La veille juridique

N°71, octobre 2018

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

Edito

Le CREOGN est sur de nombreux fronts ! Il y a quelques jours, les 17 et 18 octobre 2018, il a contribué au lancement à la Rochelle du Charente-Maritime Cybersécurité (CMCS), à l'occasion du mois de la cybersécurité. Puis il est intervenu au sein des écoles militaires de Saumur sur les enjeux de défense et de sécurité liés à la transformation numérique. Dans quelques jours, avec la complicité des professeurs François Dieu et Xavier Latour, il coorganisera avec l'université de Papeete un colloque sur la spécificité de la gendarmerie dans cette France lointaine. Puis il animera les « Conversations de Gouvieux », rendez-vous annuel sur le thème de la défense organisé par le Centre d'étude et de prospective stratégiques (CEPS). Viendra ensuite l'Agor@ parlementaire du FIC sur la

(Suite page 2)

EDITORIAL

Blockchain qui aura lieu, le 29 novembre 2018, à la Maison de la Chimie. Le 12 décembre 2018, un Atelier de recherche sera consacré au thème « les TPE et PME, les oubliées de la cybersécurité » qui préfigurera un atelier du FIC organisé avec la région de gendarmerie des Hauts-de-France et le concours de la réserve cyberdéfense. Lors du FIC (les inscriptions sont ouvertes sur forum-fic.com), le CREOGN organisera l'Agor@ PhilosoFIC sur le thème « Réseaux sociaux, je t'aime moi non plus ! », l'occasion de faire le point sur la régulation des contenus qui s'organise, notamment dans le cadre d'un futur règlement européen. Le prisme des nouvelles technologies ne nous fait pas oublier d'autres sujets, notamment l'appropriation territoriale avec l'étude attendue sur l'impact du Canal Seine-Nord sur la gendarmerie.

Il y a quelques jours, nous nous sommes réunis à Aix-en-Provence, avec le centre de recherche de l'ENSP et avec celui de l'École nationale supérieure des officiers de sapeurs-pompiers. De nombreux sujets d'intérêt nous sont communs et devraient déboucher sur un renforcement de notre coopération. Elle est aussi en mouvement avec le réseau de recherche animé par le pôle sécurité-défense du CNAM.

Comme vous pouvez le constater, le CREOGN est toujours plus actif et devrait renforcer ses capacités avec l'arrivée prochaine d'une secrétaire générale.

Bonne lecture de cette veille juridique ! Lors du CMCS, j'ai pu constater que nos publications étaient lues sur le terrain, un militaire de la gendarmerie ayant actualisé sa présentation des cyberattaques avec des informations tout juste livrées par nos soins…

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

VEILLE JURIDIQUE DE LA GENDARMERIE NATIONALE

Page 3

Sommaire

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

Déontologie et sécurité

Par M. Frédéric Debove

Dialoguez, dialoguez, il en restera toujours quelque chose !

Vingt fois sur le métier, remettez votre ouvrage : *Polissez-le sans cesse et le repolissez*… À l'instar du travail de l'écrivain si bien décrit par le poète Nicolas Boileau, la tâche du déontologue est sans fin ! mais puisque la pédagogie consiste dans l'art de la répétition, efforçons-nous inlassablement de distinguer le bien du mal dans les pratiques policières au regard des règles déontologiques professionnelles qui encadrent l'action des forces de l'ordre.

Les deux précédentes veilles (juin et septembre 2018) se rapportaient à des arrêts de la Cour de Strasbourg condamnant l'État français à la suite du décès d'un individu constaté dans le prolongement d'un contrôle routier (CEDH, *Toubache c/ France*, 7 juin 2018 et CEDH, *Semache c/ France*, 21 juin 2018). Cette première veille automnale est pour sa part consacrée à une **décision (2018-155) du Défenseur des droits en date du 29 mai 2018**, mais dont la diffusion est intervenue avec retard. Là encore, l'affaire a trait au décès d'un individu agité au moment de son interpellation par les forces de l'ordre. Sans présager des suites judiciaires apportées à ce dossier, la décision du Défenseur des droits est riche d'enseignements en considération des multiples manquements déontologiques mis au jour par les investigations menées par cette autorité administrative indépendante, de rang constitutionnel.

Déontologie et sécurité

Ils m'entraînent au bout de la nuit, les démons de minuit !

Le 5 mars 2015, peu avant minuit, M. X s'installe seul à une table en face du comptoir dans un bar. Dans un premier temps, le barman de l'établissement comme le vigile considèrent ce client comme tout à fait normal et cordial. Dans un second temps, les intéressés se voient contraints de solliciter la police, car l'intéressé change soudainement de comportement en se mettant à tenir des propos incohérents, à pousser des cris et à souffrir de tremblements étranges. À l'occasion de son appel au 17, le barman précise à l'attention de son interlocuteur que « *l'individu qui refuse de quitter son établissement n'est pas alcoolisé mais plutôt paniqué, dérangé et semble souffrir de problèmes psychiatriques* ». Traité par un brigadier de police en sa qualité d'opérateur du centre d'information et de commandement, cet appel est alors transmis à l'opérateur de la salle de commandement du commissariat local par l'intermédiaire de la salle de commandement du district, comme il est d'usage de procéder. Toutefois, à l'occasion de ces transmissions en cascade, la requête initiale devient le message suivant (« *Vous pouvez vous rapprocher du bar Y, apparemment un client qui fait un gros scandale, les clients ont peur de sortir* ») au moment où elle communiquée à l'équipage de police secours requis de se transporter sur place.

Aux alentours de minuit, l'équipage de police composé de trois fonctionnaires en tenue d'uniforme pénètre dans le bar. En considération de l'état d'agitation et des propos incohérents du client indésirable, les policiers comprennent rapidement que l'intéressé ne jouit pas de toutes ses facultés mentales et se trouve en état de délire. À l'instant où les fonctionnaires de

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

Déontologie et sécurité

police décident de procéder à l'interpellation de l'individu agité en vue d'une conduite à l'infirmerie psychiatrique de la préfecture de police, l'intéressé résiste avec force et véhémence à son menottage à telle enseigne que des effectifs sont appelés en renfort. Au plus fort de cette opération de police, cinq équipages (police-secours et BAC) se trouvent ainsi sur place. La parfaite maîtrise du client souffrant de troubles mentaux réclame alors divers gestes techniques d'intervention professionnelle : étranglement arrière, clé de bras amenée au sol, menottage en avant puis enfin menottage en arrière, pose d'un serflex au niveau des jambes, étant observé que l'immobilisation de l'individu se double pendant quelques minutes d'un « décubitus ventral » (l'individu étant plaqué face contre terre pendant qu'un policier plaçait son genou et ses mains en appui au niveau des lombaires et des omoplates pour éviter tout retournement de la personne interpellée). Une fois maîtrisé, en état d'inconscience ou d'épuisement, le client du bar est transporté horizontalement par sept fonctionnaires de police dans le fourgon de police. S'agissant du positionnement de l'individu interpellé pendant le trajet, les déclarations recueillies par le Défenseur des droits divergent très sensiblement. Certains policiers font état d'un positionnement sur le flanc durant l'intégralité du trajet tandis que d'autres font état d'une installation en position ventrale au cours du transport. Au moment de l'arrivée du fourgon devant le commissariat de police, l'équipage constate l'inconscience de la personne interpellée puis, dans un second temps, son absence de pouls. Le médecin des sapeurs-pompiers, dont l'intervention avait été naturellement requise par l'opérateur radio de la salle de commandement, constatera le décès de l'intéressé le 6 mars à 2h30, soit un peu plus de deux heures après l'arrivée du fourgon au commissariat.

Déontologie et sécurité

Aussitôt après le décès de M. X, une procédure judiciaire du chef d'homicide involontaire était diligentée par le procureur de la République territorialement compétent tandis qu'une procédure administrative était engagée parallèlement. Selon les conclusions du rapport médico-légal de synthèse établi en août 2015, « *M. X était décédé d'un œdème pulmonaire majeur résultant de l'association d'une asphyxie mécanique par traumatismes cervical et laryngé et d'un intoxication à la cocaïne* ». En novembre 2015, la procédure judiciaire était classée sans suite mais, après le dépôt d'une plainte avec constitution de partie civile, une information judiciaire était ouverte sur le fondement du crime de violences mortelles et du délit de non-assistance à personne en danger (instruction toujours en cours au moment de la rédaction de cette présente chronique). En juin 2016, l'enquête administrative donnait lieu, pour sa part, à un classement aux motifs « *qu'aucun manquement déontologique ou faute professionnelle ne pouvait être reproché aux policiers intervenus, ni au cours de l'interpellation, ni lors du placement dans le car de police, ni lors de la conduite au poste, ni dans la gestion des faits lorsque l'insuffisance respiratoire a été constatée* ».

Les paroles s'envolent mais les écrits ... manquent d'encre

Après s'être saisi d'office des circonstances funestes de la présente affaire, le Défenseur des droits a relevé plusieurs manquements aux règles déontologiques professionnelles qui gouvernent l'action des forces de l'ordre. De ces constatations découlent de nombreuses recommandations générales ou individuelles.
À titre liminaire, le Défenseur des droits constate avec regret que

Déontologie et sécurité

les fonctionnaires de police impliqués dans l'interpellation litigieuse n'avaient pas eu connaissance de la note du 8 octobre 2008 relative aux prescriptions de l'Inspection générale de la police nationale (IGPN) en matière d'usage de la force. Alors même que le Préfet de police de Paris en avait été rendu destinataire, ladite note n'avait pas été diffusée à l'ensemble des directions et services placés sous son autorité. Rédigée dans le prolongement d'un avis de l'ancienne Commission nationale de déontologie de la sécurité (avis n° 2007-83 du 14 avril 2008), cette note énonçait que « *lorsque l'immobilisation de la personne est nécessaire, la compression – tout particulièrement lorsqu'elle s'exerce sur le thorax ou l'abdomen – doit être la plus momentanée possible et relâchée dès que la personne est entravée par les moyens réglementaires et adaptés. Ainsi (...) l'immobilisation en position ventrale doit être la plus limitée possible, surtout si elle est accompagnée du menottage dans le dos de la personne allongée. Il en est de même, a fortiori, pendant le transport des personnes interpellées* ». En complément de cette première prescription, la note de l'IGPN précisait que « *préalablement à toute intervention estimée périlleuse, mettant notamment en cause une personne dangereuse pour elle-même ou pour autrui, l'information d'un médecin régulateur (centre 15) doit être systématique. C'est à lui qu'il reviendra de décider de la pertinence de l'envoi d'une équipe médicale sur place* ».
En considération des carences constatées dans la diffusion de cette note (depuis lors remplacée par une instruction du 4 novembre 2015 du directeur général de la police nationale) essentielle en termes de pratiques professionnelles, le Défenseur des droits recommande que les prescriptions qu'elle énonce soient diffusées à l'ensemble des services de police et que l'attention des destinataires soit particulièrement attirée sur les instructions dont elle est porteuse. Aussi, lorsqu'un équipage de

police est requis d'intervenir dans des circonstances impliquant une personne présentant des troubles susceptibles de compliquer sa maîtrise, il convient impérativement de procéder systématiquement à l'information d'un médecin régulateur (centre 15 ou 112) ou du centre d'appel des pompiers (18) à qui il reviendra de décider de l'opportunité de dépêcher une équipe médicale sur place.

