La veille juridique

N°58, mai 2017

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

Edito

À l'heure où cette veille juridique est publiée, nous apprenons l'agression dont a été victime Nathalie Kosciusko-Morizet, candidate aux élections législatives. Toute atteinte physique sur les personnes est inacceptable. Mais, dans un contexte électoral, un tel acte est doublement offensant puisqu'il vise aussi directement l'exercice de la démocratie. Rien ne peut justifier une telle violence. Chacun a le droit d'avoir ses opinions et de les exprimer ; mais chacun aussi doit comprendre que le respect de l'autre est une des valeurs essentielles de notre République. Notre société a parfois tendance à l'oublier, laissant trop souvent impunis des comportements qui illustrent une forme des désinhibition, de banalisation de la violence physique ou verbale. Le simple suivi de propos tenus sur les réseaux sociaux est révélateur d'un manque de retenue qu'il convient de corriger si l'on veut maintenir un « savoir-vivre ensemble ».

(Suite page 2)

EDITORIAL

La négation du respect de l'autre est aussi un des fondements de l'idéologie terroriste qui continue de sévir, comme nous le déplorons cette fois-ci sur le territoire britannique.

Le terrorisme alimente hélas ! chaque édito. Manchester et le massacre des chrétiens coptes en Égypte nous rappellent l'actualité de la menace. Une fois de plus, c'est l'innocence qui est visée pour mieux faire pression, pour mieux intimider par la terreur. Plus l'EI est affaibli sur le théâtre irako-syrien, plus les risques de répliques, notamment en Europe, sont grands. D'où l'importance de ne pas baisser la garde. Le Président de la République a décidé de créer un Centre national de contre-terrorisme, directement rattaché à l'Élysée. Dirigé par le préfet Pierre de Bousquet, ancien directeur de la DST, cet organisme agit 24h/24 et implique les services et états-majors des ministères de l'Intérieur et de la Défense, avec la participation des transports, de la santé et de l'industrie. La récente réunion de l'OTAN, suivie de celle du G7, montre que cette mobilisation contre le terrorisme est mondiale. Le maintien de l'état d'urgence (dont l'intérêt réside principalement dans les capacités juridiques qu'il offre) témoigne de la vigilance du nouveau gouvernement. Le projet de loi, dont la première ébauche a été dévoilée par un quotidien du soir, aura sans doute pour objectif de pérenniser certaines mesures, sans pour autant maintenir indéfiniment l'état d'urgence. Un débat particulièrement riche en perspective, tant sur le plan politique que juridique. Notre Veille collera au plus près de l'actualité pour mieux vous informer.

Dernière minute : le rebondissement de l'Affaire Grégory. L'assassinat de cet enfant sera sans aucun doute un « marqueur » de l'histoire de la gendarmerie au XX^{ème} siècle. L'enquête a donné l'occasion de critiques parfois virulentes et très souvent injustes à l'égard de l'action de la gendarmerie. Mais, in fine, c'est bien la gendarmerie qui a conduit les investigations sous la direction de la Chambre de l'instruction de Dijon, preuve que la confiance de la Justice est demeurée intacte. Tout en ayant une pensée pour les premiers enquêteurs – je pense au capitaine Sesmat et à ses hommes - souvent « traînés dans la boue » par une presse impitoyable. Mais on se souviendra aussi et surtout du sursaut qualitatif que cette malheureuse affaire a provoqué de la part de la gendarmerie. Au risque de porter atteinte à leur modestie, je veux rendre hommage au travail accompli, dès 1986, par les généraux

EDITORIAL

Charlot, Napora (+), Le Mercier, Caillet qui ont porté, contre « vents et marées », le plan d'action pour la police judiciaire. Aujourd'hui, le dispositif montre toute sa pertinence. La modernisation de la gendarmerie est parfois la conséquence de ses échecs, même relatifs. L'essentiel est d'en tirer les leçons. L'essentiel, c'est aussi de poursuivre sans relâche l'effort de modernisation de notre institution.

VEILLE JURIDIQUE DE LA GENDARMERIE NATIONALE

Sommaire

Déontologie et sécurité

Par M. Frédéric DEBOVE

L'art et la manière d'évacuer l'espace public

Cette avant-dernière veille déontologique avant la dispersion estivale est entièrement dédiée à deux décisions récentes du Défenseur des droits dont les enseignements sont d'une grande importance pratique pour les acteurs de terrain de la sécurité intérieure. La première décision (MDS 2016-319) se rapporte à des consignes discriminatoires à l'encontre de familles Roms présentes sur la voie publique. La seconde décision (MDS 2017-061) est en lien avec une opération de maintien de l'ordre et plus précisément avec des interpellations visant des manifestants qui n'avaient pas obtempéré aux ordres de dispersion. Dans les deux cas, le Défenseur des droits rappelle aux dépositaires de l'autorité publique l'art et la manière de procéder à l'évacuation des espaces publics dans le respect des valeurs républicaines !

Avis de fermeture de la « chasse aux Roms » !

Au cœur de la **décision MDS n°2016-319 rendue publique le 6 mars 2017** se trouve une consigne litigieuse diffusée à l'attention des effectifs d'un commissariat de police parisien au printemps 2014. Libellée « Consignes sur les Roms », cette note de service - dont la teneur avait été révélée par la presse - était rédigée comme suit :
« En complément de la consigne MCI - main courante informatisée - en date du 9 avril concernant instruction parquet mendicité famille voie publique, conformément aux instructions reçues de Mme Y, Commissaire centrale, il y a lieu dès à présent et ce jusqu'à nouvel ordre, pour les effectifs du SSP, de localiser sur l'ensemble de la circonscription (...) les familles roms vivant dans la rue et de les évincer systématiquement. Conduite systématique au SAIP - service de l'accueil et de l'investigation de proximité - ou au STJND - service de traitement judiciaire de nuit du district - en fonction de l'heure, lors de la présence de famille de Roms avec enfants. Dans le même temps, sous l'autorité du Chef de service du SSP, en vue de prochaines opérations

Déontologie et sécurité

d'évictions et d'assistance aux Roms, il est demandé aux effectifs locaux, sous le commandement des chefs d'unités, de recenser les lieux de présence de Roms sur la voie publique en précisant ceux qui se livrent à la mendicité avec ou sans enfant, avec ou sans animaux et lieux de squatts la nuit. Rédaction d'une gestion d'événements détaillée à l'issue de l'intervention pour les effectifs locaux intervenants ».
En réponse aux sollicitations des services du Défenseur des droits, la commissaire de police centrale de l'arrondissement considéré avait tenu à préciser que la consigne litigieuse s'inscrivait dans le prolongement d'instructions hiérarchiques élaborées en parfaite concertation avec la section du Parquet chargé des mineurs. Tout en reconnaissant certaines maladresses de rédaction (corrigées par une note de service ultérieure), la commissaire de police faisait observer que les instructions données étaient surtout destinées à repérer les familles en détresse, à aider les jeunes mineurs en danger et, le cas échéant, à engager des actions judiciaires à l'encontre des parents qui viendraient à manquer à leurs obligations éducatives à l'égard de leurs progénitures.
Après avoir rappelé les nombreux textes faisant obligation aux fonctionnaires de police de s'acquitter de leurs missions conformément aux principes d'impartialité et de non-discrimination (et singulièrement l'article R. 434-11 du Code de la sécurité intérieure ou bien encore l'article 40 du Code européen d'éthique de la police), le Défenseur des droits relève que les consignes « d'éviction systématiques » visant les seules familles Roms présentaient un caractère ostensiblement discriminatoire. De surcroît, les instructions se rapportant au recensement des lieux de présence de Roms sur la voie publique caractérisaient une violation manifeste de la loi « Informatique et libertés », en ce qu'il est formellement interdit de recueillir et d'enregistrer des informations faisant apparaître, directement ou indirectement, les origines raciales ou ethniques des personnes. Enfin, et plus concrètement encore, le Défenseur des droits considère comme irrégulière toute opération de police visant à l'éviction systématique des familles Roms de la voie publique. En l'occurrence, à l'issue d'un contrôle d'identité effectué à l'égard d'une femme de nationalité roumaine, accompagnée de ses deux enfants, à proximité immédiate d'un distributeur automatique de billets, un équipage de police avait demandé aux intéressés de quitter les lieux. Cette injonction est considérée comme dépourvue de base légale et

cette irrégularité est d'autant plus flagrante et manifeste que l'opération de police n'avait révélé aucun acte de mendicité ni aucun mauvais traitement à l'encontre des jeunes enfants.

De la tolérance pour les rassemblements pacifiques à la tolérance pour les errements policiers

La **décision MDS n°2017-061 du 21 mars 2017** se rapporte, quant à elle, aux circonstances dans lesquelles plusieurs membres d'un collectif ont été interpellés pour des faits de participation à une manifestation non déclarée et refus de se soumettre aux sommations de se disperser, puis conduits au commissariat de police dans le cadre d'une vérification d'identité.

Les faits de l'espèce peuvent se résumer comme suit : le 26 juin 2013, près de 500 membres du collectif des « Veilleurs » sont rassemblés place de la République à Paris. Alors même que les organisateurs de ce sit-in n'ont pas adressé aux autorités préfectorales de déclaration préalable de manifestation, ce rassemblement est toléré par les pouvoirs publics à la condition de rester pacifique et statique. Pendant toute une partie de la soirée, le rassemblement ne trouble aucunement l'ordre public, en ce sens que les membres du collectif se contentent de lire des textes ou d'entonner des chants à la lumière de bougies. Aux alentours de minuit, la manifestation statique se mue soudainement en cortège, ce qui conduit les autorités civiles à solliciter le renfort de deux escadrons de gendarmerie mobile aux fins de contenir la progression des manifestants vers le siège des institutions. En considération de la dégradation de la situation et du trouble subséquent à l'ordre public, l'autorité civile - en l'occurrence le directeur de cabinet du préfet de police de Paris - ordonne alors aux forces de l'ordre de procéder aux sommations d'usage aux fins de dispersion de l'attroupement. Dans le prolongement immédiat de ces sommations restées sans effet, les forces de l'ordre reçoivent des instructions visant à l'interpellation des manifestants récalcitrants. Regroupés dans plusieurs véhicules de transport de grand gabarit, les individus interpellés sont ensuite conduits jusqu'à un commissariat de police dans le cadre de procédures

de vérification d'identité ordonnées par le magistrat du Parquet de permanence.

Dans leur réclamation auprès du Défenseur des droits (comme dans leur plainte avec constitution de partie civile déposée auprès du Doyen des juges d'instruction du TGI de Paris) plusieurs membres du collectif (26 au total) qualifient cette opération de police d'atteinte arbitraire à leur liberté individuelle, aggravée de plusieurs manquements à la déontologie de la sécurité.

Invité à se prononcer sur le bien-fondé de ces allégations, le Défenseur des droits s'efforce, dans sa décision n°2017-061 en date du 21 mars 2017, de passer l'opération de police litigieuse au crible juridique et déontologique, non sans avoir rappelé en liminaire les grands principes gouvernant la liberté de réunion.

S'inspirant de la démarche suivie de longue date par la Cour européenne des droits de l'Homme, le Défenseur des droits commence en effet par énoncer que « toute manifestation dans un lieu public est susceptible de causer un certain désordre pour le déroulement de la vie quotidienne, y compris une perturbation de la circulation, et qu'en l'absence d'actes de violence de la part des manifestants, il est important que les pouvoirs publics fassent preuve d'une certaine tolérance pour les rassemblements pacifiques, afin que la liberté de réunion ne soit pas dépourvue de tout contenu » (V. en ce sens, CEDH, *Barraco c/ France*, 5 mars 2009). Bien mieux, le seul fait que l'organisation d'une manifestation n'ait pas été déclarée conformément aux exigences législatives ou réglementaires en vigueur ne saurait justifier en soi une atteinte à la liberté de réunion (V. notamment CEDH, *Cisse c/ France*, 9 avril 2002). Dans une société démocratique, seuls des impératifs de maintien de l'ordre ou de sécurité publics peuvent légitimement entraver le droit à la liberté de réunion pacifique. À la lumière des faits de l'espèce, le Défenseur des droits admet aisément que c'est seulement en réaction face aux débordements intempestifs de certains membres du collectif et en considération du trouble à l'ordre public à proximité des institutions que les forces de l'ordre ont été appelées à procéder aux sommations d'usage et aux interpellations subséquentes. De telles mesures étaient non seulement nécessaires à la sauvegarde de l'ordre public mais proportionnées à la finalité poursuivie. À aucun moment de l'opération de maintien de l'ordre litigieuse, les veilleurs n'ont fait l'objet d'un

dispositif d'encagement si bien qu'il leur suffisait de franchir le piquetage mis en place par les gendarmes pour quitter librement le lieu du rassemblement.

Dans leur saisine du Défenseur des droits, les réclamants dénonçaient également un détournement de la procédure de vérification d'identité au motif que cette procédure aurait été utilisée, en pratique, dans l'unique but de disperser un rassemblement qui ne matérialisait aucune infraction pénale. Tout en écartant ce grief qu'il juge mal fondé en termes de déontologie de la sécurité, le Défenseur des droits va toutefois - et à titre subsidiaire en quelque sorte - pointer du doigt un florilège de légèretés formelles qui témoigne une nouvelle fois des faiblesses persistantes de la judiciarisation du maintien de l'ordre. À bien y regarder, autant la condamnation des imprudences procédurales paraissait inévitable, autant l'absence de sanction du contournement de procédure semble plus énigmatique.
Une procédure de vérification d'identité est-elle fondamentalement la procédure la plus adaptée aux circonstances qui se trouvent à l'origine de la réclamation des membres du collectif ? On peut légitimement en douter. À s'en tenir aux dispositions du Code de procédure pénale, une vérification d'identité n'est juridiquement possible que lorsque l'opération préalable de contrôle d'identité s'avère infructueuse. En effet, c'est seulement dans l'hypothèse où l'intéressé refuse ou se trouve dans l'impossibilité de justifier de son identité qu'il peut être retenu sur place ou dans le local de police où il est conduit aux fins de vérification de son identité (art. 78-3 C. pr. pén.). Or, dans l'espèce soumise au Défenseur des droits, les veilleurs interpellés puis conduits devant un officier de police judiciaire aux fins de faire l'objet d'une vérification d'identité étaient tous en possession d'un titre d'identité. De surcroît, aucune opération d'identité n'avait été réalisée à leur endroit sur les lieux de l'interpellation. En pareilles circonstances, une conduite au commissariat dans le cadre d'une procédure de vérification d'identité paraît extrêmement douteuse. À leur décharge, les forces de l'ordre ont agi au moment des faits litigieux sur instructions préalables d'un magistrat du Parquet de permanence. Toutefois, chacun sait que l'obéissance à l'autorité légitime a ses limites et que policiers et gendarmes doivent impérativement refuser d'obéir à un ordre manifestement illégal (art. 122-4 al.2 C. pén.).

