

La veille juridique

N°68, mai 2018

Centre de recherche de l'école des officiers de la gendarmerie nationale



Edito

La date du 25 mai est passée. Le Règlement général sur la protection des données (RGPD) s'impose désormais aux 28 États membres de l'Union européenne mais aussi à tous les acteurs extérieurs qui veulent se mettre en conformité avec des dispositions protectrices. Le CREOGN a organisé, le 31 mai 2018, un atelier de recherche sur ce thème avec des interventions particulièrement riches.

Dans une certaine mesure, ce règlement a une dimension extra-territoriale. La législation européenne s'inscrit dans une démarche de souveraineté, à commencer par la souveraineté de chacun sur ses données à caractère personnel. On notera qu'au même moment est entré en vigueur le Cloud Act américain qui impose aux entreprises américaines qui stockent des données,

(Suite page 2)

EDITORIAL

y compris hors du territoire des États-Unis, de les livrer aux autorités, sans passer par la voie des Mutual Legal Assistance Treaties (MLAT), sauf en cas de conflit de législations nationales. Espérons que les hébergeurs de données de citoyens européens auront le courage de soulever cette contradiction avec le RGPD qui est on ne peut plus clair sur le sujet. Depuis le 25 mai 2018, nous recevons nombre de mails d'entreprises, de fournisseurs de services, d'administrations qui nous annoncent être en conformité avec le RGPD. Dans certains cas, l'annonce est claire, mais de nombreux documents, adressés pour recevoir notre approbation, sont aussi obscurs que la plupart des clauses générales d'utilisation (CGU). Des actions de groupe ne manqueront pas de rappeler qu'on ne s'affranchit pas des règles nouvelles. La France n'a pas promulgué, à la date du 25 mai 2018, sa loi incorporant notamment le RGPD dans la loi du 6 janvier 1978. Le désaccord entre les deux Chambres aboutit à une saisine du Conseil constitutionnel. Le 12 juin 2018, les Sages ont déclaré le projet de loi relatif à la protection des données personnelles conforme à la Constitution à l'exception de quelques mots figurant à l'article 13 et concernant les condamnations pénales et mesures de sûreté (décision 2018-765 DC du 12 juin 2018). Nous la commenterons dans la veille du mois prochain.

Le 27 juin, le CREOGN vous convie à un atelier de recherche sur la blockchain avec, notamment, la participation de Gilles Hilary, professeur à l'Université de Georgetown et chercheur associé au CREOGN. Nous essaierons d'expliquer simplement une technologie complexe qui va sans doute révolutionner les échanges en contribuant à leur sécurité. Pour s'inscrire, creogn.eogn@gendarmerie.interieur.gouv.fr.

Une fois de plus, nos auteurs sont en veille pour vous donner la



LE ZONE INTERDITE GENDARMERIE NATIONALE

EDITORIAL

primeur des évolutions législatives ou jurisprudentielles qui nous semblent couvrir les champs d'expertise des acteurs de la sécurité publique ou privée. Qu'ils soient remerciés de leur contribution ! Bonne lecture de ce numéro de la veille juridique !

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

VEILLE JURIDIQUE DE LA GENDARMERIE NATIONALE



Sommaire

- **Déontologie et sécurité**
- **Droit de l'espace numérique**
- **Actualité pénale**
- **Police administrative**
- **Droit de la sécurité privée**

Déontologie et sécurité

Par M. Frédéric Debove

Après les Black blocs, les black sites !

Cedant arma togae, concedat laurea linguae (Que les armes le cèdent à la toge, et les triomphes à l'éloquence !) : ce fragment du *De consulatu meo* de Cicéron vient immédiatement à l'esprit à la lecture de deux arrêts récents de la Cour de Strasbourg, appelés sans doute à la postérité en considération de la gravité des violations des droits de l'Homme qu'ils sanctionnent. Utilisée parfois pour affirmer la suprématie du pouvoir civil sur le pouvoir des armes, l'expression latine est surtout le symbole du passage de la guerre à la paix, de la force à celui des lois. Les affaires *Al Nashiri contre Roumanie* (requête n°33234/12) et *Abu Zubaydah contre Lituanie* (requête n°46454/11) **en date du 31 mai 2018** illustrent incontestablement la marque de la supériorité des dernières sur toute forme de guerre, y compris celle engagée contre le terrorisme. En condamnant solennellement toute dérive sécuritaire imprégnée de vengeance et d'unilatéralisme, la Cour de Strasbourg signifie à la puissante Amérique et à ses nations complices qu'une démocratie se renie lorsqu'elle plonge dans l'obscurité les valeurs pourtant imprescriptibles de l'État de droit. Si le président Barack Obama a pu affirmer que « Justice était faite » au soir de l'opération militaire ayant entraîné la mort du chef d'Al-Qaida Oussama Ben Laden (mai 2011), c'est un tout autre visage - moins guerrier et barbare - de la justice qui nous est offert ici.

Déontologie et sécurité

Quand arrestation rime avec inquisition ...

À l'évidence, les deux affaires jugées par la Cour européenne des droits de l'Homme comportent quelques points de dissemblance. Elles trouvent d'abord leur origine sur des territoires différents : la Lituanie, d'une part, et la Roumanie, d'autre part. Elles concernent ensuite des requérants détenus à Guantanamo au profil distinct : le premier, M. Husayn, apatride d'origine palestinienne, est soupçonné d'être impliqué dans les attentats du 11 septembre 2001 en sa qualité de proche lieutenant d'Oussama Ben Laden ; le second, Muhammad Al Nashiri, est un ressortissant saoudien d'origine yéménite soupçonné d'avoir participé aux attaques contre le navire américain USS Cole (2000) et le pétrolier français MV Limburg (2002) dans le golfe d'Aden. Pour le surplus, les deux affaires - objet de la présente chronique - se rapportent l'une et l'autre aux pratiques - pour le moins douteuses et expéditives - de l'agence centrale du renseignement américaine (Central Intelligence Agency, CIA) au lendemain des terribles attentats du 11 septembre 2001. Eu égard à la proximité évidente des deux affaires et pour éviter toute redondance, l'analyse sera essentiellement centrée sur l'arrêt Al Nashiri contre Roumanie, d'autant plus que cet arrêt met au jour des violations de la Convention en nombre plus important que les manquements constatés dans l'arrêt Abu Zubaydah contre la Lituanie.

**Transferts et hôtels non référencés sur
« TripAdvisor »**

M. Al Nashiri, après avoir été capturé, a été détenu dans des

Déontologie et sécurité

prisons secrètes de la CIA (black sites) en Afghanistan puis en Thaïlande. En décembre 2002, il a été transféré en Pologne, dans une autre prison secrète où il a été détenu jusqu'en juin 2003. Puis, selon le plaignant, il a fait l'objet de transferts successifs entre cinq différentes prisons de la CIA, au cours des trois années suivantes. Parmi celles-ci, une prison située en Roumanie, où il serait resté d'avril 2004 à octobre/novembre 2005. Il a finalement été transféré à Guantanamo en septembre 2006. Dans cette enclave américaine de l'île de Cuba, pendant tout le temps de sa détention par la CIA, il aurait été soumis à la torture et à d'autres formes de traitements inhumains contraires à l'article 3 de la Convention. M. Al Nashiri a décrit les traitements qui lui avaient été infligés dans un témoignage adressé en 2006 au Comité international de la Croix-Rouge (CICR) puis dans une déposition, dont les transcriptions ont été partiellement déclassifiées en 2007, faite devant le tribunal d'examen du statut de combattant (Combatant Status Review Tribunal) de l'armée américaine. Ces traitements auraient consisté notamment « à suspendre le détenu la tête en bas pendant près d'un mois, à lui faire subir des simulations de noyade, à le faire rester debout dans une boîte pendant une semaine, à le projeter contre un mur et à lui faire maintenir des positions de stress ». M. Al Nashiri a également affirmé « qu'il avait été détenu de manière continue à l'isolement et au secret pendant toute sa détention non reconnue, sans savoir où il se trouvait, ni avoir de contact avec d'autres personnes que ses interrogateurs et ses gardiens ». Le Sénat américain a rédigé un rapport sur la pratique de la torture à la CIA qui a été rendu public en 2014. On y apprend que M. Al Nashiri a été « soumis à l'alimentation par voie rectale en une occasion en 2004 alors qu'il était détenu à Bucarest, parce qu'il avait tenté de faire une grève de la faim ». Selon ce même rapport, en 2005, il était « à bout de

Déontologie et sécurité

forces ». Un rapport sur son état psychologique, rendu en 2013, a indiqué qu'il souffrait « de stress post-traumatique ». En novembre 2005, c'est au Washington Post de révéler que des pays d'Europe orientale hébergent des prisons secrètes de la CIA. Comme le souligne le rapport du Sénat américain sur la pratique de la torture à la CIA (2014), cet article a eu des conséquences puisque les autorités roumaines ont fermé le centre de détention « Site Black » dans les heures qui ont suivi les révélations du journal. La chaîne ABC news confirma, en décembre 2005, que la Roumanie faisait partie des pays où des « détenus de haute importance » avaient été emprisonnés secrètement pour le compte de la CIA. M. Al Nashiri figurait parmi eux. Le même mois, une enquête parlementaire a été ouverte en Roumanie, portant principalement sur les questions de savoir « s'il y avait eu une prison secrète de la CIA dans le pays, des transferts illicites de prisonniers vers cette prison, une circulation suspecte d'aéronefs, et s'il était possible que les autorités nationales aient participé à cette opération ». En mars 2007, le rapport définitif de la commission a répondu par la négative à toutes ces questions. En juillet 2012, une enquête pénale a été ouverte en Roumanie, à la suite d'une plainte de M. Al Nashiri. L'enquête est toujours en cours. Pour l'heure, elle n'a pas mis en exergue de responsabilité des autorités nationales dans le programme de remise. Mais aucune des informations recueillies dans le cadre de cette enquête n'a été rendue publique.

Male captum, male retentum ?

Pris illégalement et détenu illégalement ... Devant la Cour européenne des droits de l'Homme, M. Al Nashiri a prétendu en

Déontologie et sécurité

particulier « avoir été soumis à la torture et à diverses formes de violence physique et morale sur le territoire de la Roumanie sans que cet État ne procède à aucune enquête effective sur ces mauvais traitements ». Il a également soutenu que l'État roumain « avait permis qu'il soit ensuite transféré dans un autre site de détention secrète de la CIA, l'exposant ainsi à des années de traitements de ce type ainsi qu'au risque de faire l'objet d'un procès manifestement inéquitable et d'être condamné à mort ». Sur ces accusations, M. Al Nashiri a soutenu que son enlèvement secret et extrajudiciaire et sa détention arbitraire avaient enfreint les articles 2 (droit à la vie), 3 (interdiction de la torture), 5 (droit à la liberté et à la sûreté), 6 (droit à un procès équitable dans un délai raisonnable), 8 (droit au respect de la vie privée et familiale) et 13 (droit à un recours effectif) de la Convention ainsi que l'article 1^{er} du Protocole n°6 portant abolition de la peine de mort.