L'information c'est le pouvoir !

Si l'information est en effet le pouvoir, c'est à la condition d'être fiable, précise et non tronquée. Toute information parcellaire transmise par un opérateur radio à un équipage de police constitue immanquablement un manque de rigueur dont les conséquences peuvent être lourdement préjudiciables en certaines circonstances. Après avoir relevé que l'équipage primo-intervenant n'avait pas été informé par sa station directrice que le client du bar souffrait visiblement de troubles mentaux (alors même que l'appel 17 police-secours avait apporté cette précision), le Défenseur des droits recommande que soit rappelée à l'ensemble des opérateurs radio la nécessité de répercuter l'intégralité des informations qui leur sont transmises par les opérateurs de la salle de commandement et d'information. De façon plus générale, le Défenseur des droits recommande que l'ensemble des opérateurs radio – qu'ils interviennent au sein d'un centre d'information et de commandement ou au sein d'une salle de commandement d'un commissariat – reçoivent tous une formation adaptée à leurs fonctions (formation des opérateurs CIC ou SIC).

De bonnes paroles valent mieux que de mauvais coups

Appelé à se prononcer sur l'opportunité du recours initial à la force par l'équipage primo-intervenant, le Défenseur des droits fait ensuite le constat que l'intervention des policiers témoigne d'un manque évident de dialogue. À l'argument avancé par les policiers selon lequel tout dialogue est impossible en présence d'un individu dangereux, menaçant et déséquilibré mental, le Défenseur des droits rétorque que c'est précisément au regard du fait que M. X tenait des propos incohérents que le dialogue aurait dû être davantage employé, « *un contact verbal permettant d'instaurer un climat de confiance et de désamorcer un comportement agressif, tout en évitant de recourir à la force* ». Conséquence logique du constat de l'insuffisant dialogue engagé avec M. X, le Défenseur des droits considère que l'usage de la force auquel l'équipage a procédé n'était pas nécessaire dans les circonstances de l'espèce. Il s'ensuit un manquement aux dispositions de l'article R. 434-18 du Code de déontologie de la sécurité intérieure. Par-delà ce manquement imputable à l'équipage primo-intervenant, le Défenseur des droits recommande de privilégier systématiquement le dialogue en présence d'une personne en état d'agitation, peu importe l'origine de cette agitation (état alcoolique, prise de produits stupéfiants, troubles psychiatriques, etc.). Le Défenseur des droits recommande en outre qu'un module obligatoire soit intégré à la formation des fonctionnaires de police en considération du nombre important d'affaires se rapportant au décès de personnes appréhendées en état d'agitation dont il a eu à connaître.

La théorie des fruits de l'arbre empoisonné

En droit pénal, l'onde des nullités de procédure n'affecte pas seulement l'acte entaché d'irrégularité. Elle affecte également tous les actes subséquents qui puisent leur fondement dans l'acte irrégulier. C'est la fameuse théorie des fruits de l'arbre empoisonné. Faisant sienne cette théorie, le Défenseur des droits considère assez logiquement que toute la coercition en lien avec l'intervention de l'équipage primo-intervenant ou subséquente à celle-ci ne répondait pas au double impératif de nécessité et de proportionnalité inscrit à l'article R. 434-18 du Code de déontologie de la sécurité intérieure. À l'exception de l'amenée au sol, sont ainsi tour à tour stigmatisés la plupart des gestes de contrainte et d'immobilisation sur M. X lors de l'intervention dans le bar, et tout singulièrement le maintien prolongé en positionnement ventral (également appelé « decubitus ventral ») doublé d'une prise d'étranglement au sol. Identifiée à plusieurs reprises comme hautement dangereuse pour la vie par le Défenseur des droits (décision n° 2009-207), la Cour européenne des droits de l'Homme (CEDH, *Saoud c/ France,* 9 octobre 2007 ; CEDH, *Boukourou c/ France*, 16 novembre 2017) ou bien encore le Comité européen pour la prévention de la torture et des peines ou traitements inhumains ou dégradants, cette technique d'immobilisation en position ventrale doit être la plus limitée, surtout si elle est accompagnée du menottage dans le dos de la personne appréhendée. Maintenir une personne appréhendée pendant près de 6 minutes en position de « decubitus ventral » caractérise, selon l'appréciation du Défenseur des droits, un manque de discernement en même temps qu'un usage non nécessaire de la force justifiant l'engagement de poursuites

disciplinaires à l'encontre de son auteur. Par-delà le fonctionnaire de police responsable de l'immobilisation au sol, le Défenseur des droits considère que l'ensemble des policiers intervenants ont manqué à leurs obligations déontologiques de discernement et de protection à l'égard d'une personne placée sous leur responsabilité. En effet, le changement d'attitude de M. X entre le début de l'intervention et son transport dans le fourgon de police aurait dû susciter une vigilance accrue de la part des policiers sur l'état de santé et de conscience de l'intéressé. Enfin, *last but not least*, le Défenseur des droits fustige toutes les étapes de la prise en charge médicale de M. X à compter de son arrivée au commissariat. La mise en oeuvre des gestes de premiers secours est ainsi jugée déplorable : si la personne appréhendée et inconsciente a certes été placée en position latérale de sécurité, aucun geste de réanimation n'a été tenté et le commissariat n'était pas davantage équipé d'un défibrillateur. De surcroît, les informations délivrées aux pompiers par l'opérateur radio n'étaient pas suffisamment précises et circonstanciées sur la gravité de l'état de santé de M. X (s'agissant singulièrement de l'absence de pouls) pour assurer une prise en charge optimale par les secours.

En même temps qu'il recommande *in fine* des actions de formation aux gestes de premiers secours et l'équipement des commissariats en défibrillateurs, le Défenseur des droits conclut sa décision par un constat global de carence à tous les niveaux de la chaîne d'intervention : au niveau de la transmission des informations aux équipages de police sollicités pour intervenir, au niveau de l'intervention dans le bar, au niveau du transport dans le car et enfin au niveau de la mise en oeuvre des gestes de premiers secours au commissariat de police. Un contraste saisissant avec les conclusions de l'enquête administrative qui

Déontologie et sécurité

avait conclu, pour sa part, à l'absence de tout manquement déontologique ou faute professionnelle à l'encontre des policiers intervenants. Vérité en-deçà des Pyrénées, erreur au-delà … Ce qui vaut pour un peuple selon Pascal vaut assurément pour la déontologie de la sécurité !

Droit de l'espace numérique

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

Cour de justice de l'Union européenne (CJUE), Grande chambre, C-207-16, arrêt du 2 octobre 2018, Ministerio fiscal

L'accès par des autorités publiques aux données visant à l'identification des titulaires des cartes SIM activées avec un téléphone mobile volé, telles que les nom, prénom et, le cas échéant, adresse de ces titulaires, ne présente pas une gravité telle que cet accès devrait être limité, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, à la lutte contre la criminalité grave.

L'affaire concerne un ressortissant espagnol qui a déposé une plainte auprès de la police pour un vol avec violence, survenu en février 2015, au cours duquel il a été blessé et son portefeuille et son téléphone mobile ont été dérobés. Les enquêteurs ont alors demandé au juge d'instruction de les autoriser à ordonner à divers fournisseurs de services de communications électroniques la transmission des numéros de téléphone activés, entre le 16 février et le 27 février 2015, avec le code relatif à l'identité internationale d'équipement mobile (code IMEI) du téléphone mobile volé. Étaient également demandées les données à caractère personnel relatives à l'identité civile des titulaires ou des utilisateurs des numéros de téléphone correspondant aux cartes SIM activées avec ce code, telles que leurs nom, prénom et, le cas échéant, adresse.
Mais le juge d'instruction a rejeté cette demande qu'il n'estimait pas utile à l'identification des auteurs de l'infraction. Il a surtout

motivé son refus en considérant que le droit espagnol limitait ce type d'investigations aux faits graves, c'est-à-dire pour des peines privatives de liberté encourues supérieures à cinq ans.

La CJUE saisie de deux questions préjudicielles

Le ministère public espagnol a introduit un recours contre cette décision. L'Audiencia Provincial de Tarragona (cour provinciale de Tarragone) a décidé de surseoir à statuer et de poser à la CJUE les questions préjudicielles suivantes :

1)Est-il possible de déterminer la gravité suffisante des infractions, en tant que critère justifiant l'atteinte aux droits fondamentaux reconnus aux articles 7 et 8 de la Charte, uniquement en prenant en considération la peine dont peut être punie l'infraction faisant l'objet d'une enquête ou est-il nécessaire, en outre, d'identifier dans le comportement délictueux un caractère préjudiciable particulier pour des intérêts juridiques individuels ou collectifs ?

2) Le cas échéant, s'il était conforme aux principes fondamentaux de l'Union appliqués par la Cour dans son arrêt du 8 avril 2014 (Digital Rights Ireland e.a., C 293/12 et C 594/12) en tant que normes de contrôle strict de la directive 2002/58, de déterminer la gravité de l'infraction uniquement en fonction de la peine susceptible d'être infligée, quel devrait être le niveau minimal de cette peine ? Un niveau fixé de manière générale à un minimum de trois ans serait-il conforme ? »

La réponse de la CJUE

La CJUE rappelle que la directive 2002/58 régit, en vertu de son article 1er, paragraphe 1, et de son article 3, tout traitement de données à caractère personnel dans le cadre de la fourniture de services de communications électroniques. En outre, conformément à l'article 2, second alinéa, sous b), de cette directive, la notion de « données relatives au trafic » couvre « toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques et sa facturation ».
S'agissant de l'article 15, paragraphe 1, de la directive 2002/58, la Cour a déjà jugé que les mesures législatives visées par cette disposition relèvent du champ d'application de cette directive. Et ce, même si elles se rapportent à des activités propres aux États ou aux autorités étatiques, étrangères aux domaines d'activité des particuliers, et même si les finalités auxquelles de telles mesures doivent répondre recoupent substantiellement les finalités poursuivies par les activités visées à l'article 1er, paragraphe 3, de la directive 2002/58.

Dans un arrêt récent du 21 décembre 2016 (*Tele2 Sverige et Watson e.a.*, C 203/15 et C 698/15), la Cour a jugé qu'en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, seule la lutte contre la criminalité grave est susceptible de justifier un accès des autorités publiques à des données à caractère personnel conservées par les fournisseurs de services de communications qui, prises dans leur ensemble, permettent de tirer des conclusions précises concernant la vie privée des personnes dont les données sont concernées. La Cour

a toutefois exigé que l'objectif poursuivi par une réglementation régissant cet accès soit en relation avec la gravité de l'ingérence dans les droits fondamentaux en cause que cette opération entraîne. En vertu du principe de proportionnalité, une ingérence grave ne peut être justifiée, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, que par un objectif de lutte contre la criminalité devant également être qualifiée de « grave ».