En considération de la clarté des dispositions du Code de procédure pénale, les instructions du Parquet se rapportant à la mise en œuvre d'une procédure de vérification d'identité semblent davantage relever de l'illégalité manifeste que de la simple irrégularité. Il aurait sans doute été plus judicieux de considérer que les membres du collectif s'étaient rendus coupables du délit d'attroupement en refusant de se disperser après les sommations réglementaires (art. 431-4 C. pén.). Interpellés en flagrant délit (art. 53 et 67 C. pr. pén.), les intéressés pouvaient alors être présentés devant l'officier de police judiciaire le plus proche aux fins notamment de placement en garde à vue. Sans doute la garde à vue est-elle en pratique plus stigmatisante qu'une simple procédure de vérification d'identité ; toutefois, contourner les règles normales de procédure aux fins de bienveillance plus ou mois dissimulée (une vérification d'identité est en effet moins longue, moins formaliste et moins attentatoire à la présomption d'innocence qu'une garde à vue) ou de solution de confort n'est pas très satisfaisant. Et cette insatisfaction se trouve même aggravée lorsque les règles élémentaires de la vérification d'identité sont foulées au pied.

Ennemie jurée de l'arbitraire, la forme est la sœur jumelle de la liberté !

Quand bien même les garanties qui entourent la procédure de vérification d'identité sont-elles nettement moindres que celles jalonnant la garde à vue, ces règles ont le mérite d'exister et sont en principe maîtrisées par tout officier de police judiciaire. Qu'il soit fonctionnaire de police ou militaire de la gendarmerie, tout OPJ sait ou est présumé savoir que la personne retenue dispose de droits : faire aviser le procureur de la République de la vérification dont elle fait l'objet, prévenir à tout moment sa famille ou toute personne de son choix, ne pas être retenue plus de quatre heures ni davantage que le temps strictement nécessaire à l'établissement de son identité, etc. En outre, la procédure de vérification d'identité est encadrée par tout un formalisme protecteur des libertés individuelles dont la méconnaissance est d'ailleurs sanctionnée par une nullité textuelle (art. 78-3 in fine C. pr. pén.). Toute

Déontologie et sécurité

opération de vérification d'identité doit en effet donner lieu à la rédaction d'un procès-verbal dans lequel l'OPJ est appelé à mentionner les motifs qui justifient le contrôle et la vérification subséquente, ainsi que les conditions dans lesquelles la personne a été présentée devant lui, informée de ses droits et mise en mesure de les exercer. Le procès-verbal doit également préciser le jour et l'heure à partir desquels le contrôle a été effectué, le jour et l'heure de la fin de la rétention et la durée de celle-ci. En même temps que ce procès-verbal a vocation à être transmis au procureur de la République, une copie de ce même procès-verbal doit être remise à la personne retenue, dans l'hypothèse où la vérification d'identité n'est suivie d'aucune procédure d'enquête ou d'exécution adressée à l'autorité judiciaire.

En l'espèce, si la procédure de vérification d'identité est largement douteuse dans sa mise en oeuvre (V. supra), elle l'est encore plus au regard de ses modalités d'exécution. Il ressort en effet des éléments de la procédure que certaines procédures diligentées ne comportaient ni nom, ni signature d'officier de police judiciaire. En outre, aucune copie des procès-verbaux de vérification d'identité n'a été remise aux intéressés. S'ils sont édifiants en soi, tous ces manquements aux règles élémentaires de la procédure sont aggravés par le fait qu'il ne s'agit pas de dérives individuelles mais de pratiques collectives dont la persistance induit sans doute une certaine complaisance des autorités hiérarchiques. Dans ces conditions, relever un manquement au devoir de rigueur tout en recommandant qu'un rappel des dispositions du Code de procédure pénale soit effectué à l'égard des fonctionnaires de police paraît le moindre des avertissements !

Droit de l'espace numérique

Par le G[al] d'armée (2S) Marc Watin-Augouard

JURISPRUDENCE JUDICIAIRE

Tribunal de grande instance de Paris, ordonnance de référé du 12 mai 2017, Madame X. / Google France et Google Inc.

Atteinte au droit à l'image - Maintien dans un traitement de données non pertinentes - Déréférencement.

Une personne physique peut demander à un moteur de recherche de déréférencer des liens vers des pages web qui contiennent des photographies publiées sans son autorisation.

Un ancien mannequin, connu sous le nom de « Mme X. », constate que des photographies sont publiées sans son autorisation sur plusieurs sites indexés par Google. Cette personne assigne Google France devant le TGI de Paris afin d'obtenir le déréférencement des sites concernés pour violation de l'article 38 de la loi 78-17 du 06 janvier 1978, de la directive 95/46/CE du 24 octobre 1995 et de l'article 9 du Code civil, selon lequel chacun a droit au respect de sa vie privée.

L'article 38 dispose que toute personne physique a le droit de s'opposer pour des motifs légitimes à ce que des données à caractère personnel la concernant fasse l'objet d'un traitement. Elle peut également, selon l'article 40 de cette loi, « *exiger du responsable du traitement que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou effacées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite* ».

Le droit à la vie privée et la protection des données à caractère personnel n'ont pas un caractère absolu. Doit aussi être protégée la liberté d'expression et d'information. Le juge apprécie donc *in concreto*.

Google France n'étant qu'une filiale commerciale de Google Inc., l'action à son encontre est irrecevable. Mais Google Inc. intervient volontairement en demandant à la justice de préciser très exactement

les adresses concernées, la demande initiale portant sur la suppression de 49 liens.
Pour le juge des référés, la plaignante justifie l'intérêt légitime de sa démarche en avançant que les clichés, susceptibles de recevoir une connotation érotique, ont été publiés sans son autorisation et alors même qu'elle n'exerce plus la profession de mannequin. Qu'ainsi les données ne sont plus pertinentes. Or l'article 6 c) de la directive 95/46/CE, transposée dans la loi du 06 janvier 1978 en droit français, précise par ailleurs que les données à caractère personnel doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement. La violation du droit à l'image est de nature à retirer toute pertinence au maintien des données (photographies). En conséquence, Google Inc. doit supprimer le référencement de cinq URL concernées. Le déréférencement ne supprime pas les contenus mais empêche d'y accéder.

JURISPRUDENCE ADMINISTRATIVE

Conseil d'État, section du contentieux – Formation spécialisée, M. A…B…, 5 mai 2017

Fichier des services de renseignement - Formation spécialisée du Conseil d'État - Premier arrêt ordonnant la suppression de données.

Les faits à l'origine de la saisine du Conseil d'État

En janvier 2016, M. B... demande au tribunal administratif de Paris d'annuler pour excès de pouvoir les décisions, révélées par le courrier de la présidente de la Commission Nationale de l'Informatique et des Libertés (CNIL) du 24 novembre 2015, par lesquelles les ministres de la Défense et de l'Intérieur lui ont refusé l'accès aux données susceptibles de le concerner et figurant dans les traitements automatisés de

données de la Direction de la Protection et de la Sécurité de la Défense (DPSD), devenue Direction du Renseignement et de la Sécurité de la Défense (DRSD), et du service du renseignement territorial.
M.B… demande également subsidiairement de procéder à la rectification des informations erronées le concernant susceptibles de figurer dans ces traitements. Il estime, en effet, qu'il a été écarté d'une procédure de recrutement à la suite d'une enquête administrative et qu'il a perdu son emploi. Si la rectification du fichier des traitements d'antécédents judiciaires (TAJ) a bien été opérée, suite à un classement sans suite le concernant, il pense que des éléments erronés se rapportant aux faits demeurent dans les fichiers de « sécurité publique ».

Une procédure dérogatoire

Dans le cas d'espèce, la procédure permettant de mettre en œuvre le droit d'accès aux données contenues dans un fichier et, le cas échéant, le droit de rectification, relève de règles particulières : l'article 41 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés déroge aux articles 39 et 40, lorsqu'un traitement intéresse la sûreté de l'État, la défense ou la sécurité publique. La CNIL, saisie d'une telle demande, désigne l'un de ses membres appartenant ou ayant appartenu au Conseil d'État, à la Cour de cassation ou à la Cour des comptes pour mener les investigations utiles et faire procéder aux modifications nécessaires. L'article 88 du décret n°2005-1309 du 20 octobre 2005, pris en application de la loi précitée, fixe les modalités particulières de réponse à l'intéressé, dès lors que des informations ne concernent pas le domaine de l'article 41.

Le tribunal administratif de Paris, saisi par M. B…, transmet le recours au Conseil d'État. En effet, l'article L. 841-2 du Code de la sécurité intérieure attribue à une formation spécialisée de cette juridiction, dont les membres sont habilités au secret de la défense nationale, l'examen des recours relatifs à la mise en œuvre des techniques de renseignement et des fichiers intéressant la sûreté de l'État. Cette procédure,

issue de loi du 24 juillet 2015 relative au renseignement, a pour objectif d'assurer un juste équilibre entre les exigences du secret et les garanties apportées aux citoyens. Comme le souligne le Conseil d'État[1], « *la dérogation apportée au caractère contradictoire de la procédure juridictionnelle, qui a pour seul objet de porter à la connaissance des juges des éléments couverts par le secret de la défense nationale et qui ne peuvent, dès lors, être communiqués au requérant, permet à la formation spécialisée de statuer en toute connaissance de cause. Les pouvoirs dont elle est investie pour instruire les requêtes, relever d'office toutes les illégalités qu'elle constate et enjoindre à l'administration de prendre toutes mesures utiles afin de remédier aux illégalités constatées, garantissent l'effectivité du contrôle juridictionnel de l'exercice du droit d'accès indirect aux données personnelles figurant dans des traitements intéressant la sûreté de l'État* ». La Haute assemblée considère que cette procédure dérogatoire ne porte pas une atteinte excessive au caractère contradictoire de la procédure, ni ne méconnaît le droit au recours effectif, protégés respectivement par les articles 6 et 13 de la Convention européenne des droits de l'Homme.

Des données du fichier de la DRSD à effacer

La liste des fichiers, susceptibles de faire l'objet d'un contrôle par la formation spécialisée, figure à l'article R. 841-2 du Code de la sécurité intérieure. Entre ainsi dans ses attributions le contrôle du traitement automatisé de données à caractère personnel dénommé SIREX, mis en œuvre par la DRSD. Le fichier du renseignement territorial, en revanche, n'est pas visé par cet article. Le contentieux devrait donc, pour ce qui le concerne, relever du TA de Paris mais, en vertu des dispositions de l'article R. 351-4 du Code de justice administrative, le Conseil d'État est compétent pour constater qu'il n'y a pas lieu de statuer sur les conclusions relatives au fichier du renseignement

1. CE, formation spécialisée, M.B.A.C/ Ministre de la Défense et ministre de l'Intérieur, 8 février 2017.

territorial, puisqu'il ne contient aucune information concernant M. B…

Le fichier de la DRSD, quant à lui, entre dans le champ de l'article L. 773-8 du Code de justice administrative, issu de la loi du 24 juillet 2015. La formation spécialisée du Conseil d'État se réunit à huis clos pour examiner les éléments contenus dans le traitement, sans les révéler, ni révéler si le requérant figure ou non dans le traitement. Mais, dans le cas d'espèce, l'examen ayant mis en évidence que des données concernant M. B…figurent illégalement dans ce fichier, l'arrêt du Conseil d'État du 5 mai 2017 ordonne au ministère de la Défense de procéder à leur effacement. Le requérant n'est informé que du résultat, sans que des éléments protégés par le secret de la défense nationale ne lui soient divulgués.

Cet arrêt est le premier prononcé par cette nouvelle formation spécialisée qui constate l'illégalité de données contenues dans un fichier tenu par un service de renseignement.

ACTUALITÉ DU NUMÉRIQUE

DÉFENSE

Décret et arrêté du 4 mai 2017 modifiant l'organisation de l'état-major des armées

Le décret n°2017-743 du 4 mai 2017 et l'arrêté du même jour officialisent la création d'un commandement cyberdéfense au sein du ministère des Armées (état-major des armées).
L'article D3121-24-2 ajoute un officier général « commandant de la cyberdéfense » à l'organigramme de l'État-Major des Armées (EMA). Il marque ainsi l'évolution de la fonction dédiée à « l'officier général cyberdéfense », exercée depuis l'origine par le vice-amiral Coustillière. Cette création est une première étape de la montée en puissance d'une « quatrième armée », avec 2600 « cybercombattants » prévus à

l'horizon 2020.
Le commandant de la cyberdéfense exerce les missions fixées par l'article D3121-14-1 du Code de la défense. Il est ainsi chargé pour le CEMA de la conduite de la défense des systèmes d'information du ministère de la Défense (à l'exception des services de renseignement), en coordination avec l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). Il est chargé de la mise en œuvre des mesures de cyberdéfense « offensive », légalisées depuis la loi de programmation militaire du 18 décembre 2013 par l'article L2321-2 du Code de la défense. Cet article dispose que « pour répondre à une attaque informatique qui vise les systèmes affectant le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation, les services de l'Etat peuvent, dans les conditions fixées par le Premier ministre, procéder aux opérations techniques nécessaires à la caractérisation de l'attaque et à la neutralisation de ses effets en accédant aux systèmes d'information qui sont à l'origine de l'attaque ».
L'arrêté du 20 mars 2015 portant organisation de l'état-major des armées et fixant la liste des commandements, services et organismes relevant du chef d'état-major des armées ou de l'état-major des armées est modifié en conséquence :
L'officier général « commandant de la cyberdéfense » (Art. 19-1. - I.) :

- Est responsable :

- de la protection des systèmes d'information placés sous la responsabilité du chef d'état-major des armées en sa qualité d'autorité qualifiée pour la sécurité des systèmes d'information, dans les conditions définies par l'arrêté du 30 novembre 2011 susvisé ;
- de la conduite de la défense des systèmes d'information du ministère de la Défense à l'exclusion de ceux de la direction générale de la sécurité extérieure et de la direction du renseignement et de la sécurité de la défense, dans les conditions prévues à l'article D.3121-14-1 du Code de la défense ;
- de la conception, de la planification et de la conduite des opérations militaires de cyberdéfense, sous l'autorité du sous-chef d'état-major « opérations » ;

- Contribue à l'élaboration de la politique des ressources humaines de cyberdéfense (militaires en activité, réserve opérationnelle et citoyenne de cyberdéfense) ;

- Coordonne :

- la contribution des armées et organismes interarmées à la politique nationale et internationale de cyberdéfense, notamment pour l'élaboration et la mise en œuvre des plans de coopération ;
- la définition des besoins techniques spécifiques de cyberdéfense ;

- Assure la cohérence du modèle de cyberdéfense du ministère et sa coordination générale ;

- Développe et anime la réserve de la cyberdéfense.

Pour l'exercice de ses attributions, l'officier général « commandant de la cyberdéfense » commande l'état-major de la cyberdéfense. Cet état-major comprend :

- un échelon de commandement ;
- un pôle « opérations », qui comprend le centre opérationnel de la cyberdéfense ;
- un pôle « innovation et ressources » ;
- un pôle « développement et stratégie ».

Cet état-major est chargé :

- d'assister le chef du centre de planification et de conduite des opérations en matière de cyberdéfense ;
- de planifier et conduire les opérations militaires de cyberdéfense ;
- de s'assurer de l'adoption des mesures de protection et de défense des systèmes d'information placés sous la responsabilité du chef d'état-major des armées ;
- de contribuer à la préparation de l'avenir du domaine de la

cyberdéfense ;
- de participer à l'élaboration des positions du ministère de la Défense auprès des instances internationales et des organismes nationaux ne dépendant pas du ministre de la Défense.

Le commandant de la cyberdéfense dispose du centre des réserves et de la préparation opérationnelle de cyberdéfense, organisme interarmées.
Il s'appuie sur des unités spécialisées en cyberdéfense appartenant aux armées et aux organismes interarmées, sur lesquelles il exerce une autorité fonctionnelle.