Vigilat Iustitiae Oculus ... quand l'œil de la justice européenne veille

L'établissement des faits de l'espèce n'est pas aisé. La Cour observe « qu'elle n'est pas en mesure de recueillir un récit direct des faits de la part de M. Al Nashiri lui-même, celui-ci n'ayant eu depuis octobre 2002 aucun autre contact avec le monde extérieur que l'entretien avec l'équipe du CICR en 2006 et ses rencontres avec les membres de la commission militaire et avec son représentant devant les autorités américaines ». La solution de l'affaire repose donc principalement sur des preuves circonstancielles. La Cour s'appuie notamment sur le résumé analytique du rapport du Sénat américain sur la pratique de la torture à la CIA déclassifié en 2014. Dans ce document sont décrites les activités menées

Déontologie et sécurité

par la CIA, de 2001 à 2009, dans le cadre du programme « HVD ». Entrent également dans les preuves le témoignage de M. Al Nashiri figurant dans le rapport du CICR et les dépositions faites par l'intéressé au tribunal d'examen du statut de combattant. Les résultats des enquêtes internationales inspirent également la Cour : parmi eux, les trois rapports établis par Dick Marty, rapporteur suisse auprès de l'Assemblée parlementaire du Conseil de l'Europe, et les documents expurgés publiés par la CIA. De ces enquêtes internationales il est possible de tirer des informations « sur les mauvais traitements infligés aux détenus, sur la circulation d'avions dont on sait qu'ils étaient utilisés par la CIA pour les opérations de remise, sur la manière dont la CIA a payé des États étrangers pour accueillir des sites de fonctionnement du programme et sur la manière dont celui-ci s'est développé au fil des années ». Le rapport du Sénat américain sur la pratique de la torture à la CIA contient des informations précises sur les dates et les heures des transferts et sur le calendrier des interrogatoires des prisonniers de la CIA. Ce rapport fait état d'une coopération avec les autorités locales et le versement à ces autorités de plusieurs millions de dollars en échange de leur « soutien » au programme de remises extraordinaires (le montant exact des sommes versées n'est cependant pas précisé dans la version publique du rapport). Le document permet à la Cour de conclure que le centre de détention appelé « Site Black », qui est l'un de ceux où M. Al Nashiri a été détenu, se trouvait en Roumanie. Sur la base de l'ensemble de ces éléments, la Cour a donc estimé qu'il est prouvé « que la Roumanie a accueilli un centre de détention secret de la CIA de septembre 2003 à novembre 2005 et que M. Al Nashiri y a été détenu d'avril 2004 à novembre 2005 au plus tard ». Pour la juridiction, la Roumanie avait non seulement connaissance du but

Déontologie et sécurité

des activités que la CIA menait sur son territoire, mais elle a aussi coopéré. De ce fait, les allégations de M. Al Nashiri concernent des faits qui relèvent de la juridiction de la Roumanie et qui sont de nature à engager la responsabilité de l'État sur le terrain de la Convention.

3, 5, 8, 13, 6 et 2 ... roue de l'infortune ou juste prix pour la Roumanie ?

Sur le fondement de l'article 3, la Cour conclut d'abord à la violation des règles de procédure, au regard des défaillances qui apparaissent aussi bien dans l'enquête parlementaire que dans l'enquête pénale menées en Roumanie. S'agissant de l'enquête parlementaire, sa portée limitée « n'a pas permis d'identifier ni de tenir responsables les agents de l'État roumains qui se seraient rendus complices du programme de la CIA, bien qu'elle ait porté sur les mêmes éléments que les enquêtes internationales qui ont conclu qu'il était plus que probable qu'une prison secrète de la CIA ait opéré en Roumanie ». En ce qui concerne l'enquête pénale, elle n'a pas permis, depuis 2012, d'identifier la moindre responsabilité de la Roumanie quant à sa participation au programme de la CIA. En outre, la Cour considère que « le parquet roumain aurait dû ouvrir dès 2005 une enquête pénale sur les allégations extrêmement graves portées à l'égard des autorités nationales, et ce sans attendre d'être saisi par l'une des victimes alléguées. Du fait du long délai – sept ans – qui s'est écoulé avant que l'enquête ne soit ouverte, les enquêteurs n'ont pas recueilli les éléments de preuve au lendemain de la fermeture de la prison secrète installée en Roumanie, et des éléments importants tels

Déontologie et sécurité

que les données de transport aérien ont été perdus ». Sur le volet matériel de l'article 3, la Cour note que « M. Al Nashiri n'a pas été soumis en Roumanie aux techniques d'interrogatoire les plus extrêmes décrites dans son témoignage à la Croix-Rouge et dans sa déposition au tribunal d'examen du statut de combattant ». Toutefois, ce qu'il a enduré avant d'arriver dans le pays doit être pris en compte pour apprécier ses conditions de détention sur place : « il a dû se trouver dans la crainte constante de subir à nouveau les traitements cruels qui lui avaient été précédemment infligés ». C'est d'ailleurs ce que souligne le rapport du Sénat américain sur la pratique de la torture à la CIA qui a confirmé qu'il souffrait de graves problèmes psychologiques causés par les mauvais traitements subis. Quoi qu'il en soit, les conditions de détention de M. Al Nashiri en Roumanie étaient extrêmement dures. En témoignent le rapport de 2007 du CICR et le rapport du Sénat américain : « la pratique habituelle comprenait le port d'un bandeau sur les yeux ou d'une cagoule, la détention à l'isolement, le port continu d'entraves et l'exposition au bruit et à la lumière ». Pour la Cour, les souffrances ainsi infligées à M. Al Nashiri sont constitutives d'un traitement inhumain au sens de la Convention ; la Roumanie a permis ce traitement en coopérant avec la CIA. Elle a en outre laissé la CIA sortir M. Al Nashiri hors du pays, « exposant ainsi l'intéressé à un risque grave et prévisible de mauvais traitements supplémentaires ».

À « remise extraordinaire », condamnation exemplaire

À cette première condamnation sur le fondement de l'article 3 (dans ses volets procédural et matériel), s'en ajoutent d'autres

Déontologie et sécurité

tout aussi stigmatisantes pour l'État roumain. En permettant à la CIA de transférer M. Al Nashiri dans le pays puis hors du pays et de l'y détenir secrètement, la Roumanie s'est ainsi rendue coupable d'une violation grave et manifeste des articles 5 et 8 CEDH, les détentions extrajudiciaires constituant une négation totale des garanties de la Convention. Par ailleurs, l'absence de recours effectif permettant au requérant de dénoncer la violation de ses droits devant les juridictions nationales caractérise une violation de l'article 13 de la Convention CEDH. De surcroît, la Cour relève également à l'encontre de la Roumanie une violation de l'article 6 CEDH. Les autorités roumaines avaient nécessairement connaissance, au moment où M. Al Nashiri a été transféré hors de Roumanie, des nombreuses critiques faites publiquement sur les procès tenus par la commission militaire américaine, procès qui ne respectaient pas les garanties les plus élémentaires de la justice. Alors que le risque que l'intéressé ne subisse un réel déni de justice était prévisible, la Roumanie a collaboré activement à son transfert hors du territoire. Il s'ensuit un manquement au droit au procès équitable. Enfin, en permettant à la CIA de transférer M. Al Nashiri dans le ressort de la commission militaire américaine, devant laquelle il était mis en accusation et devait être jugé pour des faits passibles de la peine de mort, la Roumanie a méconnu les prescriptions des articles 2 et 3 de la Convention dans leur jeu combiné avec l'article 1^{er} du Protocole n° 6.

Après le « dégât des os », le contrat d'assurance-vie !

En l'état, l'issue du procès dirigé contre M. Al Nashiri demeure

Déontologie et sécurité

incertaine. C'est pourquoi, les juges strasbourgeois observent *in fine* que la Roumanie devrait obtenir des autorités américaines des assurances garantissant que l'intéressé ne sera pas exécuté. La Cour européenne des droits de l'Homme recommande également à l'État roumain de conclure l'enquête pénale le plus rapidement possible ; il s'agit d'éclaircir, autant que possible, les circonstances du transfert de M. Al Nashiri en Roumanie puis celles de sa sortie du pays ainsi que la manière dont il a été traité sur place. De cette enquête on devrait aussi espérer l'identification des responsables par les autorités roumaines et en déduire les sanctions pour les auteurs de ces graves manquements.

Droit de l'espace numérique

Par le G^{al} d'armée (2S) Marc Watin-Augouard

JURISPRUDENCE EUROPÉENNE

Cour de Justice de l'Union européenne - Affaire C-210/16, arrêt du 5 juin 2018, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c/ Wirtschaftsakademie Schleswig-Holstein GmbH

La notion de « responsable de traitement » de données à caractère personnel inclut l'administrateur d'une page « fan » hébergée sur un réseau social.

Dans le cadre d'un litige opposant l'autorité régionale indépendante de protection des données du Schleswig-Holstein à la Wirtschaftsakademie, la Cour de justice de l'Union européenne a été saisie par le Bundesverwaltungsgericht (Cour administrative fédérale, Allemagne) d'une demande de décision préjudicielle portant sur l'interprétation de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Si ce texte est aujourd'hui remplacé par le RGPD, la décision de la Cour serait la même en application de ce dernier, depuis le 25 mai 2018.

La Wirtschaftsakademie offre des services de formation au moyen d'une page « fan » hébergée sur Facebook. Cette page est

Droit de l'espace numérique

un compte configuré sur le réseau social qui lui permet de se présenter aux utilisateurs de ce réseau social ainsi qu'aux personnes visitant la page et de diffuser des communications de toute nature sur le marché des médias et de l'opinion. Comme le rappelle l'arrêt, les administrateurs de pages « fan » peuvent obtenir des données statistiques anonymes sur les visiteurs de ces pages à l'aide d'une fonction intitulée *Facebook Insight*, mise gratuitement à leur disposition par Facebook, selon des conditions d'utilisation non modifiables. Ces données sont collectées grâce à des *cookies* comportant chacun un code utilisateur unique, actifs pendant deux ans et sauvegardés par Facebook sur le disque dur de l'ordinateur ou sur tout autre support des visiteurs de la page « fan ». Le code utilisateur, qui peut être mis en relation avec les données de connexion des utilisateurs enregistrés sur Facebook, est collecté et traité au moment de l'ouverture des pages « fan ».

