt n° 1715 du 29 septembre 2020.

Droit de l'espace numérique

personnes ou aux biens, et dans les cas mentionnés aux articles 230-33 et 230-34 du CPP, un officier de police judiciaire peut prescrire ou mettre en place les opérations de localisation en temps réel, par tout moyen technique, d'un véhicule sans le consentement de son propriétaire ou possesseur, à la condition qu'il en informe immédiatement, par tout moyen, le procureur de la République ou le juge d'instruction. Cette immédiateté se justifie parce qu'elle permet le contrôle effectif du juge sous lequel est placée la mesure de géolocalisation qui constitue une ingérence dans la vie privée. Elle doit être interprétée strictement. Ainsi, « méconnaît l'article 230-35 du code de procédure pénale et viole l'article 8 de la Convention européenne des droits de l'homme, la chambre de l'instruction qui a déclaré régulière la mesure de géolocalisation quand il résultait de ses constatations que les enquêteurs ont procédé à la pose du dispositif de géolocalisation le 28 février 2019 à 3 heures 20 et que le juge d'instruction n'en a été informé que le 28 février 2019 à 9 heures 30, soit 6 heures 10 plus tard ».

Dans un arrêt du 19 février 2019⁷⁸, la Cour de cassation offre un autre exemple de son interprétation « à la minute près » des textes.

En l'espèce, les policiers ont sollicité du procureur de la République la mise en place d'un dispositif de suivi en temps réel d'un véhicule. L'autorisation a été accordée le 22 mars 2017 pour une durée maximale de dix-sept jours consécutifs. Le dispositif a été mis en place le 29 mars 2017 à 23 heures 51. Le 13 avril 2017, les enquêteurs ont sollicité une prolongation de la géolocalisation qui a

⁷⁸. Cour de cassation – Chambre criminelle – (18-84.671) – Arrêt n°165 du 19 février 2019.

Droit de l'espace numérique

été autorisée le 14 avril 2017 par le juge des libertés et de la détention pour une durée d'un mois à compter de sa mise en place effective. Cette affaire permet à la Cour de préciser que :

- s'agissant d'une mesure qui porte atteinte à la vie privée, toute journée durant laquelle le dispositif a été fonctionnel, même pendant une période de temps minime, doit être prise en compte dans la computation des délais. Même si la mise en place n'a été effective le 29 mars 2017 que durant quelques minutes, cette journée doit être considérée comme la première du délai de quinze jours autorisé par le procureur de la République ;
- le dispositif pouvait donc être encore exploité durant encore quatorze jours pleins de sorte que l'autorisation était valable jusqu'au 12 avril 2017 à minuit. La prolongation n'en a été autorisée par le juge des libertés et de la détention que le 14 avril 2017. Celle-ci est intervenue avant 10 heures 32. L'article 230-33 du CPP n'exige pas une continuité entre l'expiration du délai durant lequel la mesure est autorisée par le procureur de la République et la délivrance de l'autorisation du juge des libertés et de la détention faisant courir, à partir de ce moment, un nouveau délai ;
- l'ordonnance du juge des libertés et de la détention mentionne dans son dispositif que la prolongation est autorisée pour une durée d'un mois « à compter de sa mise en place effective », c'est-à-dire le 29 mars 2017. Toute exploitation de celle-ci postérieure au 28 avril 2017 à minuit est donc irrégulière. L'article 230-33 ne précise pas que la prolongation part de la date initiale, mais l'ambiguïté doit être interprétée dans un sens favorable à la protection des libertés publiques.

Droit de l'espace numérique

Sont donc affectés de nullité tous les actes d'exploitation de la géolocalisation correspondant à la période comprise entre le 13 avril 2017 à minuit et le 14 avril 2017 à 10 heures 32.

Droit de l'espace numérique

Par le capitaine/Docteur Thibaut HECKMANN

**Royal Courts of Justice, [2021] EWCA Crim 128, arrêt
du 5 février 2021, cas EncroChat**

Les données récoltées par la gendarmerie française, dans le cadre de l'affaire EncroChat, sont jugées recevables par les tribunaux britanniques. Ainsi, les juges britanniques ont décidé que l'implant (voir *infra*, p. 48) actif français ne constituait pas une interception judiciaire et ne contrevenait pas aux dispositions légales énoncées dans la loi britannique de 2016 sur les pouvoirs d'investigation.

EncroChat était l'un des plus grands services de communications chiffrées au monde avec environ 60 000 utilisateurs (20 % de Britanniques), dont les fonctionnalités étaient essentiellement exploitées par les criminels. Le service de messagerie EncroChat a été découvert par l'Institut de recherche criminelle de la gendarmerie nationale (IRCGN) en 2017 lors d'expertises judiciaires contre le crime organisé. L'enquête s'est accélérée le 10 avril 2020 par la constitution d'une Équipe commune d'enquête (ECE) entre les autorités judiciaires françaises, néerlandaises et britanniques, sous l'égide d'Eurojust, avec le soutien d'Europol. Finalement, le renseignement et la collaboration technique internationale ont abouti à l'accès aux messages déchiffrés des utilisateurs d'EncroChat grâce à la mise en place d'un dispositif technique actif sur les téléphones d'EncroChat dont les serveurs se trouvaient en France. Le logiciel (implant) leur a permis de lire plusieurs millions

Droit de l'espace numérique

de messages chiffrés et d'enregistrer les mots de passe de chiffrement des téléphones. Les forces de l'ordre du monde entier ont ainsi pu procéder à près de 1 100 arrestations, à la saisie de plus de 35 tonnes de drogues et plus de 169 millions d'euros. En droit français, la technique développée par la gendarmerie répond au cadre juridique de la captation de données informatiques constituant une technique spéciale d'enquête prévue par l'article 706-102-1 du Code de procédure pénale : « Il peut être recouru à la mise en place d'un dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, de les conserver et de les transmettre, telles qu'elles sont stockées dans un système informatique, telles qu'elles s'affichent sur un écran pour l'utilisateur [...], telles qu'il les y introduit par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques ». Cette mesure est strictement encadrée au cours de l'information judiciaire par le juge d'instruction après avis du procureur de la République (article 706-95-12 du Code de procédure pénale). Ainsi, les données récoltées par la gendarmerie française, dans le cadre de l'affaire EncroChat, sont recevables par les tribunaux français.

EncroChat et le droit britannique

Les autorités françaises ont évoqué, en conférence de presse, avoir développé un dispositif technique, appelé « implant », qui leur a permis d'accéder à des informations cruciales qui ont ensuite été partagées avec la National Crime Agency (NCA) du Royaume-Uni. La NCA, dans le cadre de l'opération Venetic, a ainsi pu collecter des

Droit de l'espace numérique

milliers de messages avant que la faille de sécurité ne soit connue et que le réseau EncroChat ne mette fin à son service. Décrite par le directeur des enquêtes de la NCA comme « l'opération la plus vaste jamais menée contre le crime organisé », l'opération française a déjà abouti à 750 arrestations au Royaume-Uni et à la saisie de plus de 55 millions de livres sterling. Cependant, en vertu du droit britannique, les preuves interceptées lors du transfert de messages ne peuvent pas être utilisées devant les tribunaux et doivent être utilisées uniquement à des fins de renseignement⁷⁹, après l'autorisation d'un Secrétaire d'État et du juge⁸⁰.

La position de la défense

Les avocats de quatre accusés ont fait appel de la validité du dispositif technique utilisé par la France et ont demandé à ce que toutes les données récoltées dans le cadre de l'affaire EncroChat soient jugées irrecevables par les tribunaux britanniques⁸¹. L'argument principal était que le dispositif français constituait une interception des données entre le téléphone et le serveur d'EncroChat. Cependant, l'*Investigatory Powers Act* de 2016 autorise formellement que le contenu des communications obtenues directement et/ou physiquement sur un téléphone ou un ordinateur soit utilisé comme preuve devant un tribunal⁸². L'article reste valable

⁷⁹. Part 2, *Interception of communication, Investigatory Powers Act 2016, Parliament of the United Kingdom*, 29 November 2016.

⁸⁰. « *The act introduced a double lock that requires interception warrants to be authorised by a secretary of state and approved by a judge* ».

⁸¹. R v Director of Public Prosecutions [2020] EWHC 2967 Admin.

⁸². Part 5, *Equipment Interference, Investigatory Powers Act 2016, Parliament of the United Kingdom*, 29 November 2016.

Droit de l'espace numérique

dans le cas où le contenu est extrait physiquement du téléphone (par exemple dans le cas de l'expertise réalisée après la saisie du téléphone) mais également dans le cas où un logiciel est installé sur le téléphone, permettant ainsi l'extraction indirecte des données⁸³.

La Cour d'appel met un terme au débat

Ainsi, le 5 février 2021, l'arrêt de la Cour d'appel dans l'affaire A & Others [2021] EWCA Crim 128 a été rendu et permet de mettre un terme au débat. L'arrêt a effectivement rejeté les arguments pour mettre fin à l'utilisation des données obtenues à partir du réseau de communication EncroChat dans les procédures judiciaires. En termes simples, les juges ont affirmé que les données obtenues par les forces de l'ordre françaises et néerlandaises ne constituaient pas une interception mais une intervention directe sur le téléphone et ne contrevenaient donc pas aux dispositions légales énoncées dans la loi de 2016 sur les pouvoirs d'investigation. Les juges ont décidé que, dans un premier temps, les données étaient en réalité stockées temporairement en clair dans la mémoire des appareils puis que les données étaient chiffrées par le téléphone avant d'être transmises chiffrées sur le serveur d'EncroChat. Les juges indiquent que le logiciel permettait de copier les messages du téléphone avant leur chiffrement (directement depuis la mémoire du téléphone) et que ces messages étaient envoyés non chiffrés sur un serveur de la

⁸³. « *Equipment interference warrants may authorise both physical interference [...] and remote interference (e.g. installing a piece of software on to a device over a wired and/or wireless network in order to remotely extract information from the device)* ».