UNION EUROPÉENNE

Vers une réglementation sur la localisation des données ?

La Commission européenne a annoncé, lors de l'évaluation du marché unique numérique, la rédaction prochaine d'un texte sur la libre circulation des données qui n'ont pas un caractère personnel. Le document, dont on ignore aujourd'hui la nature (directive ou règlement ?), devrait être présenté à l'automne 2017. Ce texte portera notamment sur la disponibilité des données, sur leur portabilité et sur leur localisation. Cette question revient régulièrement dans les débats relatifs à la souveraineté « du numérique » ou à la souveraineté à « l'ère du numérique ». Certains prétendent qu'il n'y a pas de souveraineté sans stockage des données dans des *data centers* implantés sur le territoire national, d'autres élargissent cet impératif au territoire de l'Europe (tel était l'objet d'un amendement déposé au Sénat lors de l'examen de la loi pour une République numérique), d'autres, enfin, considèrent que l'important n'est pas le lieu de stockage mais la sécurité que le prestataire du *cloud computing* offre aux données qui lui sont confiées. Cette question était au cœur des débats du *Cloud Independence Day* où le CREOGN est intervenu, le 6 juin 2017.
La libre circulation des données se heurte aujourd'hui à des différences de réglementation selon les pays européens. Par exemple, en France, le

Code du patrimoine impose aux collectivités territoriales de stocker leurs données sur le territoire national. En Allemagne ou au Luxembourg, ce sont les données financières ou fiscales qui font l'objet d'un traitement particulier. Les promoteurs du texte souhaitent qu'à l'exception des données relatives à la sécurité nationale, les données puissent être indistinctement hébergées dans des *data centers* européens, selon des normes de sécurité communes.

Droit de l'espace numérique

Par M. Xavier Leonetti

Le juge du cyber et le cyberjuge

Internet fait désormais partie de nos vies. Tous les jours, à chaque instant, nous sollicitons cet assistant multifonctions afin de répondre aux questions les plus diverses ou dans le but de gérer nos tâches quotidiennes (rendez-vous, démarches administratives, réservations de sorties …). La vie sans le numérique ne paraît donc plus possible. Mais à quel prix ? Il semble que la vague du progrès numérique nous submerge, entraînant notre abandon à ces nouveaux dieux du quotidien.

Dans ce contexte, jamais, sans doute, le prédateur n'a été aussi près de sa victime, puisque au moyen des smartphones et des objets connectés il est partout et constamment avec elle, et peut-être demain en elle, avec le recours à des organes ou prothèses connectés.
Jamais aussi le délinquant n'a été aussi loin de son juge, ne serait-ce qu'en raison des frontières juridiques et de la lenteur de la coopération judiciaire comparée à la vitesse des transactions sur la Toile.

Par conséquent, l'office du juge doit intégrer le cyberespace, à la fois comme la matière de son action, mais également comme un outil de travail et d'accompagnement dans sa prise de décision.

Cybercrime et « nouvelles » infractions ?

En matière de cybercriminalité, il existe trois grandes catégories d'infractions cybercriminelles observées :

- La première est relative aux infractions liées aux Systèmes d'information et de Traitement Automatisé des Données (STAD). Il s'agit par exemple, d'intrusions sur un serveur informatique, ou de piratage de données ;

Droit de l'espace numérique

- La seconde catégorie regroupe les infractions liées aux formes de criminalité « traditionnelles » qui utilisent Internet et les nouvelles technologies de l'information et de la communication (NTIC) comme étant de nouveaux modes opératoires. Ainsi, un véhicule volé qui était précédemment revendu via les annonces gratuites de la presse est aujourd'hui vendu par l'intermédiaire de sites Internet spécialisés dans la vente de particuliers à particuliers ;

- La troisième catégorie présente les infractions commises par Internet relatives à la dignité ou à la personnalité et les atteintes sexuelles commises par ce même biais. Ces infractions traditionnelles connaissent aussi une nouvelle vie sur le Web, au moyen notamment de l'anonymat offert par Internet.

En premier lieu, il convient de souligner que l'étude des formes de cybercriminalité se révèle parcellaire, car elle dépend de la performance des outils de comptage utilisés par l'administration. Or, en la matière les différents services de l'État utilisent chacun des grilles d'analyse et de comptage différentes. Il s'agit d'un véritable « château kafkaïen ».
Par exemple, s'agissant de l'utilisation du logiciel « Cassiopée », l'application est déjà interconnectée avec celle de la gendarmerie et bientôt avec celle de la police. Cependant, les critères de « Cassiopée » ne sont pas identiques à ceux utilisés par la police et la gendarmerie. Si bien qu'il n'existe pas de continuité statistique entre les ministères de l'Intérieur et de la Justice. C'est d'ailleurs ce que relevait le Premier ministre, en octobre 2014, à l'occasion du séminaire de rentrée des auditeurs de l'Institut National des Hautes Études de la Sécurité et de la Justice (INHESJ) et de l'Institut des Hautes Études de la Défense Nationale (IHEDN) : « *Les systèmes d'information des forces de sécurité d'une part, et de la justice d'autre part, sont structurellement incapables de communiquer* ».
De surcroît, il convient de ne pas oublier qu'une partie des faits statistiques sont traités en dehors du système pénal. Par exemple, le Groupement d'Intérêt Économique (GIE) des cartes bancaires peut être amené à traiter de phénomènes cybercriminels dans le cadre de

solutions de conflits à l'amiable.
Enfin, le « chiffre noir » de la cybercriminalité est l'un des plus élevés, souvent parce que les personnes physiques ou morales visées ignorent les faits. En effet, une entreprise met en moyenne 229 jours pour découvrir la menace dont elle fait l'objet.

Ensuite, l'étude statistique permet de relever que plus de 90 % des 70 000 cyberinfractions recensées en 2015 par l'Observatoire National de la Délinquance et des Réponses Pénales (ONDRP) sont des escroqueries et des attaques financières. C'est-à-dire qu'à l'image de l'économie réelle qui repose sur la confiance, l'économie souterraine se nourrit de la confiance que l'escroc crée au préjudice de sa victime. La particularité de l'espace cyber est que les internautes font preuve d'une crédulité excessive.
En effet, il apparaît que dans l'espace virtuel les individus font preuve d'une négligence plus importante que dans le monde réel. Ainsi, imagine-t-on des personnes distribuer sur la voie publique des prospectus décrivant leurs habitudes illustrés par des photos de leur vie intime ? Non, pourtant, des millions d'internautes le font chaque jour sur Facebook. De même, si une personne vêtue d'un uniforme « Orange » ou « SFR » abordait les passants en leur demandant leur numéro de carte bleue, obtiendrait-elle satisfaction ? Sans doute pas. Malheureusement, sur Internet, cette pratique (dite de « phishing ») fait plusieurs milliers de victimes tous les mois.
De sorte que ces cyberinfractions ne constituent que la mutation numérique d'infractions traditionnelles d'escroqueries ou d'abus de confiance.

De même, l'ère du numérique accentue les menaces qui pèsent sur l'État et sur son fonctionnement démocratique, au travers notamment des possibilités de piratages ou d'intrusions. Par exemple, ces derniers mois, les États-Unis ont été confrontés à des suspicions de piratages informatiques à l'encontre de la campagne électorale présidentielle. Cette situation unique dans l'histoire politique américaine nous enseigne que les acteurs de la vie publique et politique doivent très tôt acquérir des réflexes d'hygiène et de sécurité numérique. À défaut, les informations qu'ils détiennent se trouvent susceptibles d'être interceptées ou modifiées par des tiers ou des puissances étrangères.

On peut ainsi imaginer en France le piratage des listes électorales détenues sur les serveurs informatiques des mairies. Il s'agirait alors moins de compromettre que de désorganiser un scrutin permettant alors de créer un doute sur la sincérité des élections. Dans un contexte de défiance vis-à- vis des autorités publiques et politiques, ce risque est réel, d'autant que les scrutins sont de plus en plus nombreux (dernièrement à Notre-Dame des Landes par exemple). C'est pourquoi une démarche particulière de prévention à destination des partis politiques a été initiée à l'automne 2015 par l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI).

La riposte judiciaire aux cybercrimes

L'arsenal pénal permettant de réprimer les comportements délinquants s'est particulièrement étoffé, notamment depuis l'adoption de la LOPPSI2 du 14 mars 2011.
Ainsi, les atteintes aux systèmes automatisés de données (art 323-1 à 323-7 du CP) permettent de réprimer les nouveaux types d'infractions. Ainsi de l'accès ou du maintien frauduleux dans un système de traitement automatisé de données (C. pén., art. 323-1, al. 1er) permettant de réprimer le phishing qui consiste à soutirer des informations personnelles à des internautes en leur envoyant un courriel usurpant l'identité d'une banque ou d'un site marchand. (TGI Paris, 2 sept. 2004). De même, s'agissant de la participation à un groupement de pirates (art. 323-4) : ainsi, lorsque des participants n'ignoraient pas que les informations échangées avaient pour finalité de commettre des atteintes au système informatique d'accès à Canal plus, leur participation à l'entente est pénalement répréhensible (T. corr. Carpentras, 25 juin 2004).

En matière de traitement de données à caractère personnel, l'article 226-16 du Code pénal permet de sanctionner la mise en ligne du nom d'une personne au sein du contenu rédactionnel d'un site web qui est un traitement automatisé de données nominatives au sens de l'article 5 de la loi de 1978, et qui nécessite la déclaration à la CNIL du site web

concerné.

S'agissant de la procédure pénale, le Code de procédure pénale ne fait référence qu'indirectement à la notion de cybercriminalité. S'agissant par exemple du mandat d'arrêt européen, par dérogation, l'article 695-23 du CPP en prévoit l'exécution sans contrôle de la double incrimination des faits reprochés lorsque les agissements considérés entrent notamment dans la catégorie de la « cybercriminalité », de la « contrefaçon » ou de la « falsification des moyens de paiement ».

Depuis 2013 également, des travaux ont été engagés par le ministère de l'Intérieur visant à renforcer et mieux coordonner les moyens d'action en matière de prévention et de lutte contre la cybercriminalité.
Ainsi, il convient de souligner que la police et la gendarmerie nationales disposent de cyberenquêteurs dont la spécialité croît selon le niveau d'infraction. Par exemple, la police nationale s'est récemment dotée d'une sous-direction de lutte contre la cybercriminalité. De même, au sein du Pôle Judiciaire de la Gendarmerie Nationale (PJGN), la Division de Lutte Contre la Cybercriminalité (DLCC) dispose de compétences uniques en matière de cybercrime destinées à appuyer les unités locales. Par ailleurs, l'action de la gendarmerie se trouve renforcée de l'apport du réseau de la réserve citoyenne cyberdéfense placée sous l'autorité du ministère de la Défense. À leurs côtés, la Direction Générale de la Sécurité Intérieure (DGSI) dispose de compétences spécifiques, notamment s'agissant de cyberradicalisation ou de lutte contre le cyberespionnage.
Rappelons, d'ailleurs, que les articles 706-102-1 à 706-102-6 du CPP créent une nouvelle catégorie de technique d'enquête, relative aux captations des données informatiques. Il s'agit d'un dispositif ayant pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, les conserver et les transmettre. En outre, s'agissant de la consultation des données personnelles à distance par des enquêteurs, la Cour de cassation, dans un arrêt du 6 novembre 2013, a retenu qu'il s'agit d'une *«simple mesure d'investigation et non d'une perquisition distincte exigeant une nouvelle décision [d'un] magistrat».*

Au sein du ministère de la Défense, le Centre d'Analyse et de Lutte Informatique Défensive (CALID) opère une veille et une analyse des nouvelles cybermenaces et assure également la cyberprotection des opérations extérieures de la France.
Enfin, du point de vue interministériel, l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI), créée en 2009, édicte les règles de sécurité des systèmes d'information de l'État et joue le rôle de gardien des « opérateurs d'importance vitale ».

Au niveau européen, plusieurs organisations ont en charge des missions de cybersécurité. En particulier, le Centre de criminalité en haute technologie d'EUROPOL qui a pour mission de mener des actions de coordination, de soutien opérationnel, d'analyse stratégique et de formation. De même, le Centre européen de lutte contre la cybercriminalité (EC3) centralise l'expertise et l'information, soutient les enquêtes criminelles et promeut les solutions à l'échelle de l'Union européenne, se concentrant sur les activités illicites en ligne menées par des organisations criminelles.
À noter que, le 2 avril 2014, une opération coordonnée par INTERPOL a permis d'interpeller 58 personnes impliquées dans un réseau criminel responsable d'affaires de « sextorsion ». Cette affaire fait suite au suicide de Daniel Perryd, un adolescent écossais victime d'une tentative de chantage sur Internet.

L'office du juge à l'heure du cyberespace

En premier lieu, l'espace cyber opère de perpétuelles mutations des champs infractionnels. Citons, notamment, l'apparition des monnaies virtuelles. Ces dernières sont des moyens de transaction permettant d'effectuer des paiements en ligne. Ainsi, contrairement à une devise officielle, une monnaie virtuelle n'est pas l'incarnation de l'autorité de l'État ou d'une banque centrale. C'est pourquoi, au cours du mois de juillet 2014, une plate-forme de bitcoins a été démantelée en Midi-Pyrénées dans le cadre d'une enquête diligentée par la division

économique et financière de la gendarmerie nationale. Plus de 200 000 euros de bitcoins ont été saisis à la suite de mouvements suspects constatés sur les réseaux numériques.

Ensuite, le monde virtuel révolutionne l'office du juge en ce qu'il conduit à revoir la nature même des modes d'enquêtes, de poursuites et de procès. En particulier, les réseaux sociaux sont parfois considérés comme étant de véritables adjoints de sécurité. Ainsi, sur la Toile, plusieurs plate-formes de signalement des comportements suspects voire infractionnels se sont développés. On se souvient à cet égard de l'affaire du lanceur du chat survenue en 2014, au cours de laquelle un adolescent s'était filmé en train de maltraiter l'animal. Ce dossier a permis d'illustrer la complémentarité possible entre les internautes et les services de police. Pour autant, il convient de rappeler que dans plus de 90 % des cas, les traques conduites par des internautes justiciers se soldent par un échec et le Web ne doit pas devenir un « Far-West » où chacun règle ses comptes et tente de faire la loi.
Par exemple, certains groupes de militants, tels que les « Anonymous » (dont n'importe qui peut se prévaloir), se mêlent de nombreuses causes sous prétexte de lutter contre les injustices. Mais, souvent, ils peuvent se tromper de cible et lyncher la mauvaise personne. Ainsi, dans le Missouri (États-Unis), à la suite de la mort de Michael Brown lors d'une intervention policière, Anonymous a publié sur Twitter l'identité du policier que le groupe pensait être à l'origine de l'homicide du jeune homme. Mais Anonymous s'est trompé d'identité, dévoilant le nom d'un policier nullement concerné.

Enfin, une autre question se pose au regard de la mise en ligne et en accès libre et gratuit de toutes les décisions de justice. Bertrand Louvel, premier président de la Cour de cassation indiquait, lors de sa rentrée vendredi 13 janvier, *« la mise en ligne nécessaire, commandée par les progrès de notre temps, de l'ensemble des décisions de l'ordre judiciaire* (…) *ouvre sur des horizons insoupçonnés »*. Cette réforme issue de la loi Lemaire du 7 octobre 2016 permettra l'analyse de la jurisprudence par des algorithmes et donc mettra en évidence dans certains cas les écarts entre les décisions rendues par deux chambres d'un même tribunal.