Dans les circonstances de l'espèce, la CJUE ne statue pas sur la durée de la peine encourue. Elle considère que « l'article 15, paragraphe 1, de la directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009, lu à la lumière des articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens que l'accès d'autorités publiques aux données visant à l'identification des titulaires des cartes SIM activées avec un téléphone mobile volé, telles que les nom, prénom et, le cas échéant, adresse de ces titulaires, comporte une ingérence dans les droits fondamentaux de ces derniers, consacrés à ces articles de la Charte des droits fondamentaux. Mais cet accès ne présente pas une gravité telle justifiant une limitation à la lutte contre la criminalité grave, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales.

Cour européenne des droits de l'Homme, arrêt (n° 58170/13, 62322/14 et 24960/15) Big Brother Watch et autres c. Royaume Uni, 13 septembre 2018

La mise en œuvre d'un système de surveillance massive n'est pas en soi attentatoire à la Convention de sauvegarde des droits de l'Homme et des libertés fondamentales.

La Cour européenne des droits de l'Homme (CEDH) examine les conditions dans lesquelles le Royaume-Uni a mis en place un système de surveillance massive au bénéfice de ses services de renseignement. Sa saisine s'inscrit dans le contexte des retombées de l'affaire PRISM, révélée par Edward Snowden, et de la multiplication des techniques intrusives liée à la lutte contre le terrorisme.

Déjà, en juin 2018, elle avait conclu que la législation et la pratique suédoises dans le domaine du renseignement électromagnétique n'emportaient pas violation de la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales (*Centrum För Rättvisa c. Suède,* arrêt du 19 juin 2018). Elle a considéré notamment que le système suédois, concernant tout usager de téléphonie mobile et d'Internet, offrait des garanties adéquates et suffisantes contre l'arbitraire et le risque d'abus. La Cour avait alors mis en exergue la légitimité de l'action de l'État en matière de sécurité nationale. Elle reconnaît, en effet, la gravité des menaces qui pèsent actuellement sur de nombreux État contractants, notamment le terrorisme international et les autres infractions graves (trafic de stupéfiants, traite d'êtres

humains, exploitation sexuelle d'enfants, cybercriminalité). Elle prend également acte du fait que les avancées technologiques permettent plus facilement aux terroristes et aux criminels d'agir masqués sur Internet. Un État peut donc utiliser un système d'interception massive s'il l'estime nécessaire dans l'intérêt de la sécurité nationale.

Dans le cas d'espèce, la CEDH est saisie par Big Brother Watch, une organisation de défense des libertés civiles et de la vie privée, ainsi que par des journalistes qui contestent la légalité de trois régimes de surveillance institués au Royaume-Uni : l'interception massive de communications électroniques, le partage de renseignements avec des États étrangers et l'obtention de données de communications auprès de fournisseurs de services.

C'est la première fois que la Cour porte son regard sur l'interception et l'exploitation de données de communication (à distinguer des données de contenus). Il en est de même du partage de renseignements, c'est-à-dire de la manière dont les autorités demandent et reçoivent des renseignements d'origine électromagnétique de la part d'États étrangers.

Conformément à sa jurisprudence, la Cour juge que l'utilisation d'un système d'interception massive n'emporte pas en soi violation de la Convention.

Mais sa mise en œuvre doit être accompagnée de garanties. Le droit national doit préciser la nature des infractions susceptibles de donner lieu à une interception, les catégories de personnes susceptibles d'être concernées, la durée maximale de l'interception, les modalités exigées pour l'examen, l'utilisation, la conservation, l'effacement ou la destruction des données recueillies. Doivent être également explicitées les règles présidant à la communication des données à d'autres États.

Au regard de la loi britannique applicable au moment de sa

saisine (le Royaume-Uni a adopté une nouvelle législation en 2016 sur les pouvoirs d'enquête), la Cour, tout en délivrant un satisfecit aux services de Sa Majesté, conclut à la violation des articles 8 (droit au respect de la vie privée, protection des données à caractère personnel) et 10 (droit à la liberté d'expression, en particulier des journalistes) de la Convention européenne de sauvegarde des droits de l'Homme et des libertés individuelles.

S'agissant des données de communication, la Cour fait référence à la jurisprudence de la Cour de justice de l'Union européenne (CJUE) (arrêts *Digital Rights Ireland* C-293/12 et C-594/12, et *Tele2 Sverige* C-2013/15 et C-698/15). L'accès aux métadonnées de communication doit être strictement nécessaire à la réalisation de l'objectif poursuivi. Dans le cas de la lutte contre la criminalité, il doit être limité à la lutte contre les infractions graves. La CEDH ajoute que la CJUE « a en outre suggéré que l'accès à l'information soit soumis à un examen préalable par un tribunal ou une autorité administrative indépendante, et que les données concernées devraient être conservées dans l'Union européenne ». État de l'Union européenne, le Royaume-Uni doit respecter, dans son droit national, le principe de la primauté du droit européen sur le droit interne.

Le droit interne britannique, tel qu'interprété par les autorités nationales à la lumière des récents arrêts de la CJUE, exige que tout régime permettant aux autorités d'accéder aux données conservées par les services de communication limite l'accès au but de combattre les « infractions graves ». Cet accès doit être soumis à un contrôle préalable par un tribunal ou un organe administratif indépendant. Le régime du chapitre II de la loi portant réglementation des pouvoirs d'enquête[1] autorise l'accès

1. Regulation of Investigatory Powers Act 2000, 1er août 2000.

aux données conservées aux fins de la lutte contre la criminalité et, sauf dans le cas où l'accès est demandé pour déterminer la source du journaliste, il n'est pas soumis à un contrôle préalable par un tribunal ou un organe administratif indépendant. Il ne peut donc être conforme à la loi au sens de l'article 8 de la Convention. Si la Cour constate que la Commission des pouvoirs d'enquête, organe spécialement chargé au Royaume-Uni d'examiner les plaintes pour surveillance secrète, offre à présent un recours dont les requérants doivent se prévaloir aux fins de l'épuisement des voies de recours internes et de l'examen de recevabilité, tel n'est pas le cas pour la période visée par le recours.
S'agissant de la France, l'affaire « Association confraternelle de la presse judiciaire c. France et 11 autres requêtes » est pendante devant la CJUE. Elle fait suite à des requêtes introduites par des avocats et des journalistes, ainsi que par des personnes morales en lien avec ces professions, au sujet des mesures de surveillance par des moyens électroniques contenues dans la loi française du 24 juillet 2015 relative au renseignement.

Cour de cassation, Chambre sociale (N° 16-11690), 12 septembre 2018, Mme X/ Mme Y

Ne constituent pas une faute grave justifiant un licenciement les propos injurieux tenus sur un compte Facebook qui n'est accessible qu'à un nombre limité de personnes.

Madame Y. est salariée d'une agence immobilière. Ayant tenu des propos injurieux et offensants à l'égard de son employeur

par le biais d'un groupe dénommé « Extermination des directrices chieuses » du réseau social Facebook, elle fait l'objet d'une procédure de licenciement pour faute grave. Après la juridiction prud'hommale, c'est la Cour d'appel de Paris qui a statué sur le licenciement en considérant ce licenciement pour faute grave dépourvu de cause réelle et sérieuse.
Cet arrêt est contesté par la partie adverse qui considère que caractérise une faute grave, la seule diffusion, publique ou privée, par le salarié sur le réseau social Facebook, de propos injurieux et humiliants à l'encontre de son employeur. La Cour d'appel, selon elle, aurait dû au moins constater que ces propos étaient constitutifs d'une cause réelle et sérieuse de licenciement.
La Cour de cassation confirme la position des juges d'appel. Les propos tenus par Mme Y. n'ont été accessibles qu'à un groupe fermé de personnes peu nombreuses, composé de quatorze personnes, agréées par elle, de sorte qu'ils relèvent d'une conversation de nature privée non constitutive de faute grave. Selon la Haute juridiction, la Cour d'appel a fait une juste appréciation de l'article L. 1235-1 du Code du travail, en décidant que le grief ne constituait pas une cause réelle et sérieuse de licenciement.

CNIL - Délibération de la formation restreinte n° SAN-2018-009 du 6 septembre 2018 prononçant une sanction pécuniaire à l'encontre de la société Assistance Centre d'Appels

La société incriminée exerce une activité de télésurveillance d'ascenseurs et de parkings. Elle emploie 14 personnes dont 13 téléopérateurs. L'affaire débute avec une plainte relative à la

mise en place d'un dispositif de vidéosurveillance/ vidéoprotection dans ses locaux. La Commission nationale de l'informatique et des libertés (CNIL) opère en novembre 2016 une mission de contrôle. Sur place, les agents de la CNIL vont additionner les découvertes :

- un dispositif de pointage biométrique à des fins de contrôle des horaires des salariés est mis en œuvre, sans autorisation de la CNIL ;
- un dispositif d'enregistrement des appels téléphoniques est installé sans que les salariés en soient informés ;
- l'identité du responsable du traitement et le droit d'opposition dont ils disposent ne sont pas connus des interlocuteurs lors d'un appel entrant ;
- la gestion des mots de passe n'est pas conforme aux règles qui s'y rapportent.

Par mise en demeure en date du 26 juillet 2017, la présidente de la CNIL enjoint à la société, sous un délai de trois mois :

- de ne collecter et traiter que des données adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs et, en particulier, de cesser d'utiliser le dispositif biométrique de reconnaissance de l'empreinte digitale pour contrôler les horaires des salariés et supprimer toutes les

données qui ont été collectées par un tel dispositif ;

- de procéder à l'information des personnes concernées et notamment des salariés (notamment sur leur droit d'opposition à l'enregistrement) ;
- de prendre toutes mesures pour garantir la sécurité et la confidentialité des données à caractère personnel.

S'ensuit une succession d'échanges qui souligne la patience de la CNIL. La décision, notifiée à la société le 31 juillet 2017, fait l'objet d'une réponse en octobre, par laquelle celle-ci précise que le dispositif de pointage par code n'est plus opérationnel et que les données enregistrées sont purgées régulièrement. Considérant que ce courrier ne répond pas à une demande de compléments du 21 novembre 2017, la Présidente de la CNIL adresse un courrier de relance à la société le 12 janvier 2018. Insatisfaite de la réponse, elle envoie sur place une mission de contrôle en mars 2018. La délégation constate alors que le dispositif biométrique permettant le contrôle des horaires des salariés est toujours installé et qu'aucune mesure de sécurité n'a été mise en place sur leurs postes de travail . En outre, sont enregistrées au sein du logiciel les traces de pointage par empreinte digitale relevées entre le 30 août 2011 et le 28 mars 2018. S'ajoutent les défauts d'information relative à leurs droits des personnes, appelants ou salariés.
Considérant que les manquements constatés ont persisté après l'expiration du délai imparti dans la mise en demeure, la Présidente de la Commission saisit la commission restreinte de la CNIL en vue de prononcer une sanction.
S'appuyant sur les dispositions de la loi en vigueur au moment

des faits (avant la mise en application du Règlement général sur la protection des données), la formation restreinte prononce une sanction pécuniaire de 10 000 euros (le chiffre d'affaires de l'entreprise est de 816 691 euros en 2017) pour recours à des données biométriques sans justifier des circonstances exceptionnelles, manquement à l'obligation d'informer les personnes ainsi qu'à l'obligation d'assurer la sécurité et la confidentialité des données.
En raison de la persistance des faits reprochés durant 15 mois, malgré les nombreuses diligences effectuées par les services de la CNIL, la formation restreinte décide de rendre publique sa décision.