Droit de l'espace numérique

gendarmerie française. Les juges rappellent que, dans ce cas, il ne s'agit pas d'une interception pendant l'envoi (ce que n'autorise pas la loi britannique) et que cela ne constitue donc pas une interception. Les juges précisent que cela se justifie d'autant plus que, lors de la transmission proprement dite, le message est chiffré et donc non exploitable par la gendarmerie française. De plus, ils affirment que les métadonnées obtenues par la gendarmerie (par exemple le nom de l'utilisateur) étaient uniquement présentes dans la mémoire du téléphone et non lors de la transmission, ce qui démontre que les données ont été récupérées dans la mémoire du téléphone et non lors de leur transmission. Dans l'arrêt rendu, les juges comparent le processus à celui de l'envoi d'une lettre : « Le processus consiste à rédiger la lettre (rédaction du message non chiffré), à la mettre dans une enveloppe (chiffrement), à apposer un timbre (destinataire) puis à placer la lettre dans la boîte postale (envoi sur le serveur d'EncroChat) ». Ainsi, seule la récupération du message lors de sa transmission implique une interception mais pas les premiers éléments du processus. L'implant français récupérant le message avant son envoi, cela ne peut constituer une interception en droit britannique. Les juges ont donc conclu que les communications transmises au Royaume-Uni n'ont pas été obtenues pendant leur transmission, mais pendant leur stockage dans la mémoire du téléphone. L'arrêt permet également de préciser que l'interception ne peut être retenue que si elle a lieu directement lors de la transmission des données provenant d'un signal radio, d'un câble ou d'une fibre optique mais pas si les données sont copiées à partir de la mémoire de l'appareil cible. Actuellement, de nombreuses affaires fondées sur des preuves obtenues par les

Droit de l'espace numérique

autorités françaises sont jugées devant les tribunaux britanniques ; toutes les contestations judiciaires quant à la légalité de la manière dont ces preuves ont été obtenues par les forces de l'ordre ont été rejetées grâce à l'arrêt de la Cour d'appel dans l'affaire [2021] EWCA Crim 128.

Droit de l'espace numérique

Par le Général d'armée (2S) Marc Watin-Augouard

Tribunal judiciaire de Paris, ordonnance de référé du 4 mars 2021, Présidente de la Commission nationale de l'informatique et des libertés (CNIL)/ Orange, Free, Bouygues Telecom, SFR

Faute de pouvoir agir sur l'hébergeur, l'éditeur ou l'auteur d'un fichier contenant des données médicales à caractère personnel, diffusées de manière illicite, le juge des référés, en application de la Loi pour la confiance dans l'économie numérique (LCEN), enjoint aux fournisseurs d'accès à Internet (FAI) de bloquer l'accès à un service de communication au public en ligne «***.gg ».**

Une violation concernant des données personnelles et médicales de près de 500 000 patients a été révélée au mois de février 2021. Ces données particulièrement sensibles au sens de l'article 9 du Règlement général sur la protection des données (RGPD) ont été illégalement collectées et rassemblées dans un fichier informatique rendu accessible en ligne. Dès la connaissance de cette violation, les services de la Commission nationale de l'informatique et des libertés (CNIL) ont procédé à une opération de contrôle en ligne, en application de la décision n° 2021-028C du 24 février 2021 de sa présidente. Il est apparu qu'un forum de discussion partageait par un lien de téléchargement direct un fichier hébergé sur un serveur tiers et contenant les données concernées. Ce fichier contient 491 840 lignes qui correspondent chacune à une personne bien

Droit de l'espace numérique

identifiée. Sur chaque ligne sont mentionnés :

- son nom d'usage (éventuellement accompagné de son nom patronymique) et son prénom ;
- sa date de naissance ;
- son numéro de téléphone fixe et/ou de son portable ;
- son numéro de sécurité sociale (NIR) ;
- son adresse postale et son adresse électronique.

D'autres données sont également publiées : nom et coordonnées du médecin traitant, date de la dernière visite médicale, nom de l'assuré social dont le patient est ayant droit, groupe sanguin, facteur rhésus, existence ou non d'une affection de longue durée. S'ajoutent des commentaires non dénués de données à caractère personnel.

La CNIL tente d'intervenir auprès de l'hébergeur, de l'éditeur et de l'auteur, mais sans succès, situés à l'étranger ou inconnus. Elle se tourne alors vers le juge des référés. L'article 21 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés dispose que : « En cas d'atteinte grave et immédiate aux droits et libertés mentionnés à l'article 1^{er} de la présente loi, le président de la commission peut en outre demander, par la voie du référé, à la juridiction compétente d'ordonner, le cas échéant sous astreinte, toute mesure nécessaire à la sauvegarde de ces droits et libertés ».

Le référé est prévu par l'article 6.I-8 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique : « L'autorité judiciaire peut prescrire en référé ou sur requête, à toutes

Droit de l'espace numérique

personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services ou, à défaut, à toutes personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne. » Par référé d'heure à heure en date du 1^{er} mars 2021, la CNIL demande au juge d'enjoindre la SA Orange, la SAS Free, la SA SFR et la SA Bouygues Telecom de mettre en œuvre ou de faire mettre en œuvre, sans délai et de manière définitive et illimitée, toutes mesures les plus adaptées et les plus efficaces de surveillance ciblées de nature à assurer le blocage effectif du fichier « full fr *****.7z » ou, à défaut, du service de communication au public en ligne « *****.gg » sur les réseaux des défendeurs ou, à défaut, l'adresse URL « https://*****.gg/*****.7z ».

Pour faire cesser l'atteinte grave et immédiate aux droits et libertés des personnes, le juge des référés enjoint les sociétés visées *supra* de mettre en œuvre ou de faire mettre en œuvre, sans délai et pour une période de 18 mois à compter de la présente décision, toutes mesures les plus adaptées et les plus efficaces de surveillance ciblées de nature à assurer le blocage effectif, sur leurs réseaux, du service de communication au public en ligne « *****.gg » qui correspond à un nom de domaine national de premier niveau réservé à l'île de Guernesey. Faute de pouvoir obtenir le retrait du fichier, devant le mutisme de l'hébergeur, la société Cloudflare, dont

Droit de l'espace numérique

le siège social est à San Francisco, la procédure de blocage est la seule possible.

Tribunal judiciaire de Paris, ordonnance de référé du 25 février 2021, Mme X./ Twitter International Company

La plaignante a créé une chaîne sur la plateforme YouTube ayant vocation à partager les moments de loisirs de sa famille et dont ses enfants sont les protagonistes principaux. En juillet 2020, elle est alertée de la création d'un hashtag sur la plateforme Twitter, afin de dénoncer une prétendue emprise nocive et une instrumentalisation par elle de ses enfants mis en scène dans les vidéos publiées. Un compte intitulé « X.@X. », accessible à l'adresse URL « <https://twitter.com/X> », participe à cette dénonciation sur les réseaux sociaux et incite à sa diffusion la plus large, comme en atteste un procès-verbal de constat d'huissier en date du 21 septembre 2020. Afin d'interrompre le délai court de prescription, Mme X. dépose une plainte avec constitution de partie civile du chef de diffamation publique envers un particulier, en date du 23 octobre 2020, auprès du doyen des juges d'instruction du tribunal judiciaire de Paris. Craignant un risque de dépérissement de la preuve, eu égard à l'état d'avancement du dossier devant le magistrat, elle saisit le tribunal par voie de référé sur la base des articles 145 du Code de procédure civile et 6- I.2, 6-I.8 et 6.II alinéas 1 et 3 de la loi n° 2004-575 du 21 juin 2004 (LCEN).

Droit de l'espace numérique

Art 145 CPC (référé expertise)

« S'il existe un motif légitime de conserver ou d'établir avant tout procès la preuve de faits dont pourrait dépendre la solution d'un litige, les mesures d'instruction légalement admissibles peuvent être ordonnées à la demande de tout intéressé, sur requête ou en référé. »

Art 6-I.2 LCEN

« Les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services ne peuvent pas voir leur responsabilité civile engagée du fait des activités ou des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de leur caractère manifestement illicite ou de faits et circonstances faisant apparaître ce caractère ou si, dès le moment où elles en ont eu cette connaissance, elles ont agi promptement pour retirer ces données ou en rendre l'accès impossible. »

Art 6-I. LCEN

« L'autorité judiciaire peut prescrire en référé ou sur requête, aux personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services ou, à défaut, à toute personne dont l'activité est d'offrir un accès à des services de communication au

Droit de l'espace numérique

public en ligne, toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne. »

Art.6. II al 1 et 3

« Les personnes mentionnées aux 1 et 2 du I (*ndlr* : voir art. 6-I ci-dessus) détiennent et conservent les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires.

Elles fournissent aux personnes qui éditent un service de communication au public en ligne des moyens techniques permettant à celles-ci de satisfaire aux conditions d'identification prévues au III.

L'autorité judiciaire peut requérir communication auprès des prestataires mentionnés aux 1 et 2 du I des données mentionnées au premier alinéa. »

La plaignante demande que Twitter soit enjoint à lui fournir l'ensemble des données d'identification en sa possession et notamment les IP de connexion, les ports sources de connexion, les nom et prénom, la dénomination sociale, les adresses postales associées, les adresses de courrier électronique associées et les numéros de téléphone utilisés lors de la création du compte Twitter « X. », accessible à l'adresse URL incriminée ainsi que l'ensemble des données d'identification associées aux publications litigieuses, accessibles à d'autres URL. Le décret du 25 février 2011⁸⁴ précise la

⁸⁴. Décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne.

Droit de l'espace numérique

liste des données collectées par les hébergeurs pour chaque opération de création de contenu (article 1^{er}) et la durée de conservation requise (article 3), celle-ci étant d'un an à compter de la résiliation du contrat souscrit lors de la création d'un compte ou de la fermeture de celui-ci pour ce qui concerne les données fournies lors de la souscription du compte considéré.