En outre, l'analyse de la jurisprudence constitue un pas de plus vers la création d'une justice prédictive. Comme le souligne Chantal Arens, première présidente de la Cour d'appel, le big data en matière de justice *« peut conduire à une justice prédictive allant de l'identification des références de décisions à des profils de juges ayant rendu tel ou tel type de décision »*. Selon elle, « *l'acte de juger devient instable* ». La prédiction judiciaire fait donc peser un risque sur l'office du juge en ce qu'il pourrait conduire, si ce n'est à sa disparition pure et simple, tout au moins à la raréfaction des affaires qui lui sont soumises, réduisant celles-ci aux seuls cas non répertoriés dans la jurisprudence numérique. Recueillant, exploitant et analysant l'ensemble des décisions de justice, sachant qu'à elle seule la Cour de cassation dispose d'une base de données de 1,5 million d'arrêts, une intelligence artificielle pourrait bien rendre des décisions de manière autonome. À l'image du logiciel médical « Watson » qui propose des diagnostics sur la base de l'analyse de centaines de critères, l'analyse d'un dossier judiciaire pourrait également s'effectuer par simple consultation d'un algorithme. Aux États-Unis, la police utilise déjà ce type de logiciel afin de prédire les infractions en fonction de milliers de paramètres statistiques (géographie, météo, données sociales, consultations Google, publications sur les réseaux sociaux, …).
Bien évidemment, comme tous les outils numériques d'accès ouvert, ces logiciels et bases de données sont exposés aux intrusions malveillantes dont on imagine les effets dévastateurs. Les protections à mettre en œuvre doivent être à la hauteur de l'enjeu.

Ainsi, comme le souligne Myriam Quéméner, magistrate et conseiller juridique auprès du préfet en charge de la cybersécurité : *« lutter efficacement contre la cybercriminalité est un enjeu majeur pour les années à venir. Cette démarche est indissociable de l'amélioration de la connaissance des nouveaux vecteurs d'information tels qu'Internet et les réseaux numériques ».*

Déjà, l'organisation judiciaire entend s'adapter à ces nouvelles menaces et les anticiper. Ainsi, en septembre 2014, les services du Parquet de Paris ont été réorganisés afin d'être plus efficaces dans le traitement des dossiers financiers, de cybercriminalité et de santé

publique. Désormais, le Parquet financier de Paris comporte un pôle cybercriminalité (« section F1 ») au sein de la division économique, financière et commerciale. Le Parquet de Paris demeure cependant le seul à disposer d'une section spécialisée dans la lutte contre « la délinquance astucieuse et la cybercriminalité ». Cette section traite plus particulièrement des dossiers d'atteintes aux systèmes de traitement automatisé de données commises à l'encontre des services de l'État et des entreprises situées à Paris.

Les juridictions interrégionales spécialisées (JIRS) ont à connaître de nombreux cas de cybercriminalité, de même que plusieurs Cours d'appel qui ont désigné au sein de leurs effectifs des magistrats référents pour les questions de cyberterrorisme.
Enfin, la loi du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure a reconnu à tout juge d'instruction la possibilité de décider de la captation à distance des données informatiques, dans le cadre des dispositions spécifiques relatives à la criminalité et à la délinquance organisée.

L'enjeu est donc de maintenir le processus de spécialisation judiciaire amorcé avec la création d'un pôle spécialisé au sein du parquet de Paris. Comme nous l'avons vu, les cybermenaces sont multiples, complexes et diffuses et recommandent de ce fait la création de structures adaptées et spécialisées.
De surcroît, nous faisons face à une délinquance de masse, où les infractions sont ventilées « façon puzzle » sur l'ensemble du territoire. Par conséquent, le regroupement des infractions (au niveau des JIRS par exemple) doit permettre d'étoffer un dossier permettant par la suite de rendre plus légitime le recours à une coopération internationale.

Xavier Leonetti est chercheur associé au CREOGN et Substitut du procureur au Parquet général d'Aix-en-Provence.

CENTRE DE RECHERCHE DE L'ECOLE DES OFFICIERS DE LA GENDARMERIE NATIONALE

Par M. Gilles Hilary

WannaCry et la diffusion des « zero day exploits »

Que s'est-il passé?

Le vendredi 12 mai 2017, WannaCry a commencé à affecter les ordinateurs dans le monde entier. L'épidémie a commencé en Asie au début de la matinée et s'est répandue dans la journée. Plus de 200 000 ordinateurs auraient été infectés[1]. À titre d'exemple, seize hôpitaux britanniques n'ont pas pu accéder à leurs systèmes. Des entreprises comme Renault, Deutsche Bahn et Telephonica ont également été touchées. Le 14 mai, les effets de WannaCry se faisaient sentir sur tous les continents.

L'origine de l'incident peut être attribuée à la National Security Agency (NSA). L'agence américaine chargée du renseignement via l'analyse des signaux électroniques a développé un outil, appelé EternalBlue, pour exploiter une vulnérabilité dans les anciennes versions du système d'exploitation de Microsoft. Ces versions ne bénéficient plus du support technique de l'entreprise américaine mais sont encore couramment utilisées. Par exemple, Windows XP, commercialisé en 2001, fonctionne toujours sur plus de 5 % des ordinateurs Windows. EternalBlue permet aux machines de recevoir des fichiers sur des ports réseaux censés être bloqués. Ce logiciel peut désactiver les machines, collecter du renseignement et atteindre d'autres objectifs en exploitant des vulnérabilités non connues des éditeurs de logiciel (ces vulnérabilités sont connues sous le nom de «« zero day exploits »).

Naturellement, les outils tels que EternalBlue devaient rester confidentiels mais la NSA a connu plusieurs fuites au cours de ces dernières années. Par exemple, le Federal Bureau of Investigation (FBI) a arrêté

1. Cependant, l'estimation semble avoir été faite en examinant le nombre de machines qui ont accédé à une URL liée à WannaCry, ce qui a pu conduire à une exagération significative du nombre de machines réellement infectées.

Droit de l'espace numérique

Harold Martin en 2016. Cet employé de Booz Allen Hamilton, un sous-traitant pour la NSA, a été mis en examen pour la détention illégale dans son garage de téraoctets de données et de codes informatiques confidentiels. En avril 2017, les Shadow Brokers, un groupe ayant des liens supposés avec les services de renseignement russes, ont mis les outils de la NSA en ligne. Dès lors, toute personne possédant un minimum d'expertise technique pouvait les utiliser pour ses propres besoins. En réponse, Microsoft a développé un patch de sécurité pour combler la faille mais celui-ci n'a pas toujours été déployé par les utilisateurs. Par exemple, certains logiciels obtenus illégalement ne peuvent pas le télécharger.

D'autres logiciels tels que Wannacry et Adylbuzz ont ensuite été développés pour profiter d'EternalBlue. WannaCry est un rançongiciel (« ransomware »), un type de logiciel malveillant qui bloque l'accès aux données de la victime jusqu'à ce qu'une rançon soit payée. Le 12 mai 2017, lorsque WannaCry a commencé à affecter les ordinateurs en Asie tôt le matin, les victimes ont été invitées à payer 300 dollars en bitcoins dans les trois jours (le prix augmentant ensuite à 600 dollars). Le logiciel malveillant (« malware ») s'est ensuite répandu dans le monde entier. Cependant, un expert indépendant britannique a rapidement identifié une faille critique dans le programme : WannaCry essayait systématiquement d'accéder à une URL particulière (qui était directement codée dans le logiciel malveillant) et se désactivait s'il ne pouvait pas y accéder. Il est possible que cette procédure ait été conçue comme un dispositif de sécurité pour empêcher un examen du logiciel dans des environnements stériles (« sandboxes ») où l'accès à l'URL aurait été impossible. Dans le cas où le logiciel ne pouvait accéder à cette URL, il se désactivait pour empêcher l'examen du code. Lorsque l'analyste britannique a acheté l'URL (pour moins de 11 dollars), il a réussi à ralentir considérablement la propagation de WannaCry. Le 14 mars 2017, Microsoft a publié un patch de sécurité en urgence qui protégeait les utilisateurs de la version XP de son système d'exploitation. Le 15 mai, l'attaque était essentiellement contenue. Le 18 mai, trois chercheurs français identifièrent un moyen de décrypter les fichiers infectés par WannaCry dans certains cas.

Droit de l'espace numérique

En parallèle du développement de WannaCry, un logiciel distinct baptisé Adylkuzz exploitait aussi la vulnérabilité EternalBlue. Le but de ce deuxième logiciel malveillant était différent de celui de WannaCry. Les crypto-monnaies telles que Bitcoin ou Ether sont des actifs numériques créés par des communautés décentralisées grâce à la mise en œuvre d'algorithmes sur des ordinateurs individuels. Ce processus (appelé « extraction minière » ou « mining ») nécessite du temps informatique et de l'électricité et coûte donc cher. Adylkuzz s'est concentré sur l'extraction de Monero (une crypto-monnaie axée sur la protection de la vie privée) dont la capitalisation boursière augmente régulièrement depuis 2014. Cependant, Adylkuzz s'assurait que les bénéfices de l'extraction allaient aux pirates informatiques. Ironiquement, l'une des fonctionnalités d'Adylkuzz était de combler la faille exploitée par EternalBlue. En d'autres termes, Adylkuzz a complètement protégé les machines infectées de WannaCry.

Quelles ont été certaines des conséquences de WannaCry?

WannaCry a été la plus grande attaque de rançongiciel de l'histoire. Son effet a été global avec, selon les estimations, des ordinateurs infectés dans plus de 150 pays en seulement 72 heures. La Russie, l'Ukraine et plus généralement les pays de l'ancienne Union Soviétique ont été particulièrement touchés. Les ordinateurs des ministères de l'Intérieur de la Russie et de la Chine ont été infectés. Cependant, les autorités conseillèrent le public de ne pas payer la rançon et ce conseil a été largement suivi. Les comptes Bitcoin mis en place par les pirates informatiques ont reçu un peu plus de 100 000 dollars et ce montant n'a pas été transféré jusqu'à présent. Si la motivation était financière, WannaCry a été un échec.

Les autres coûts sont difficiles à estimer. Aucun effet sur les infrastructures critiques et aucun effet durable majeur n'ont été signalés. Par exemple, les hôpitaux britanniques ont récupéré des données sauvegardées et ont rapidement repris leurs opérations. Malgré l'ampleur de l'attaque, ses effets semblent être relativement peu importants pour

l'économie mondiale et même pour les pays les plus touchés.

En réaction à WannaCry et à l'exploitation des actifs de la NSA, les législateurs des États-Unis ont décidé d'examiner la politique concernant la divulgation des « zero day exploits ». La décision de publier une vulnérabilité identifiée par les services de renseignement américains est actuellement prise dans un cadre administratif, le Vulnerability Equities Process (VEP), qui suit une approche basée sur une analyse coût-avantage. Maintenir le secret autour des « zero day exploits » préserve un avantage certain pour les services de renseignement ou même pour les forces de l'ordre mais rend l'écosystème cyber plus vulnérable en préservant des failles de sécurité. Le 17 mai 2017, cinq jours seulement après l'émergence de WannaCry, les législateurs américains ont présenté un projet de loi, le Patch Act, pour formaliser le processus de décision et garantir l'examen des « exploits » par un conseil indépendant. Si elle est adoptée, la loi Patch créerait un cadre légal et non plus seulement administratif (et donc soumis au bon vouloir du pouvoir exécutif).

Qui était derrière WannaCry?

L'attribution de la responsabilité de WannaCry reste incertaine à ce stade et repose largement sur des preuves circonstancielles. WannaCry possède deux composantes, le vecteur d'infection des réseaux (la partie qui installe le logiciel malveillant dans les ordinateurs) et le crypto-verrouilleur (la partie qui crypte les fichiers). La première composante peut être attribuée directement à la fuite provenant de la NSA. Divers acteurs ont noté des similitudes dans la deuxième composante avec des codes informatiques qui ont été utilisés dans le passé par un groupe baptisé « Lazarus ». On a déjà attribué la responsabilité d'incidents cyber à ce groupe, probablement lié aux services de renseignement nord-coréens. Par exemple, Lazarus a été accusé d'exécuter différentes attaques par déni de service (DDoS) visant des organisations sud-coréennes dès 2009. Une attaque DDoS tente de rendre un service en ligne indisponible en le submergeant par du trafic

provenant de sources multiples comme des chapelets d'ordinateurs préalablement infectés. Le groupe a aussi été accusé en 2014 d'avoir organisé le piratage de Sony Pictures qui entraîna la fuite d'un grand volume d'informations confidentielles et de films inédits. En 2016, Lazarus a été accusé d'avoir orchestré des cyberattaques contre trois institutions financières. En particulier, une attaque sophistiquée et intégrée sur la banque centrale du Bangladesh a presque conduit au vol d'un milliard de dollars (les paiements ont été arrêtés après la disparition de 80 millions de dollars).

Ces épisodes ont mis en évidence un degré croissant de sophistication dans le codage, le renseignement et la technique financière. À l'opposé, WannaCry a été mal exécuté, avec de nombreuses erreurs de programmation qui ont ralenti sa progression et ont rendu difficiles les paiements en ligne. Cela a conduit certains commentateurs à suggérer que le but de l'attaque était d'embarrasser la NSA plutôt que de collecter de l'argent. Une autre possibilité est que des individus associés à Lazarus aient exécuté l'attaque sans le soutien de l'organisation. L'analyse linguistique suggère que les notes de rançon ont été écrites par des individus parlant une forme de chinois méridional (et non le coréen) ; Macao est souvent décrit comme une base d'opérations majeure pour les services nord-coréens.

Que pouvons-nous apprendre de WannaCry ?

Sur le plan technologique, WannaCry n'a pas introduit d'innovations dans le codage et la menace de rançongiciel était déjà connue. EternalBlue a déjà été utilisé comme vecteur de pénétration par d'autres logiciels malveillants mais ceux-ci avaient des objectifs plus ciblés. Cependant, nous pouvons faire deux observations.

Premièrement, les ordinateurs infectés exécutaient des versions anciennes de Windows qui ne bénéficient plus du support technique de Microsoft. Par exemple, les médias ont indiqué qu'une étude menée par la société de cybersécurité Citrix a révélé que 90 % des hôpitaux

britanniques du NHS utilisaient encore Windows XP en 2016. Il peut être tentant d'attribuer cette dépendance à une technologie obsolète à l'incompétence et à un financement inadéquat. Cependant, il est important de noter que de nombreux dispositifs médicaux utilisent des logiciels spécialisés qui ne peuvent pas migrer facilement vers des systèmes d'exploitation plus récents. Ce problème d'évolution va probablement croître avec le développement des objets connectés qui font partie de systèmes complexes. Beaucoup de ces périphériques ne seront pas conçus avec des fonctionnalités de sécurité robustes et perdront le support technique de leur fabricant après quelques années de service. L'identification rapide des composants défectueux du système et l'installation de correctifs de sécurité qui ne dégradent pas leur interopérabilité vont devenir de plus en plus critiques.