Par Mme Claudia Ghica-Lemarchand

FRAUDE FISCALE – LOI N° 2018-898 DU 23 OCTOBRE 2018 RELATIVE A LA LUTTE CONTRE LA FRAUDE

La loi relative à la lutte contre la fraude a été publiée au JO du 24 octobre 2018. Elle tend à mettre en œuvre le principe fondamental de contribution de chacun aux charges publiques à hauteur de ses facultés, qui est un des piliers de notre organisation sociale. Si l'erreur est admissible, si le Gouvernement doit faire des efforts pour mieux expliquer et faire accepter les charges, la loi s'articule autour de trois idées – mieux détecter, appréhender et sanctionner la fraude.
Le premier titre renforce les moyens de lutte et facilite les échanges de données entre les administrations concourant à la lutte contre les fraudes fiscales, sociales et douanières et la transmission d'informations par les plateformes d'économie collaborative. L'article 28-2 du Code de procédure pénale, relatif aux pouvoirs de police spéciale attribués aux agents des services fiscaux, est modifié pour permettre d'affecter des officiers fiscaux judiciaires au sein du ministère chargé du budget, complémentairement aux moyens dont dispose la police judiciaire du ministère de l'Intérieur. Cela renforcera les outils de l'État pour détecter et déjouer les fraudes les plus complexes. La loi renforce aussi les moyens dont disposent les agents des douanes pour lutter contre les logiciels dits « permissifs », conçus pour permettre et dissimuler la fraude, à l'instar de ceux dont bénéficient déjà les agents de la direction générale des finances publiques. Les agents des douanes pourront ainsi se faire communiquer par

les éditeurs, concepteurs, distributeurs ou toute personne susceptible de manipuler les logiciels, le code source et la documentation des logiciels qu'ils proposent. L'article prévoit également un dispositif d'amende de 15 % du chiffre d'affaires pour les infractions relevées dans ce cadre. La loi permet aussi de croiser les données et déclarations contenues dans les fichiers auxquels les agents du fisc auront désormais accès largement, puisque le texte vise les « fichiers, copies de fichiers nécessaires à la réalisation des traitements et résultats de traitements réalisés mis à disposition ou remis par le contribuable », le résultat de la comparaison lui étant opposable.

Elle ouvre également l'accès de certains fichiers à des agents de l'inspection du travail, des unions de recouvrement des cotisations de sécurité sociale et d'allocations familiales (URSSAF) et de la caisse de la mutualité sociale agricole (MSA), spécialisés dans la lutte contre le travail illégal. Elle rend destinataires des informations contenues dans le Répertoire national commun de la protection sociale (RNCPS) certains agents de l'inspection du travail et officiers et agents de police judiciaire. La loi précise aussi les obligations fiscales et sociales imposées aux plateformes d'économie collaborative (obligation d'information des utilisateurs depuis 2017, et de déclaration à l'administration des revenus réalisés par ces derniers à compter de 2019), afin d'assurer une meilleure intelligibilité de la loi pour les plateformes et une meilleure exploitabilité des données collectées par l'administration pour améliorer ses capacités de détection de la fraude. Le législateur saisit l'occasion pour introduire des dispositions spécifiques relatives aux abus de marché (article L. 621-10-2 du Code monétaire et financier) résultant du règlement européen du 16 avril 2014, mais aussi pour modifier le Code des douanes et le livre des procédures fiscales afin de

faciliter la remise de certaines données.

Le titre II est consacré au renforcement des sanctions en matière de fraude fiscale, sociale et douanière. La loi prévoit par défaut l'application de la peine complémentaire de publication et de diffusion des décisions de condamnation pour fraude fiscale, aujourd'hui prononcées de manière facultative par le juge répressif. Elle ne serait pas pour autant automatique, pour en assurer la conformité à la Constitution, et pourrait être écartée par décision motivée du juge. Le législateur crée plusieurs sanctions prenant en compte diverses situations. Une amende spéciale prend la forme d'une sanction administrative, exclusive des sanctions pénales, applicable aux personnes qui concourent, par leurs prestations de services, à l'élaboration de montages frauduleux ou abusifs. Elle vise à sanctionner les professionnels complices des manquements fiscaux et sociaux, qui portent une grave atteinte au principe d'équité entre les contribuables et cotisants, et aux règles de leur profession. Cette sanction serait assortie d'un recours juridictionnel effectif, garant des droits de la défense. La loi aggrave la répression pénale des délits de fraude fiscale en prévoyant que le montant des amendes puisse être porté au double du produit tiré de l'infraction pour les personnes physiques, et au décuple pour les personnes morales. Le volet de la coopération internationale et européenne est pris en compte, car le texte complète la liste française des États et territoires non coopératifs en matière fiscale afin qu'elle intègre celle adoptée par l'Union européenne en décembre 2017. Ainsi, les transactions effectuées depuis ou vers les États et territoires non coopératifs inscrits sur la liste européenne seront également soumises à des mesures fiscales dissuasives ainsi qu'à des obligations et contrôles renforcés, afin d'intensifier les moyens de la lutte contre la fraude et l'évasion fiscales.

Le titre III réforme la procédure de poursuite de la fraude fiscale et contient une des mesures les plus polémiques et emblématiques – l'assouplissement du monopole de l'administration fiscale, appelé « verrou de Bercy ». Le nouvel article L. 228 du livre des procédures fiscales prévoit un mécanisme d'articulation des poursuites entre l'administration fiscale et le procureur de la République. Sans préjudice des plaintes dont elle prend l'initiative, l'administration est tenue de dénoncer au procureur de la République les faits d'un montant des droits supérieur à 100 000 €, assortis de majorations de 40 %, 80 % ou 100 %. Dans ce cas, l'action publique pour l'application des sanctions pénales est exercée sans plainte préalable de l'administration. Cette déclaration obligatoire n'est pas applicable aux contribuables ayant déposé spontanément une déclaration rectificative. Pour les autres contentieux, les plaintes sont déposées par l'administration à son initiative, sur avis conforme de la commission des infractions fiscales. La nouvelle obligation de dénonciation n'empêche pas l'administration fiscale de conclure une transaction avec la personne. Par ailleurs, la loi permet d'appliquer, dans le cadre de la fraude fiscale, la procédure de comparution sur reconnaissance préalable de culpabilité et la convention judiciaire d'intérêt public créée par la loi du 9 décembre 2016 et figurant à l'article 41-1-2 du Code de procédure pénale.

LANCEUR D'ALERTE – CHAMBRE CRIMINELLE – 17 OCTOBRE 2018

L'arrêt rendu par la Chambre criminelle le 17 octobre 2018

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

revient sur la nature de la protection accordée aux lanceurs d'alerte et pose la question de son application éventuelle aux inspecteurs du travail.

En l'espèce, une inspectrice du travail a reçu anonymement sur sa boîte mail des messages contenant des documents confidentiels relatifs à une entreprise qui avaient été obtenus de façon clandestine. Elle a supprimé toute trace de ces messages, ce qui tend à prouver sa connaissance de la provenance frauduleuse de ces informations. Elle les a aussi communiquées au conseil national de l'inspection du travail et à diverses organisations syndicales. Elle a été condamnée, d'une part, pour recel, et d'autre part, pour violation du secret professionnel. Elle conteste sa responsabilité pénale doublement.

Le délit de recel ne serait pas constitué, car son correspondant lui a transféré des documents qui tendaient à prouver la commission d'infractions au sein de l'entreprise visée. À ce titre, il avait agi en tant que lanceur d'alerte. Puisque l'infraction d'origine disparaît, le recel, infraction de conséquence, disparaît aussi. Le délit de violation du secret professionnel ne pourrait pas plus lui être reproché, pour deux raisons qu'elles avaient déjà développées devant les juges du fond. D'une part, elle répondait aux critères de définition des lanceurs d'alerte et bénéficiait de la protection de l'article 122-9 du Code pénal issu de la loi du 9 décembre 2016. D'autre part, elle avait communiqué les documents qui lui semblaient nécessaires à l'exercice des droits de la défense dans l'hypothèse où un conflit l'opposerait à la société qui faisait entrave au contrôle exercé. Les juges du fond étaient restés sourds à ses arguments, notant qu'elle n'avait pas communiqué les informations au procureur de la République, ce qui prouvait qu'il n'y avait pas de certitude de commission d'une infraction, puisque la loi du 9 décembre 2016 n'introduisait pas une cause

d'irresponsabilité mais une simple protection fonctionnelle et qu'au moment où elle a utilisé les documents, aucun contentieux ne l'opposait ni à son employeur, ni à la société contrôlée pour qu'elle ait besoin de se défendre.
Sans répondre à ses arguments, la Cour de cassation annule (sans cassation) l'arrêt et renvoie pour qu'une application de la nouvelle règle de droit relative aux lanceurs d'alerte soit faite. En effet, la Chambre criminelle constate que la loi du 9 décembre 2016 instaurant la protection des lanceurs d'alerte est une loi de fond plus douce, puisqu'elle a instauré une nouvelle cause d'irresponsabilité pénale au bénéfice de la personne ayant porté atteinte à un secret protégé par la loi. Ainsi, la Cour de cassation apporte deux précisions intéressantes. D'une part, l'article 122-9 contient une disposition d'irresponsabilité pénale générale qui a vocation à exonérer la personne de sa responsabilité pénale et ne prévoit pas seulement une procédure de protection fonctionnelle. D'autre part, elle tire les conséquences de cette qualification juridique en permettant à toute personne, y compris un inspecteur du travail, d'en bénéficier. L'article 122-9 sera au centre de l'examen des juges de renvoi du point de vue des conditions particulières posées.