Twitter conteste la procédure suivie en considérant que le référé vient s'ajouter à une ouverture d'information. Le tribunal rejette cette objection : « Le motif légitime, en l'espèce, dont peut se prévaloir Mme X., consiste à établir la preuve de l'identité du possesseur de compte Twitter, éventuels auteurs des dommages dont elle se dit victime. Il lui appartient, qu'il s'agisse de responsabilité civile ou pénale, d'exposer le fait personnel de l'auteur, pour lequel elle entend voir dévoiler l'anonymat. [...] Le dépôt d'une plainte avec constitution de partie civile du chef de diffamation publique, auquel il a été procédé en l'espèce le 23 octobre 2020, permettant d'empêcher la prescription de l'action publique, n'exclut pas, en soi, la possibilité de solliciter une mesure d'instruction sur le fondement de l'article 145 du Code de procédure pénale, dès lors que l'intervention du juge d'instruction ne se limite nullement à la recherche de l'auteur des propos litigieux et qu'est établie l'existence d'un motif légitime tenant, notamment, à la durée de conservation des données d'identification ».

Sur la communication des données, le tribunal, afin de garantir la proportionnalité de la mesure ordonnée, limite la demande d'identification aux seules données utiles à la réunion des éléments susceptibles de commander la solution du litige potentiel, eu égard aux données que l'hébergeur est amené à collecter en application

Droit de l'espace numérique

des dispositions de l'article 1^{er} du décret du 25 février 2011, soit :

- les types de protocoles et l'adresse IP utilisés pour la connexion au service ;
- au moment de la création du compte, l'identifiant de cette connexion ;
- la date de création du compte ;
- les nom et prénom ou la raison sociale du titulaire du compte ;
- les pseudonymes utilisés ;
- les adresses de courrier électronique ou de comptes associés.

On notera que la conservation des données de connexion est un sujet qui oppose la France à la Cour de justice de l'Union européenne. Cette juridiction a, récemment encore (arrêt du 6 octobre 2020, *Quadrature du Net contre gouvernement français* – voir [La veille juridique](#) n° 91, novembre 2020, p. 13-29), condamné l'obligation généralisée et indifférenciée de collecte et de conservation des données, confirmant ainsi sa jurisprudence *Tele2* (arrêt du 21 décembre 2016). Fort de cet arrêt, Free vient de saisir le Conseil d'État.

Actualité pénale

Claudia GHICA-LEMARCHAND

DROIT DE SE TAIRE

Le droit de ne pas contribuer à sa propre incrimination, que l'on appelle aussi droit de ne pas s'auto-accuser ou s'auto-incriminer, prend sa source dans la présomption d'innocence et le droit au procès équitable. Le Pacte des droits civils et politiques de 1966 le consacre formellement dans son article 14 §3 littera g, « toute personne accusée d'une infraction ayant le droit à ne pas être forcée de témoigner contre elle-même ou de s'avouer coupable », mais lui assigne un domaine d'application relativement restreint. En revanche, la jurisprudence européenne l'ouvre largement en puisant dans l'inspiration du principe « *nemo se ipsum accusare tenetur* ». « Même si l'article 6 Conv. EDH ne le mentionne pas expressément, (...) le droit de ne pas contribuer à sa propre incrimination est une norme internationalement reconnue et qui est au cœur du procès équitable » (CEDH 3 mai 2001, *J.B. c/ Suisse*, § 64). S'il est une notion procédurale centrale, « le droit de se taire et le droit de ne pas contribuer à sa propre incrimination sont au cœur de la notion de procès équitable » (CEDH 8 février 1996, *John Murray c/RU*) ou « étroitement lié au principe de la présomption d'innocence » (CEDH 17 décembre 1996, *Saunders c/ Royaume-Uni*, § 68), il revêt aussi un aspect substantiel puisqu'il exclut l'emploi de la force (CEDH Gr. Ch. 11 juillet 2006, *Jalloh c/ Allemagne*) et écarte de la procédure des éléments de preuve recueillis au mépris de l'article 3 interdisant les traitements inhumains, dégradants et de la torture en vue d'obtenir des aveux (CEDH 17 janvier 2007, *Göçmen c/ Turquie*). Son « but

Actualité pénale

[est] de protéger l'accusé contre une coercition abusive de la part des autorités et, ainsi, d'éviter les erreurs judiciaires et d'atteindre les buts de l'article 6 » (CEDH 10 mars 2009, *Bykov c/ Russie*, § 92). Le droit de ne pas s'auto-incriminer s'entend largement comme révélant le choix de ne pas s'exprimer oralement devant des policiers, des enquêteurs, des magistrats, mais aussi le droit de refuser de s'exprimer par écrit. S'il connaît plusieurs manifestations, parmi lesquelles le droit de refuser de produire certains documents (CEDH 25 février 1993, *Funke c/ France*) ou de se soumettre à certaines investigations ou prélèvements, la procédure pénale le relie notamment au droit de se taire ou de garder le silence à tel point qu'une rivalité s'établit entre les deux notions. Si les premières décisions en la matière considèrent le droit de garder le silence comme l'essence même du droit de ne pas s'auto-incriminer, analyse matérialisée par la forme même des motivations considérant l'article 6 comme attribuant le droit pour tout accusé « de se taire et de ne point contribuer à sa propre accusation » (CEDH 8 février 1996, *Murray c/ Royaume-Uni*, R.S.C. 1997, p. 476, obs. KOERING-JOULIN), l'ordre de préséance change ultérieurement. Le droit de ne pas s'auto-incriminer est utilisé en premier par les juges, car il est le fondement même de tous les autres droits qui en découlent : il ne peut être admis que des mesures d'investigation portent atteinte « à la substance même du droit de ne pas s'auto-incriminer et du droit de garder le silence » (CEDH 21 décembre 2000, *Heaney et Mc Guinney c/ Irlande*, § 55). Le droit de garder le silence devient une manifestation du droit de ne pas s'incriminer : « Le droit de ne pas s'incriminer soi-même est au cœur de la notion de procès équitable... et il tend principalement au respect de la volonté d'un accusé de garder le silence » (CEDH 17 décembre 1996, *Saunders c/*

Actualité pénale

Royaume-Uni, § 68).

Le principe général de ne pas s'auto-incriminer peut neutraliser l'obligation de collaborer aux mesures d'investigation. Il s'analyse comme un prolongement naturel des droits de la défense. Ainsi, son respect doit être assuré dans les procédures judiciaires, comme dans le cadre des procédures administratives, notamment douanières (Crim. 24 février 2009, Bull. n° 46), fiscales, etc. S'il s'applique aussi bien aux personnes physiques qu'aux personnes morales, la question se pose de savoir s'il s'applique à toutes les phases de la procédure pénale. Le droit français a assuré une réception progressive au droit de ne pas contribuer à sa propre incrimination inspiré par la tradition anglaise. Le droit au silence, sujet éminemment classique, même s'il a vu sa force affermie par des réformes successives, se trouve renouvelé et relancé par plusieurs arrêts récents, émanant de juridictions différentes.

Conseil constitutionnel n° 2020-886 QPC du 4 mars 2021 – Information du prévenu du droit qu'il a de se taire devant le juge des libertés et de la détention en cas de comparution immédiate

Le Conseil constitutionnel est saisi d'une question prioritaire de constitutionnalité (QPC) relative à l'article 396 du Code de procédure pénale mettent en place la comparution immédiate du prévenu devant le juge des libertés et de la détention (JLD) dans l'hypothèse dans laquelle une mesure de détention provisoire semble nécessaire. Cette procédure méconnaîtrait le principe de la présomption d'innocence, dont découle le droit de se taire, ainsi que les droits de la défense, dans la mesure où elle ne prévoit pas que le JLD doit notifier au prévenu qui comparait devant lui son

Actualité pénale

droit de garder le silence. Cette absence aurait plusieurs conséquences défavorables à l'égard de la personne concernée – le juge doit apprécier les charges, ce qui peut conduire la personne à faire des déclarations auto-incriminantes qui seraient consignées dans le procès-verbal et pourraient être apportées à la connaissance du tribunal chargé de statuer sur sa culpabilité. Naît ainsi « une différence de traitement inconstitutionnelle entre les prévenus jugés en comparution immédiate selon qu'ils sont traduits devant le tribunal correctionnel le jour même de sa saisine ou seulement après avoir comparu devant le juge des libertés et de la détention, lorsque la réunion du tribunal est impossible le jour même ».

Le Conseil constitutionnel constate l'inconstitutionnalité de l'article 396 du Code de procédure pénale, car « lorsqu'il est invité par le juge des libertés et de la détention à présenter ses observations, le prévenu peut être amené à reconnaître les faits qui lui sont reprochés », alors que, de surcroît, « le fait même que le juge des libertés et de la détention invite le prévenu à présenter ses observations peut être de nature à lui laisser croire qu'il ne dispose pas du droit de se taire ». Si la décision du JLD est sans incidence sur la qualification des faits retenus et soumis au tribunal correctionnel, les observations du prévenu consignées dans le procès-verbal sont susceptibles d'être portées à la connaissance de ce tribunal. Le Conseil constitutionnel s'appuie sur l'article 9 de la Déclaration des droits de l'Homme et du citoyen qui garantit la présomption d'innocence, de laquelle « résulte le principe selon lequel nul n'est tenu de s'accuser, dont découle le droit de se taire ».

Sans aucune autre considération, le Conseil constitutionnel décide que l'article 396 porte atteinte au droit de se taire, mais choisit d'aménager ses effets dans le temps. L'inconstitutionnalité est

Actualité pénale

assortie d'effet différé, car l'abrogation prend effet au 31 décembre 2021 afin d'éviter des conséquences manifestement excessives. Les décisions prises sur son fondement ne pourront pas être contestées sur le fondement de l'inconstitutionnalité. En revanche, à compter de la publication de la décision, le JLD intervenant dans le cadre de l'article 396 doit informer le prévenu de son droit de se taire.