Deuxièmement, WannaCry a fait la une des médias internationaux avec des titres tels que « la catastrophe de rançongiciel de WannaCry expliquée » (un exemple pris sur le site du Washington Post). Les dommages réels ont été plus limités que ce que ces manchettes ne suggèrent. Les prix des actions des entreprises vendant des produits de cybersécurité sophistiqués ont augmenté de manière significative bien que les solutions techniques (par exemple, l'installation des correctifs de sécurité, les sauvegardes de données) fussent relativement faciles à mettre en œuvre. L'impact perçu de WannaCry a été probablement plus grand que son effet réel. Les problèmes de sécurité informatique sont souvent difficiles à expliquer et peuvent être source d'anxiété pour le grand public. Les entreprises qui vendent des solutions de cybersécurité exacerbent naturellement ceci avec des messages alarmistes. Cette anxiété peut être directement exploitée dans le futur par des adversaires. Les grands États ont la capacité d'infliger des dommages très significatifs sur les infrastructures critiques mais de telles attaques engendreraient probablement des ripostes toutes aussi dévastatrices. En revanche, il serait difficile pour des États démocratiques de répondre à une campagne cyber qui infligerait des dommages symboliques importants mais des dégâts physiques minimaux, en particulier si cette attaque se déroule sous une fausse signature. Les exemples incluent des attaques à grande échelle visant les médias (comme sur TV5, par exemple) ou sur des panneaux

électroniques dans des gares ou des aéroports couplés à des attaques limitées sur des objectifs importants (par exemple, en ciblant un petit nombre de systèmes de contrôle industriel dans les usines chimiques). Dans des scénarios comme celui-ci, l'impact des événements rares mais graves créerait l'impression de conséquences catastrophiques, tandis que les cas bénins mais à fort impact médiatique créeraient une caisse de résonance. Les auteurs de telles attaques pourraient estimer qu'elles resteraient sous le seuil d'escalade en dépit de leurs conséquences politiques importantes. Dans ce contexte, une communication efficace des autorités est cruciale pour prévenir les réactions irrationnelles du public et pour minimiser les conséquences psychologiques des attaques cyber.

Gilles Hilary est chercheur associé au CREOGN et Chaired Professor, Houston Term Professor, Georgetown University.

Par Mme Claudia Ghica-Lemarchand

L'ENQUÊTE EUROPÉENNE – ENTRÉE EN VIGUEUR 22 MAI 2017

Décret n° 2017-511 du 7 avril 2017 relatif à la décision d'enquête européenne en matière pénale
Ordonnance n° 2016-1636 du 1er décembre 2016 relative à la décision d'enquête européenne en matière pénale

L'ordonnance du 1er décembre 2016 et le décret du 7 avril 2017 transposent la décision d'enquête européenne qui constituera, en matière pénale, le socle commun de la coopération judiciaire au sein de l'Union européenne. Ces textes ont profondément modifié le Code de procédure pénale sur ce point et le nouveau dispositif est entré en vigueur le 22 mai 2017. L'ordonnance du 1er décembre 2016 a été éclipsée par une autre ordonnance adoptée le même jour, l'ordonnance n° 2016-1635 renforçant le dispositif français de lutte contre le blanchiment et le financement du terrorisme, les deux étant autorisées par l'article 118 de la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale. Transposant en droit français la directive 2014/41/UE du Parlement européen et du Conseil du 3 avril 2014 concernant la décision d'enquête européenne en matière pénale (date de transposition avant le 22 mai 2017), l'ordonnance introduit une nouvelle section dans le cadre des dispositions relatives à l'entraide entre la France et les autres États membres de l'Union européenne (article 694-14 et suivants) dans le Code de procédure pénale, dispositions précédant celles relatives aux équipes communes d'enquête, Eurojust, le gel de biens ou l'échange simplifié d'informations. Ainsi, elle parachève la coopération et la reconnaissance mutuelle en matière pénale pré-sententielle. Si le choix d'une transposition par ordonnance en matière pénale suscite des interrogations du point de vue de la méthode employée et de l'instrument utilisé, il convient de souligner la très grande fidélité à la directive des mesures françaises adoptées.

La décision d'enquête européenne est la règle de droit commun applicable aux demandes d'entraide entre les États membres de l'Union européenne, puisque l'article 694-15 prévoit qu'elle s'applique « sauf lorsqu'il en est disposé autrement par le présent code ». Elle constitue une forme aboutie de coopération internationale en matière d'investigation, constituant à ce titre le pendant de la procédure du mandat d'arrêt européen en matière de remise de personne. La décision d'enquête européenne est « une décision judiciaire émise par un État membre, appelé État d'émission, demandant à un autre État membre, appelé État d'exécution, (…) de réaliser dans un certain délai sur son territoire des investigations tendant à l'obtention d'éléments de preuve relatifs à une infraction pénale ou à la communication d'éléments de preuve déjà en sa possession ». Cela peut se traduire par des mesures d'investigation portant sur des éléments matériels (« avoir pour objet d'empêcher provisoirement sur le territoire de l'État d'exécution toute opération de destruction, de transformation, de déplacement, de transfert ou d'aliénation d'éléments susceptibles d'être utilisés comme preuve ») ou sur des personnes (« avoir aussi pour objet le transfèrement temporaire dans l'État d'émission d'une personne détenue dans l'État d'exécution, afin de permettre la réalisation dans l'État d'émission d'actes de procédure exigeant la présence de cette personne, ou le transfèrement temporaire dans l'État d'exécution d'une personne détenue dans l'État d'émission aux fins de participer sur ce territoire aux investigations demandées ») à visée probatoire. Selon le décret du 7 avril 2017, le magistrat doit préciser si les éléments matériels doivent lui être transférés ou conservés dans l'État d'exécution, sans préjudice d'une modification ultérieure de la demande initiale (article D 47-1-5, Code de procédure pénale). Si la demande d'enquête européenne implique le transfèrement ou le transit de la personne sur le territoire d'un État membre de l'Union européenne, la procédure est suivie par le directeur de l'administration pénitentiaire du ministère de la Justice, « en veillant à ce que l'état physique et mental de la personne concernée, ainsi que le niveau de sécurité requis, soient pris en compte » (articles D 47-1-6 s.). L'audition par visioconférence doit être aussi envisagée (article D 47-1-20).
Le champ d'application de cette demande de communication d'éléments est large car elle peut « porter sur la violation par une personne des obligations résultant d'une condamnation pénale, même si cette

violation ne constitue pas une infraction ». Néanmoins, la décision d'enquête européenne ne doit pas se substituer aux autres mécanismes de coopération européenne. Ainsi, l'article 694-18 prévoit expressément que ce mécanisme est exclu pour les équipes communes d'enquête, pour la procédure des articles 695-9-1 à 695-9-30 sur le gel de biens susceptibles de confiscation, sauf si cette dernière a une visée probatoire, pour une demande d'observation transfrontalière en application de l'article 40 de la convention d'application des accords de Schengen du 19 juin 1990. Mais le mécanisme est aussi implicitement exclu lorsqu'il empiète sur le champ d'application du mandat d'arrêt européen. Ainsi, l'article 694-15, dernier alinéa, prévoit que la décision d'enquête européenne ne peut aboutir au transfèrement d'une personne en cas de « violation des obligations résultant d'une condamnation pénale ». Le principe de la décision d'enquête européenne est celui de la reconnaissance mutuelle et de l'équivalence des conditions d'exécution. Ainsi, selon l'article 694-17, le mécanisme est reconnu sans « aucune formalité obligatoire » et son exécution est assimilée aux actes de droit interne puisqu'elle se fait « de la même manière et selon les mêmes modalités ». Une clause de sauvegarde est prévue par le texte qui admet un motif valable « de non-reconnaissance, de non-exécution ou de report de la décision » mais le soumet à une double condition – la prévision préalable par le législateur français dans le Code de procédure pénale et l'instauration de « formalités expressément demandées par l'autorité d'émission non contraires aux principes fondamentaux du droit de l'État d'exécution ».

L'ordonnance définit des dispositions générales applicables à toutes les demandes d'enquête européenne. La décision émane du procureur de la République, du juge d'instruction, de la chambre de l'instruction et de son président ainsi que des juridictions de jugement ou d'application des peines et de leurs présidents et elle est soumise aux règles de procédure de droit commun, notamment lorsqu'il y a une autorisation préalable du juge des libertés et de la détention. Le dispositif soumet la compétence à la qualité de membre de « l'autorité judiciaire », article 694-20, alinéa 3, ce qui est discutable du point de vue du droit européen mais, incontestablement, en réserve le monopole aux magistrats. La décision peut être prise d'office ou « sur demande de la

personne suspecte ou poursuivie, de la victime ou de la partie civile ». La décision d'enquête européenne s'inscrit dans le cadre de l'enquête européenne participative et proactive qui permet au magistrat de se transporter sur le territoire d'un autre État et émettre sur place cette décision. Le magistrat peut donc agir en dehors de son ressort territorial et dans un cadre international, ce qui donne un cadre très actif à cette forme de coopération, s'éloignant de la forme classique de la commission rogatoire internationale. Le Code de procédure pénale fixe les formalités obligatoires des décisions d'enquête européenne qui figurent sur un formulaire comportant l'identité et la qualité du magistrat d'émission, l'objet et les motifs de la décision, les informations nécessaires sur la personne concernée, la description des mesures et preuves attendues de l'État d'exécution, le cas échéant, les antécédents de demande ou le délai d'exécution. Le décret du 7 avril 2017 renvoie expressément au formulaire figurant en annexe de la directive et rappelle les exigences de traduction et de transmission par tout moyen « permettant de laisser une trace écrite ». À ces conditions, « le contenu est certifié comme étant exact et correct par l'autorité judiciaire d'émission ». La décision d'enquête européenne s'inscrit dans le cadre d'une coopération directe simplifiée et échappe au contrôle centralisé de l'entraide internationale. Ainsi, la transmission de la demande se fait directement « aux autorités compétentes de l'État d'exécution par tout moyen permettant de laisser une trace écrite et d'en établir l'authenticité ». L'ordonnance précise aussi les conséquences de la procédure pénale menée dans l'État d'exécution. Ainsi, les investigations peuvent être contestées dans cet État. Si elles font l'objet d'une décision de nullité sur place, cette décision ne s'impose pas aux autorités françaises et n'entraîne pas *ipso facto* la nullité des éléments communiqués aux autorités françaises. En revanche, ces derniers ne peuvent pas constituer le seul fondement de la condamnation de la personne. Le non-respect des délais d'exécution requis ne constitue pas une cause de nullité.

L'ordonnance prévoit aussi un certain nombre de dispositions particulières visant certaines mesures d'enquête. D'une part, le dispositif assure une protection renforcée à la personne puisque les demandes d'enquête européenne portant sur les personnes sont plus strictement

encadrées. La première hypothèse est celle d'une personne détenue sur le territoire national qui ne peut être transférée dans un autre État que si trois conditions sont remplies : son consentement, la nécessité, que la mesure ne soit pas susceptible de prolonger sa détention (article 694-25). La deuxième hypothèse est celle d'une personne détenue sur le territoire d'un État membre et transférée sur le territoire national qui ne peut obtenir sa mise en liberté que sur demande de l'État d'exécution. Le juge est tenu par le cadre initial de la décision d'enquête européenne. Ainsi, il ne peut soumettre « à aucune poursuite ni aucune mesure restrictive ou privative de liberté pour des faits commis ou des condamnations prononcées avant son départ du territoire de l'État d'exécution et qui ne sont pas mentionnés dans la décision d'enquête européenne ». D'autre part, l'ordonnance fixe des règles plus strictes quant à certaines demandes d'investigation particulières. Lorsque la demande porte sur des comptes ou des opérations bancaires, le magistrat indique « les raisons pour lesquelles il considère que les informations demandées sont susceptibles d'être utiles à la manifestation de la vérité et les raisons qui l'amènent à supposer que des banques situées dans l'État d'exécution détiennent le compte » (article 694-27, Code de procédure pénale). Pour l'assistance technique requise pour la mise en place d'une interception de télécommunications, doivent être précisées « les informations nécessaires à l'identification de la personne visée par la demande d'interception, la durée souhaitée de l'interception et toutes les données techniques nécessaires à la mise en place de la mesure » (article 694-28).
L'ordonnance du 1er décembre 2016 a choisi de préciser les règles relatives à la reconnaissance et l'exécution par les autorités judiciaires françaises d'une décision d'enquête européenne émanant d'un autre État membre. La demande d'enquête européenne est possible en matière répressive, au sens large du terme selon la définition européenne, et ne se limite pas au droit pénal *stricto sensu* (« soit des procédures pénales, soit des procédures qui ne sont pas relatives à des infractions pénales mais qui sont engagées contre des personnes physiques ou morales par des autorités administratives ou judiciaires pour des faits punissables dans l'État d'émission au titre d'infractions aux règles de droit et par une décision pouvant donner lieu à un recours devant une juridiction compétente, notamment en matière pénale »,

selon l'article 694-29). Les procédures administratives menées par les autorités administratives indépendantes, notamment en matière boursière, financière, concurrentielle, disciplinaire, fiscale, etc., pourraient relever de ce mécanisme. Afin de limiter le champ très large d'application de cette procédure, l'article 694-29 a choisi de le soumettre à une condition formelle préalable – l'émission ou la validation par une autorité judiciaire, devenue garante de la pertinence de la procédure. La décision d'enquête européenne est exécutée dans deux cadres différents. Lorsque les actes d'investigations se réalisent dans le cadre d'une instruction préparatoire ou nécessitent l'intervention d'un juge des libertés et de la détention, la décision appartient au juge d'instruction qui peut donner commission rogatoire aux « officiers ou agents de police judiciaire ». Dans les autres cas, le procureur de la République est compétent. Toute autre personne saisie de cette demande doit se déclarer incompétente et communiquer à ces deux magistrats.
Les magistrats saisis peuvent refuser la demande d'enquête judiciaire dans plusieurs cas :

- un privilège ou une immunité fait obstacle à son exécution ;
- risque de constituer une violation des principes garantis dans le cadre de la liberté de la presse appelant des règles particulières de responsabilité pénale ;
- les informations classifiées « secret défense nationale », selon l'article 413-9 du Code pénal ;
- des actes contraires aux règles applicables aux procédures internes ;
- la violation du principe « *ne bis in idem* » conduisant à de nouvelles poursuites ou sanctions ;
- une application partielle et particulière de la règle de la double incrimination - « si les faits motivant la décision d'enquête européenne ne constituent pas une infraction pénale selon la loi

française alors qu'ils ont été commis en tout ou en partie sur le territoire national et qu'il existe des raisons sérieuses de penser qu'ils n'ont pas été commis sur le territoire de l'État d'émission » - il s'agit d'éviter qu'un État fasse pression sur la France pour punir un comportement qui ne serait pas pénalisé en France, s'immisçant de fait dans sa politique pénale ;

- lorsque la mesure d'enquête serait contraire aux garanties de la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales et la charte des droits fondamentaux de l'Union européenne, il est intéressant de noter l'ordre de référence retenu par le législateur ;

- lorsque les faits ne constituent pas une infraction en France, manifestation du principe classique de la réciprocité d'incrimination, connaissant une limite de taille, puisque l'entraide ne peut être refusée dans certaines hypothèses.