FICHIERS DE POLICE – RAPPORT D'INFORMATION N° 1335 – ASSEMBLÉE NATIONALE – 17 OCTOBRE 2018

Un rapport d'information sur les fichiers mis à la disposition des forces de sécurité a été déposé auprès de l'Assemblée Nationale par les députés Didier PARIS et Pierre MOREL-A-L'HUISSIER le

17 octobre 2018. La mission d'information était composée de 18 membres, intervenant moins de 10 ans après le précédent rapport sur ce sujet qui datait de 2009 (Batho-Benisti). Le périmètre de l'étude est large, incluant l'ensemble des services de police et de gendarmerie et ceux accomplissant des missions de renseignement ainsi que la Direction générale de la sécurité intérieure (DGSI), rattachée au ministère de l'Intérieur. Elle a ciblé non seulement les fichiers dont ces services ont la responsabilité, mais également ceux auxquels ils ont ou souhaiteraient avoir accès, y compris lorsque leurs finalités sont purement administratives (Sécurité sociale). Si le précédent rapport pointait un pourcentage alarmant de fichiers dépourvus de base légale, la pratique actuelle montre que les fichiers nationaux et locaux ont été régularisés, l'enjeu actuel majeur tenant à la protection des données personnelles plus qu'à la régularisation des fichiers. À ce titre, la mission souligne le rôle central de la Commission nationale de l'informatique et des libertés (CNIL) qui opère un contrôle *a priori* dans la création de tels fichiers, mais aussi *a posteriori* pour leur mise en œuvre. Les contrôles exercés depuis 2015 (une trentaine) ont conduit à deux mises en demeure et aucune sanction. Par conséquent, la mission propose de mieux associer les services de la CNIL en amont du dépôt officiel des demandes d'avis sur les actes réglementaires de création des fichiers, de façon à résoudre les difficultés juridiques ou techniques susceptibles de se poser. Néanmoins, il y aurait maintien du régime dérogatoire des fichiers intéressant la sécurité de l'État, la défense ou la sécurité publique.

Les trois fichiers qui retiennent l'attention sont soumis à un double contrôle de la CNIL et des magistrats (magistrats du Parquet territorialement compétent et magistrats référents pour

l'ensemble du territoire). De surcroît, ils peuvent aussi faire l'objet d'un contrôle juridictionnel au regard des différentes normes qui les régissent aussi bien au plan national – Conseil constitutionnel, Conseil d'État ou Cour de cassation – qu'au plan européen – Cour européenne des droits de l'Homme et Cour de justice de l'Union européenne.

Il y a, d'une part, le **Traitement des antécédents judiciaires (TAJ)** qui est utilisé dans le cadre des enquêtes judiciaires afin de faciliter la constatation des infractions, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs et est alimenté, à la fois, par la police et la gendarmerie. Le TAJ est géré conjointement par les directions de la police et de la gendarmerie nationales. Il contient les informations relatives aux personnes mises en cause ou aux victimes d'infractions ou aux personnes faisant l'objet d'une enquête pour recherche des causes de la mort ou de la disparition. Il existe 18,9 millions de fiches de personnes mises en cause et plus de 87 millions d'affaires répertoriées dans le TAJ.

D'autre part, le **Fichier automatisé d'empreintes digitales (FAED)** a pour finalité principale de faciliter la recherche et l'identification des auteurs de crimes et de délits, ainsi que la poursuite, l'instruction et le jugement des procédures criminelles et délictuelles dont l'autorité judiciaire est saisie. Il est géré par le Service central de la police technique et scientifique (SCPTS). Il contient les traces relevées dans le cadre d'une enquête, les empreintes digitales et palmaires de personnes mises en cause, leur état civil, les données de l'affaire et de la procédure. Actuellement, 6,2 millions de personnes et 220 000 traces non résolues sont enregistrées dans le FAED.

Enfin, le **Fichier national automatisé des empreintes génétiques (FNAEG)** est utilisé, en application de l'article 706-54 du Code de

procédure pénale, pour effectuer des rapprochements entre les empreintes génétiques prélevées sur des personnes mises en cause ou condamnées ou issues de traces biologiques prélevées sur des scènes d'infractions, et les profils déjà enregistrés dans la base de données. Il est aussi géré par le SCPTS. Y sont enregistrées les empreintes génétiques non identifiées relevées sur les lieux d'une infraction, les empreintes génétiques des personnes condamnées sur le fondement de l'article 706-55 du Code de procédure pénale, les données d'état civil des personnes identifiées, les éléments de l'affaire et la procédure.

La loi a mis en place des systèmes d'habilitation, d'authentification et de traçabilité afin de garantir la protection et la sécurité des données personnelles. Le Code de déontologie de la police et de la gendarmerie nationales énonce clairement l'obligation pour les agents de se conformer aux dispositions législatives et réglementaires relatives à la création et à l'utilisation des fichiers, de les alimenter et de les consulter dans le strict respect de leurs finalités et règles propres. Si l'authentification repose sur un système commun police-gendarmerie, elle peut se faire par identifiant et mot de passe. La mission propose la suppression de ce mode d'authentification au profit de celui par carte professionnelle qui offre plus de garanties en matière de sécurité et de confidentialité. De la même manière, elle propose aussi de développer, notamment par des procédés algorithmiques, l'analyse massive des données recueillies grâce à la traçabilité pour détecter plus largement les comportements irréguliers d'utilisation des fichiers.

La mission d'information constate que les fichiers mis à la disposition des forces de sécurité sont trop nombreux et forment un ensemble trop complexe. Elle en distingue plusieurs types.

D'une part, les fichiers à caractère administratif sont destinés à enregistrer des données administratives sur des personnes, des objets ou des moyens de transport. D'autre part, les fichiers judiciaires ont pour objet la collecte et la centralisation de renseignements destinés à lutter contre des infractions. De plus, il y a les fichiers de renseignement qui peuvent désigner les fichiers mis en œuvre par les services spécialisés de renseignement ainsi que ceux mis en œuvre par l'ensemble des services du ministère de l'intérieur chargés du renseignement de sécurité intérieur et territorial, ce qui inclut les fichiers mis en œuvre par la Direction générale de la police nationale (DGPN) et la Direction générale de la gendarmerie nationale (DGGN), par exemple le fichier « Prévention des atteintes à la sécurité publique » (PASP) mis en œuvre par la DGPN et le fichier « Gestion de l'information et prévention des atteintes à la sécurité publique » (GIPASP) mis en œuvre par la DGGN. Enfin, il y a les fichiers de rapprochement destinés à lutter contre la délinquance sérielle, comme le fichier SALVAC (système d'analyse des liens de la violence associée aux crimes) et les fichiers ou logiciels de rapprochement et d'analyse criminelle utilisés dans le cadre d'une même enquête, comme ANACRIM, qui facilitent le travail d'analyse. Par conséquent, la mission milite pour mener, au sein du ministère de l'Intérieur, une réflexion globale sur la rationalisation des fichiers existants, s'appuyant sur une analyse de leur finalité et de leur utilisation par les forces de sécurité. Cette réflexion est d'autant plus nécessaire que les fichiers mis à la disposition des forces de sécurité font l'objet d'un encadrement juridique particulièrement complexe, qui entremêle des normes d'origines et de niveaux différents dont l'harmonisation se révèle parfois difficile. Le cadre législatif a été modifié à de nombreuses reprises et s'y ajoute un « éparpillement réglementaire ». Les règles applicables

aux différents fichiers sont multiples et diverses sans pouvoir y déceler une cohérence.
La mission souligne les réels progrès en matière d'alimentation des fichiers et de saisie des données par l'utilisation de logiciels de rédaction et d'alimentation automatiques. Néanmoins, de multiples difficultés demeurent – le doute sur la qualification pénale des faits ne permet pas de déterminer avec précision la durée de conservation des données, mise à jour des fichiers effectuée de manière manuelle, etc. À ce titre, des mesures simples peuvent être adoptées, à l'instar de l'interconnexion de CASSIOPEE (Chaîne Applicative Supportant le Système d'Information Oriente Procédure pénale Et Enfants) vers TAJ, en remplacement des fiches navettes, mesure expérimentée dans plusieurs juridictions.

Les fichiers sont aussi confrontés à la vague terroriste et à la montée en puissance des enquêtes administratives qu'elle génère. Les forces de sécurité ont un besoin fort de fiabilisation des identités (difficultés d'établir certaines identités avec certitude, notamment en cas d'identités multiples) et d'interconnexion. La mission s'est penchée sur le ficher TES, Titres électroniques sécurisés. Ce fichier administratif contient les images numérisées des empreintes digitales et de la photographie de l'ensemble des demandeurs de cartes nationales d'identité et de passeports. L'interconnexion avec ce fichier semble une fausse bonne idée, pour trois raisons. La première difficulté est d'ordre technique, car son architecture exclut la possibilité d'interroger ce fichier par les empreintes digitales. La deuxième est d'ordre juridique, car le Conseil constitutionnel, dans sa décision du 22 mars 2012, a censuré des dispositions législatives qui autorisaient l'interrogation d'un traitement

destiné à recueillir les données biométriques à des fins de délivrance ou de renouvellement des titres d'identité et de voyage et de vérification de l'identité du possesseur d'un tel titre, mais aussi à d'autres fins de police administrative ou judiciaire. Enfin, la troisième raison est d'ordre politique et ne permet pas de mettre en place un fichier de contrôle de la population, contrairement à d'autres pays où l'idée est acceptée.

La proposition phare est donc de procéder à la mise en relation du FAED, du FNAEG et du TAJ. Cette mise en relation pourrait se traduire par la création d'une base-pivot faisant le lien entre ces trois applications. La Cour des comptes, dans son rapport de décembre 2016, avait déjà proposé de connecter le FAED et le FNAEG à une base commune d'identité des personnes signalisées pour améliorer la fiabilité des identités et repérer plus systématiquement les individus signalisés déjà présents dans l'une des bases et nettoyer les éventuels doublons. Mais la mission d'information donne sa préférence à la mise en relation du FAED, du FNAEG et du TAJ qui pourrait, de manière plus réaliste et certainement moins coûteuse, prendre la forme d'un identifiant commun pour l'inscription dans ces trois bases de données. La référence serait la PPMEC (la personne physique mise en cause) et on accéderait au dossier soit par son état civil, soit par ses empreintes, génétiques ou papillaires.
La mise en relation et la sécurisation des fichiers semblent bénéficier d'un consensus des pouvoirs publics français (faisabilité technique, réforme juridique modeste et coût modéré), mais aussi d'une compatibilité avec le droit européen, plus particulièrement le système d'information Schengen.
La mission conseille aussi la mise en place de certaines interconnexions entre fichiers de nature différente. Retient plus

particulièrement l'attention la proposition de mettre en place une interconnexion entre le TAJ et le casier judiciaire national pour permettre l'inscription dans le TAJ des condamnations. À défaut d'une telle interconnexion, il convient d'autoriser l'accès des policiers et des gendarmes ainsi que des agents des services chargés des enquêtes administratives au bulletin n° 1 du casier judiciaire.
De manière générale, il est envisagé de mettre en œuvre une interface entre les différents fichiers auxquels un agent a accès, permettant leur consultation simultanée à partir de la saisie d'une identité ou d'un identifiant technique. Pour optimiser l'utilisation, il faut étudier la possibilité de mettre en œuvre, dans le cadre de cette interface, un système d'alerte de présence indiquant uniquement si une personne est inscrite au sein d'autres fichiers auxquels l'agent n'a pas accès.