Pour considérer l'administrateur de page « fan » comme co-responsable d'un traitement de données à caractère personnel, la Cour produit le raisonnement suivant :

- Facebook reçoit, enregistre et traite les informations stockées dans les *cookies* notamment lorsqu'une personne visite « les services Facebook, les services proposés par d'autres compagnies Facebook et des services proposés par d'autres entreprises qui utilisent les services Facebook ». En outre, d'autres entités, telles que les partenaires de Facebook ou même des tiers, « sont susceptibles d'utiliser des *cookies* sur les services Facebook pour [proposer des services directement à ce réseau social] ainsi qu'aux entreprises qui font de la publicité sur Facebook » ;

Droit de l'espace numérique

- ces traitements de données à caractère personnel visent notamment à permettre, d'une part, à Facebook d'améliorer son système de publicité qu'il diffuse à travers son réseau et, d'autre part, à l'administrateur de la page « fan » d'obtenir des statistiques établies par Facebook à partir des visites de cette page, à des fins de gestion de la promotion de son activité, lui permettant de connaître, par exemple, le profil des visiteurs qui apprécient sa page « fan » ou qui utilisent ses applications, afin qu'il puisse leur proposer un contenu plus pertinent et développer des fonctionnalités susceptibles de les intéresser davantage ;
- l'administrateur d'une page « fan » hébergée sur Facebook, par la création d'une telle page, offre à Facebook la possibilité de placer des *cookies* sur l'ordinateur ou sur tout autre appareil de la personne ayant visité sa page « fan », que cette personne dispose ou non d'un compte Facebook ;
- la création d'une page « fan » sur Facebook implique de la part de son administrateur une action de paramétrage, en fonction, notamment, de son audience cible ainsi que d'objectifs de gestion ou de promotion de ses activités, qui influe sur le traitement de données à caractère personnel aux fins de l'établissement des statistiques établies à partir des visites de la page « fan ». Cet administrateur peut, à l'aide de filtres mis à sa disposition par Facebook, définir les critères à partir desquels ces statistiques doivent être établies et même désigner les catégories de personnes qui vont faire l'objet de l'exploitation de leurs données à caractère personnel par Facebook. Il en est ainsi de l'âge, du sexe, de la situation amoureuse, de la profession, des

Droit de l'espace numérique

informations sur le style de vie et les centres d'intérêt de son audience cible ainsi que des informations concernant les achats et le comportement d'achat en ligne des visiteurs de sa page, les catégories de produits ou de services qui l'intéressent le plus, de même que des données géographiques qui permettent à l'administrateur de la page « fan » de savoir où effectuer des promotions spéciales ou organiser des événements et, de manière plus générale, de cibler au mieux son offre d'informations.

En conséquence, l'administrateur d'une page « fan » hébergée sur Facebook contribue au traitement des données à caractère personnel des visiteurs de sa page. Il doit être, en l'occurrence, qualifié de responsable au sein de l'Union, conjointement avec Facebook Ireland, de ce traitement, ce qui permet d'assurer une protection plus complète des visiteurs des pages « fan ». Cette responsabilité partagée n'est cependant pas équivalente et doit être analysée en tenant compte de chaque cas d'espèce.

JURISPRUDENCE CONSTITUTIONNELLE

Conseil constitutionnel, décision n° 2018-706 QPC du 18 mai 2018

L'article 421-2-5 du Code pénal est conforme à la Constitution. Les actes de terrorisme, dont l'apologie est réprimée, sont des infractions d'une particulière gravité, susceptibles de porter atteinte à la vie ou aux biens.

Droit de l'espace numérique

L'atteinte portée à la liberté d'expression et de communication par les dispositions contestées est nécessaire, adaptée et proportionnée à l'objectif poursuivi.

Jean-Marc Rouillan, ancien membre d'Action directe, a été condamné en mai 2017 à 18 mois de prison dont 10 avec sursis pour apologie du terrorisme après avoir souligné le « courage » des terroristes ayant agi sur le territoire national en 2015. La Cour de cassation (Chambre criminelle, arrêt n° 400 du 27 février 2018) a saisi le Conseil constitutionnel, le 6 mars 2018, d'une question prioritaire de constitutionnalité portant plus particulièrement sur l'article 421-2-5 du Code pénal. L'article en cause réprime le délit d'apologie publique d'actes de terrorisme d'une peine de cinq ans d'emprisonnement et de 75 000 euros d'amende, peine portée à sept ans d'emprisonnement et à 100 000 euros d'amende, lorsque le délit a été commis en utilisant un service de communication au public en ligne. Cette aggravation est d'autant plus nécessaire que l'utilisation d'Internet donne un impact très important aux propos tenus, notamment en raison de la viralité des réseaux sociaux.

M. Rouillan soutenait, d'une part, que les dispositions réprimant l'apologie d'actes de terrorisme méconnaîtraient le principe de légalité des délits et des peines, faute pour le législateur d'avoir suffisamment circonscrit le champ d'application de ce délit. Il estimait, d'autre part, que ces dispositions violeraient la liberté d'expression, au motif notamment qu'elles incrimineraient un comportement sans imposer que son auteur manifeste une intention terroriste et sans exiger un risque avéré de passage à l'acte terroriste.

Droit de l'espace numérique

S'agissant du principe de légalité des délits et des peines, le Conseil constitutionnel constate que l'article 421-2-5 exige que le comportement incriminé doive inciter à porter un jugement favorable sur une infraction expressément qualifiée par la loi d'« acte de terrorisme » ou sur son auteur. Ce comportement doit, par ailleurs, se matérialiser par des propos, images ou actes présentant un caractère public, c'est-à-dire dans des circonstances traduisant la volonté de leur auteur de les rendre publics. Pour les Sages, les dispositions contestées de l'article 421-2-5 du Code pénal ne revêtent pas un caractère équivoque et sont suffisamment précises pour garantir contre le risque d'arbitraire. Le grief tiré de la méconnaissance du principe de légalité des délits et des peines doit donc être écarté.

En ce qui concerne l'atteinte à la liberté d'expression et de communication, le Conseil constitutionnel relève, notamment, qu'en instituant le délit d'apologie publique d'actes de terrorisme, le législateur a entendu prévenir la commission de tels actes et éviter la diffusion de propos faisant l'éloge d'actes ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur. Ce faisant, « il a poursuivi l'objectif de valeur constitutionnelle de prévention des atteintes à l'ordre public et des infractions, dont participe l'objectif de lutte contre le terrorisme. En outre, l'apologie publique, par la large diffusion des idées et propos dangereux qu'elle favorise, crée par elle-même un trouble à l'ordre public. Les actes de terrorisme dont l'apologie est réprimée sont des infractions d'une particulière gravité, susceptibles de porter atteinte à la vie ou aux biens. L'atteinte portée à la liberté d'expression et de communication par les dispositions contestées est donc nécessaire, adaptée et proportionnée à l'objectif poursuivi par le législateur. Les dispositions contestées ne méconnaissent donc pas cette liberté.

Droit de l'espace numérique

C'est la troisième décision QPC du Conseil constitutionnel portant sur la loi pénale et intéressant le champ du numérique. Rappelons qu'il a, le 15 décembre 2017, sanctionné la consultation habituelle des sites à caractère terroriste (ancien article 421-2-5-2 du Code pénal) considérant que cet article n'était ni nécessaire, ni adapté, ni proportionné.

Plus récemment, le Conseil constitutionnel (décision n° 2018-696 QPC du 30 mars 2018), a déclaré conforme à la Constitution l'article 434-15-2 du Code pénal qui incrimine « toute personne », dont les prestataires de moyens de cryptologie, qui ne remet pas aux autorités judiciaires la clef de déchiffrement relative à un document pouvant avoir servi à la préparation ou à la commission d'une infraction ou dont la connaissance aurait pu éviter un crime ou délit ou en limiter les conséquences. Cet article ne porte pas atteinte au droit de ne pas s'accuser ni au droit au respect de la vie privée et au secret des correspondances.

ACTUALITÉ

3^{ème} rapport d'Alexandre Linden, personnalité qualifiée pour le contrôle de mesures de retrait, de blocage ou de déréférencement des sites illicites

La loi n° 2014-1353 du 13 novembre 2014, renforçant les dispositions relatives à la lutte contre le terrorisme, a créé l'article 6-1 de la loi pour la confiance dans l'économie numérique instituant une procédure de retrait, de blocage ou de déréférencement des

Droit de l'espace numérique

sites à caractère terroriste ou à caractère pédopornographique. Une personnalité qualifiée, désignée au sein de la Commission nationale de l'informatique et des libertés (CNIL), est chargée du contrôle du bien-fondé des mesures demandées par le ministère de l'Intérieur (Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication - OCLCTIC). En cas d'irrégularité, cette personnalité peut recommander à l'autorité administrative d'y mettre fin et, à défaut de suivi de cette recommandation, saisir la juridiction administrative compétente en référé ou sur requête.

Depuis sa nomination, Alexandre Linden, ancien avocat général près la Cour de cassation, a rendu trois rapports, le dernier portant sur la période mars 2017-février 2018. Ce rapport souligne l'accroissement considérable du nombre de dossiers dont il a été saisi, comme en témoigne le tableau ci-après :

	De- mandes de retrait	Retraits effectués	Demandes de blocage	Demandes de déréféren- cement
Totaux (2017-2018)	35110	7724	763	3115
Totaux (2016-2017)	2561	2305	874	2077
Totaux (2015-2016)	1439	1179	312	855
Augmentation de l'activité de contrôle par rapport à la période précédente	+ 1270 %	+235 %	-13 %	+ 50 %

Source : Rapport Linden 2018-2017-2016

Droit de l'espace numérique

Sur la dernière période, le terrorisme représente 93 % des demandes de retrait, 89 % des demandes de blocage et 84 % de demandes de déréférencement. La personnalité qualifiée a procédé à 34 séances de contrôle (+21 %) mais elle a surtout vu le volume des contenus vérifiés augmenter de manière très significative, qu'Alexandre Linden explique notamment par l'augmentation sensible du nombre des enquêteurs de la cellule de l'OCLCTIC spécialisée pour la prise des mesures administratives. De son côté, il se plaint de l'insuffisance des moyens humains consacrés à sa mission : seuls les collaborateurs de la CNIL se déclarant volontaires pour assister la personnalité qualifiée sont désignés à cette fin, ce qui n'est pas suffisant pour assurer de manière pérenne la mission d'assistance de la personnalité qualifiée dans le cadre de ses missions. C'est d'ailleurs sur ce point que s'achève le rapport en des termes qui ne cachent pas une certaine amertume : « *Il convient néanmoins d'insister sur les conséquences de l'insuffisance des moyens humains et techniques, nécessaires à l'accomplissement de la mission de la personnalité qualifiée. Faute de renforcement significatif de ces moyens, les difficultés rencontrées par celle-ci pour remplir sa mission pourraient s'aggraver. Elles risqueraient même de compromettre l'effectivité de son contrôle sur l'ensemble des demandes de retrait de contenus, de blocage ou de déréférencement de sites si l'augmentation de leur nombre constatée en 2017 devait se poursuivre* ».

Alexandre Linden souligne le rôle majeur des hébergeurs et des fournisseurs d'accès à Internet (FAI) dans la lutte contre la provocation à la commission d'actes de terrorisme et leur apologie. Twitter a ainsi annoncé avoir supprimé, entre août 2015 et décembre 2017, plus de 1,2 million de comptes pour apologie au terrorisme, les gouvernements n'ayant été à l'origine que de 0,2 % des suppressions de comptes durant le second semestre

Droit de l'espace numérique

2017. C'est tout l'enjeu des échanges entre l'Union européenne et les réseaux sociaux.

Cybersecurity Tech Accord

À l'initiative de Microsoft, 34 multinationales, dont Facebook et ABB, ont signé le 17 avril 2018 un *Cybersecurity Tech Accord* destiné à lutter contre les attaques informatiques. Ce texte est-il la première étape d'une « Convention de Genève du numérique » ?

Microsoft l'avait annoncé au Forum international de la cybersécurité (FIC) 2018 : l'entreprise de Redmond a rassemblé un nombre significatif d'acteurs privés autour d'une déclaration qui ambitionne de devenir une Convention internationale. L'accord s'appuie sur quatre principes :

1. *Nous protégerons partout tous nos clients et utilisateurs.*
Nous nous efforcerons de protéger tous nos utilisateurs et clients des cyberattaques - qu'il s'agisse d'une personne, d'une organisation ou d'un gouvernement - indépendamment de leur perspicacité technique, de leur culture ou de leur emplacement, ou des motivations de l'agresseur, qu'elles soient criminelles ou géopolitiques. Nous concevons, développons et fournissons des produits et services qui privilégient la sécurité, la confidentialité, l'intégrité et la fiabilité, et réduisent ainsi la probabilité, la fréquence, l'exploitabilité et la gravité des vulnérabilités.
2. *Nous nous opposerons aux cyberattaques contre les citoyens et les entreprises.*

Droit de l'espace numérique

Nous protégerons contre l'altération et l'exploitation des produits et services technologiques pendant leur développement, leur conception, leur distribution et leur utilisation. Nous n'allons pas aider les gouvernements à lancer des cyberattaques contre des citoyens et des entreprises innocents.