Cette décision est intéressante, car elle intervient dans un domaine inattendu et de manière indirecte. En effet, même s'il y a eu de nombreuses évolutions et contestations sur l'information de se taire dans le cadre de la phase d'enquête, le Code de procédure pénale le prévoyait dans le cadre de l'instruction. Les articles 116, à l'égard du mis en examen, et 113-4, à l'égard du témoin assisté, font obligation au juge d'instruction d'informer la personne « de son droit de faire des déclarations, de répondre aux questions qui lui sont posées ou de se taire ». Ce droit est indirectement renforcé par le fait que le mis en examen et le témoin assisté ne sont pas soumis à l'obligation de prêter serment, ce qui renforce leur droit au silence, même si les juges peuvent déduire des conséquences négatives de son exercice. Mais si le droit de se taire est un droit général qui perdure tout au long de la procédure, le juge n'est pas obligé de le rappeler à toute nouvel acte de procédure. Ainsi, dans un arrêt récent rendu le 4 novembre 2020, n° 20-84.046, la Chambre criminelle affirme « qu'aucun texte ne fait obligation au magistrat instructeur, de renouveler, à l'occasion de chaque acte, l'avertissement [de ce] droit [...] », de sorte que la nullité des actes ne peut être prononcée lorsque la personne ne peut démontrer aucun grief ni aucune atteinte à ses droits. Il convient d'attendre les

Actualité pénale

nouvelles dispositions relatives aux obligations du juge des libertés et de la détention pour avoir le tableau complet des obligations faites aux magistrats.

Crim. 12 janvier 2021, n° 20-85.841 (QPC) ; Crim. 27 janvier 2021, n° 20-86.037 ; Crim. 9 février 2021, n° 20-86.533 (QPC) ; Crim. 10 février 2021, n° 20-86.310 (QPC) ; Crim. 16 février 2021, n° 20-86.537 (QPC) ; Crim. 24 février 2021, n° 20-86.537

La multitude des arrêts relatifs à la notification du droit de se taire démontre un renouvellement et une vivacité de la question dans la jurisprudence récente. Si certaines réponses sont encore attendues, ces décisions permettent de renforcer la notification du droit de se taire. La Cour de cassation est confrontée à une série de QPC portant sur l'information du droit de se taire, devant les juridictions d'instruction plus particulièrement. Elles prennent une importance particulière à la suite de la transmission de la QPC de décembre 2020 au Conseil constitutionnel qui a abouti à la déclaration d'inconstitutionnalité commentée précédemment.

Les QPC visent l'article 199 du Code de procédure pénale régissant l'audience devant la chambre de l'instruction lorsqu'elle statue en appel et est déclinée selon les différents objets de l'audience.

Dans l'arrêt du 12 janvier 2021, la Chambre criminelle statue sur l'appel soumis à la chambre de l'instruction lorsqu'elle statue sur la requête en nullité de la mise en examen. À cette fin, elle apprécie la comparution personnelle des parties qui ne peuvent pas présenter des observations, mais doivent répondre aux questions que les juges estiment utiles à l'instruction du dossier. Dans ce contexte, la personne peut faire des déclarations, sans avoir reçu notification de

Actualité pénale

son droit de se taire. La QPC considère que ce dispositif est contraire au principe selon lequel nul n'est tenu de s'accuser et aux droits de la défense. La Chambre criminelle décide de transmettre cette question au Conseil constitutionnel.

Lorsque la personne comparaît devant la chambre de l'instruction qui statue sur la détention provisoire, elle n'est pas informée de son droit de se taire « alors que la chambre de l'instruction doit s'assurer que les conditions légales de la détention provisoire sont réunies, et notamment de l'existence d'indices graves ou concordants rendant vraisemblable la participation de la personne mise en examen aux faits reprochés (Crim. 14 octobre 2020, n° 20-82.961, publié au bulletin) », ce qui méconnaîtrait les droits et libertés constitutionnellement garantis et plus particulièrement les articles 6, 9 et 16 de la Déclaration des droits de l'Homme et du citoyen de 1789. La Chambre criminelle, dans son arrêt du 9 février 2021, décide de renvoyer la QPC au Conseil constitutionnel, car la personne détenue peut être amenée à faire des déclarations qui resteront au dossier de la procédure. Or, « en l'absence d'une notification préalable à la personne détenue de son droit de se taire, il pourrait être porté atteinte à son droit de ne pas s'accuser ». L'arrêt du 16 février porte sur une QPC identique, raison pour laquelle la Cour de cassation décide de ne pas renvoyer au Conseil constitutionnel. En application de l'article R 49-33 du Code de procédure pénale, la Cour de cassation n'est pas tenue de renvoyer au Conseil constitutionnel une question prioritaire de constitutionnalité mettant en cause, par les mêmes motifs, une disposition législative dont le Conseil constitutionnel est déjà saisi, mais elle diffère sa décision jusqu'à l'intervention de la décision. En revanche, dans son arrêt du 10 février 2021, la Chambre

Actualité pénale

criminelle décide de renvoyer une QPC portant sur le même article 199 et l'absence de l'information du droit de se taire mais appliquée à la procédure de l'appel formé contre une ordonnance de règlement, donc de renvoi devant une juridiction de jugement. La déclaration d'inconstitutionnalité fait planer un doute sérieux sur la constitutionnalité de ces dispositions, mais la Cour de cassation complique la situation en apportant sa propre appréciation de ces dispositions.

Dans l'arrêt du 27 janvier 2021, une personne est mise en accusation devant la Cour d'assises pour violences volontaires ayant entraîné la mort sans intention de la donner par personne ayant autorité sur la victime. Elle fait appel de l'ordonnance du juge d'instruction devant la chambre de l'instruction qui confirme la décision. La personne forme un pourvoi en cassation dans lequel elle fait valoir la violation de l'article 6 de la Convention de sauvegarde des droits de l'Homme et des libertés fondamentales (CSDHLF) dans la mesure où la chambre de l'instruction ne l'informe pas de son droit de répondre aux questions ou de se taire. La Chambre criminelle rejette le pourvoi en estimant « la personne mise en examen n'a pas comparu au sens de l'article 199 du code de procédure pénale et n'a à aucun moment, au cours des débats, été entendue sur les faits qui lui sont reprochés ou sur la nature des charges pesant sur elle ». Même si elle affirme un principe général d'information de la personne de son droit de faire des déclarations, de répondre aux questions qui lui sont posées ou de se taire par la chambre de l'instruction, elle le limite au cadre de l'article 199.

Dans l'arrêt du 24 février 2021, une personne est mise en examen et placée en détention provisoire le même jour. Sa demande de mise

Actualité pénale

en liberté est rejetée par le JLD et l'appel confirme cette décision. Il forme un pourvoi en cassation dans lequel il exploite, à la fois, l'inconstitutionnalité et l'inconventionnalité de l'article 199 du code de procédure pénale, plus particulièrement la procédure devant la chambre de l'instruction statuant sur la détention provisoire. D'une part, la déclaration d'inconstitutionnalité de l'article 199 priverait la décision de base légale puisque la chambre de l'instruction n'a pas informé le mis en examen de son droit de se taire. D'autre part, la méconnaissance de l'obligation d'informer la personne de son droit de se taire constitue une violation de l'article 6 de la CSDHLF. La Cour de cassation écarte facilement la première branche du moyen. En décidant de ne pas renvoyer la QPC formulée par l'intéressé (l'arrêt rendu le 16 février 2021 sus-cité), la Chambre criminelle refuse de statuer dans un délai de temps rapproché et diffère sa décision, même si l'individu est privé de sa liberté. La seconde branche du moyen retient l'attention.

La Chambre criminelle assure une interprétation large au droit à l'information issu de l'article 6 CSDHLF dans la mesure où « une juridiction prononçant un renvoi devant la juridiction de jugement ou une déclaration de culpabilité ne peut tenir compte, à l'encontre de la personne poursuivie, de déclarations sur les faits effectuées par celle-ci devant cette juridiction ou devant une juridiction différente sans que l'intéressé ait été informé, par la juridiction qui les a recueillies, de son droit de se taire, lorsqu'une telle information était nécessaire ». Or, la Cour de cassation estimait précédemment (Crim. 7 août 2019, n° 19-83.508) que cette information n'avait pas à être donnée lors d'une audience au cours de laquelle est examinée la détention provisoire de la personne mise en examen, car son audition a pour objet non pas d'apprécier la nature des indices

Actualité pénale

pesant sur elle, mais d'examiner la nécessité d'un placement ou d'un maintien en détention. Le contentieux des mesures de sûreté était soumis à un régime juridique différent des décisions sur la suite de la procédure, notamment le renvoi devant la juridiction de jugement. Une jurisprudence récente produit un effet incident. Dans un arrêt rendu le 27 janvier 2021 (n° 20-85.990), la Cour de cassation juge désormais « qu'il se déduit de l'article 5 1. c de la Convention européenne des droits de l'homme que la chambre de l'instruction, à chacun des stades de la procédure, doit s'assurer, même d'office, que les conditions légales des mesures de sûreté sont réunies, en constatant expressément l'existence d'indices graves ou concordants rendant vraisemblable la participation comme auteur ou complice de la personne mise en examen à la commission des infractions dont le juge d'instruction est saisi ». Dans la mesure où ces déclarations sont consignées dans le dossier renvoyé à la juridiction de jugement chargée de se prononcer sur la culpabilité, le droit de se taire doit nécessairement être apporté à la connaissance de la personne afin de pouvoir les prendre en compte. La Cour de cassation aboutit à une conclusion nuancée. « Le défaut d'information du droit de se taire est sans incidence sur la régularité de la décision rendue en matière de mesure de sûreté » qui ne trouve pas entachée de nullité. En l'espèce, la confirmation du refus de mise en liberté par la chambre de l'instruction est valable. Mais, « à défaut d'une telle information, les déclarations de l'intéressé ne pourront (...) être utilisées à son encontre par les juridictions appelées à prononcer un renvoi devant la juridiction de jugement ou une déclaration de culpabilité ». La chambre de l'instruction devra en faire abstraction lorsqu'elle sera amenée à statuer sur le bien-fondé de la mise en examen, qui relève d'un

Actualité pénale

contentieux distinct de celui des mesures de sûreté.