Le Fichier des personnes recherchées (FPR) est un outil efficace dans la lutte anti-terroriste, mais son fonctionnement peut être amélioré. Le fichier contient des inscriptions de personnes faisant l'objet de mesures de recherche pour motif judiciaire, administratif ou d'ordre public (alimenté par la gendarmerie, la police, le services des douanes, les services centraux du ministère de l'Intérieur, les préfectures, etc.) et est subdivisé en différentes catégories auxquelles correspondent des fiches particulières, parmi lesquelles les fiches S pour sûreté de l'État. Pour ces dernières, il existe plusieurs motifs d'inscription (ultra-gauche, ultra-droite, terrorisme autonomiste, espionnage, animalisme, etc.), même si les plus courants restent le terrorisme islamiste. Le rapport met en garde contre une confusion sur la finalité de la fiche S créée par les récentes affaires qui ont médiatisé cet outil. La fiche S est « un outil de suivi des personnes et de collecte du

renseignement. Elle ne préjuge pas nécessairement de la dangerosité de l'individu concerné mais signifie seulement qu'un service souhaite obtenir une remontée d'information en cas de contrôle de l'intéressé à l'occasion d'un déplacement ». Trop détaillée, elle nécessite trop de temps pour prendre connaissance de la conduite à adopter. Il convient d'en modifier le contenu afin de faire ressortir visuellement sur la fiche S, de manière immédiate, la « conduite à tenir » face à la personne contrôlée.
Le Fichier des signalements pour la prévention de la radicalisation à caractère terroriste (FSPTR) est une base de données spécialisée dans la lutte anti-terroriste gérée par l'Unité de coordination dans la lutte anti-terroriste (UCLAT) ; il recense et centralise les informations relatives aux personnes qui, engagées dans un processus de radicalisation, sont susceptibles de vouloir se rendre à l'étranger sur un théâtre d'opérations de groupements terroristes ou de vouloir prendre part à des activités à caractère terroriste. Si le fichier a prouvé son utilité en matière de partage de l'information (gendarmerie, police, préfets ou agents spécialement désignés par ces derniers), il permet aussi d'élaborer les politiques publiques de prévention et de lutte contre la radicalisation. Si la mission se montre hostile à son ouverture à un spectre plus large de personnes (élus publics), son accès devrait être permis aux procureurs de la République, étant donné qu'ils participent aux groupes d'évaluation départementaux et devraient pouvoir bénéficier des mêmes informations que les autres participants.

Le rapport reprend une réflexion d'une grande actualité et fort sensible concernant « la montée en puissance des enquêtes administratives ». Si traditionnellement ce type d'enquêtes étaient menées pour des emplois publics participant à l'exercice

des missions de souveraineté de l'État, les emplois publics et privés relevant de la défense ou de la sécurité de l'État, l'accès à des zones protégées ou l'utilisation de matériel dangereux, aujourd'hui elles sont plus largement autorisées pour les emplois en lien direct avec la sécurité des biens ou des personnes dans les entreprises de transport public, l'organisation de « grands événements », les demandes de naturalisation ou de titres de séjour. Or, l'extension du champ des enquêtes administratives et leur diversité font peser des charges très lourdes sur les forces de sécurité, au détriment de leurs autres missions. C'est la raison de la création du Service national des enquêtes administratives et de sécurité (SNEAS) et du Commandement spécialisé pour la sécurité nucléaire (CoSSeN). La mission propose d'élargir le champ de compétence du SNEAS pour soulager les missions de la gendarmerie et de la police nationales. Mais cela doit s'accompagner de l'amélioration de la protection des données personnelles et du droit à l'information des personnes qui doit être mise en œuvre au moment de leur inscription dans le fichier, incluant notamment la communication d'informations sur la durée de conservation des données, leur utilisation possible dans le cadre d'enquêtes administratives ainsi que sur les possibilités de demander leur effacement anticipé.

Toutes ces modifications doivent se faire dans la prise en compte du contexte européen pour une amélioration de la coopération (par exemple, une transmission automatisée des antécédents judiciaires dans le cadre de l'Union européenne) et la prise en compte des évolutions technologiques offertes par l'intelligence artificielle, qui se révèle être un outil précieux de traitement de masse des données, l'augmentation des potentialités des équipements mobiles, le recours à la biométrie en mobilité.

FICHIERS DE POLICE – TRIBUNAL DES CONFLITS – 8 OCTOBRE 2018 – COMPÉTENCE JUDICIAIRE

Le Tribunal des conflits a dû trancher un conflit d'incompétence négative relatif à l'effacement des données du fichier de Traitement des antécédents judiciaires (TAJ).
Une personne mise en cause dans une procédure criminelle et placée sous statut de témoin assisté a bénéficié d'un non-lieu. Elle a conséquemment demandé sa désinscription, dite « effacement », de divers fichiers dans lesquels elle pensait figurer. Le procureur de la République ayant rejeté sa requête, elle a saisi le juge des libertés et de la détention qui a ordonné la mesure sollicitée pour le fichier des empreintes génétiques (FNAEG) et pour le fichier des empreintes digitales (FAED). Le juge judiciaire s'est déclaré incompétent pour le TAJ et sa fonctionnalité biométrique dite CANONGE, relevant de la fonctionnalité de police administrative. La personne a saisi le tribunal administratif qui a décliné sa compétence. Il a fait appel et la cour administrative d'appel a renvoyé la question de compétence au Tribunal des conflits.
Le Tribunal des conflits décide de la compétence de la juridiction judiciaire. L'article 230-8 du Code de procédure pénale donne compétence au procureur de la République de décider de l'effacement ou de la rectification des données personnelles. Même si cette compétence a été accordée par une loi postérieure à la décision prise en l'espèce par le procureur de la République, la loi du 3 juin 2016, cette loi est une loi de procédure qui est soumise au principe d'application immédiate, tant qu'un jugement au fond n'a pas été rendu en première instance.

Le Tribunal des conflits tranche donc le conflit de compétence en faveur du juge judiciaire, par application des dispositions légales postérieures apportant un régime juridique particulier.

GARDE À VUE – CONSEIL CONSTITUTIONNEL – 14 SEPTEMBRE 2018 – QPC 2018-730

Le Conseil constitutionnel a été saisi d'une question prioritaire de constitutionnalité portant sur l'article 706-113 du Code de procédure pénale qui méconnaîtrait les droits de la défense au motif que, en cas de placement en garde à vue d'un majeur protégé, les dispositions n'imposent pas à l'officier de police judiciaire d'aviser son curateur ou son tuteur, ainsi que le juge des tutelles. La personne protégée ne disposant pas toujours du discernement nécessaire à l'exercice de ses droits, l'absence de cette garantie ne saurait être suppléée, lors de son placement en garde à vue, par la seule notification de son droit de faire prévenir son curateur ou son tuteur. Le Conseil constitutionnel commence par relever que l'obligation d'information s'impose lorsque le majeur protégé fait l'objet de poursuites ou d'une alternative aux poursuites (médiation, composition pénale, comparution sur reconnaissance préalable de culpabilité, etc.). En cas de placement en garde à vue, le majeur protégé ne voit pas sa situation particulière prise en compte dans la mesure où il est informé de ses droits comme tout autre majeur et peut lui-même demander à ce que son tuteur ou curateur soit informé, au même titre que toute autre personne exigerait que soit prévenue la personne de son choix. Mais faute de discernement suffisant, le majeur protégé peut ne pas appréhender la gravité de la situation

et opérer des choix à son détriment, notamment du point de vue du droit à l'information et à l'assistance d'un avocat. L'absence de prise en compte de sa situation de vulnérabilité particulière méconnaît les droits de la défense et est, à ce titre, inconstitutionnelle.
En revanche, le Conseil constitutionnel module les effets de sa décision dans le temps. La déclaration d'inconstitutionnalité bénéficie à l'auteur de la QPC et s'applique à toutes les instances en cours ; en revanche, l'abrogation prend effet à partir du 1er octobre 2019 et les gardes à vue ne peuvent être contestées sur ce fondement.

CONSTITUTION DE PARTIE CIVILE DU PRÉSIDENT DE LA RÉPUBLIQUE – COUR EUROPÉENNE DES DROITS DE L'HOMME 18 OCTOBRE 2018 – THIAM C/ France

En septembre 2008, la banque Société Générale dépose plainte contre un individu pour faux, usage de faux et escroquerie, à la suite de la contestation d'opérations bancaires par M. Nicolas Sarkozy, alors Président de la République en exercice. En octobre 2008, le procureur de la République ouvre une information judiciaire des chefs d'escroquerie en bande organisée. Au cours de l'instruction, M. Sarkozy se constitue partie civile. Le juge d'instruction ordonne le renvoi de l'individu devant le tribunal correctionnel pour avoir obtenu l'ouverture de lignes téléphoniques, la remise de téléphones portables et le paiement des abonnements, en utilisant des références bancaires appartenant à des tiers.

Devant le tribunal, le requérant soulève l'irrecevabilité de la constitution de partie civile de M. Sarkozy. Le tribunal déclare le requérant coupable des faits qui lui étaient reprochés et le condamne à un an d'emprisonnement. Il juge la constitution de partie civile de M. Sarkozy recevable, au nom du droit d'accès à un tribunal mais sursoit à statuer sur sa demande de dommages et intérêts. La Cour d'appel réforme le jugement et condamne le requérant à huit mois d'emprisonnement et à indemniser M. Sarkozy au titre de l'action civile.

Le requérant forme un pourvoi en cassation et demanda entre-temps à la Cour de cassation de soumettre au Conseil Constitutionnel une question prioritaire de constitutionnalité (QPC) relative à la compatibilité de l'article 2 du Code de procédure pénale avec le respect de la séparation des pouvoirs et des droits de la défense ainsi que du droit à un procès équitable. La Cour de cassation décide de ne pas renvoyer la QPC au motif que la question n'est pas nouvelle et ne présente pas un caractère sérieux en ce qu'elle soulève, en réalité, une question qui relève de l'office du juge judiciaire.

En juin 2012, l'Assemblée plénière de la Cour de cassation considère que le Président de la République, en sa qualité de victime, est recevable à exercer les droits de la partie civile pendant la durée de son mandat. Elle estime que le prévenu ne démontre pas avoir souffert d'une atteinte portée par les institutions françaises au droit au procès équitable dès lors que la seule nomination des juges par le Président de la République ne crée pas pour autant une dépendance à son égard et que chacune des parties a pu présenter ses arguments et discuter ceux de son adversaire tout au long de l'instruction préparatoire et des débats

devant le tribunal puis devant la Cour d'appel. La Cour de cassation casse avec renvoi l'arrêt d'appel en ce qui concerne le défaut de motivation de la peine d'emprisonnement ferme prononcée à l'encontre du requérant. La Cour d'appel de renvoi infirme la peine prononcée à l'encontre du requérant et le condamne à dix mois d'emprisonnement avec sursis.

Le requérant saisit la Cour européenne des droits de l'Homme (CEDH) en invoquant l'article 6, plus particulièrement le droit à un procès équitable et le droit de faire interroger les témoins, et le fait que la constitution de partie civile du Président de la République rompt l'égalité des armes et porte atteinte au droit à un tribunal indépendant et impartial.