3. *Nous aiderons les utilisateurs, les clients et les développeurs à renforcer la protection contre les cyberattaques.*

Nous fournirons à nos utilisateurs, clients et à l'ensemble de l'écosystème des développeurs des informations et des outils leur permettant de comprendre les menaces actuelles et futures et de se protéger contre elles. Nous soutiendrons la société civile, les gouvernements et les organisations internationales dans leurs efforts pour faire progresser la sécurité dans le cyberspace et pour renforcer la capacité de cybersécurité dans les économies développées et émergentes.

4. *Nous serons partenaires pour augmenter la cybersécurité.*

Nous travaillerons ensemble et établirons des partenariats formels et informels avec des chercheurs de l'industrie, de la société civile et de la sécurité, à travers des technologies propriétaires et open source pour améliorer la collaboration technique, la divulgation coordonnée des vulnérabilités et le partage des menaces et de codes malveillants introduits dans le cyberspace. Nous encouragerons le partage d'informations à l'échelle mondiale et les efforts civils pour identifier, prévenir, détecter, réagir et récupérer des cyberattaques et assurer des réponses flexibles à la sécurité de l'écosystème technologique mondial. Afin de s'assurer qu'un partenariat significatif est établi grâce à la mise en œuvre de l'Accord sur la technologie, nous, les entreprises soussignées, continuerons de définir les activités de

Droit de l'espace numérique

collaboration que nous entreprendrons pour promouvoir cet Accord. Nous rendrons également compte publiquement de nos progrès dans la réalisation de ces objectifs.

La démarche est incontestablement originale. Elle répond aux échecs successifs de la communauté internationale en quête d'une gouvernance de l'espace numérique. À Dubaï (2012), l'Union internationale des télécommunications (UIT) n'avait pas pu trouver un accord. En juin 2017, le Groupe d'experts gouvernementaux (GGE), missionné par l'ONU, s'est séparé sans faire émerger un consensus sur l'application du droit international. L'initiative semble aujourd'hui reposer sur le secteur privé. Il est vrai qu'il tient une place essentielle dans la cybersécurité. Mais pour les États, c'est tout de même un désaveu ! Si l'élaboration de la Convention devait aboutir, ce serait bien la première fois qu'un instrument de droit international serait le fruit de la seule initiative privée.

Actualité pénale

Par Mme Claudia Ghica-Lemarchand

PREUVE

La Cour de cassation a précisé les règles de preuve dans deux arrêts rendus le 9 mai 2018 qui retiennent l'attention.

INFILTRATION – GÉOLOCALISATION

Crim. 9 mai 2018, n° 17-86558, publ. à venir au Bull.

L'arrêt rappelle utilement les règles applicables à l'infiltration et précise le régime de la géolocalisation.

Le 8 janvier 2016, l'Office central pour la répression du trafic de stupéfiants (OCRTIS) a reçu des informations du Service de sécurité intérieure du Pérou relatives à l'organisation d'un trafic de cocaïne en provenance de ce pays à destination de la France. L'enquête a permis d'identifier un suspect et un indicateur a fourni un autre renseignement sur une personne essayant d'entrer en relation avec des bagagistes susceptibles de sortir des valises de stupéfiants de l'aéroport Charles de Gaulle – Roissy. Le Service Interministériel d'Assistance Technique a été saisi afin de mettre en place une opération d'infiltration. Un agent infiltré s'est présenté comme susceptible de sortir les bagages contenant de la cocaïne. L'agent a sorti de l'aéroport une valise de 15 kg de stupéfiants et l'a remise en échange de 45 000 €. Un dispositif de géolocalisation en temps réel a permis de suivre le véhicule, d'identifier les personnes impliquées dans le trafic et plusieurs opérations d'importation. L'agent infiltré a procédé à plusieurs opérations du même type, consistant à récupérer des valises de

Actualité pénale

plusieurs dizaines de kilogrammes de cocaïne en échange d'argent comme rémunération de ses services. Une opération d'interpellation a été mise en place 8 mois après le début de l'infiltration. De nombreuses personnes ont été mises en examen pour importation de stupéfiants en bande organisée, infractions à la législation sur les stupéfiants et association de malfaiteurs. Les contacts de l'agent infiltré ont demandé l'annulation des pièces de la procédure, qui a été refusée par la chambre de l'instruction. La Cour de cassation examine les deux pourvois déposés par les personnes mises en examen.

Le premier pourvoi repose sur un moyen unique fondé sur la loyauté de la preuve et visant les articles 6 de la Convention européenne des droits de l'Homme, l'article préliminaire et 706-81 et suivants du Code de procédure pénale définissant le régime juridique de l'infiltration. L'infiltration d'un officier ou agent de police judiciaire spécialement habilité est autorisée par un magistrat et peut être utilisée pour un crime ou un délit les autorisant à commettre, si nécessaire, certains actes constituant des infractions mentionnées à l'article 706-82 constituant une cause d'exonération spéciale de responsabilité pénale. Une loi du 19 décembre 1991 avait permis aux OPJ de procéder à des surveillances et des livraisons surveillées dans le cadre du trafic de stupéfiants, mais c'est la loi du 9 mars 2004 relative à la lutte contre la criminalité organisée qui a étendu le champ d'application de la procédure d'infiltration dans ce cadre général de la délinquance organisée. Mais l'article 706-81 pose une limite absolue puisque « à peine de nullité, ces actes ne peuvent constituer une incitation à commettre des infractions ».

L'arrêt de la chambre de l'instruction considère que l'intervention de l'agent infiltré dans le cadre du trafic actif en provenance du Pérou s'est faite « en l'absence de toute

Actualité pénale

provocation à la commission d'infractions de sa part et de la part de l'agent infiltré, d'atteinte au principe de loyauté dans la recherche de preuves ou au droit à un procès équitable ». Le pourvoi conteste cette appréciation au moyen de trois arguments. D'une part, l'indicateur ayant présenté l'agent infiltré comme faux bagagiste aurait surveillé le groupe avant le signalement des opérations par le Pérou, « procédé » qui serait « assimilable à une opération d'infiltration sauvage précédant l'opération d'infiltration autorisée et qui s'est révélé déterminant du passage à l'acte, non prévu par la loi et qui élude les règles de procédure des articles 706-81 et suivants du code de procédure pénale, est illégal et caractérise un détournement de procédure ». D'autre part, l'intervention de l'agent infiltré serait une conséquence de cette surveillance préalable, sauvage et serait contaminée par l'illégalité de la procédure. Enfin, l'intervention de l'OCTRIS était une provocation à la commission de l'infraction parce que seul le fait de leur présenter l'agent infiltré comme bagagiste « avait transformé l'impossible en possible ». Ce dernier argument met l'accent sur le fait que l'intervention du bagagiste accomplissait l'infraction qui autrement restait au stade d'un projet criminel.

La Chambre criminelle de la Cour de cassation rejette le pourvoi, puisque l'arrêt contesté a établi que « ni l'informateur ni l'agent infiltré n'ont provoqué à la commission de l'infraction », se contentant « de mettre en relation avec ce service une équipe de trafiquants opérant depuis le Pérou et souhaitant importer de la cocaïne en France, à la recherche d'un bagagiste pour faire sortir le produit de l'aéroport, l'agent infiltré ayant répondu à la demande formulée de réceptionner le produit à son arrivée sur le territoire national ».

La Chambre criminelle applique strictement la limite posée par le

Actualité pénale

Code de procédure pénale aux infiltrations policières qui ne doivent en aucun cas être des incitations à la commission de l'infraction, mais peuvent être des provocations à la preuve, conformément à l'article 706-81. Cette limite imposée aux infiltrations est une application spéciale du principe général de loyauté de la preuve. Afin de déterminer la validité d'un moyen de preuve, il convient de distinguer entre la provocation à la commission de l'infraction, strictement interdite, car elle vicie la procédure, et la provocation à la preuve de l'infraction, qui est autorisée, car elle ne viole pas les règles du procès équitable. Cette distinction s'applique exclusivement à la preuve émanant de l'autorité publique, la preuve émanant des parties privées étant plus souplement appréciée par les juges.

Le régime juridique des articles 706-81 et suivants applique les principes généraux. D'une part, la Convention de sauvegarde des droits de l'Homme et des libertés fondamentales et la jurisprudence de la Cour européenne des droits de l'Homme mettent l'accent sur la loyauté de la preuve comme clé de voûte du procès équitable. Dans de nombreux arrêts (CEDH 5 février 2008, Ramanauskas c/ Lituanie), la CEDH rappelle la distinction entre les infiltrations policières admises, car strictement circonscrites, et les provocations policières qui privent la personne *ab initio* d'un procès équitable et définit les critères permettant de les différencier. En cas de provocation policière, les agents ne se contentent pas d'examiner d'une manière purement passive l'activité délictueuse, mais exercent sur la personne une influence de nature à l'inciter à commettre l'infraction, ce qui constitue un contournement des principes européens du procès équitable. Une simple rumeur selon laquelle la personne se livrerait à une activité délictueuse ne suffit pas et l'agent infiltré qui propose une somme d'argent à une personne pour la

Actualité pénale

corrompre provoque la commission même de l'infraction, privant la procédure de fondement légal. En revanche, l'équité de la procédure est respectée lorsque l'agent infiltré sert d'intermédiaire pour des ventes de stupéfiants qui avaient commencé avant l'opération d'infiltration (CEDH 4 novembre 2010, Bannikova c/ Russie). Si les éléments de preuve fournis par les autorités nationales permettent aux juges de s'assurer de l'intention pré-existante de la personne mise en cause de commettre l'infraction, l'intervention de l'agent infiltré est accessoire et permet seulement de révéler la preuve, respectant les règles du procès équitable. D'autre part, l'article préliminaire du Code de procédure pénale se révèle le réceptacle des principes définis par la jurisprudence européenne et inscrit cette distinction dans le droit positif. Si la Chambre criminelle de la Cour de cassation a pu appliquer cette distinction, l'admission des infiltrations policières dans la procédure pénale a permis de l'inscrire dans la loi. Lorsque la provocation vise simplement à prouver l'infraction, la preuve est admise, car l'intervention de l'autorité publique ne crée pas l'infraction, elle sert simplement à la révéler (Crim. 22 avril 1992, Bull. n°169). Qu'il s'agisse d'agents qui assistent à la commission de l'infraction ou qui sont infiltrés dans le processus infractionnel, tant qu'ils restent passifs, sans provoquer d'une quelconque manière l'infraction, leur intervention ne vicie pas la preuve, car l'infraction se serait déroulée avec ou sans leur intervention. Les articles 706-81 et suivants du Code de procédure pénale ont inscrit dans la loi la distinction jurisprudentielle entre les provocations à la preuve de l'infraction et celles à la commission de l'infraction, sanctionnées par la nullité.