Le magistrat demande à l'autorité d'émission toute information utile complémentaire. Il existe, néanmoins, un cadre dans lequel l'entraide judiciaire s'impose, même si la France ne reconnaît pas l'interdiction frappant le comportement, la force de cette obligation étant variable. Ainsi, l'article 694-32 retient une liste de comportements pour lesquels le juge ne peut refuser la coopération, même si les faits ne sont pas incriminés en droit français, s'il s'agit, dans l'État d'émission, d'infraction contre les personnes ou contre les biens entraînant une peine privative de liberté d'au moins trois ans (participation à une organisation criminelle, terrorisme, traite des êtres humains, exploitation sexuelle des enfants, trafic de stupéfiants, d'armes, d'organes, de biens culturels, de véhicules volés, corruption, fraude, blanchiment, cybercriminalité, homicide volontaire, viol, racisme et xénophobie, vol organisé, escroquerie, fausse monnaie, contrefaçon, incendie volontaire, crimes relevant de la compétence de la CPI, etc.). L'article 694-33 va encore plus loin, puisque l'exécution de la demande d'enquête européenne s'impose alors même que les faits ne sont pas incriminés en droit français ou que la mesure d'investigation demandée n'est pas autorisée

CENTRE DE RECHERCHE DE L'ECOLE DES OFFICIERS DE LA GENDARMERIE NATIONALE

en droit français pour l'infraction retenue par l'État d'émission, dans un certain nombre de cas : les éléments de preuve qui sont déjà en possession des autorités françaises ; « les informations contenues dans des traitements automatisés de données à caractère personnel mis en œuvre par les services de la police nationale et de la gendarmerie nationale ou les autorités judiciaires directement accessibles dans le cadre d'une procédure pénale » ; l'audition d'un témoin, d'un expert, d'une victime, d'un suspect, d'une personne poursuivie ou d'un tiers ; l'identification d'abonné téléphone ou Internet ; « toute autre mesure d'enquête non intrusive qui ne porte pas atteinte aux droits ou libertés individuels ».

Si le principe de coopération judiciaire dans le cadre de l'Union européenne est horizontal et direct, puisque les demandes d'enquête européenne se transmettent directement entre les magistrats compétents, échappant de ce fait à un contrôle centralisé, politique et hiérarchique, ce dernier peut être utilisé pour bloquer certaines demandes. Ainsi, l'article 694-34 prévoit le retour de ce contrôle lorsque « l'exécution de la décision d'enquête européenne risque de nuire à des intérêts nationaux essentiels en matière de sécurité, de mettre en danger la source d'information ou de comporter l'utilisation d'informations ayant fait l'objet d'une classification en application des dispositions de l'article 413-9 du code pénal et se rapportant à des activités de renseignement ». Dans ce cas, le ministère de la Justice peut refuser la demande après avoir consulté l'autorité d'émission et lui avoir demandé des informations utiles. La demande d'enquête européenne doit être exécutée dans un délai raisonnable pour montrer son utilité. Si le principe veut qu'elle soit assimilée à une demande d'investigation interne et qu'elle déclenche la même célérité, cette assimilation peut se révéler contre-productive dans certains cas. C'est la raison pour laquelle l'ordonnance du 1er décembre 2016 a fixé un délai butoir de trente jours après la réception de la décision émanant de l'État d'émission pour que le magistrat informe le demandeur de son acceptation ou de son refus. S'il lui est impossible de respecter ce délai, il doit en informer l'autorité d'émission, lui indiquer le délai estimé et les raisons du retard. Le délai initial peut ainsi être prolongé de trente jours maximum.

L'exécution de la décision d'enquête européenne se fait « conformément aux formalités et procédures expressément indiquées par l'autorité d'émission ». Dans le prolongement de la véritable révolution subie par la coopération internationale dans le cadre de l'Union européenne, notamment dans la loi du 9 mars 2004, l'ordonnance de 2016 inscrit la décision d'enquête européenne sous le signe d'une véritable intégration européenne. En faisant exception au principe « *locus regit actum* », l'ordonnance du 1er décembre 2016 y substitue la législation de l'État d'émission. L'application de la « loi du for », celle du lieu où les faits sont jugés, résumée par l'adage cité, s'explique par l'histoire et la logique. Les autorités judiciaires requises appliquent une législation qu'elles connaissent et qui représente la garantie de la souveraineté de leur État. La souveraineté nationale, clé de voûte traditionnelle du système d'entraide pénale internationale, semble se dédoubler pour garantir aussi bien la souveraineté organique que la souveraineté fonctionnelle. Ainsi, le principe d'autonomie de l'Etat présente le double visage de la souveraineté judiciaire et de la souveraineté juridictionnelle. L'adage « *locus regit actum* » résume l'emprise procédurale de la loi du for s'appliquant aux conditions de fond et de forme des actes accomplis, adage selon lequel l'État étranger ne saurait prétendre y substituer celle de son propre droit, ni y subordonner la validité de l'acte. Normalement, l'investigation requise doit se faire dans le respect des règles procédurales internes, d'autant plus que l'ordonnance du 1er décembre 2016 l'assimile à une demande d'investigation du même type dans l'ordre interne. Pourtant, le Code de procédure pénale modifie l'analyse retenue, puisque l'article 694-36 le prévoit expressément. L'adage « *forum regit actum* » devient le principe dans la décision d'enquête européenne, puisque l'État requis respecte les formalités et les procédures expressément indiquées par l'État requérant. Mais plus encore, il peut être noté que cette règle devient le principe dans le cadre de l'entraide judiciaire dans le cadre de l'Union européenne, puisqu'elle s'applique aussi dans les autres cadres de coopération. Ce qui était une grande révolution dans la loi du 9 mars 2004 et semblait admis à titre dérogatoire, est prolongé et généralisé par l'ordonnance de 2016. Le nouveau système renforce ainsi l'utilité des preuves recueillies, mais aboutit à l'application, sur le sol de l'État requis, d'une loi procédurale étrangère recelant, à ce titre, un double

danger. D'une part, la connaissance du droit étranger par les juges nationaux est insuffisante. À ce titre, le décret du 7 avril 2017 prévoit que le magistrat impliqué dans la demande d'enquête européenne « consulte directement et par tout moyen approprié, y compris par le biais du système de télécommunications du Réseau judiciaire européen, l'autorité étrangère d'exécution ou d'émission pour faciliter la reconnaissance et l'exécution de la décision, notamment pour régler toute difficulté relative à la transmission ou à l'authenticité d'un document nécessaire à l'exécution de cette décision » (article D 47-1-1, Code de procédure pénale). D'autre part, l'État perd de sa force en acceptant de voir ses juges appliquer une loi sur laquelle il n'a aucun contrôle. C'est la raison pour laquelle l'ordonnance de 2016 prévoit deux garanties essentielles dont l'objectif est identique – permettre l'application de règles plus protectrices tout en faisant obstacle à une réduction indirecte et implicite des droits. La première garantie est de droit interne et exclut de son champ d'application toute disposition contraire qui réduirait « les droits des parties et les garanties procédurales appliquant les principes fondamentaux prévus à l'article préliminaire du présent code » (article 694-36). La deuxième garantie est une garantie européenne, au sens le plus large du terme, impliquant à la fois l'Union européenne et le Conseil de l'Europe, qui prévoit de refuser toute mesure incompatible avec « la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales et la charte des droits fondamentaux de l'Union européenne » (article 694-31,7°). L'exécution de la demande d'enquête européenne doit intervenir « dans les meilleurs délais », ce qui est soumis à une appréciation *in concreto* des juges, mais ne peut dépasser un délai de quatre-vingt-dix jours, sauf s'il y a une raison valable de la reporter ou « si elle risque de nuire à une enquête ou à des poursuites en cours ou si les objets, documents ou données concernés sont déjà utilisés dans le cadre d'une autre procédure ». L'ordonnance du 1er décembre 2016 a prévu l'hypothèse dans laquelle la mesure d'investigation demandée par l'État d'émission n'existe pas en droit français – « le magistrat saisi a recours, chaque fois que cela s'avère possible, à toute autre mesure d'investigation permettant d'obtenir les éléments demandés par l'autorité d'émission ». Le principe « d'utilité par équivalence » semble admis *de facto*. De la même manière, « qui peut le plus, peut le

moins », donc le « magistrat saisi peut également ordonner une autre mesure d'enquête que celle demandée si elle permet d'obtenir le même résultat de façon moins intrusive » (article 694-38). Le parallélisme n'est pas de droit. Si le magistrat considère que d'autres investigations seraient utiles, il ne peut les décider de sa propre initiative, il doit en informer l'autorité d'émission qui en décidera, le cas échéant (article 694-40).

Les mesures d'exécution de la demande d'enquête européenne peuvent faire l'objet de recours ou contestations de droit commun, exercés dans les mêmes conditions et selon les mêmes modalités. Ces recours ne sont pas suspensifs de droit. Les arguments de fond ne peuvent être invoqués, car ils ne peuvent être discutés que devant l'État d'émission. Les coûts d'exécution sont, en principe, à la charge de l'État d'exécution, sauf lorsqu'ils sont considérés comme trop élevés, auquel cas ils peuvent être partagés. Sont assumés par l'État d'émission les frais de transfèrement de personne et de transcription ou déchiffrement de communications interceptées. L'ordonnance a modifié la procédure applicable en matière d'interception de communication en introduisant un nouvel article 100-8. « Lorsqu'une interception de correspondances émises par la voie des communications électroniques concerne une adresse de communication qui est utilisée sur le territoire d'un État membre de l'Union européenne, et qu'elle n'est pas réalisée dans le cadre d'une décision d'enquête européenne, le juge d'instruction ou l'officier de police judiciaire par lui commis notifie cette interception à l'autorité compétente de cet État si la personne visée par cette interception se trouve sur son territoire ». Il est intéressant de noter que la notification peut se faire avant, pendant ou après la réalisation de l'interception, s'il est établi que la personne s'est trouvée sur le territoire de cet État. Si cette procédure n'était pas possible dans l'État d'exécution et exclusivement sur demande de l'autorité compétente de l'État membre dans les quatre-vingt-seize heures suivant la réception de la notification, l'interception peut être interrompue ou ne pas être effectuée. Les données obtenues ne peuvent être utilisées et doivent être retirées du dossier de procédure. Le décret du 7 avril 2017 modifie en conséquence la partie réglementaire du Code de procédure pénale, plus précisément les articles D32-2 et suivants, précisant la déroulement et les formulaires à respecter dans le cadre de cette procédure.

BRÈVES

Contravention - Certificat qualité de l'air

Décret n° 2017-782 du 5 mai 2017 renforçant les sanctions pour non-respect de l'usage des certificats qualité de l'air et des mesures d'urgence arrêtées en cas d'épisode de pollution atmosphérique

Le décret crée une contravention en cas d'absence de présentation de certificat qualité de l'air pour un véhicule circulant dans une zone à circulation restreinte, en cas de violation des mesures d'urgence arrêtées en cas de pic de pollution atmosphérique et modifie le Code de la route, ainsi que le Code de l'environnement. L'article R 411-9 du Code de la route prévoit que le fait de contrevenir aux mesures de suspension ou de restriction de la circulation mentionnées au présent article, ou de circuler dans le périmètre des restrictions de circulation instaurées est passible d'amendes de quatrième ou de troisième classe, selon les différentes catégories dont le véhicule en infraction relève. Le texte entre en vigueur au 1er juillet 2017.

Contravention - Procédure - Exceptions de nullité

Crim. 26 avril 2017, n° 15-85909 ; Crim. 26 avril 2017, n° 16-84539 ; Crim. 26 avril 2017, n° 16-82742, publ. à venir au Bull.

Dans le premier arrêt, un procès-verbal est dressé pour stationnement gênant sur une voie publique spécialement désignée par arrêté municipal. Cité devant la juridiction de proximité, l'auteur de la contravention est représenté par son père qui fait valoir, d'une part, que cet arrêté municipal édictait illicitement une interdiction générale de stationner non conforme aux dispositions de l'article R. 417-10 du Code de la route, d'autre part, que cette interdiction ne faisait l'objet, à la date d'établissement du procès-verbal, d'aucune signalisation par panneau ou marquage au sol. Il soulève ainsi une exception d'illégalité et une

exception d'inopposabilité. Sans répondre à ses arguments, le jugement considère que le prévenu a bien commis les faits qui lui sont reprochés à partir du moment où il n'apporte pas la preuve contraire aux énonciations du procès-verbal de contravention régulièrement établi, qui applique les dispositions de l'arrêté municipal considérant que « les véhicules stationnés en dehors des emplacements payants matérialisés sur la chaussée sont considérés en stationnement gênant ». La Cour de cassation casse et annule cette décision, car elle reproche aux juges du fond de ne pas avoir justifié leur décision, puisqu'ils n'ont pas répondu « aux exceptions d'illégalité et d'inopposabilité de l'arrêté municipal précité proposées oralement pour le prévenu, avant toute défense au fond, et reprises explicitement dans le jugement ». La Chambre criminelle rappelle dans un attendu à portée générale que « tout jugement ou arrêt doit comporter les motifs propres à justifier la décision et répondre aux chefs péremptoires des conclusions des parties ; que l'insuffisance ou la contradiction des motifs équivaut à leur absence ».

Dans le deuxième arrêt, une personne condamnée à l'annulation du permis de conduire et à l'interdiction d'en solliciter un nouveau pendant un jour a été poursuivie pour conduite en état alcoolique et conduite malgré l'annulation de son permis. Relaxée de ce dernier chef, elle a été condamnée à une peine de trois mois d'emprisonnement avec sursis, obligation d'accomplir un travail d'intérêt général et deux mois de suspension du permis de conduire. La Cour d'appel a confirmé l'analyse en considérant que « la décision d'annulation du permis de conduire est de nature contradictoire et a, en conséquence, acquis un caractère exécutoire » dix jours après la première décision. La Cour de cassation casse et annule la décision en visant l'article L. 224-16 du Code de la route qui dispose que l'exécution d'une mesure d'annulation du permis de conduire ne prend effet qu'à compter du jour de la notification de la mesure par l'agent de l'autorité chargé de l'exécution.

Dans le troisième arrêt, une personne poursuivie pour avoir franchi un feu rouge au volant de son véhicule, représentée par son avocat, a présenté des observations orales à la barre, exploitant l'imprécision des mentions du procès-verbal tenant au permis de l'intéressé et au lieu de

CENTRE DE RECHERCHE DE L'ECOLE DES OFFICIERS DE LA GENDARMERIE NATIONALE

commission des faits. Le juge de proximité a invité l'avocat à déposer des conclusions écrites, en vertu de l'article 459 du Code de procédure pénale. Ne s'estimant pas régulièrement saisi de ces exceptions en l'absence d'un écrit, le juge de proximité s'est prononcé. La Cour de cassation infirme l'analyse de la juridiction, puisque « les articles 385 et 522, alinéa 4, du Code de procédure pénale n'exigeant pas que les exceptions de nullité soient soutenues par écrit », néanmoins elle ne censure pas la décision « dès lors qu'en raison de l'absence de conclusions écrites, la Cour de cassation n'est pas en mesure d'exercer son contrôle sur les réponses apportées par la juridiction ». La Cour de cassation rejette le second moyen qui remet en cause l'appréciation souveraine des juges du fond, puisqu'il ressort des débats que le prévenu a bien commis l'infraction.