En ce qui concerne le grief tiré de la violation de l'égalité des armes, la CEDH considère que M. Sarkozy n'a pas mis en mouvement l'action publique, donc l'intervention du Président dans la procédure n'a pas privé le prévenu d'une égalité de traitement eu égard à l'exercice de ces actions. Si la Constitution ne permet pas de recueillir le témoignage du Président de la République, cela ne prive pas le procès d'équité puisque les juridictions nationales n'ont fait référence à aucune preuve apportée par la partie civile dont il aurait fallu vérifier la crédibilité et la fiabilité au cours d'une audience. Aucun élément ne permet de retenir une rupture de l'égalité des armes ou du contradictoire dans la mesure où rien dans le dossier n'indique que l'intervention de M. Sarkozy ait encouragé le ministère public à des agissements visant à influencer indûment la juridiction pénale ou à empêcher le requérant de se défendre efficacement.

En ce qui concerne le grief de manque d'impartialité du tribunal

appelé à juger le requérant, la Cour rappelle que la culpabilité de M. Thiam a été établie par des éléments de preuve indépendants de l'action civile de M. Sarkozy. Le déroulement du procès du requérant ne révèle rien qui ait porté atteinte à son impartialité. Concernant l'indépendance du tribunal appelé à juger le requérant, la Cour relève, tout d'abord, que la durée du mandat des juges et l'existence d'une protection contre les pressions extérieures étaient de nature à garantir leur indépendance fonctionnelle et à les protéger des pressions extérieures, notamment vis-à-vis du pouvoir exécutif. En droit français, l'inamovibilité est constitutionnellement garantie et s'accompagne de règles précises relatives à l'avancement et à la discipline des magistrats permettant au Conseil supérieur de la magistrature (CSM) d'intervenir. Notamment, si la nomination des juges émane du Président de la République, ce pouvoir suppose un « avis conforme » du CSM, ce qui signifie que l'exécutif ne pourrait pas nommer un magistrat à l'encontre de cet avis. Même si M. Sarkozy était encore président du CSM lorsque les juges du tribunal correctionnel et de la Cour d'appel ont décidé de la cause du requérant, son intervention ne suffit pas à établir un manque d'indépendance. Depuis, une révision de la Constitution française, issue de la loi du 23 juillet 2008, est entrée en vigueur et a transféré la présidence du CSM du Président de la République au premier président de la Cour de cassation.

Police administrative

Par M. Ludovic Guinamant

La Cour suprême indienne valide la constitutionnalité du plus important fichier biométrique du monde

Cour suprême de l'Inde, 26 septembre 2018, n° 494/2012

L'arrêt du 26 septembre 2018, de 1448 pages, est la première décision d'une juridiction suprême, qui a nécessité 38 jours d'audience, se prononçant sur la validité constitutionnelle d'un fichier d'identification biométrique (photographie des iris, du visage et empreintes digitales) associé à une carte nationale biométrique. Le système comprend également un numéro national d'identification à 12 chiffres associé à chaque personne.

Loin d'être le scénario d'une nouvelle dystopie, *Aadhaar*, mot issu de l'hindi signifiant « base » ou « fondation », a été conceptualisé en 2006 et mis en œuvre à compter de 2010. À ce jour, plus d'un milliard d'individus sont enregistrés dans cette base de données.

Il faut également préciser que la presse internationale a relaté ces derniers des cas de fraudes et d'accès non autorisés à la base *Aadhaar*, notamment grâce à ses connexions avec les entreprises.

L'objectif du gouvernement indien était originalement de pouvoir identifier chacun de ses citoyens afin qu'ils puissent tous pouvoir avoir accès à leurs droits. Toutefois, les opposants au programme ont saisi la juridiction suprême en considérant que le

Police administrative

système mis en place était un système global de surveillance de la population portant atteinte aux droits fondamentaux, dont la vie privée.

Les magistrats ont néanmoins conclu que la base de données, et la carte associée, ne portait pas atteinte au droit à la vie privée des citoyens indiens mais que la Constitution indienne interdisait l'accès et le partage des informations contenues dans la base à des acteurs privés.

Par ailleurs, constatant également les risques de cybersécurité, la Cour suprême indienne a demandé au gouvernement de voter une loi particulière sur la protection des données personnelles.

En France, le Conseil d'État valide le décret créant le traitement « titres électroniques sécurisés » (TES)

Conseil d'État, 18 octobre 2018, 10ème et 9ème chambres réunies, n° 404996, 405036, 405710, 405895, 406299, 406347, 406421 et 408359

L'association la Quadrature du Net, la Ligue des droits de l'Homme et des particuliers ont demandé au Conseil d'État l'annulation du décret n° 2016-1460 du 28 octobre 2016 autorisant la création d'un traitement de données à caractère personnel relatif aux cartes d'identité.

Tout d'abord, le Conseil d'État écarte le premier moyen des

requérants qui contestaient le fait que la création d'un traitement qui était susceptible de concerner « la quasi-totalité de la population française » relève du pouvoir réglementaire. En effet, le Conseil d'État constate que le traitement n'avait pas pour effet de fixer des règles relatives aux garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques et l'article 27 de la loi du 6 janvier 1978 prévoyait bien que ce type de traitement relevait du pouvoir réglementaire.

En ce qui concerne les atteintes à la vie privée, le Conseil d'État indique que *« ce traitement n'a pour finalité que de permettre l'instruction des demandes relatives à ces titres et de prévenir et détecter leur falsification et leur contrefaçon. La création d'un tel traitement, destiné à préserver l'intégrité des données à caractère personnel nécessaires à la délivrance des titres d'identité et de voyage aux fins de sécuriser la délivrance de ces titres et d'améliorer l'efficacité de la lutte contre la fraude et qui, au surplus, facilite, par la centralisation des données recueillies, les démarches des usagers, est ainsi justifiée par un motif d'intérêt général. Il suit de là que les finalités ainsi poursuivies, qui excluent toute possibilité d'identifier une personne à partir de ses données biométriques, sont au nombre de celles qui justifient qu'il puisse être porté, par la création de ce traitement centralisé de données à caractère personnel, atteinte au droit des individus au respect de leur vie privée ».*

Concernant l'accès aux données biométriques, le Conseil d'État ajoute que, conformément à sa finalité d'authentification, *« l'accès à ce traitement ne peut se faire que par l'identité du porteur du titre d'identité, à l'exclusion, en raison des modalités mêmes de fonctionnement du traitement, de toute recherche à partir des données biométriques elles-mêmes », puis précise que « la consultation des*

empreintes digitales contenues dans le traitement informatisé ne peut servir qu'à confirmer que la personne présentant une demande de renouvellement d'un passeport ou d'une carte nationalité d'identité est bien celle à laquelle ce titre a été initialement délivré ou à s'assurer de l'absence de falsification des données contenues dans le composant électronique du passeport et, lorsqu'il aura été mis en œuvre, dans celui de la carte nationale d'identité » pour en déduire que *« la collecte des images numérisées du visage et des empreintes digitales des titulaires de passeports ou de cartes nationales d'identité, sans que soit requis le consentement mentionné à l'article 6 de la loi du 6 janvier 1978, et la centralisation de leur traitement informatisé, compte tenu des restrictions et précautions dont ce traitement est assorti, sont en adéquation avec les finalités légitimes du traitement ainsi institué et ne portent pas au droit des individus au respect de leur vie privée une atteinte disproportionnée aux buts de protection de l'ordre public en vue desquels ce traitement a été créé ».*

Le Conseil d'État se prononce sur la présence des journalistes lors des opérations de police judiciaire

Conseil d'État, 19 octobre 2018, 6ème chambre, n° 411915

L'association de la presse judiciaire a saisi le Conseil d'État d'une demande d'annulation de la dépêche CRIM-PJ n° 2017-0063-A8 du 27 avril 2017 du garde des Sceaux, ministre de la justice concernant l'incidence de l'arrêt de la Cour de cassation du 10 janvier 2017 relatif au secret de l'enquête et de l'instruction sur les autorisations de reportages journalistiques délivrées par les

Police administrative

autorités judiciaires. Elle évoque notamment que cette dépêche porte une atteinte disproportionnée à la liberté des journalistes garantie par l'article 10 de la convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales.

Toutefois, le Conseil d'État écarte ce moyen en précisant que « *le secret de l'enquête et de l'instruction et l'interdiction corrélative faite à un journaliste d'assister à une perquisition et, le cas échéant, d'en capter le son ou l'image sont justifiés, d'une part, par les exigences de recherche des auteurs d'infraction et de bonne administration de la justice et, d'autre part, par la protection des droits à la présomption d'innocence et au secret de la vie privée des personnes concernées garantis par les articles 6 et 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales* ».

En outre, le Conseil d'État ajoute que « *l'article 11 du code de procédure pénale permet au procureur de la République, soit d'office, soit à la demande de la juridiction d'instruction ou des parties, de rendre publics des " éléments objectifs tirés de la procédure ", à la condition qu'ils ne comportent aucune appréciation sur le bien-fondé des charges retenues contre les personnes mises en cause. Les parties et leurs avocats sont également libres de communiquer des informations sur le déroulement de l'enquête ou de l'instruction* ».

Droit d'asile : la Cour nationale du droit d'asile se prononce sur la situation au nord du Mali et reconnaît un climat de violence de basse intensité

CNDA, 1ère section, 2ème chambre, 24 juillet 2018, n° 17043779

Police administrative

La Cour nationale du droit d'asile (CNDA) tire les conséquences de la persistance d'un conflit armé dans le centre et le nord du Mali et d'une instabilité des conditions de sécurité dans ces régions engendrée par les opérations militaires qui opposent les forces armées maliennes soutenues par l'armée française et la MINUSMA (Mission multidimensionnelle intégrée des Nations Unies pour la stabilisation au Mali), les différents groupes rebelles touaregs, des groupes terroristes islamistes et des groupes d'autodéfense.

Elle insiste sur le fait que le conflit engendre, par ricochet, de graves menaces sur les civils en citant des chiffres récents relatifs aux victimes, aux incidents sécuritaires, aux violations des droits de l'Homme et aux déplacements de populations, ainsi que sur les difficultés éprouvées par l'État malien à rétablir son autorité sur le territoire affecté par la violence. En particulier, les derniers rapports onusiens (29 mars et 6 juin 2018) font état d'une détérioration de la situation sécuritaire et humanitaire dans le centre et le nord du Mali.

En l'espèce, la CNDA considère qu'eu égard tant au contexte général de violence aveugle de « basse intensité » que d'éléments propres à la situation personnelle du requérant (isolement familial, jeune âge, absence de ressources liée à la destruction de son commerce), ce dernier est regardé comme étant personnellement exposé, en cas de retour, à une menace grave et individuelle contre sa vie ou sa personne au sens du c) de l'article L. 712-1 du Code de l'entrée et du séjour des étrangers et du droit d'asile (CESEDA).