Il en résulte que l'information du droit de se taire est obligatoire devant la chambre de l'instruction lorsqu'elle statue sur les mesures de sûreté, donc la détention provisoire, mais pas lorsqu'elle statue sur la mise en examen et la suite de la procédure. Si le progrès des droits de la défense est évident, il semble bridé par cette réserve. Les décisions attendues du Conseil constitutionnel devraient dissiper les doutes en la matière.

En conclusion, il est intéressant de constater que le droit au silence continue de secouer la procédure pénale une décennie après l'arrêt Brusco, rendu le 14 octobre 2010, dans lequel la Cour européenne des droits de l'Homme avait condamné la France pour violation du droit du requérant de ne pas contribuer à sa propre incrimination et de garder le silence, violation aggravée par l'assistance tardive d'un avocat qui n'avait pu l'informer correctement de ces droits. Si la loi du 14 avril 2011 l'a réintroduit dans la phase de l'enquête de police, c'est la loi n° 2014-535 du 27 mai 2014 portant transposition de la directive n° 2012/13/UE du Parlement européen et du Conseil du 22 mai 2012 relative au droit à l'information dans le cadre des procédures pénales qui l'a généralisé et étendu à l'ensemble de la procédure pénale. Il s'applique à toutes les phases de la procédure, qu'il s'agisse de l'enquête de police, à l'égard du suspect gardé à vue (art. 63-1) ou entendu librement (art. 61-1), ou de l'examen de l'affaire par les juridictions d'instruction, qu'il s'agisse de la mise en examen par la juridiction de l'instruction (art. 116) ou du placement sous le statut de témoin assisté (art. 113-4), mais aussi devant les juridictions de jugement, qu'elles statuent en matière contraventionnelle (art. 535), délictuelle (art. 406) ou criminelle (art.

Actualité pénale

328). Dans le sillage de la jurisprudence du Conseil constitutionnel, l'obligation d'information du droit de se taire sera étendue aux autres phases se déroulant devant les juridictions d'instruction, qu'elles portent sur la détention provisoire, la mise en liberté, la suite de la procédure et affecteront largement, non plus seulement le juge d'instruction, mais aussi la chambre de l'instruction et le juge des libertés et de la détention, à terme.

La Cour de Justice de l'Union européenne vient aussi apporter sa pierre à l'édifice. Dans un arrêt du 2 février 2021 (Grande chambre, *DB c/ Commission nazionale per la societa et la Borsa*), la Cour considère qu'une personne physique soumise à une enquête administrative pour délit d'initié a le droit de garder le silence. D'une part, les sanctions prononcées en la matière peuvent revêtir un caractère pénal. D'autre part, même si elles ne présentent pas de caractère pénal, le droit au silence doit être garanti dans le cadre des procédures administratives, telles que celles organisées en droit de la concurrence. Cependant, le droit au silence ne peut justifier tout refus de coopération avec les autorités. En revanche, les autorités ne doivent pas sanctionner le refus de répondre aux questions posées. Les articles 47 et 48 de la Charte des droits fondamentaux (droit au recours effectif, présomption d'innocence et droits de la défense) « doivent être interprétés en ce sens qu'ils permettent aux États membres de ne pas sanctionner une personne physique qui, dans le cadre d'une enquête menée à son égard par l'autorité compétente au titre de cette directive ou de ce règlement, refuse de fournir à celle-ci des réponses susceptibles de faire ressortir sa responsabilité pour une infraction passible de sanctions administratives présentant un caractère pénal ou sa responsabilité pénale ».

BRÈVES

JUSTICE PÉNALE DES MINEURS

Loi 2021-218 du 26 février ratifiant l'ordonnance n° 2019-950 du 11 septembre 2019 portant partie législative du Code de la justice pénale des mineurs

La loi du 26 février 2021 a ratifié l'ordonnance constituant le Code de la justice pénale des mineurs (CJPM), déjà commentée dans la veille lors de son adoption (voir [La veille juridique](#) n° 80, septembre 2019, p. 36-44). La loi maintient le socle du dispositif et apporte quelques modifications mineures.

Le Titre préliminaire du CJPM constitue une déclaration de principe et permet d'insuffler l'autonomie du droit pénal des mineurs et la prépondérance de la prévention sur la répression. L'article L 11-1 pose le principe de responsabilité pénale des mineurs lorsqu'ils sont capables de discernement et pose une présomption de discernement pour les mineurs de plus de treize ans ainsi qu'une présomption de non-discernement pour les mineurs de moins de treize ans. La loi du 26 février 2021 apporte une précision utile, même nécessaire, car elle ajoute un alinéa supplémentaire qui précise la notion. « Est capable de discernement le mineur qui a compris et voulu son acte et qui est apte à comprendre le sens de la procédure pénale dont il fait l'objet ». Il est possible d'identifier ici l'inspiration de l'arrêt de principe rendu par la Chambre criminelle le 13 décembre 1956, dit Laboube, dans lequel elle exige que le mineur soit doté de l'intelligence et de la volonté afin d'engager sa

Actualité pénale

responsabilité pénale. D'autres modifications de cohérence ou d'articulation sont effectuées. Il en est une qui retient l'attention. L'article L 111-1 énumère les mesures éducatives applicables à « l'enfant et adolescent », termes qui sont venus remplacer « le mineur » figurant dans le texte initial de l'ordonnance. Le choix est éminemment politique, car il allège la charge répressive de la désignation de l'auteur de l'infraction. Néanmoins, il présente un inconvénient juridique qui est celui de son manque de précision. Si le mineur est objectivement désigné par son âge, quelles sont les caractéristiques des enfants et adolescents ? Comment les distinguer entre eux ? Et des autres catégories de personnes qui seraient « des adultes », ou des « jeunes », ou des « aînés » ? Cette confusion est regrettable.

Mais la mesure la plus importante est le nouveau report de l'entrée en vigueur du CJPM. Si elle était prévue le 31 mars 2021, elle a été reportée au 30 septembre 2021. Les discussions actuelles autour des phénomènes de bandes, des violences urbaines qui flambent, ne devraient pas entraîner de modifications de ce texte, le garde des Sceaux se montrant fort protecteur de ce texte qui a engagé juridiquement et politiquement la majorité.

PRÉSENTATION OU PUBLICATION DE COMPTES INFIDÈLES

Crim. 17 février 2021, n° 20-82.068, publ. à venir

Dans le cadre d'un groupe de sociétés, les comptes consolidés sont présentés avec une survalorisation des actifs afin de masquer les fautes de gestion commises au cours du mandat de gestion assumé

Actualité pénale

par l'une d'entre elles. Après avoir découvert avoir été trompés, les associés ont porté plainte du chef de présentation de comptes inexacts. Une information judiciaire a été ouverte et le juge d'instruction a rendu une ordonnance de non-lieu confirmée par la chambre de l'instruction au motif que la présentation des comptes consolidés n'est prévue par aucune disposition du Code de commerce. La Chambre criminelle est saisie de pourvoi. Si elle apporte des précisions sur la méthode d'évaluation des flux futurs pouvant être utilisée pour établir les comptes, qui rend contestables la survalorisation et surtout sa proportion, c'est le périmètre de l'incrimination de la présentation de comptes inexacts qui retient l'attention. La Cour de cassation affirme de façon claire et péremptoire que « la présentation des comptes annuels consolidés (...) est exclue du champ d'application du délit de présentation ou publication de comptes infidèles prévu par l'article L. 242-6, 2°, du code de commerce ».

Les comptes consolidés sont destinés à présenter dans des comptes uniques et synthétiques la situation et le résultat du groupe, comme si les sociétés qui en sont membres ne formaient qu'une seule entité comptable. Si l'article L 247-1, II, prévoit un délit d'omission d'établissement de comptes sociaux, puni de 9 000 euros d'amende, aucun texte ne prévoit le délit de présentation de comptes inexacts. Pour rappel, les articles L 242-6, 2°, pour les sociétés anonymes, et L 241-3, 3°, pour les sociétés à responsabilité limitée, répriment deux comportements distincts portant sur la présentation (communication aux actionnaires ou associés) ou sur la publication (communication aux tiers) de comptes annuels inexacts. Les comptes annuels se composent du bilan, du compte de résultat et d'une annexe comptable et ils doivent être « réguliers, sincères et

Actualité pénale

donner une image fidèle du patrimoine, de la situation financière et du résultat de l'entreprise », selon l'article L 123-14 C. com. Dès lors qu'ils sont inexacts, donc ne donnent pas « une image fidèle » de l'entreprise, le délit est constitué. Mais l'incrimination est soumise au principe d'interprétation stricte et ne peut être appliquée à des éléments qui ne figurent pas dans sa définition. Ainsi, les comptes consolidés, qui ne sont pas énumérés dans les comptes annuels, ne peuvent être intégrés dans le périmètre du délit de présentation de comptes inexacts. À la différence de l'article L 247-1,II, qui vise spécifiquement les comptes consolidés en permettant de leur appliquer le délit d'omission d'établissement de comptes sociaux.

PREUVE - PRÉSUMPTION - MATIÈRE DOUANIÈRE

Crim. 17 février 2021, n° 20-81.282

À l'occasion du contrôle routier d'un camion, les agents des douanes ont découvert 870 kg de cannabis. Le passager du camion a été poursuivi du chef d'importation en contrebande de marchandises prohibées. Les premiers juges l'ont condamné, notamment, à une amende douanière de 1 700 000 euros et à la confiscation du camion. La Cour d'appel l'a relaxé car son intention délictueuse n'était pas établie. Les juges retiennent particulièrement des éléments de contexte – « la sincérité de ses premières déclarations sur les circonstances du voyage confirmées par l'enquête, son absence de contacts téléphoniques avec "le chef" en cours de route, sa mise à l'écart lors des discussions d'étapes, et la chronologie des événements, les caisses en bois dissimulant la résine de cannabis ayant été chargées dans la remorque avant la date à laquelle il avait

Actualité pénale

participé au reste du chargement » – qui permettent d'établir son ignorance quant à la présence de la résine de cannabis saisie, ignorance confortée par sa mise hors de cause par son co-prévenu, le conducteur du camion. La Cour d'appel conclut qu'il ne peut être « fait grief au prévenu, non initié au trafic de stupéfiants, d'avoir manqué de lucidité sur les comportements suspects du conducteur et de son chef, s'agissant de son unique voyage », ce qui constitue une absence d'élément intentionnel. La Cour de cassation casse l'arrêt en reprochant aux juges de s'être fondés sur des « éléments inopérants ».