Le pourvoi formulé par l'autre personne mise en cause développe plusieurs moyens, mais seuls ceux relatifs à la

Actualité pénale

géolocalisation seront étudiés, puisqu'ils conduisent à une cassation au visa des articles 230-32 et suivants. Ces derniers ont été introduits par la loi n° 2014-372 du 28 mars 2014 relative à la géolocalisation, adoptée à la suite de deux arrêts remarquables de la Cour de cassation (Crim. 22 octobre 2013, Bull. n° 196 et 197) qui considéraient que la géolocalisation devrait être admise dans le cadre de l'instruction, opérée sous le contrôle d'un juge, mais qu'elle devait être invalidée dans le cadre des enquêtes préliminaires, le contrôle par le procureur de la République étant insuffisant, puisque n'étant pas considéré comme une autorité judiciaire au sens de la Convention européenne de sauvegarde des droits de l'Homme.

La géolocalisation est définie par le Code de procédure pénale comme « tout moyen technique destiné à la localisation en temps réel, sur l'ensemble du territoire national, d'une personne, à l'insu de celle-ci, d'un véhicule ou de tout autre objet, sans le consentement de son propriétaire ou de son possesseur » et est autorisée dans le cadre des enquêtes et instructions pour tous les crimes et délits punis d'au moins cinq ans d'emprisonnement, sauf les délits relatifs aux évasions ou entraves à la saisine de la justice où le plancher de l'emprisonnement est abaissé à trois ans, et les enquêtes pour mort, disparition ou fuite de la personne. D'une durée initiale de 15 jours, décidée par le procureur de la République, elle peut être prolongée d'un mois par le juge des libertés et de la détention, renouvelable dans les mêmes conditions. Sa décision n'a pas de caractère juridictionnel et n'est susceptible d'aucun recours. En cas « d'urgence résultant d'un risque imminent de dépérissement des preuves ou d'atteinte grave aux personnes ou aux biens », les opérations peuvent être mises en place par un officier de police judiciaire qui doit en informer immédiatement, par tout moyen, le procureur de la République

Actualité pénale

ou le juge d'instruction. Ces magistrats disposent d'un délai de vingt-quatre heures pour prescrire, par décision écrite, la poursuite des opérations. Trois hypothèses peuvent se manifester. Dans le premier cas, ils peuvent ordonner la mainlevée. Dans le deuxième cas, ils ne font rien et leur silence équivaut à la fin de la mesure. Dans la troisième hypothèse, ils peuvent autoriser la géolocalisation avec une obligation supplémentaire posée à l'article 230-35 du Code de procédure pénale, car « l'autorisation comporte l'énoncé des circonstances de fait établissant l'existence du risque imminent ».

En l'espèce, plusieurs contestations visant la géolocalisation ont été formulées. D'une part, les mesures de géolocalisation visaient le véhicule utilisé par la personne mise en examen mais appartenant à sa concubine, qui n'était pas encore devenue sa femme à l'époque des faits. L'arrêt de la chambre de l'instruction refuse le droit à la personne mise en examen de contester les mesures de géolocalisation, car elle « ne pouvait se prévaloir d'aucun droit sur le véhicule géolocalisé », ayant déclaré qu'elle n'était propriétaire d'aucun véhicule et que l'origine des fonds pour acquérir celui-ci demeurait inexplicite. D'autre part, les enquêteurs ont demandé au Procureur de la République d'autoriser les mesures de géolocalisation. Mais ils n'ont pas procédé à une mise en place immédiate de la surveillance dès l'obtention de l'autorisation, ils ne se sont pas placés non plus dans le cadre de la procédure d'urgence qui les autorisait à agir sans attendre l'intervention du magistrat et le dossier de la procédure ne contient qu'une autorisation datant du lendemain de la mise en place de la mesure. Enfin, si les policiers pouvaient décider la mise en place d'une mesure de géolocalisation de 24 heures, cela contraint le magistrat autorisant la prolongation de la mesure à respecter strictement les conditions de l'article 230-35, ne pouvant pas se

Actualité pénale

contenter de déduire que « l'urgence résultant du risque imminent de déperdition des preuves était caractérisée ». En décidant ainsi, la chambre de l'instruction, n'ayant pas « le pouvoir de pallier le manque de motivation de l'autorisation écrite du procureur de la République qui ne comportait ni référence à la géolocalisation déjà mise en place, ni énoncé des circonstances de fait établissant l'existence d'un risque imminent de déperdition des preuves ou d'atteinte grave aux personnes ou aux biens », viole le Code de procédure pénale.

La Cour de cassation approuve l'analyse stricte des conditions de la géolocalisation proposée par le pourvoi et casse l'arrêt. Si elle applique formellement les règles des nullités, l'arrêt permet de préciser la géolocalisation. Les articles 171 et 802 définissent les nullités. Le premier de ces textes prévoit qu'il y a « nullité lorsque la méconnaissance d'une formalité substantielle prévue par une disposition du présent code ou toute autre disposition de procédure pénale a porté atteinte aux intérêts de la partie qu'elle concerne » renforcé par le second qui limite les nullités à cette hypothèse.

La Chambre criminelle applique la combinaison de ces deux textes à l'espèce et affirme, qu'en principe, « la méconnaissance des formalités substantielles régissant les géolocalisations peut être invoquée à l'appui d'une demande d'annulation d'actes ou de pièces de procédure par la partie titulaire d'un droit sur l'objet géolocalisé ou qui établit qu'il a, à l'occasion d'une telle investigation, été porté atteinte à sa vie privée ». Elle reprend ainsi dans le contexte de la géolocalisation la formule de principe qui régit désormais le régime juridique des nullités substantielles. En application de cette règle, la Cour de cassation casse l'arrêt de la chambre de l'instruction qui a refusé la nullité de la géolocalisation, alors même qu'elle constatait, d'une part,

Actualité pénale

« que l'intéressé avait l'usage habituel du véhicule en cause, dont il n'était pas prétendu qu'il était détenu frauduleusement » et que, d'autre part, « l'autorisation écrite du procureur de la République a été donnée postérieurement à la mise en place du dispositif de géolocalisation, sans mise en œuvre préalable des dispositions de l'article 230-35 du code de procédure pénale ».

La Cour de cassation interprète strictement les conditions de la géolocalisation et étend le droit de demander la protection légale des articles 230-32 à toutes les personnes qui verraient leur droit à la vie privée violée et ne le limite pas aux seules personnes visées par la mesure ou qui seraient propriétaires des objets concernés. La géolocalisation constitue en soi une violation du droit à l'intimité de la vie privée et est soumise à un régime juridique strict imposé par la sauvegarde des droits fondamentaux, autant sur le plan national qu'international. Ces dispositions techniques garantissent une pleine protection des droits fondamentaux, mais elles ne doivent pas vider de sens toute investigation policière et paralyser l'action des pouvoirs publics. En effet, la Cour européenne des droits de l'Homme (CEDH 2 septembre 2010, *Uzun c/ Allemagne*) a considéré que ces mesures d'investigation, lorsqu'elles étaient prévisibles et accessibles, nécessaires dans une société démocratique et proportionnées à la gravité de l'atteinte, ne constituaient pas une violation de la vie privée (article 8), ni du procès équitable (article 6). Mais cette admission au titre de moyens d'investigation s'accompagne d'une limitation stricte de leur emploi prévue par le Code de procédure pénale.

Actualité pénale

PREUVE – GÉOLOCALISATION

Crim. 9 mai 2018, n° 17-86638

Dans un arrêt rendu le même jour, la Chambre criminelle continue de préciser le régime juridique des mesures de géolocalisation.

Une personne a dénoncé un individu comme étant fournisseur de drogue, conduisant à l'ouverture d'une enquête préliminaire. Au terme d'un mois, un officier de police judiciaire a mis en place un moyen de géolocalisation en temps réel, en vertu de l'article 230-35 du Code de procédure pénale, justifié par « le risque imminent de dépérissement des preuves caractérisé par les déplacements réguliers » de l'individu suivi au volant de ce véhicule. Par une autorisation datée du même jour, le Procureur de la République a autorisé la prolongation pour quinze jours de la mesure « au visa d'un risque imminent de dépérissement des preuves ou d'atteintes graves aux personnes ou aux biens sans autre caractérisation ». Mis en examen, l'individu dépose une requête en nullité des mesures de géolocalisation de ce véhicule, ainsi que des autres véhicules qu'il possédait, et de tous les actes subséquents. La chambre de l'instruction rejette la demande de nullité du dispositif de géolocalisation de l'Audi, le véhicule directement concerné, mais l'accorde pour les deux autres véhicules. Un pourvoi est formé, proposant deux moyens qui prospèrent et retiennent l'attention.

Le premier moyen repose sur la validité même de la mesure de géolocalisation et, plus particulièrement, sur l'article 230-35 du Code de procédure pénale. Ce dernier autorise l'officier de police judiciaire à mettre en place une mesure de géolocalisation de sa

Actualité pénale

propre initiative. Néanmoins, cette procédure n'étant pas soumise au contrôle d'un magistrat, elle est encadrée par des conditions extrêmement strictes, qu'elles soient de fond ou de forme. D'une part, elle ne peut être utilisée qu'en « cas d'urgence résultant d'un risque imminent de dépérissement des preuves ou d'atteinte grave aux personnes ou aux biens ». D'autre part, elle ne peut être décidée que par un officier de police judiciaire pour une durée très limitée de 24 heures. Enfin, elle est contrôlée par un magistrat, le procureur de la République ou le juge d'instruction. Non seulement ce dernier doit être informé de la mesure dès sa mise en place, par tout moyen, mais il lui incombe d'agir pour la maintenir. S'il peut décider de sa mainlevée à tout moment, l'inaction du magistrat équivaut à la fin de la mesure. S'il décide de la maintenir, « l'autorisation comporte l'énoncé des circonstances de fait établissant l'existence du risque imminent mentionné à ce même alinéa », celle-là même qui aura justifié l'application immédiate de la géolocalisation directement par l'OPJ. Ce régime est applicable, sauf si la mesure de géolocalisation nécessite l'introduction dans un lieu d'habitation, auquel cas l'OPJ doit recueillir l'accord donné par tout moyen, émanant du juge des libertés et de la détention.

La chambre de l'instruction a rejeté la demande de nullité en considérant que le procureur de la République avait autorisé la prolongation de quinze jours de la mesure en justifiant du risque imminent de dépérissement des preuves que l'OPJ lui-même avait expliqué dans l'information donnée quant à la mise en œuvre de la mesure de géolocalisation en l'absence de l'autorisation préalable du procureur de la République. Le pourvoi conteste, en premier lieu, l'utilisation de la mesure de géolocalisation en urgence par l'OPJ en tant que « mesure particulièrement intrusive et attentatoire à la vie privée » qui « ne

Actualité pénale

peut s'entendre que d'une urgence particulière, caractérisée et sur laquelle le juge exerce a posteriori son contrôle ». Agissant dans le cadre d'une enquête préliminaire, les policiers ont justifié l'urgence par les déplacements réguliers que l'individu effectuait à bord de ce véhicule. Or, dans ce cas, l'utilisation régulière du véhicule démontrait qu'il n'y avait aucune urgence de nature à aboutir à un dépérissement des preuves, mais simplement un moyen de le surveiller et de pallier l'impossibilité de surveiller physiquement l'individu et ses déplacements.