Ces trois arrêts apportent des précisions intéressantes relatives à la preuve et aux débats en matière contraventionnelle. Si les juges du fond invitent les avocats au respect de l'article 459 du Code de procédure pénale permettant au prévenu, aux autres parties et à leurs avocats de déposer des conclusions, la Cour de cassation tempère cette règle par les articles 385 et 522 du même Code selon lesquels les exceptions de nullité présentées en matière contraventionnelle sont soumises au même régime juridique que dans des autres matières et doivent donc être présentées, sous peine d'irrecevabilité, *in limine litis*. En revanche, l'oralité des débats devant la juridiction pénale ne permet pas de leur imposer une forme écrite, alors que l'article 459 les soumet à une règle formelle, devant être visées par le greffier et le président et leur dépôt notifié dans la procédure. Cette formalité semble frapper d'irrecevabilité les exceptions de nullité orales. Ce n'est pas l'avis de la Cour de cassation qui considère que les exceptions de nullité soutenues oralement doivent être considérées comme valablement présentées dans le cadre de la procédure. Si la liberté et l'oralité des débats sont protégées par cette analyse, la conséquence directe n'est pas aussi importante. La Chambre criminelle considère qu'elle ne peut examiner le bien-fondé de l'exception de nullité, dans la mesure où « en raison de l'absence de conclusions écrites, la Cour de cassation n'est pas en mesure d'exercer son contrôle sur les réponses apportées par la juridiction ». La forme orale des conclusions est suffisante, mais elle ne

permet pas le contrôle de l'appréciation juridique par les juges de l'ordre supérieur, ce qui réduit considérablement l'intérêt pratique de ces arrêts.

Armes

Décret n° 2017-909 du 9 mai 2017 relatif au contrôle de la circulation des armes et des matériels de guerre

Le décret modifie la répartition de compétences en matière de contrôle de la circulation des armes. Le ministère de la Défense demeure compétent pour les seuls matériels de guerre, au titre de la sécurité nationale, tandis que les armes civiles sont confiées au ministère de l'Intérieur, au titre de la sécurité publique. Chacun des deux ministères est désormais respectivement en charge du classement des armes et matériels relevant de son champ de compétence, de la délivrance des autorisations de fabrication, de commerce, d'importation, d'exportation et de transfert intracommunautaire de ces mêmes armes et matériels ainsi que du contrôle des professionnels concernés. Les dispositions relatives au ministère de la Défense figurent dans le Code de la défense, alors que celles relatives au ministère de l'Intérieur sont intégrées au Code de la sécurité intérieure.
Le premier chapitre modifie le Code de la sécurité intérieure. Apparaît une nouvelle catégorie d'arme – l'arme de spectacle, définie comme « toute arme à feu transformée de manière à ne pouvoir tirer qu'une munition à blanc destinée à provoquer uniquement un effet sonore » qui reste classée dans sa catégorie d'origine (article R. 311-1).
Le décret modifie par ailleurs les modalités du classement des armes civiles et instaure, pour ces mêmes armes, un nouveau dispositif d'enregistrement. « En vue de garantir leur traçabilité, toutes les armes à feu fabriquées, importées ou introduites en France, sont enregistrées selon des modalités définies par un arrêté du ministre de l'Intérieur » (article R 311-4). L'application de ces dispositions est systématique et intervient préalablement à toute mise sur le marché. Il

renforce également la sécurité publique en restreignant les possibilités d'acquisition et de détention de certaines armes, particulièrement dangereuses, ou de leur présentation au public par les professionnels, à titre d'essai ou de démonstration (vente aux enchères, ouverture de magasins dédiés, fabrication, commerce, marquage). L'autorisation ne peut être accordée à des personnes condamnées à une mesure de sûreté d'hospitalisation d'office à la suite de la commission d'une infraction ou hospitalisées sans leur consentement en raison de troubles mentaux. De nouvelles dispositions relatives aux acquisition, détention et transfert au sein de l'Union européenne, importations et exportations ont été adoptées (article R. 316-1 et suivants). En revanche, les dispositifs applicables aux transferts de matériels de guerre aux armées, notamment sur des opérations extérieures et aux clubs de tir sportifs et leurs adhérents sont simplifiés.

Par M. Ludovic Guinamant

Le contrôle entier du comportement d'un fonctionnaire qui se prévaut de la qualité de « lanceur d'alerte » par le Conseil d'État

Conseil d'État, 5ème et 4ème chambres réunies, 24 mai 2017, n°389785
Conseil d'État, 5ème et 4ème chambres réunies, 31 mars 2017, n°392316

Mme B., adjointe de sécurité à la police aux frontières, a cosigné, sous le titre *« Omerta dans la police - abus de pouvoir, homophobie, racisme, sexisme »*, un ouvrage publié en 2010 et imputant à cette institution un certain nombre d'abus.

Par un arrêté du 26 juillet 2011, le ministre de l'Intérieur s'est fondé sur ce comportement, qu'il a qualifié de manquement à l'obligation de réserve, pour suspendre l'intéressée de ses fonctions pour une durée de dix-huit mois, dont douze assortis du sursis.

Le tribunal administratif de Paris a rejeté, par un jugement du 6 décembre 2012, le recours pour excès de pouvoir formé par Mme B. contre cette décision ainsi que sa demande d'indemnité. Mme B. a fait appel de cette décision et par un arrêt du 31 décembre 2014 la Cour administrative d'appel de Paris a rejeté son appel.

La Cour administrative d'appel de Paris a jugé que Mme B. avait délibérément manqué à son obligation de réserve en cosignant et en promouvant dans les médias un ouvrage portant de graves accusations contre le service de police au sein duquel elle était affectée et contre la politique gouvernementale en matière de police, et que ces accusations, souvent formulées de manière outrancière, étaient de nature à jeter le discrédit sur l'institution policière dans son ensemble. Elle ajoute, en outre, que Mme B. n'avait saisi le procureur de la République, sur le fondement de l'article 40 du Code de procédure pénale, que d'une

partie seulement des faits qu'elle prétendait dénoncer dans cet ouvrage, qu'elle avait publié cet ouvrage avant que la Haute autorité de lutte contre les discriminations et pour l'égalité n'émette un avis sur les faits dont elle l'avait saisie et qu'enfin, elle avait agi dans une intention délibérément polémique. Elle en a déduit, par conséquent, que Mme B. ne pouvait se prévaloir d'aucun *« devoir d'alerte »* pour justifier la publication de son ouvrage.

La question posée par l'adjointe de sécurité était donc de savoir si un fonctionnaire pouvait mettre en cause son administration au nom de la liberté d'expression en se considérant comme un « lanceur d'alerte », compte tenu des manquements graves qu'il souhaitait mettre en avant.

Le Conseil d'État, saisi en cassation du litige, a rejeté le pourvoi en considérant notamment que la Cour n'avait pas commis d'erreur de droit au regard de la portée de l'article 10 de la Convention européenne des droits de l'Homme qui consacre la liberté d'expression.

Il sera également mentionné que le Conseil d'État a mis fin à la longue procédure administrative, débutée en 2008, opposant un commandant de police avec son administration en raison de la transmission de deux fiches de célébrités provenant de l'ancien fichier STIC à un organe de presse. Pour ces faits, le commandant de police avait été sanctionné d'une mise à la retraite d'office.

Saisi pour la seconde fois du litige, le Conseil d'État a considéré, par un arrêt du 31 mars 2017, que *« si la communication des deux fiches extraites du STIC à un journaliste avait été motivée pour partie par son souhait de dénoncer les dysfonctionnements de ce fichier, ces faits, connus d'un grand nombre de personnes, avaient déjà été portés à la connaissance de sa hiérarchie et du procureur de la République et étaient l'objet d'un contrôle de la commission nationale informatique et libertés et, d'autre part, que la volonté de M. A. de dénoncer publiquement les dysfonctionnements du fichier STIC ne pouvait expliquer les nombreuses consultations de ce fichier, dont il avait déclaré lui-même qu'elles avaient été effectuées à titre personnel « par curiosité » ».*

Dans ces conditions, le Palais Royal considère que le fonctionnaire ne pouvait pas se prévaloir de l'article 10 de la Convention européenne de sauvegarde des droits de l'Homme.

Fermeture administrative d'un débit de boissons et proportionnalité de la mesure de police

Conseil d'État, juge des référés, 17 mai 2017, n°410453

Par un courrier du 9 mars 2017, remis en mains propres le 20 mars, le préfet de police a invité la gérante de la société Animations Loisirs Evénements (ALE), qui exploite rue de Ponthieu à Paris 8ème un établissement sous l'enseigne « Le Trust », à faire valoir ses observations sur les troubles à l'ordre et à la sécurité publics, susceptibles de fonder une fermeture administrative de l'établissement au titre des dispositions de l'article L.3332-15 2° du Code de la santé publique.

Par un arrêté du 2 mai 2017, le préfet de police a décidé la fermeture administrative pour une durée de trente jours, du 4 mai au 2 juin 2017 inclus. La société ALE relève appel de l'ordonnance du 9 mai 2017 par laquelle le juge des référés du tribunal administratif de Paris, statuant sur le fondement de l'article L. 521-2 du Code de justice administrative, avait rejeté sa demande tendant à la suspension de l'exécution de l'arrêté du 2 mai 2017.

La fermeture de l'établissement avait été prononcée au motif unique que, le 23 février 2017 vers 5 heures 45, un différend entre clients de cet établissement, en état d'ivresse, avait éclaté au sein de celui-ci et s'était poursuivi sur la voie publique. Un client de l'établissement, qui se trouvait dehors, a tenté de s'interposer et a été violemment pris à parti par un individu lui-même client de l'établissement, qui lui a porté un coup au visage, lui fracturant le nez. Cette personne, blessée à l'arrière du crâne lors de sa chute, a perdu connaissance et a dû être transportée à l'hôpital par les sapeurs-pompiers, l'auteur des coups ayant pour sa part été déféré au Parquet à l'issue de sa garde à vue. Par ailleurs,

les forces de police ont dû faire usage de gaz lacrymogène pour disperser les autres protagonistes de ces incidents.

Néanmoins, la société requérante soutenait devant le Conseil d'État que la durée de trente jours de fermeture était manifestement disproportionnée au regard des faits qui fondaient cette mesure.

S'agissant du contrôle de la proportionnalité de la mesure de police, le Conseil d'État ne se limite pas à l'existence matérielle des faits reprochés mais il se fonde également sur l'ensemble des pièces du dossier pour apprécier la légalité de la durée de la mesure de police.

Ainsi, bien que ne figurant par dans l'arrêté litigieux, le juge des référés a constaté que, le 14 janvier 2017, une rixe entre plusieurs individus, décrits comme virulents dans le registre de main courante versé au dossier, avait déjà éclaté devant l'établissement « Le Trust », contraignant les forces de l'ordre à intervenir en faisant usage de gaz lacrymogène. En outre, une jeune femme saignant du nez s'était à cette occasion plainte aux policiers d'avoir été frappée par un des vigiles de l'établissement. L'instruction a également fait apparaître que la rue de Ponthieu, à Paris, est le lieu de troubles à l'ordre public récurrents et particulièrement graves aux abords des établissements de même nature que « Le Trust ».

Compte tenu de ces éléments de contexte, le juge des référés du Conseil d'État a considéré que la mesure de police prise n'était pas manifestement disproportionnée.

Ainsi, dans le cadre du contrôle de la durée de la mesure de police administrative, l'administration peut se fonder sur des faits qui n'ont pas fait l'objet d'un débat contradictoire et qui ne figurent pas dans les motifs de la fermeture administrative.

Le contrôle entier de la mesure de police s'entend, par conséquent, également sur l'appréciation globale de la situation à l'origine de la mesure.

Police administrative

Décès en raison de crues : condamnation du maire de la commune en raison de sa carence dans l'exercice de ses pouvoirs de police

Cour administrative d'appel de Bordeaux, 19 mai 2017, n°15BX00859

Le 4 janvier 2011, vers 19 heures, 4 individus, qui franchissaient avec un véhicule un ponceau situé chemin de Pavé, dans la commune des Abymes, ont été emportés par les eaux de la ravine en crue à la suite de pluies importantes qui ont affecté la zone.

Les ayants droit des victimes ont saisi le tribunal administratif de la Guadeloupe de demandes tendant à la condamnation de la commune et de l'État à leur verser un montant total de 310 000 euros en réparation du préjudice moral lié au décès des victimes. Par un jugement du 29 janvier 2015, le tribunal administratif de la Guadeloupe a, d'une part, mis hors de cause l'État, d'autre part, limité la responsabilité de la commune à 30 % des conséquences dommageables de l'accident et l'a condamnée à verser aux ayants droit la somme totale de 25 000 euros en réparation du préjudice moral qu'ils ont subi.

Les ayants droit relèvent appel du jugement en tant qu'il a exonéré la commune des Abymes partiellement de sa responsabilité et a limité le montant des indemnités.

Au visa de l'article L. 2212-2 du Code général des collectivités territoriales, la Cour administrative d'appel de Bordeaux constate que Météo France avait émis le 4 janvier 2011 un bulletin de vigilance jaune prévoyant de « fortes pluies/orage » correspondant à un impact modéré et appelant à la prudence en cas de circulation dans des zones inondées, en particulier pour le franchissement des gués ou de passages bas encaissés.
Ce bulletin a été transmis ce même jour entre 16 h 30 et 16 h 45 par le préfet de la région Guadeloupe à tous les services de l'État et aux collectivités locales concernées et a contacté la police municipale des

Police administrative

Abymes par téléphone. Dès 16 h 30, les premières interventions de sauvetage sur la commune des Abymes ont été réalisées par le SDIS.

Les pluies s'étant également intensifiées sur cette zone, une cellule de crise a été mise en place dès 18 heures, afin de faciliter la coordination des interventions locales. Dès le début de la montée des eaux, la route départementale 101, située à proximité de la voie en cause et qui supporte normalement la circulation de transit, a été rendue impraticable.

Ainsi, les juges d'appel de Bordeaux considèrent qu'alors que le chemin de Pavé était utilisé par les automobilistes comme itinéraire secondaire compte tenu des incidents survenus sur la RD 101, que cette voie était connue pour être inondable et que les pluies présentaient un caractère exceptionnel, la commune disposait des informations lui permettant d'évaluer et de mettre en œuvre des mesures de prévention et de sécurité adaptées aux circonstances, notamment en interdisant l'accès du pont de chemin de Pavé.

Les juges d'appel considèrent ainsi que la commune des Abymes a commis une faute, née de sa carence à utiliser ses pouvoirs de police, de nature à engager sa responsabilité en s'abstenant de prendre les dispositions nécessaires pour assurer la sécurité des usagers du chemin.

Toutefois, après avoir caractérisé la faute, les mêmes juges considèrent que les victimes ont participé elles-mêmes à leur propre dommage. Ils constatent ainsi que bien qu'aucun panneau n'interdise l'accès des lieux ou n'en signale le danger, les victimes savaient qu'elles allaient emprunter, compte tenu de leur connaissance du chemin de Pavé, un ponceau dépourvu de barrières ou de parapets. Ainsi, en dépit de la ravine en crue en raison des fortes pluies inondant le pont, de l'absence de visibilité due à la tombée de la nuit et des mises en garde des personnes présentes sur les lieux leur conseillant de renoncer, les victimes ont décidé de le franchir à bord d'un véhicule de type 4X4. Les victimes ont, par ailleurs, persisté dans leur choix d'effectuer cette

Police administrative

traversée, alors qu'elle a été très rapidement rendue difficile, le véhicule ayant connu un premier problème de circulation. Enfin, la Cour administrative de Bordeaux conclut que les victimes ont commis une très grave imprudence en s'avançant sur le pont dans de telles conditions, laquelle est de nature à atténuer la responsabilité de la commune.