L'article 392, alinéa 1^{er}, du Code des douanes établit une présomption en réputant le détenteur de marchandises de fraude responsable de la fraude. La Cour de cassation rappelle qu'il « ne peut combattre cette présomption qu'en rapportant la preuve des diligences effectuées pour s'assurer de la nature de la marchandise transportée afin d'établir sa bonne foi ». Or, en l'espèce, le prévenu n'a pas rapporté la preuve des diligences effectuées pour s'assurer de la nature des marchandises transportées. En l'absence de preuve de sa bonne foi, il ne peut s'abstraire de la responsabilité de principe établie par le Code des douanes.

Si la solution semble relever du droit pénal de forme, sa portée ne peut être comprise que si l'on part du droit pénal de fond. Le comportement visé par l'espèce relève d'un concours de qualifications car il tombe, à la fois, sous le coup d'une qualification établie par le Code pénal (trafic de stupéfiants) et d'une qualification établie par le Code des douanes (importation en contrebande de marchandises prohibées). Le choix de la qualification détermine le régime juridique applicable à l'infraction. Le régime juridique établi par le Code des douanes est plus exigeant

Actualité pénale

que celui établi par le Code pénal. En droit pénal, le fardeau de la preuve pèse sur le ministère public, car il supporte l'accusation. À ce titre, il doit établir tous les éléments constitutifs de l'infraction, avec les difficultés inhérentes à l'établissement de l'élément moral, plus particulièrement. Le droit douanier inverse la logique et se montre plus favorable à la répression. Le Code des douanes établit une présomption de responsabilité en cas de détention des marchandises de fraude. Ce n'est plus au ministère public de prouver l'élément moral de cette détention frauduleuse, mais au prévenu d'établir sa bonne foi. La *probatio diabolica* change de côté. Tout comme il est difficile pour le ministère public d'établir l'intention délictueuse, il est difficile, pour ne pas dire impossible, au prévenu d'établir sa bonne foi. Le fardeau de la preuve détermine l'issue de l'affaire et celui qui ne peut s'acquitter de son devoir en subit les conséquences négatives.

L'arrêt illustre, une nouvelle fois, la vigueur et la rigueur du droit douanier qui se montre plus offensif et répressif que le droit pénal. L'utilisation des présomptions de culpabilité par l'établissement de certains éléments constitutifs des qualifications pénales pose des questions en droit pénal, d'où une utilisation timide, alors qu'elle est plus facile et fréquente dans d'autres matières. Les présomptions de responsabilité sont admises par une jurisprudence concordante du Conseil constitutionnel, de la Cour européenne des droits de l'Homme et de la Cour de cassation à deux conditions. D'une part, elles doivent être simples et céder devant la preuve contraire. D'autre part, elles doivent être vraisemblables et assurer une proportionnalité entre le procédé employé et l'importance de l'enjeu. L'arrêt rendu par la Chambre criminelle semble légitimer la présomption de responsabilité établie par l'article 392 du Code des

Actualité pénale

douanes. La première condition est formellement vérifiée. Le détenteur des marchandises de fraude est réputé responsable, mais il peut échapper à cette responsabilité s'il apporte la preuve de sa bonne foi. La présomption peut ainsi être combattue par la preuve contraire, donc elle a un caractère simple. La deuxième condition est implicite. Le juge admet que la présomption de responsabilité soit utilisée dans le cadre de la contrebande de stupéfiants et la balance effectuée montre que la valeur protégée, la lutte contre le trafic de stupéfiants, justifie l'utilisation d'une technique juridique de présomption.

Élisabeth Rolin

STATUT ET QUALITÉ DE RÉFUGIÉ

Conseil d'État, 12 février 2021, OFPRA, n° 431239¹

Cet arrêt permet de revenir sur la distinction entre le statut de réfugié et la qualité de réfugié et de préciser, dans le cadre d'une procédure de retrait du statut de réfugié, ce qu'est « le délit constituant un acte de terrorisme ».

La réforme du droit d'asile en 2015² a renforcé les garanties accordées aux personnes ayant besoin d'une protection internationale³. Elle a ainsi parachevé la transposition de la directive 2013/33/UE du Parlement européen et du Conseil du 26 juin 2013 établissant des normes pour l'accueil des personnes demandant la protection internationale, directive dite « accueil » de 2013. Elle a également transposé deux autres directives :

- la directive 2013/32/UE du Parlement européen et du Conseil du 26 juin 2013 relative à des procédures communes pour l'octroi et le retrait de la protection internationale, directive dite « procédures »

1. Mentionné aux tables du recueil Lebon. Les conclusions de G. Odinet, rapporteur public, sont disponibles sur le site <http://www.conseil-etat.fr/fr/arianeweb/CRP/conclusion/2021-02-12/431239>.

2. La loi n° 2015-925 du 29 juillet 2015 relative à la réforme du droit d'asile a transposé les nouvelles directives, elle est publiée au JORF n° 0174 du 30 juillet 2015, NOR : INTX1412525L.

3. Projet de loi relatif à la réforme de l'asile, 22 juillet 2014. Disponible sur : https://www.legifrance.gouv.fr/contenu/Media/Files/autour-de-la-loi/legislatif-et-reglementaire/etudes-d-impact-des-lois/ei_art_39_2014/

Police administrative

de 2013 ;

- la directive 2011/95/UE du Parlement européen et du Conseil du 13 décembre 2011 concernant les normes relatives aux conditions que doivent remplir les ressortissants des pays tiers ou les apatrides pour pouvoir bénéficier d'une protection internationale, directive dite « qualification » de 2011.

Ces trois directives européennes constituent le « paquet asile ». Dans le respect de la Convention de Genève du 28 juillet 1951 et du protocole signé à New York le 31 janvier 1967 relatifs au statut des réfugiés, ces trois directives ont pour objectif que tous les États membres appliquent des critères communs pour l'identification des personnes nécessitant une protection internationale. En outre, un niveau minimal d'avantages doit être accordé à ces personnes dans tous les États membres sous le contrôle de la Cour de justice de l'Union européenne (CJUE).

Les conditions d'octroi de l'asile en France sont définies aux articles L. 711-1 à L. 714-1 du Code de l'entrée et du séjour des étrangers et du droit d'asile (CESEDA). L'article L. 711-6 du CESEDA prévoit que le statut de réfugié est refusé ou qu'il est mis fin à ce statut lorsque :

1° il y a des raisons sérieuses de considérer que la présence en France de la personne concernée constitue une menace grave pour la sûreté de l'État ;

2° la personne concernée a été condamnée en dernier ressort en France, dans un État membre de l'Union européenne ou dans un État tiers figurant sur la liste, fixée par décret en Conseil d'État, des États dont la France reconnaît les législations et juridictions pénales au vu

Police administrative

de l'application du droit dans le cadre d'un régime démocratique et des circonstances politiques générales, soit pour un crime, soit pour un délit constituant un acte de terrorisme ou puni de dix ans d'emprisonnement, et lorsque sa présence constitue une menace grave pour la société française.

L'arrêt du 12 février 2021 du Conseil d'État, en cassation, concerne l'application du 2° de l'article L. 711-6 du CESEDA lorsque la personne a été condamnée en dernier ressort en France pour un délit constituant un acte de terrorisme et que sa présence constitue une menace grave pour la société française.

Cet arrêt permet de rappeler, tout d'abord, la distinction opérée entre la qualité de réfugié de celle du statut de réfugié dans la ligne de la jurisprudence de la CJUE. Ensuite, il vient préciser ce qu'est « le délit constituant un acte de terrorisme » pour l'application des dispositions du 2° de l'article L. 711-6 du CESEDA.

M. A., de nationalité russe et d'origine tchéchène, s'est vu reconnaître la qualité de réfugié par une décision de l'Office français de protection des réfugiés et apatrides (OFPRA) du 25 août 2011. Par une décision du 20 février 2017 prise en application du 2° de l'article L. 711-6 du CESEDA, l'OFPRA a mis fin à son statut de réfugié, en estimant qu'en raison de quatre condamnations pénales entre 2011 et 2016, dont une prononcée le 18 février 2015 par le tribunal correctionnel de Nice pour des faits d'apologie publique d'un acte de terrorisme, sa présence sur le territoire français constituait une menace grave pour la société. Le requérant a

Police administrative

contesté cette décision devant la Cour nationale du droit d'asile (CNDA). Cette juridiction administrative spécialisée est compétente pour connaître des décisions relatives aux demandes d'asile⁴. Juridiction de plein contentieux, elle peut annuler les décisions prises par le directeur général de l'OFPRA mais aussi substituer sa propre décision à cette dernière en se prononçant elle-même sur le droit du demandeur à la qualité de réfugié ou au bénéfice de la protection subsidiaire⁵. Au cas d'espèce, la CNDA a annulé la décision de l'OFPRA en jugeant que M. A. avait été condamné pour un délit ne constituant pas un acte de terrorisme et l'a rétabli dans le statut de réfugié. L'OFPRA s'est pourvu en cassation contre cette dernière décision en date du 2 avril 2019.

I. La distinction entre la qualité et le statut de réfugié

La CJUE, par un arrêt de grande chambre du 14 mai 2019 (C-391/16, C-77/17 et C-78/17), confirme la distinction entre la qualité de réfugié et le statut de réfugié. L'octroi du statut de réfugié présente un caractère purement réconitif de la qualité de réfugié, ce qui signifie que si une personne a obtenu la qualité de réfugié en raison des risques encourus pour sa vie ou sa sécurité dans son pays

4. <http://www.cnda.fr/La-CNDA/Competences-de-la-CNDA>. La CNDA statue en premier et dernier ressort sur les recours formés contre les décisions de l'OFPRA. Placée sous le contrôle de cassation du Conseil d'État, elle a une compétence nationale.