La Chambre criminelle donne raison, doublement, à ce premier moyen du pourvoi. D'une part, la demande initiale émanant de l'OPJ ne remplit pas les conditions de l'article 230-35, car le procès-verbal « établi par l'officier de police judiciaire après l'information donnée au procureur de la République n'énonçait que la nécessité d'exercer de manière efficace une surveillance physique de (l'intéressé) et de pouvoir suivre techniquement les déplacements de la voiture qu'il pouvait être amené à utiliser pour ses déplacements ». D'autre part, « l'autorisation de prolongation donnée par le procureur de la République ne comportait aucun énoncé des circonstances de fait établissant l'existence d'un risque imminent de dépérissement des preuves ou d'atteinte grave aux personnes ou aux biens ». La Chambre criminelle considère que le défaut initial de justification de la géolocalisation est continué par l'autorisation de prolongation donnée par le procureur. L'hypothèse étudiée par l'arrêt est intéressante, elle démontre que le défaut initial de la procédure n'est pas corrigé ou redressé par la suite. Il serait intéressant de se demander que déciderait la Cour de cassation si la justification initiale défailante se trouvait justifiée par une autorisation de prolongation conforme du procureur de la République. Est-ce que la justification postérieure permettrait à la mesure

Actualité pénale

d'échapper à la nullité ou est-ce que le défaut initial saperait la légalité de toute la procédure ?

Le deuxième moyen a trait au régime juridique des nullités en application des articles 170, 173, 174 et 802. L'article 170 définit les personnes pouvant saisir la chambre de l'instruction afin de demander la nullité d'une pièce - le juge d'instruction, le procureur de la République, les parties ou le témoin assisté. Les articles 173 et 174 déterminent la procédure à suivre en cas de demande de nullité et les pouvoirs de la chambre de l'instruction. L'article 802 prévoit que la nullité peut être prononcée par toute juridiction, y compris par la Cour de cassation, « en cas de violation des formes prescrites par la loi à peine de nullité ou d'inobservation des formalités substantielles » mais uniquement « lorsque celle-ci a eu pour effet de porter atteinte aux intérêts de la partie qu'elle concerne ». La chambre de l'instruction a prononcé la nullité de la géolocalisation des deux véhicules supplémentaires, mais a refusé la nullité des actes subséquents de procédure. Selon le pourvoi, cette analyse n'est pas possible. Soit la nullité est refusée, car la géolocalisation est justifiée, soit elle ne l'est pas et, dans ce cas, elle entraîne la nullité de tous les actes subséquents qui n'ont été possibles que sur le fondement de ces premières investigations. Encore une fois, l'analyse proposée par le pourvoi prospère.

La Chambre criminelle casse et annule l'arrêt de la chambre de l'instruction ayant prononcé la nullité de la géolocalisation mais considérant que les autres éléments du dossier ne sont pas susceptibles d'annulation. La dissociation des différentes pièces de la procédure n'est pas interdite, mais obligation est faite aux juges de démontrer « que les actes annulés n'étaient pas le support nécessaire et exclusif des autres actes de la procédure ». À défaut, la décision des juges est considérée comme entachée

Actualité pénale

d'illégalité et est frappée de cassation.

Le contrôle judiciaire des mesures de géolocalisation, notamment en cas de mise en place sur initiative de l'OPJ, est renforcé progressivement, conformément à l'esprit initial de la jurisprudence et de la loi du 28 mars 2014. La mesure, attentatoire aux droits fondamentaux et à la vie privée, est contrôlée, en premier lieu, par un magistrat, procureur de la République ou juge d'instruction et, ensuite, par la chambre de l'instruction, incarnant l'intervention de l'autorité judiciaire. À ce titre, elle ne peut se contenter d'un contrôle formel des pièces de procédure, elle doit vérifier le respect des conditions de fond, comme de forme, de la géolocalisation.

PRINCIPE NE BIS IN IDEM – ASSOCIATION DE MALFAITEURS ET BANDE ORGANISÉE

Crim. 16 mai 2018, n° 17-81151, publ. Bull. à venir

Dans le cadre d'une vaste fraude à la TVA par la vente dissimulée de cartes prépayées, plusieurs prévenus sont condamnés pour avoir participé à des faits d'escroquerie en bande organisée consistant à avoir obtenu une diminution de TVA en donnant l'apparence de livraisons intra-communautaires entre plusieurs sociétés françaises et diverses sociétés de droit belge, luxembourgeois, espagnol ou portugais, à des ventes à grande échelle de cartes téléphoniques prépayées d'opérateurs français à des sociétés qui étaient en réalité situées sur le territoire national. Certains d'entre eux sont concomitamment condamnés pour des faits d'association de malfaiteurs, commis dans les mêmes circonstances de temps et de lieu, ayant consisté, en vue de la

Actualité pénale

commission du délit d'escroquerie en bande organisée, en l'organisation de rendez-vous, la constitution de sociétés fictives à l'étranger ou encore l'établissement de faux documents. Sur les huit prévenus condamnés, deux forment des pourvois en cassation et contestent, à la fois, les qualifications pénales retenues, ainsi que la condamnation solidaire à une somme supérieure à 6 000 000 € équivalant à l'impôt dont le paiement a été éludé, à hauteur de leur participation à l'infraction. Seuls les moyens concernant les qualifications pénales seront étudiés.

Le premier pourvoi est formé par une personne ayant été condamnée pour escroquerie en bande organisée, mais relaxée pour association de malfaiteurs. Elle conteste, d'une part, la qualification d'escroquerie qui n'a pas été justifiée par les juges du fond, qui se sont concentrés sur le rôle qu'elle a joué dans l'organisation de la fraude. Or, « l'escroquerie suppose de la victime ou d'un tiers qu'il remette à l'auteur de l'infraction des fonds, des valeurs ou un bien quelconque, qu'il fournisse un service ou qu'il consente un acte opérant obligation ou décharge ». Selon le pourvoi, « en se bornant à relever des manœuvres frauduleuses visant à éluder le paiement de la TVA, sans établir la remise que les manœuvres frauduleuses auraient poussé le trésor public à consentir une remise », l'article 313-1 du Code pénal définissant l'escroquerie a été violé. Elle conteste, d'autre part, l'utilisation de la circonstance de bande organisée puisque les juges ont considéré qu'elle a participé « en toute connaissance de cause, comme co-auteur, aux escroqueries en bande organisée qui lui sont reprochées, en recevant livraison, de manière occulte, de cartes qu'elle était chargée de revendre, dont elle ne pouvait ignorer qu'elles s'inscrivaient dans le cadre d'une opération visant à frauder le fisc et en revendant ces cartes le tout en liquide et sans facture », sans établir la préméditation des infractions et une organisation

Actualité pénale

structurée entre ses membres qui sont les éléments constitutifs de la circonstance aggravante de la bande organisée. En effet, l'article 132-71 définit la circonstance aggravante de la bande organisée comme « tout groupement formé ou toute entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs infractions ». La participation matérielle, critère objectif, se double d'une volonté de participer à cette entente particulière, relevant d'un critère subjectif. Le second pourvoi exploite cette même critique et soutient une contradiction dans le raisonnement des juges ayant retenu la bande organisée, alors même qu'ils ont relevé « que les manœuvres avaient été réalisées par plusieurs équipes qui n'étaient pas toujours composées de la même manière, l'organisation ayant évolué », que la personne poursuivie « en particulier n'ayant été que l'un des transporteurs de fonds en liquide, ayant succédé à un autre transporteur, pour une durée inférieure à huit mois », ce qui excluait la bande organisée.

La Chambre criminelle réunit les moyens et les rejette au titre d'une démonstration unique concernant, à la fois, la qualification de l'infraction et la circonstance aggravante. Le délit d'escroquerie est constitué « dès lors que la déclaration frauduleuse d'opérations non imposables au titre de la TVA, lorsque cette déclaration est acceptée par l'administration, vaut décharge au sens des dispositions de l'article 313-1 du code pénal ». Ensuite, la bande organisée a été caractérisée par les juges du fond dans les deux éléments constitutifs de l'infraction, la préméditation et la commission au moyen d'une organisation structurée, puisque les deux personnes condamnées étaient en lien étroit avec les commanditaires « comme les ayant mis tous deux en rapport, lesquels étaient les principales chevilles ouvrières des faits poursuivis, le premier au stade de la mise en

Actualité pénale

place des livraisons intra-communautaires fictives, le second au stade de l'écoulement, sur le territoire national, des cartes téléphoniques prépayées » et « même si le rôle de [M.X.] a été, pour l'essentiel, contingenté à une mission précise, celle de transporter des fonds en liquide, il a assumé ce rôle en sachant parfaitement son importance dans le schéma frauduleux mis en place ». Cette dernière précision est extrêmement importante et montre que la Cour de cassation a une interprétation large de la notion de bande organisée qui est appréciée selon un critère subjectif qui prévaut sur le critère objectif. La circonstance aggravante est constituée « peu important que les diverses fonctions nécessaires à la mise en oeuvre du mode opératoire ainsi conçu n'aient pas été exercées par les mêmes personnes pendant toute la période de commission des faits poursuivis ». La volonté de la personne de participer à l'organisation l'emporte sur l'organisation matérielle de son intervention.

La deuxième personne condamnée soulève un autre moyen qui repose sur sa condamnation pour association de malfaiteurs. Elle en conteste, en premier lieu, la qualification. L'article 450-1 du Code pénal définit l'association de malfaiteurs comme « tout groupement formé ou entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'un ou plusieurs crimes ou d'un ou plusieurs délits punis d'au moins cinq ans d'emprisonnement ». Selon le pourvoi, cette définition exige « une participation personnelle et directe de l'auteur à la préparation d'un crime ou d'un délit ». Or, en l'espèce, la personne condamnée « s'était borné[e] à prendre la suite d'exécutants précédents, sans avoir participé personnellement à la préparation de l'infraction » et « n'avait eu que la mission précise de transporter des fonds sur une période de huit mois, ayant succédé à un autre transporteur, et qu'il avait parfois, à

Actualité pénale

cette occasion, sur les indications qu'on lui donnait, confectionné des factures fictives sur instruction des organisateurs de la fraude, quand ceux-ci ne pouvaient par le faire eux-mêmes, tout en ignorant à quoi ces factures pouvaient correspondre ». Ensuite, la personne conteste la double qualification des mêmes faits de « sa prétendue participation au réaménagement de l'organisation via son entente avec les principaux organisateurs, et sa participation à des tâches nécessaires à la réalisation de l'escroquerie, notamment la confection de factures fictives » comme élément constitutif d'une infraction, à savoir l'association de malfaiteurs, et comme circonstance aggravante d'une autre infraction, la bande organisée accompagnant l'escroquerie.

La Chambre criminelle saisit l'occasion de rendre un arrêt de principe énonçant une solution claire en la matière, mettant fin aux différentes spéculations en doctrine et à certaines hésitations jurisprudentielles. Au visa du principe *ne bis in idem*, la Cour de cassation affirme que « des faits qui procèdent de manière indissociable d'une action unique caractérisée par une seule intention coupable ne peuvent être retenus comme élément constitutif d'une infraction et circonstance aggravante d'une autre infraction ». La cassation, en l'espèce, se fonde sur le fait que les juges du fond ont retenu « des faits constitutifs d'association de malfaiteurs indissociables de ceux caractérisant la bande organisée comme circonstance aggravante de l'infraction d'escroquerie dont elle a déclaré le prévenu coupable ».