Il s'agit dans ce cas d'espèce d'une jurisprudence constante des juridictions administratives mais force est de constater l'augmentation sensible des contentieux en responsabilité résultant des carences fautives des autorités dans l'exercice des pouvoirs de police.

Il sera rappelé ici que la faute simple est suffisante pour engager la responsabilité de l'autorité de police. Les domaines dans lesquels la faute lourde est encore exigée diminue progressivement (renseignement, police judiciaire,…).

On peut également se demander si l'augmentation de ces décisions de justice ne va pas, par voie de conséquence, augmenter les constitutions de partie civile devant les juridictions pénales sur le fondement des articles 221-6 et 222-19 du Code pénal réprimant les homicides et blessures involontaires.

Droit des collectivités territoriales

Par M. Xavier Latour

Les collectivités territoriales et la radicalisation : quelles évolutions ?

Dans un rapport sénatorial du 11 avril 2017, intitulé « Les collectivités territoriales et la prévention de la radicalisation », deux parlementaires (MM. Bockel et Carvounas) abordent une question éminemment d'actualité.
Après un constat qui fera sans doute consensus, les préconisations variées soulèveront vraisemblablement davantage de questions.

Un constat lucide

Le rapport commence utilement par cerner la notion de radicalisation.

Celle-ci n'apparaît que tardivement. Pendant plusieurs années, la France laisse se développer un extrémisme religieux sans en cerner suffisamment les contours. Le départ de jeunes Français pour des zones contrôlées par les djihadistes retient à peine l'attention. Plus grave, la cécité de la majorité des chercheurs est aggravée par le parti pris de ceux qui préfèrent voir l'islam radical sous le seul angle de la pratique rigoureuse de la religion (quiétisme) ou des ruptures sociales. Les discours anti-occidentaux sont analysés comme un exutoire qui détournerait du passage à l'acte. La dimension politique de l'islam radical a longtemps été sous-évaluée. Le lien entre radicalisation et djihadisme s'impose difficilement en raison d'une réticence à concevoir la radicalisation religieuse comme une étape vers la violence.

Il faut attendre 2014 pour voir s'affirmer une prise de conscience plus nette du danger. La multiplication des départs vers la Syrie impose une réaction étatique qui prend la forme du premier plan de lutte contre la radicalisation.
Tout en ayant le mérite d'exister, il souffre d'un manque d'éléments aidant à cerner plus précisément les facteurs incitatifs au départ. Le

second plan, en 2016, réoriente l'approche en direction de la menace radicale sur le territoire national. À ce titre, les actions s'élargissent, ce qui implique d'associer les collectivités territoriales. Cette nouvelle piste de coproduction suppose de sérieux efforts. Les acteurs locaux demeurent, en effet, marqués par la laïcité qui ne les a pas habitués à appréhender des phénomènes religieux. De plus, la radicalisation déroute en étant le résultat de multiples facteurs (environnement social, fragilité psychologique, éléments religieux…).
Les travaux théoriques à la disposition des collectivités se répartissent en deux catégories. Les premiers sont axés sur la radicalisation comportementale (approche anglo-saxonne). Ils sous-tendent une approche libérale à l'égard des discours, dès lors qu'ils ne s'accompagnent pas de violences physiques. Les autres relèvent de la radicalisation cognitive (approche européenne), davantage axée sur la prise en compte des pensées de l'individu.
Force est de constater qu'il n'existe pas de violence sans passage préalable par la radicalisation théorique. En d'autres termes, l'extrémisme nourrit le terrorisme. En s'appuyant sur les travaux de l'Unité de Coordination de la Lutte Antiterroriste (UCLAT), les rapporteurs insistent, en tout état de cause, sur le lien entre l'existence de cercles salafistes et le nombre de départs pour les zones djihadistes.

Sans sous-estimer le rôle de l'Internet, la radicalisation semble nécessiter à un moment ou à un autre un contact humain. Certains lieux ou certains réseaux (associatifs, sportifs, amicaux…) facilitent la rencontre (y compris en milieu carcéral).

Parmi ces réseaux, les bandes jouent un rôle important. En leur sein, la radicalisation et la délinquance se rejoignent, voire fusionnent. La bande sert de cadre d'endoctrinement et de durcissement, la religion justifie l'action délinquante contre les mécréants, les revenus tirés des infractions financent de futures actions. L'influence du facteur humain est d'autant plus forte que l'individu, sans être qualifiable de fou au sens psychiatrique du terme, n'en est pas moins parfois fragile psychologiquement et ce, pour des raisons multiples.

Une fois les contours de la radicalisation cernés, le rapport s'intéresse

à son ampleur. Sur la base des chiffres du fichier de traitement des signalements pour la prévention de la radicalisation, la France compterait 17 393 individus radicalisés, à la dangerosité variable. À cela s'ajouteraient 2046 personnes présentes dans des zones de combat en Syrie ou en Iraq. Le Nord, l'Île-de-France et le Sud-Est abritent le plus de radicalisés.

Dans ce contexte, les collectivités territoriales doivent mettre en œuvre une prévention complexe de la radicalisation.
À défaut d'être unicausale et parce qu'elle est le résultat d'un processus, la radicalisation impose aux collectivités une approche à plusieurs niveaux. La prévention porte sur plusieurs facteurs (individu, famille, ordre public…) afin de détecter le plus en amont possible des « signaux faibles ». Naturellement, les collectivités n'agissent que sur des éléments du processus qu'elles maîtrisent et bénéficient de leur connaissance du tissu social.
Les communes sont très sollicitées en raison de leurs compétences de proximité. La radicalisation impacte la quasi-totalité de leurs domaines d'action : le scolaire, l'aide sociale, la culture et même l'urbanisme. Les maires sont, en outre, les titulaires de prérogatives de police administrative.
Les départements agissent, quant à eux, principalement sur l'environnement social (aide sociale à l'enfance, protection maternelle et infantile par exemple).
Plus en retrait, les régions s'impliquent cependant dans l'éducation à l'échelon des lycées de l'enseignement professionnel.

Le rôle des collectivités a gagné en importance avec le développement de la radicalisation d'individus relativement isolés et discrets, ce qui les rend encore plus dangereux (djihadisme de troisième génération selon Gilles Kepel). Leur existence fait d'ailleurs peser de graves menaces sur les collectivités elles-mêmes. Elles ne sont pas uniquement des actrices de la prévention, elles constituent aussi des cibles ou sont exposées à la pression directe des radicaux (entrisme, prise de contrôle d'associations, multiplication des revendications communautaristes…).

Droit des collectivités territoriales

Malgré l'ampleur du phénomène, les collectivités se mobilisent de manière très inégale. Certaines collectivités se sentent peu concernées ou disent manquer de moyens. D'autres encore se défaussent sur l'État. Les plus actives ont initié des actions diverses à destination des jeunes (kits pédagogiques), de la sensibilisation des personnels municipaux et des élus, de la détection des signaux faibles, du soutien aux familles… Ces politiques locales nécessitent une pluralité d'intervenants pour lutter contre l'endoctrinement et construire un contre-discours. Plus généralement, la détection précoce est prioritaire.

Certaines communes ont, dans ce but, créé des cellules d'échange sur la radicalisation tandis que des départements ont constitué des plateformes de traitement et de suivi des signalements. Ces initiatives ne se dissocient pas des actions engagées par l'Etat (préfecture, autorités judiciaires). Selon les cas, les personnes radicalisées participent à des programmes qui mettent l'accent sur l'emprise mentale dont elles sont l'objet ou davantage sur leur vision de l'islam.
Les départements participent en mettant l'accent sur les mineurs, voire en suspendant le versement de certaines allocations pour des individus n'ayant plus une résidence stable sur le territoire.
Toutes peuvent aussi trouver du soutien dans des réseaux européens, voire internationaux (aux Émirats arabes unis principalement).

Les préconisations variées

Les rapporteurs regrettent, à juste titre, les inégalités territoriales sur un sujet aussi crucial. Pour y mettre fin, ils plaident en faveur de la construction de pratiques plus homogènes. Face à la diversité des initiatives, souvent cofinancées par l'État, les rapporteurs commencent par préconiser une évaluation rigoureuse menée à l'échelon national des programmes de prise en charge des personnes en voie de radicalisation. Cette suggestion recoupe les constats souvent négatifs de certaines actions. L'évaluation permettrait non seulement d'améliorer les dispositifs, mais aussi de mieux orienter les financements.

Droit des collectivités territoriales

Dans un autre registre, le rapport développe l'idée de s'inspirer des stratégies territoriales de prévention de la délinquance pour construire des stratégies de prévention de la radicalisation. Ainsi, l'État donnerait toujours l'impulsion, mais les collectivités bénéficieraient d'une marge de manœuvre adaptée aux réalités de leur territoire. Elles cesseraient d'être les prestataires de services utilisés par l'administration étatique déconcentrée, pour devenir des acteurs de premier plan. La réorientation opérée par le plan 2016 d'action contre la radicalisation en faveur des collectivités devrait, dès lors, être accentuée.
Le bon niveau d'action, selon les auteurs, serait la commune ou l'intercommunalité. Le Conseil Local de Sécurité et de Prévention de la Délinquance (CLSPD) s'ouvrirait alors aux enjeux de la radicalisation. Il associerait les services infradépartementaux de l'État et le Conseil départemental.
L'action du Conseil serait facilitée par un diagnostic précis de l'état de la radicalisation sur le territoire et des moyens d'y faire face, réalisé, notamment, en partenariat avec les forces de sécurité. L'action des collectivités se focaliserait sur : la détection et le signalement de la radicalisation et des réseaux, la prévention primaire dont certains moyens recouperaient la prévention de la délinquance (avec le tissu associatif par exemple), une partie de la prévention secondaire des éléments déjà en voie de radicalisation (stages, formations, approche théologique, lutte contre la déscolarisation et contrôle des établissements hors contrat…) et, éventuellement, de la prévention tertiaire en partenariat avec l'autorité judiciaire.
La pertinence de l'échelon communal ne fait guère de doute. En revanche et malgré l'optimisme des auteurs, l'action dans le cadre des intercommunalités suscite plus de questions en raison des difficultés déjà rencontrées en matière de prévention de la délinquance malgré les obligations imposées par le Code général des collectivités territoriales. Par ailleurs, les CLSPD n'ont pas toujours donné satisfaction. Les travaux relatifs à leur hétérogénéité et à leurs difficultés de fonctionnement sont nombreux. On voit mal ce qui pourrait éviter ces travers en matière de radicalisation. L'aménagement des CLSPD grâce, par exemple, à la création de groupes thématiques restreints limiterait, selon les rédacteurs, les risques de dispersion, mais serait-ce suffisant ?

Droit des collectivités territoriales

Le rapport rappelle logiquement que l'action des collectivités territoriales ne doit pas entraver l'action de l'État. Ce dernier demeure totalement responsable de la lutte contre le terrorisme et du renseignement. Les rédacteurs soulignent que les polices municipales n'ont pas à entrer, ne serait-ce qu'un peu, dans ces domaines.
Les auteurs identifient trois niveaux de coopération.

Le premier intéresse le ministère de l'Intérieur. Il doit rester le chef de file de la politique menée en s'appuyant sur le Comité Interministériel de Prévention de la Délinquance et de la Radicalisation (CIPDR), l'UCLAT et l'état-major de prévention du terrorisme (le rapport n' interroge pas les liens entre les deux structures). La politique nationale est, ensuite, déclinée à l'échelon déconcentré par les préfets de département, lesquels agissent, enfin, en étroite relation avec les maires.
L'implication accrue des maires justifierait qu'ils nomment des référents. Ceux-ci faciliteraient la circulation des informations avec les autorités départementales et amélioreraient l'efficacité des signalements.

Alors que l'État a donné des gages de volontarisme en matière de partenariat (rôle du CIPDR, rapprochement avec les associations d'élus), celui-ci peut encore être approfondi, selon les rapporteurs.
L'information globale des collectivités exige de nouveaux efforts. Trop de collectivités ignorent l'existence des actions engagées par l'État dans le cadre du plan national d'action contre la radicalisation, du CIPDR ou des conventions conclues avec les associations d'élus. Les cellules de veille présidées par les préfets manquent, par exemple, de visibilité. Afin d'y remédier, les sénateurs appellent les sous-préfets à s'impliquer davantage et à aller vers les élus.
En outre, le rapport établit un parallèle intéressant entre les transferts d'informations en matière de délinquance et ceux relatifs à la radicalisation. Forces de l'ordre et autorités judiciaires sont tenues de donner aux maires différents éléments sur le fondement du CSI (articles L 132-2 et 132-3). Une piste de réflexion consiste à transposer ces dispositifs à la radicalisation. Tandis que l'État a besoin des remontées issues de signalements, l'inverse est aussi vrai. Les collectivités territo-

Droit des collectivités territoriales

riales souffrent parfois d'un déficit de dialogue et sont en attente de réciprocité. L'idée est pertinente, bien que, sur ce point également, l'expérience de la prévention de la délinquance laisse entrevoir de sérieux obstacles.

Les rédacteurs soulignent, par ailleurs, un manque d'informations sur la situation de la radicalisation sur le territoire des collectivités. L'information d'ambiance, déjà inégale, ne suffit pas. Les élus ont besoin d'éléments relatifs à des situations précises, surtout lorsqu'elles concernent leurs domaines de compétences. Les sénateurs écartent, à juste titre, la communication des fiches S, en adoptant une ligne comparable à celle du ministère de l'Intérieur (contenu inadapté, problème de confidentialité, mise en alerte des suspects…). En pratique, les élus s'exposeraient à des difficultés d'interprétation et d'utilisation.
À défaut d'utiliser les fiches S, les élus auraient besoin d'accéder à d'autres données. Celles contenues dans le fichier des auteurs d'infractions terroristes leur sont déjà, théoriquement, accessibles, sur le fondement de l'article 706-25-9 du Code de procédure pénale. Néanmoins, en pratique, peu d'élus connaissent cette faculté. De plus, le fichier ne contient pas les éléments relatifs à l'apologie du terrorisme, à la consultation habituelle de sites djihadistes (même si les condamnations sont rares sur ce fondement), et, en principe, aux mineurs de 13 à 18 ans.
La question demeure entière pour les personnes non condamnées et présentant un risque. Certaines communes bénéficient de l'aide des préfectures, certaines seulement. La circulation de l'information est trop disparate. Une clarification des procédures et des obligations répondrait à un véritable besoin qui s'exprime encore plus en situation de crise.
Les rédacteurs suggèrent même la création d'un fichier spécialisé, un de plus, destiné aux exécutifs territoriaux, ou le développement d'enquêtes administratives au moment de l'embauche de certains personnels. La question de la faisabilité demeure cependant entière.
Rien ne pourra se faire sans moyens financiers. Or, malgré l'augmentation substantielle du Fonds Interministériel de Prévention de la Délinquance et de la Radicalisation (CIPDR), la part affectée à la prévention de la radicalisation demeure insuffisante. Les sénateurs plaident donc

en faveur d'une augmentation de ce poste, tout en facilitant l'accès des petites et moyennes communes à ces financements.

Directeur de publication :	Colonel Laurent Vidal
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 Xavier Leonetti Gilles Hilary
Equipe éditoriale :	Odile NETZER