5. Le bénéfice de la protection subsidiaire est accordé à toute personne dont la situation ne répond pas à la définition du statut de réfugié mais pour laquelle il existe des motifs sérieux et avérés de croire qu'elle courrait dans son pays un risque réel de subir l'une des atteintes graves définies par l'article L. 712-1 du CESEDA.

Police administrative

d'origine, l'État ne peut remettre en cause la qualité de réfugié. Il pourra seulement mettre fin au statut de réfugié, car cette personne, même dangereuse dans le pays d'accueil, serait elle-même en danger si elle retournait dans son pays d'origine.

C'est ce raisonnement qui a conduit le Conseil d'État à considérer que les conditions d'application de l'article L. 711-6 pris pour la transposition des dispositions du 4, de l'article 14 de la directive 2011/95/UE du 13 décembre 2011, pouvaient seulement conduire l'OFPROA puis, le cas échéant, le juge de l'asile, à priver du statut de réfugié et non de la qualité de réfugié, la personne concernée qui a été condamnée en dernier ressort en France pour un délit constituant un acte de terrorisme et à condition que sa présence constitue une menace grave pour la société française⁶. Par suite, il résulte de ces dispositions que la possibilité de refuser le statut de réfugié ou d'y mettre fin est sans incidence sur le fait que l'intéressé a ou conserve la qualité de réfugié, dès lors qu'il en remplit toujours les conditions. Cette faculté de le priver du statut de réfugié reste subordonnée à deux conditions cumulatives, dont l'une est d'avoir fait l'objet d'une des condamnations qui y sont limitativement énumérées, notamment pour un délit constituant un acte de terrorisme.

En pratique donc, la personne qui se voit *seulement* retirer le statut de réfugié dans le cadre prévu par le paragraphe 4, de l'article 14 de la directive, tout en continuant à jouir de la qualité de réfugié, sera à l'abri de mesures d'éloignement si ce n'est dans un État distinct de

⁶. CE, 19 juin 2020, n°s, 416032, 416121, Rec. 218 av. concl. A. Lallet.

Police administrative

son pays d'origine qu'elle fuit. Ces dispositions de la directive, particulièrement protectrices, conduisent aussi le juge administratif à faire une interprétation stricte de l'article L. 711-6 du CESEDA qui en assure la transposition.

II. La définition du délit constituant un acte de terrorisme

Au cas d'espèce, l'OFPPA puis le ministre de l'Intérieur dans ses observations devant le juge de cassation soutenaient qu'il y aurait une notion de délit constituant un acte de terrorisme au sens de l'article L. 711-6 du CESEDA qui serait indépendante et distincte de la législation pénale et inclurait des délits qui ne constituent pas des actes de terrorisme dans la loi pénale.

Le Conseil d'État s'en tient à une lecture stricte du Code pénal en retenant que l'apologie publique des actes de terrorisme incriminée à l'article 421-2-5 du Code pénal n'est pas qualifiée elle-même d'acte de terrorisme. Le Conseil constitutionnel en a également déduit que ce délit ne constituait pas un acte de terrorisme et ne pouvait donc fonder une condamnation à la peine complémentaire de confiscation instaurée par l'article 422-6 du Code pénal à l'encontre des personnes coupables d'acte de terrorisme⁷.

En conséquence, le juge de cassation considère que la CNDA n'a pas commis d'erreur de droit en relevant que les délits ayant donné lieu aux condamnations de M. A. étaient punis de peines inférieures à dix ans d'emprisonnement et que les faits d'apologie publique d'un acte

⁷. Cons. Const. 18 mai 2018, n° 2018-706 QPC.

Police administrative

de terrorisme pour lesquels il avait été condamné le 18 février 2015 ne constituaient pas un acte de terrorisme.

Par suite, le pourvoi de l'OFPRA est rejeté. M. A. conserve son statut de réfugié qui avait été rétabli par la CNDA et, en tout état de cause, sa qualité de réfugié.

Xavier Latour

Réflexions sur les relations entre l'État et la sécurité privée

La filière de la sécurité privée entretient avec l'État des relations d'intensité variable et fluctuante.

La compréhension de cette relation est compliquée par la nature même des intéressés alors que la proposition de la loi relative à la sécurité globale entend apporter une nouvelle pierre à l'édifice.

La filière de la sécurité privée se divise en deux branches : les activités privées de sécurité soumises au Livre 6 du Code de la sécurité intérieure (CSI), et celles qui ne le sont pas. L'hétérogénéité caractérise, par ailleurs, ces deux catégories.

L'article L 611-1 CSI liste les activités réglementées. Le Livre 6 régit aussi les activités de formation, ainsi que celle d'agent de recherches privées.

La sécurité privée ne se limite pas aux activités réglementées. Elle englobe différents domaines qui relèvent de la sécurité tout en échappant à un cadre défini par l'État. Le conseil en sécurité-sûreté, l'intelligence économique, l'installation de systèmes électroniques illustrent l'existence de cette zone grise. Car, si l'État n'a pas pu ou pas voulu fixer leurs modalités de fonctionnement, il n'ignore pas, au contraire, l'importance des opérateurs concernés.

Si les uns et les autres évoquent souvent un partenariat, ce couple oscille entre attirance et parfois, une forme d'indifférence, voire de déception.

Droit des collectivités territoriales et de la sécurité privée

Les affirmations répétées en boucle depuis des années sur la coproduction, puis sur le *continuum* de sécurité, limiteraient les réflexions à des thèmes connus, même convenus. Sous cet angle, la délimitation des missions représente peut-être la principale difficulté. Pour le reste, un apparent consensus semble s'imposer autour de la moralisation et de la professionnalisation d'activités solidement réglementées, au moins pour certaines. Pourtant, les réflexes, les habitudes n'empêchent pas de porter un regard novateur, éventuellement décalé, comme le colloque organisé le 21 janvier 2021 par l'Université Paris Descartes s'est proposé de le faire.

En d'autres termes, ne convient-il pas de se méfier des évidences ? Tandis que l'État serait en droit de se demander si la sécurité privée a la capacité de se transformer, cette dernière ne traverse-t-elle pas, de son côté, une crise de couple ? Certains reproches et doutes paraissent récurrents, malgré les réformes (comme la création du Conseil national des activités privées de sécurité – CNAPS) et les bonnes intentions de chacun.

Tout cela renvoie à la nature des rapports entre l'État et la sécurité privée qui ne peut se comprendre qu'après avoir reconstitué l'historique du couple, les origines de sa relation.

Les origines de la relation

L'étroitesse de la relation paraît indiscutable. Elle relèverait de l'évidence justifiée, d'une part, par l'importance du régalien en matière de sécurité et, d'autre part, par des motifs économiques qui

Droit des collectivités territoriales et de la sécurité privée

expliqueraient l'existence d'un mariage de raison.

L'importance du régalien

La sécurité est l'un des facteurs explicatifs de l'État. Par conséquent, l'article 12 de la Déclaration des droits de l'Homme et du citoyen consacré à la force publique apparaît comme une évidence. Celle-ci est d'ailleurs confortée par l'article L 111-1 CSI selon lequel il revient à l'État d'assurer la sécurité.

L'État ne percevait pas toujours l'intérêt de la sphère privée. Après tout, des entreprises vendaient des prestations limitées (surveillance, gardiennage en majorité) à des clients privés, ou créaient leur service interne, au périmètre nécessairement restreint. Ainsi, l'État a laissé se développer une offre privée de sécurité sans s'en préoccuper outre mesure. Jusqu'en 1983, la filière a prospéré en suivant principalement la loi du marché. L'absence de relation a alors conduit à des errements et des déviances de toutes sortes, y compris les plus tragiques.

Puis, l'État a opté pour une autre approche. Il a suscité une relation de plus en plus étroite avec la sécurité privée.

La volonté de rompre avec les dysfonctionnements du passé combinée à l'anticipation de la pluralité d'intervenants dans le domaine de la sécurité l'a ainsi conduit à la rédaction de la loi n° 83-629 du 12 juillet 1983 sur la sécurité privée.

Les décennies suivantes s'inscrivent dans la continuité. L'État opérateur devient aussi un État régulateur. Parce que la sécurité

Droit des collectivités territoriales et de la sécurité privée

privée se développe, parce qu'elle touche au régalién et à l'exercice des libertés, il a vocation à l'encadrer. Il procède, dans un premier temps, de manière principalement unilatérale, guidé par une certaine méfiance. Puis, progressivement, il construit un droit plus partenarial qui culmine avec l'insertion d'une partie de la filière dans le CSI, en 2012, et la création du CNAPS parallèlement. Le droit matériel change, lui aussi. La puissance publique autorise de nouvelles activités (protection embarquée à bord des navires), ou améliore l'exercice d'autres (armement de la protection rapprochée par exemple).

L'État n'était pas le seul à avoir intérêt à ce mariage de raison. La filière privée entendait bien tirer économiquement parti de la relation.

L'importance économique

Un mariage de raison signifie souvent l'existence d'intérêts économiques mutuels.

Du côté de l'État, le recours à des prestataires privés rejoint les préoccupations de la nouvelle gestion publique. Une filière privée de la sécurité, performante aux yeux de l'État, lui permet d'envisager un recentrage de ses activités sur un cœur de métier difficile à identifier. Les prestataires de services allègent la charge dans de nombreux domaines.

La puissance publique s'est résolue à ne pas systématiquement augmenter les effectifs de la police et de la gendarmerie nationales.

Droit des collectivités territoriales et de la sécurité privée

Elle a aussi œuvré au développement des partenariats, conçus comme de véritables concours de police. Cette évolution correspond-elle à un affaiblissement de l'État ou, au contraire, à son renforcement ? L'affaiblissement résulterait d'un transfert de missions et d'une réduction des formes de contrôle traditionnelles par fragmentation. Là où l'administration déconcentrée (les préfectures) était compétente, un établissement public (le CNAPS) les remplace sans avoir l'exclusivité. À cette fin, il s'allie avec des intérêts privés, quitte à prendre le risque de se laisser influencer par eux.