Cette solution claire mérite d'être saluée. Elle permet de distinguer deux situations qui ont été brouillées ces dernières années. Lorsque l'infraction est entrée en phase d'exécution, les faits de préméditation et d'organisation sont retenus dans le cadre de la bande organisée qui constitue une circonstance aggravante et

Actualité pénale

permet de relever le seuil de la répression. Lorsque les infractions projetées ne sont pas encore entrées en phase d'exécution, pour éviter l'impunité, l'association de malfaiteurs permet d'entrer en voie de répression. Dans ce cas, la préméditation et l'organisation sont des éléments constitutifs de l'infraction elle-même. L'association de malfaiteurs et la bande organisée ne se distinguent pas par leurs éléments constitutifs, mais par leur déroulement temporel. L'association de malfaiteurs se place en amont de la commission des infractions projetées, la bande organisée en aval des infractions tentées ou entièrement consommées.

BRÈVE

ERREUR DE DROIT

Crim. 3 mai 2018, n° 17-82746, publ. Bull. à venir

Deux personnes physiques, en tant que cogérantes d'une société, ont organisé des soirées de loto au profit de diverses associations pour lesquelles elles faisaient de la publicité dans la presse régionale. L'organisation de jeux de hasard est soumise à une réglementation spéciale qu'elles n'ont pas respectée. Elles sont poursuivies pour violation de la réglementation et pour ne pas avoir établi une comptabilité et une déclaration mensuelle du chiffre d'affaires en tant que maison de jeux. Le tribunal, suivi par la Cour d'appel, est entré en voie de relaxe au motif que « lors de la création de la société, les cogérantes ont choisi un expert-comptable, que ce dernier a écrit à l'administration fiscale en détaillant l'activité de la société, que l'administration fiscale a

Actualité pénale

répondu à l'expert-comptable sur la comptabilisation des gains de jeu au titre de la TVA ». Les cogérantes ont pris des précautions qui démontrent l'absence de tout caractère de dissimulation, ce qui écarte ainsi l'infraction d'élément intentionnel. Un pourvoi est formé par l'administration des douanes pour contester le caractère invincible de l'erreur de droit, ainsi que son existence. La Cour de cassation casse l'arrêt au visa de l'article 122-3 du Code pénal.

L'article 122-3 du Code pénal s'inscrit dans le chapitre consacré aux causes d'irresponsabilité ou d'atténuation de la responsabilité pénale et définit l'erreur de droit. « N'est pas pénalement responsable la personne qui justifie avoir cru, par une erreur sur le droit qu'elle n'était pas en mesure d'éviter, pouvoir légitimement accomplir l'acte ». Cause d'irresponsabilité subjective, l'erreur de droit fait disparaître l'imputabilité – l'auteur de l'acte n'a pas compris qu'il était en train de commettre une infraction. Introduite par le nouveau Code pénal, l'erreur de droit révolutionne la théorie du droit, car elle admet qu'une personne puisse ignorer le caractère interdit de l'acte, s'opposant à la fiction juridique selon laquelle « nul n'est censé ignorer la loi ». L'erreur de droit repose sur une information erronée émanant de l'administration publique, qui est invincible et absolue dans l'esprit de l'auteur de l'infraction. Au moment de l'action, ce dernier est persuadé de commettre un acte autorisé. Mais il n'est pas exempté de toute vérification et l'absence de diligence de sa part lui interdit de se prévaloir de cette cause d'irresponsabilité. Mais la pratique judiciaire s'est chargée de réduire considérablement le champ d'application de l'erreur de droit, à tel point qu'elle n'est presque jamais utilisée.

L'espèce est intéressante. Les prévenues se sont adressées à un expert-comptable qui s'est adressé à l'administration fiscale. Il

Actualité pénale

convient de comprendre que la consultation de l'expert-comptable, personne privée, ne peut nullement être source de l'erreur de droit. Seule la consultation par son intermédiaire de l'administration fiscale, une autorité publique permet de déclencher le bénéfice de l'article 122-3. La Cour de cassation ne s'étend pas sur les conditions particulières de l'espèce puisque l'Administration fiscale a répondu par un rescrit, dont la nature semble incompatible avec l'erreur de droit, et portant sur d'autres éléments que ceux faisant l'objet de l'erreur de droit. Elle préfère se pencher sur les conditions que doit remplir l'erreur de droit. La Cour de cassation reproche aux juges du fond de ne pas avoir caractérisé « l'existence d'une erreur de droit inévitable des prévenues sur la légalité de leur activité et alors que celles-ci étaient, dès le début de l'activité de la société, redevables de leurs obligations fiscales en matière de contributions indirectes ». L'erreur invincible doit être une certitude absolue dans l'esprit de l'auteur de commettre un acte autorisé et parfaitement légal. Or, en l'espèce, l'administration fiscale interrogée par l'expert-comptable avait gardé le silence et il n'était pas possible de l'interpréter comme ayant induit en erreur les cogérantes. Sans le dire, car elle ne peut pas se pencher sur le fond de l'affaire, la Cour de cassation insinue même le contraire – le fait d'avoir interrogé l'Administration fiscale aurait tendance à démontrer qu'il y avait un doute sur le régime fiscal de l'activité dans l'esprit des prévenues.

L'enseignement apporté par la Cour de cassation est doublement intéressant. D'une part, la personne qui se prévaut de la cause d'irresponsabilité doit la prouver, elle ne peut être présumée. D'autre part, l'appréciation de l'erreur de droit est subjective et les juges peuvent tenir compte de la qualité de la personne pour apprécier le caractère inévitable de l'erreur. La qualité de

Actualité pénale

professionnel du prévenu conduit à une appréciation plus sévère de la connaissance des obligations légales pesant sur lui, restreignant de fait l'admission de l'erreur de droit à son bénéfice.

Police administrative

Par M. Ludovic Guinamant

Lutte contre la piraterie en haute mer : l'État peut-il être condamné pour responsabilité sans faute pour avoir refusé le déploiement d'équipes militaires de protection embarquée sur un navire civil ?

Cour administrative de Bordeaux, 24 mai 2018, n° 15BX00402

Les Terres Australes et Antarctiques Françaises (TAAF) ont conclu le 24 avril 2009 un contrat portant sur la vente du navire de recherches scientifiques « La Curieuse » à la société de droit mauricien Indian Ocean exploration (IOE) Ltd. En vue d'une mission de prospection sous-marine profonde autour de Mayotte, au sud du 12^{ème} parallèle, en partenariat avec une société mauricienne, la société IOE a sollicité du ministre de la Défense, par courrier du 15 février 2011, le bénéfice d'une équipe militaire de protection embarquée (EPE) contre la piraterie.

Une décision implicite de rejet lui ayant été opposée, la société a renoncé à cette opération.

La société a alors saisi le tribunal administratif de La Réunion en faisant notamment valoir que ce refus de concours des forces armées, dès lors qu'elle remplissait les conditions pour bénéficier de la protection des forces publiques contre les actes de piraterie maritime, lui a occasionné un préjudice anormal et spécial de nature à engager la responsabilité sans faute de l'État.

Dans un premier temps, les magistrats de la Cour administrative de Bordeaux constatent qu'à la date d'acquisition du navire, la société de droit mauricien avait connaissance « que les activités de navigation, de recherches scientifiques et d'armement qu'elle effectuerait dans l'Océan Indien étaient soumises à une recrudescence des actes

Police administrative

de piraterie ». Ainsi, l'arrêt est motivé par le fait qu'il « résulte en particulier de la cartographie Isemar de la piraterie en 2008 que le golfe d'Aden et le canal du Mozambique étaient déjà identifiés comme des zones à risque. De surcroît, dès la fin de l'année 2008, la zone d'attaque des pirates somaliens s'était étendue au sud vers le canal du Mozambique et à l'Ouest vers la zone économique exclusive des Seychelles ».

La Cour ajoute également qu'aucune « disposition ou convention ni aucun principe n'impose à l'État français qu'il assure la protection individuelle des navires battant son pavillon contre la piraterie » et que, dès lors, la société, en contractant, avait bien conscience qu'elle assumait un risque d'être victime d'acte de piraterie.

Elle conclut, dès lors, qu'au « regard de l'aléa afférent à l'exploitation dans cette zone, connu de la société, la perte d'un contrat d'armement consécutif au refus de protection embarquée ne peut être regardée comme ayant constitué un aléa excédant ceux que comportait l'exploitation d'un navire dans l'Océan Indien et comme emportant pour la société requérante des conséquences génératrices d'un préjudice anormal et spécial ».

Contrôle de proportionnalité par le juge de l'UE d'une législation nationale prévoyant une amende pour l'absence de déclaration, par une personne physique, de capitaux entrant ou sortant de cet État sans sortir du territoire de l'Union européenne

Cour de justice de l'Union européenne, 31 mai 2018, n° C-190/17

Le 10 août 2014, M. Z., ressortissant chinois, a fait enregistrer ses bagages à l'aéroport de Grande Canarie (Espagne) pour un vol à

Police administrative

destination de Hong Kong (Chine), avec escales à Madrid (Espagne) et à Amsterdam (Pays-Bas). À l'occasion d'un contrôle effectué lors de l'escale à l'aéroport de Madrid-Barajas, il a été constaté que les bagages de M. Z. contenaient un montant de 92 900 euros en argent liquide, que celui-ci avait omis de déclarer. Ce montant a fait l'objet d'une saisie. Le 15 avril 2015, le Secretario General del Tesoro y Política Financiera dépendant du ministère de l'Économie et de la Compétitivité, a infligé une amende administrative de 91 900 euros à M. Z., après avoir relevé, au titre des circonstances aggravantes, le montant élevé de la somme non déclarée, l'absence de justification de l'origine licite de l'argent liquide, l'incohérence des déclarations de l'intéressé concernant son activité professionnelle et le fait que l'argent liquide se trouvait dans un endroit qui indiquait l'intention délibérée de le dissimuler.

La juridiction espagnole saisit la Cour de justice de l'Union européenne (CJUE) afin de savoir si M. Z. était soumis à l'obligation de déclaration alors que l'argent n'avait pas quitté le territoire de l'Union européenne, étant donné que l'intéressé ne pouvait, avant son arrivée sur le territoire chinois, avoir accès à l'argent se trouvant dans ses bagages enregistrés à l'aéroport de Grande Canarie et si l'amende infligée au titre de la loi espagnole était proportionnée.

La CJUE considère qu'en vertu du droit européen (règlement n° 1889/2005 du 26 octobre 2005), M. Z. devait déclarer l'argent aux autorités néerlandaises et non aux autorités espagnoles, dès lors qu'il était censé sortir du territoire de l'Union par l'aéroport d'Amsterdam.

Toutefois, les magistrats européens ajoutent que le règlement 1889/2005 ne s'oppose pas, en principe, à une réglementation d'un État membre imposant d'autres obligations de déclaration

Police administrative

que celles qu'il prévoit. Néanmoins, en l'espèce, après avoir effectué un contrôle de proportionnalité de la législation espagnole, ils concluent que le droit européen s'oppose à une réglementation d'un État membre qui prévoit que le manquement à l'obligation de déclarer des sommes importantes d'argent liquide entrant ou sortant du territoire de cet État est passible d'une amende pouvant aller jusqu'au double du montant non déclaré.