À l'inverse, le renforcement impliquerait de nouvelles formes de régulation, donc d'extension moderne de l'État. Il entrerait dans le champ d'activités dont il se désintéressait auparavant. Plus qu'une conception néo-libérale, d'encadrement conjoint avec la filière au sein du CNAPS, l'État dissimulerait une volonté de reprise en mains. Il serait ainsi doublement gagnant. À l'allègement des finances publiques s'ajouterait une instrumentalisation du partenaire. Même quand il associe au CNAPS les représentants du secteur privé, il les sélectionne et les maintient dans une position minoritaire.

Localement, les communes ont peut-être accentué la tendance, en ayant été les laboratoires de la privatisation autant que du partenariat. La croissance de la vidéoprotection leur doit beaucoup, tout comme celle des relations liées à l'événementiel.

Le privé avait aussi beaucoup à gagner d'une intervention de l'État. Un secteur moralisé et professionnalisé est nécessairement plus attractif, donc plus vendeur. Un secteur réglementé permet de recentrer l'activité sur ses opérateurs les plus solides.

Les entreprises avaient besoin d'améliorer leur image. La

Droit des collectivités territoriales et de la sécurité privée

réglementation les aidait à rassurer les clients privés autant que publics. La création du CNAPS, ou la rédaction d'un Code de déontologie poursuivaient aussi des objectifs économiques. En 2011, l'assainissement du secteur a sous-tendu la réforme de l'encadrement normatif. Il devait conduire à la disparition des entreprises peu fiables dans un mouvement de valorisation des prestations.

Cette attente perdure. Elle a justifié les revendications relatives à une réglementation applicable aux centres de formation. Elle se retrouve dans les débats consacrés à la sous-traitance, à la garantie financière, à la lutte contre la concurrence déloyale, ou encore au niveau des prix pratiqués. À qui s'adresse le secteur si ce n'est à l'État ?

Il espère de lui une intervention capable de revivifier le *continuum* de sécurité. Il se place dans son giron, autant par habitude qu'en raison d'une forme de réalisme.

L'État et la filière de la sécurité partagent des intérêts communs. La notion de compétences régaliennes n'empêche pas, au contraire, de les faire converger. La coproduction d'un côté et la réglementation de l'autre scellent une union certes déséquilibrée, mais réelle, dont la nature mérite d'être questionnée.

La nature de la relation

L'État et la filière de sécurité ont tout du couple uni. Pourtant, au-delà des apparences, en dépit de la solidité affichée des liens, l'existence de possibles facteurs de crise ne surprendrait pas.

Droit des collectivités territoriales et de la sécurité privée

D'un couple uni

Après presque quarante ans de vie commune, les liens entre les deux se concrétisent de différentes façons.

D'abord, l'État s'est restructuré. Longtemps peu considérée en tant que telle, la sécurité privée est entrée plus nettement dans la sphère étatique. D'un simple objet de contrôle préfectoral, elle est devenue un interlocuteur reconnu.

La création du délégué interministériel à la sécurité privée, puis sa transformation en un délégué ministériel aux coopérations de sécurité le prouvent. De plus, la Direction des libertés publiques et des affaires juridiques du ministère de l'Intérieur travaille avec les différents acteurs pour faire évoluer le cadre légal et réglementaire.

La création du CNAPS illustre cette démarche, au demeurant assez classique, de dialogue entre le décideur et le sujet du droit. Cependant, tous les secteurs ne fonctionnent pas en entretenant avec la puissance publique des relations aussi fortes que celles qui existent à l'intérieur du CNAPS. Le collège, la commission nationale d'agrément et de contrôle, ainsi que les commissions locales du même type supposent un travail en commun.

Les discours témoignent, ensuite, de l'étroitesse des liens. La question ne se pose plus de savoir si la filière doit être un partenaire de l'État, mais comment l'associer, non seulement de manière plus efficiente, mais encore davantage à la protection des biens et des personnes.

Droit des collectivités territoriales et de la sécurité privée

Lorsque l'État s'exprime sur l'avenir de la sécurité privée, il s'interroge sur des améliorations potentielles, tout en confirmant le principe du *continuum*. Il rappelle systématiquement sa volonté d'une co-construction de différents pans de sa politique publique de sécurité. Le Livre blanc sur la sécurité intérieure et la loi sur la sécurité globale manifestent cette volonté soutenue par la filière.

Enfin, le droit reflète les évolutions de la relation.

Le champ des missions de la sécurité privée s'est constamment étendu. Parfois, l'État a validé un transfert d'activités. Il a, de la sorte, autorisé la protection embarquée à bord des navires. Il a aussi favorisé le retrait des forces publiques de certaines activités de protection armée au profit d'une sécurité privée renforcée (article L 611-1bis CSI). Autrement, l'État a légiféré pour faciliter la participation du privé à certaines opérations, comme le fonctionnement des périmètres de protection (article L 226-1 CSI), sans opposition du Conseil constitutionnel. Un mouvement comparable intéresse les transports en commun. Déjà, la loi n° 2016-339 du 22 mars 2016 avait constitué une étape importante, prolongée par la loi n° 2019-1428 du 24 décembre 2019 d'orientation des mobilités (article L 1631-5 du Code des transports sur les équipes cynotechniques).

Dans d'autres cas encore, la puissance publique était prête à répondre à une demande de professionnels d'entrer dans le champ des activités réglementées. Sans la censure par le Conseil constitutionnel des dispositions relatives à l'intelligence économique (DC du 10 mars 2011), le conseil en sécurité-sûreté aurait vraisemblablement été inséré dans le Livre 6 du CSI. Le

Droit des collectivités territoriales et de la sécurité privée

dialogue entre l'État et la filière n'a pas seulement trait au CSI. Il aboutit parfois à d'autres formes d'encadrement. Le recours à la certification relève de cette approche, applicable à la protection embarquée (article L 616-1 CSI) et à la formation (article L 625-2 CSI).

La consolidation du partenariat passe, par ailleurs, par différents instruments faiblement contraignants en droit, mais politiquement significatifs. Plusieurs types de convention sous-tendent ce mouvement (centres commerciaux, coopérations locales de sécurité, tourisme).

Malgré la cohésion affichée, la relation n'en est pas moins déséquilibrée. Il ne peut en être autrement quand l'un des partenaires est l'État.

À la crise de couple ?

Si elle devait exister, elle ne serait ni inquiétante ni surprenante au regard de l'évolution normale d'une relation bilatérale faite de hauts, de bas, de questionnements et de remises en cause. Des causes de fond seraient à chercher, sans exclure des éléments plus conjoncturels.

Dans les années 2010, trente ans après le vote de la loi du 12 juillet 1983 et dans le contexte de la création du CNAPS, la doctrine s'interrogeait déjà sur l'avenir de la sécurité privée, en particulier de ses relations avec l'État.

La qualité du dialogue avec les interlocuteurs ministériels relève

Droit des collectivités territoriales et de la sécurité privée

d'une approche subjective. Le fait qu'elle revienne régulièrement incite à ne pas l'écartier pour cette seule raison. Les attentes ou les espoirs déçus ne sont d'ailleurs pas à sens unique. L'État entretient aussi des regrets. La structuration de la représentation demeure ainsi un thème d'intérêt, en dépit de la fusion de deux organisations patronales, le Syndicat national des entreprises de sécurité privée (SNES) et l'Union des entreprises de sécurité privée (USP), pour former le Groupement des entreprises de sécurité (GES).

Également, des sujets jugés importants n'ont toujours pas trouvé de solutions. Leur liste est longue et hétéroclite. Elle comprend le sort à réserver à la prévention de l'incendie, la protection juridique des agents, la sous-traitance, le juste prix... Or, sans attendre les résultats du Livre blanc et le texte qui en découle, plusieurs lois votées ces dernières années offraient la possibilité d'agir.

Au-delà, le fonctionnement du CNAPS focalise l'attention, malgré les efforts constamment entrepris pour l'améliorer. Pour s'en tenir à des considérations juridiques, quelques points émergent particulièrement. Ils concernent le déroulement des contrôles, l'instruction des dossiers disciplinaires, le fonctionnement des instances disciplinaires, ou encore la publication des décisions rendues. Les difficultés relatives aux opérations de délivrance des agréments accentuent la déception.

Au titre des éléments conjoncturels, quelques situations ont contribué à faire douter la filière privée.

Alors que les travaux relatifs au Livre blanc sur la sécurité intérieure auraient dû surtout être l'occasion d'un dialogue constructif, ils laisseront une impression mitigée. Pouvait-il en être autrement, la diversité des sujets à aborder et des interlocuteurs supposant

Droit des collectivités territoriales et de la sécurité privée

inévitablement un processus assez lourd et une forme de dilution ? La crise sanitaire du printemps 2020 a aussi provoqué l'incompréhension. En plus des difficultés de fonctionnement, ou perçues comme telles, du CNAPS, particulièrement les activités de surveillance et de gardiennage ont eu le sentiment d'être oubliées. Pourtant massivement engagées sur le terrain, les entreprises ont regretté la faiblesse, voire l'absence d'aide de l'État. Si les paroles espérées ont eu du mal à venir, le soutien matériel a, quant à lui, été déficient. Il n'en suffisait pas plus pour remettre en cause la réalité du *continuum*.

Pris isolément, ces différents éléments conserveraient une portée limitée. Leur addition change la donne, particulièrement dans un environnement dégradé par la crise sanitaire. Les relations entre l'État et la sécurité privée évolueront nécessairement. Tout l'enjeu reste de savoir comment.

<i>Directeur de publication :</i>	Colonel Dominique SCHOENHER
<i>Rédacteur en chef :</i>	G^{al} d'armée (2S) Marc WATIN-AUGOUARD
<i>Rédacteurs :</i>	G^{al} d'armée (2S) Marc WATIN-AUGOUARD Frédéric DEBOVE Claudia GHICA-LEMARCHAND Xavier LATOUR Elisabeth ROLIN Capitaine Thibaut HECKMANN Capitaine Matthieu AUDIBERT
<i>Équipe éditoriale :</i>	Odile NETZER