Liberté d'expression et terrorisme : la CEDH déclare irrecevable pour détournement de la liberté d'expression la requête déposée par une chaîne de télévision danoise

Cour européenne des droits de l'Homme, 24 mai 2018, n° 24683/14

La société Roj TV A/S est une entreprise et une chaîne de télévision danoise, qui avait obtenu une licence de diffusion délivrée par l'autorité danoise de radiotélédiffusion en 2003. Elle diffusait ses programmes depuis 2004, par satellite, principalement en kurde, en Europe et au Moyen-Orient. En septembre 2010, Roj TV et sa société mère furent accusées d'infraction aux dispositions sur la lutte contre le terrorisme du Code pénal danois. Il leur était reproché d'avoir fait l'apologie du PKK dans des programmes diffusés de juin 2006 à septembre 2010. En janvier 2012, notant que le PKK figurait sur la liste des organisations terroristes dans l'Union européenne, au Canada, aux États-Unis, en Australie et au Royaume-Uni, et que la chaîne ne présentait que le point de vue de cette organisation, le tribunal municipal de Copenhague jugea que le diffuseur avait été en infraction de février 2008 à septembre 2010 et le condamna au

Police administrative

paiement d'une amende d'un montant de 2,6 millions de couronnes danoises. La cour régionale du Danemark oriental confirma le verdict de culpabilité. Elle estima toutefois que la période concernée avait commencé dès juin 2006. Elle porta le montant de l'amende à 5 millions de couronnes et retira également à Roj TV sa licence de diffusion. La société requérante obtint l'autorisation de contester l'interdiction de diffusion devant la Cour suprême mais, en février 2014, celle-ci confirma cette mesure, à la majorité.

Invoquant l'article 10 de la Convention européenne des droits de l'Homme, Roj TV A/S soutenait que sa condamnation par les juridictions danoises et la peine que celles-ci lui avaient imposée avaient porté atteinte à sa liberté d'expression.

Toutefois, la Cour européenne des droits de l'Homme (CEDH), rappelant les termes de l'article 17 de la Convention disposant que « aucune des dispositions de la présente Convention ne peut être interprétée comme impliquant pour un État, un groupement ou un individu, un droit quelconque de se livrer à une activité ou d'accomplir un acte visant à la destruction des droits ou libertés reconnus dans la présente Convention ou à des limitations plus amples de ces droits et libertés que celles prévues à ladite Convention », déclare la requête irrecevable au motif que la société Roj TV a tenté de détourner l'article 10 garantissant la liberté d'expression, dès lors qu'entre 2006 et 2010, elle était financée dans une mesure importante par le PKK, que les programmes en cause incitaient à la violence et soutenaient des activités terroristes, et qu'ils étaient diffusés auprès d'un large public à la télévision.

Droit de la sécurité privée

Par M. Xavier Latour

Sécurité privée et levée de doutes

Parmi les relations entre les forces de sécurité publiques et la sécurité privée, la question des interventions sur alarme présente parfois des difficultés.

Les plus sérieuses intéressent le juge administratif. Il doit alors statuer sur la légalité des sanctions financières infligées aux sociétés privées pour violation de leurs obligations en la matière. Les contentieux ne sont pas si fréquents (une cinquantaine de décisions depuis 2008), et encore moins ceux qui retiennent l'attention des grandes revues juridiques.

Tel est pourtant le cas d'une décision de la Cour administrative d'appel de Nantes (CAA Nantes du 26 janvier 2018, n° 16NT04068, AJDA, 2018, p. 891, obs. FX Bréchet).

Ces dernières années, les progrès de la technologie alliés à la baisse des prix de l'électronique ont favorisé l'installation d'alarmes dans des locaux privés (habitation, commerce...). Certains systèmes sont reliés à des centres de télésurveillance chargés de vérifier à distance la véracité d'une éventuelle effraction, éventuellement de déclencher l'intervention d'un rondier privé, voire des forces de l'ordre.

Le cadre juridique général

Afin d'éviter que les opérateurs privés se déchargent trop

Droit de la sécurité privée

rapidement sur les forces publiques, le droit encadre les relations entre eux. Le Code de la sécurité intérieure (CSI) contient ainsi des dispositions relatives à l'obligation de levée de doute (article L. 613-6).

Dans le cadre de cette procédure, une ligne téléphonique spéciale est ouverte (articles D 613-17 à 23 CSI). Dès lors, le dirigeant d'une société privée de sécurité ne peut pas utiliser le numéro du standard des forces de l'ordre en l'absence de numéro réservé et invoquer l'état de nécessité pour s'exonérer de sa responsabilité (Cass. crim., 22 septembre 1999, n° 98-84.520, X. : *Bull crim.* 1999, n° 193, 615 ; D. 2000, 114 ; *Rev. sc. crim.* 2000, note Bouloc, 385).

L'appel injustifié d'une société privée de surveillance à la police ou à la gendarmerie, faute d'avoir préalablement vérifié le bien-fondé de l'alarme, est pécuniairement sanctionné (au maximum 450 euros par appel injustifié).

Une circulaire du 26 mars 2015 interprète les conditions d'application de ces dispositions.

La contestation de la sanction pécuniaire s'appuie, en général, sur les divergences d'appréciation de la levée de doute.

Le juge vérifie, d'abord, si les opérateurs privés ont procédé à une levée de doute préalable à la sollicitation des forces de l'ordre.

Les deux actions ne peuvent pas être concomitantes.

Droit de la sécurité privée

Ensuite, le télésurveilleur n'a pas à avoir la certitude qu'une infraction se commet. Une présomption suffit.

Elle se fonde alors sur les vérifications qu'il opère, à distance ou sur place. Dans ces conditions, l'administration ne peut pas se contenter de constater l'inutilité *a posteriori* d'un appel aux forces de l'ordre pour en conclure que cet appel était injustifié et sanctionner la société de sécurité (TA Marseille, 29 avril 2010, n° 0703791, *Sté Euro protection surveillance*).

Par ailleurs, la levée de doute exige un recueil d'informations effectif. Cela peut passer par l'envoi d'un agent de sécurité (non habilité à pénétrer dans des locaux privés), ou d'un système à distance.

Ainsi, l'incapacité de joindre l'occupant des lieux ou un tiers de confiance ne constitue pas une levée de doute. Chaque déclenchement doit donc faire l'objet d'un traitement spécifique (TA Strasbourg, 16 mai 2012, n° 1103943, *Sté Euro Protection Surveillance c/ Préfet de la Moselle : AJDA 2012*, note Richard, 1960).

L'adaptation de la levée de doute en fonction des situations

À ce stade, la situation se complique selon qu'il s'agit d'une alarme déclenchée de manière active (par un individu utilisant, par exemple, un bouton d'alerte), ou de manière passive (détection électronique).

Comme le remarque le rapporteur public Bréchet concluant sur la décision nantaise, jusqu'en 2018, les juges appréciaient moins

Droit de la sécurité privée

sévèrement les vérifications opérées sur une alarme active que sur un déclenchement passif. Cette distinction s'expliquait par les aléas inhérents à un dispositif électronique, alors qu'un déclenchement volontaire laisse présumer une infraction effective.

Dans l'hypothèse d'une alarme passive, l'entreprise doit non seulement procéder à des appels de vérification, mais encore rassembler des éléments plus concrets (captation d'images ou de sons par exemple ; TA Lille, 23 juin 2016, n° 1300457).

Dans une logique comparable, la levée de doute par une simple utilisation d'un système d'écoute sans plus de vérification (pas de contre-appel) ne suffit pas (TA Melun, 27 janvier 2017, n° 1502754).

Selon la circulaire et dans le cas d'une levée de doute à partir d'images, celles-ci doivent être dénuées de toute ambiguïté (la circulaire se réfère à des éléments « non équivoques »). Dans le cas contraire, deux contre-appels téléphoniques au client s'imposent. En cas d'échec, des vérifications par d'autres moyens sont nécessaires (rondier par exemple).

Cette exigence peut aussi justifier une meilleure connaissance de la situation du client par l'entreprise de surveillance (habitudes des employés, intervention de tiers dans les locaux...). Cette approche est, à juste titre, défendue par Monsieur Bréchet.

Elle s'inscrirait dans le cadre de l'amélioration des prestations fournies, au-delà des seules interventions injustifiées des forces de l'ordre. En effet, le développement de la télésurveillance ne s'accompagne pas systématiquement d'une prestation de qualité. La situation du client fait-elle l'objet de mises à jour régulières ? Les questionnaires de situation sont-ils suffisamment précis ?

Droit de la sécurité privée

Dans le cas, d'une alarme active, la situation se complique davantage.

A priori, le déclenchement volontaire présente moins de risque d'erreur qu'un système de détection électronique. C'est pourquoi, jusqu'à présent, les juges étaient moins regardants. Cela ne les avait pas empêchés de constater une violation de la levée de doute par une société qui, sur déclenchement d'un code « alerte » par un abonné, s'était contentée, sans plus demander de précision, d'une affirmation téléphonique selon laquelle la personne aurait été agressée par des voisins. L'agression se imitait, en réalité, au dépôt d'ordures dans son jardin (CAA Nancy, 17 décembre 2012, n° 12NC01020).

La décision nantaise infléchit cette ligne en direction d'une plus grande exigence.

Comme le souligne M. Bréchet, le déclenchement humain est lui aussi sujet à l'erreur. Dans de nombreux cas, des tiers (voisins, société de nettoyage...) font une mauvaise manipulation et ne penseraient pas à répondre aux appels téléphoniques de la société de surveillance.

Il poursuit en distinguant le déclenchement qui émet un signal de « contrainte » et celui qui émet un signal « d'alerte », en attachant à cette distinction une présomption plus ou moins forte d'erreur de manipulation. L'alarme « contrainte » laisserait supposer plus facilement une pression menaçante sur le client conduisant à une appréciation plus souple de la levée de doute, quand l'alarme « alerte » impliquerait un risque plus grand d'erreur.

Ainsi, en cas de « contrainte », l'échec des contre-appels n'entacherait pas la levée de doute d'insuffisance, tandis qu'en cas « d'alerte », des vérifications supplémentaires s'imposeraient

Droit de la sécurité privée

(sauf dans le cas de locaux sensibles : bijouteries par exemple).

Cette interprétation, aussi intéressante soit-elle, laisse une impression de raffinement excessif. Elle se fonde sur une analyse supposée des causes d'erreurs. Elle entre dans une subtilité assez peu compatible avec ce qui peut être une situation d'urgence.

À quoi sert d'enfermer la levée de doute dans de telles contraintes, sauf à donner le sentiment d'une volonté de sauver la légalité d'amendes administratives au demeurant assez modestes ?

Le raisonnement est un art qui perd de son intérêt lorsqu'il devient difficilement compréhensible et potentiellement contre-productif. L'insécurité ne concerne pas seulement des sites sensibles. Tout un chacun mérite attention.

Directeur de publication :	Lieutenant-Colonel Jean-Marc JAFFRE
Rédacteur en chef :	G ^{al} d'armée (2S) Marc WATIN-AUGOUARD
Rédacteurs :	G ^{al} d'armée (2S) Marc WATIN-AUGOUARD Frédéric DEBOVE Ludovic GUINAMANT Claudia GHICA-LEMARCHAND Xavier LATOUR
Equipe éditoriale :	Odile NETZER