Police administrative

Gestation pour autrui : la Cour de cassation saisit la CEDH pour avis

Cour de cassation, arrêt n° 638 du 5 octobre 2018, Assemblée plénière

La Cour de cassation, par un arrêt du 5 octobre 2018, a adressé à la Cour européenne des droits de l'Homme une demande d'avis consultatif sur les questions suivantes :

« 1) En refusant de transcrire sur les registres de l'état civil l'acte de naissance d'un enfant né à l'étranger à l'issue d'une gestation pour autrui en ce qu'il désigne comme étant sa « mère légale » la « mère d'intention », alors que la transcription de l'acte a été admise en tant qu'il désigne le « père d'intention », père biologique de l'enfant, un État-partie excède-t-il la marge d'appréciation dont il dispose au regard de l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales ? A cet égard, y a-t-il lieu de distinguer selon que l'enfant est conçu ou non avec les gamètes de la « mère d'intention ?

2) Dans l'hypothèse d'une réponse positive à l'une des deux questions précédentes, la possibilité pour la mère d'intention d'adopter l'enfant de son conjoint, père biologique, ce qui constitue un mode d'établissement de la filiation à son égard, permet-elle de respecter les exigences de l'article 8 de la Convention ? »

Le 16 octobre 2018, la CEDH a reçu la demande d'avis consultatif soumise par la Cour de cassation française.

Police administrative

Il s'agit de la première demande d'avis consultatif reçue par la Cour depuis l'entrée en vigueur du Protocole n° 16 à la Convention européenne des droits de l'Homme le 1er août 2018. Le Protocole n° 16 permet à de hautes juridictions, telles que désignées par les États membres concernés qui ont ratifié le texte, d'adresser à la Cour des demandes d'avis consultatifs sur des questions de principe relatives à l'interprétation ou à l'application des droits et libertés définis par la Convention ou ses protocoles. Les demandes d'avis consultatifs interviennent dans le cadre d'affaires pendantes devant la juridiction nationale. La Cour dispose d'un pouvoir discrétionnaire pour accepter ou non une telle demande. La décision d'acceptation sera prise par un collège de cinq juges qui devra motiver tout refus d'accepter la demande. Les avis consultatifs, rendus par la Grande Chambre, seront motivés et non contraignants. Ils seront publiés et transmis à la juridiction qui en a fait la demande ainsi qu'à la Haute Partie contractante dont elle relève. Les juges pourront rendre une opinion séparée. Le collège et la Grande Chambre comprendront de plein droit le juge élu au titre de la Haute Partie contractante dont relève la juridiction qui a formulé la demande.

Droit des collectivités territoriales et de la sécurité privée

Par M. Xavier Latour

« D'un continuum de sécurité vers une sécurité globale »

À la demande de l'exécutif, les députés Alice Thourot et Jean-Michel Fauvergue apportent de nouveaux éléments de réflexion relatifs aux relations entre les différents acteurs de la sécurité en France dans un rapport très attendu intitulé « D'un continuum de sécurité vers une sécurité globale », rédigé à la demande du Premier ministre, et rendu le 11 septembre 2018.

La mission, ambitieuse, consistait à identifier comment améliorer les relations entre les différentes personnes mobilisées au service de la sécurité.
Pour cela, ils ont réfléchi « aux contours et aux règles » d'une « sécurité globale » (p. 16). Après plus de six mois de travail et de nombreuses auditions (professionnels, organisations syndicales, élus, universitaires...), ils produisent une étude substantielle (175 pages). Les conclusions ont d'ailleurs été qualifiées par le ministre de l'Intérieur comme étant « très stimulantes et porteuses d'une plus grande efficacité » (conférence de presse du 6 septembre 2018).
Leurs 78 propositions, certaines générales, d'autres plus techniques, et d'un intérêt variable, sont précédées d'un constat classique.

Droit des collectivités territoriales et de la sécurité privée

Le constat

Alors que la demande de sécurité ne se dément pas, l'État n'est plus capable d'y répondre seul. Face à des niveaux de délinquance élevés, des actions concrètes s'imposent. Pourtant, les contraintes budgétaires expliquent la prudence avec laquelle l'État recrute des policiers et des gendarmes. Seule la menace terroriste l'a incité à faire repartir les effectifs à la hausse. Par ailleurs, la recherche de l'efficience guide les politiques publiques de sécurité. Les noms peuvent changer (Révision générale des politiques publiques – RGPP –, Modernisation de l'action publique – MAP –, Action publique 2022...), les objectifs persistent.
Les forces nationales (250 000 gendarmes et policiers) doivent être mieux employées. À ce titre, les parlementaires ont pris en considération la construction d'une police de sécurité du quotidien. Cette dernière suppose, en effet, de dégager des effectifs policiers recentrés sur leur « cœur de métier ». Policiers et gendarmes doivent, par voie de conséquence, s'appuyer sur d'autres acteurs de la sécurité.

Traditionnellement garants de l'ordre public dans la commune, les maires participent activement à la prévention de la délinquance (art. L 132-1, Code de la sécurité intérieure – CSI). Outre l'intérêt politique qu'ils y trouvent parfois, l'État les a poussés à développer des polices municipales (21 500 policiers municipaux). Leur équipement (armement) ainsi que leurs prérogatives (palpations, sécurisation des transports publics, constatation d'infraction...) se sont accrus.

Parallèlement, une offre de sécurité privée a répondu à une forte demande, tant de la part de donneurs d'ordre publics que privés. En plus de salariés recrutés par des services internes aux entreprises, 165 000 personnes travaillent pour le compte de prestataires de services. Or, comme pour les polices municipales, l'État a favorisé leur expansion. Le cadre juridique applicable (Livre 6 CSI) a, notamment, pour ambition d'en faire des partenaires fiables. Les tentatives de moralisation et de professionnalisation du secteur ne permettent pas seulement à l'État de réguler une activité sensible, elles justifient la potentielle diversification des missions confiées au privé. Si les activités demeurent essentiellement subsidiaires, des signaux d'évolution sont perceptibles, comme l'autorisation d'une surveillance armée (loi n° 2017-258 du 28 fév. 2017) ou la participation d'agents privés aux périmètres de protection (loi n° 2017-1510 du 30 oct. 2017 ; QPC, n° 2017-695 du 29 mars 2018).

Dans ce contexte, depuis les années 1980, la coproduction de sécurité constitue une forme de mantra pour l'État. Les dispositifs institutionnels (Conseils locaux de sécurité et de prévention de la délinquance – CLSPD – par exemple) et instruments juridiques (comme les conventions de coordination entre les forces nationales et les polices municipales) ne remplissent pas toujours leur rôle. Les acteurs de la sécurité sont supposés se concerter et, par voie de conséquence, se rapprocher pour mieux agir. La réalité diffère cependant.
D'abord, la coproduction a parfois tendance à s'essouffler. Les facteurs humains l'expliquent en partie (manque de disponibilité, tendance au cloisonnement). Ensuite, la coproduction exige

de clarifier les missions de chacun. Enfin, les obstacles juridiques existent, comme en témoigne la jurisprudence sur l'interdiction de la délégation des pouvoirs de police, dans le prolongement de l'article 12 de la Déclaration des droits de l'Homme.

Ainsi, la sécurité globale suppose de nouvelles doctrines d'emploi.
Si les polices municipales sont soumises au Livre 5 CSI, les maires les utilisent de façon très différente.
En ce qui concerne la sécurité privée, la Cour des comptes, dans son rapport annuel 2018, avait insisté sur plusieurs insuffisances rappelées par les parlementaires. Malgré les progrès accomplis et les réussites ponctuelles (sûreté aéroportuaire, événementiel), le secteur se caractérise par son « atomisation » (p. 27) et sa fragilité. De plus, comme le soulignait la Cour des comptes, « l'absence de stratégie d'externalisation » (Tome 1, p. 179) complique le principe même de la coproduction. La lettre de mission du Premier ministre reprend cette idée. Elle évoque une absence de « doctrine et de vision prospective ». Pour autant, les faiblesses du secteur ne sont pas une « fatalité » (p. 28). Au contraire, elle adopte le postulat, plus guère contesté, selon lequel « leur association est désormais indispensable » (p. 32).

Une fois le constat établi, le rapport expose des propositions transversales ou spécifiques aux différents acteurs.

Les propositions transversales

Les ressources humaines

En dehors de **passages assez convenus sur l'utilité et la valorisation des réserves** opérationnelles de la police et de la gendarmerie, trois idées retiennent l'attention.

Le rapport commence par aborder la refonte de la formation. Les auteurs adhèrent à l'idée, déjà avancée en 2012 (IGA, IGEN, IGAS, Rapport sur la formation aux métiers de la sécurité privée), de la création d'une filière intégrée du collège au supérieur (BTS « sécurité » par exemple), destinée à la sécurité publique (sans remettre en cause le recrutement par concours) et à la sécurité privée. L'État en contrôlerait le développement et le fonctionnement pour gagner en homogénéité autant qu'en rigueur.
Les députés ont conscience que « la mise en œuvre ne sera pas aisée » (p. 37), ce qui est un euphémisme. Outre la diversité des acteurs concernés (Éducation nationale, entreprises, formations privées...), la seule question des moyens à mobiliser pour faire fonctionner des diplômes nationaux hypothèque une voie pourtant intéressante à suivre. De plus, en dépit du lien établi entre le manque de formations adéquates et la faiblesse de l'encadrement intermédiaire dans la sécurité privée, les entreprises accepteront-elles d'embaucher ce type de salariés, dont la rémunération est difficile à répercuter sur les prix de vente ?

La mission promeut aussi le projet ancien d'une école nationale des polices municipales (p. 65), en rupture avec le rôle actuellement joué par le Centre national de la fonction publique territoriale (CNFPT). Or, une telle école ferait sans doute une large place à des formateurs issus des forces nationales. Un tronc commun de formation et des stages dans les services de l'État (p. 67) renforceraient les relations entre les forces. En revanche, la réflexion n'aborde pas le sujet sensible de l'éclatement de la formation des forces nationales, alors qu'il défend l'idée de l'approfondissement des mutualisations entre elles (p. 50).

La mission traite, par ailleurs, de manière originale, des passerelles entre les différents métiers. Elle plaide en faveur de mobilités facilitées (p. 40 et 41), comme d'un meilleur recours à la validation des acquis et de l'expérience. Elle préconise la suppression de la limite d'âge pour passer les concours lorsque le candidat a acquis une expérience en sécurité privée ou en police municipale (p. 39).
Les intentions sont bonnes. Pourtant, les passerelles risquent bien de demeurer à sens unique, tant les cultures professionnelles sont différentes, voire hermétiques. Alors que les policiers et les gendarmes considèrent comme normal d'aller travailler ailleurs, l'inverse n'est pas vrai. L'évolution des règles de droit changera-t-elle aisément les mentalités ?

Les instruments de coordination

Nationalement, le délégué aux coopérations de sécurité semble condamné. La concurrence du Conseil national des activités privées de sécurité (CNAPS) et le poids de la Direction des libertés

publiques et des affaires juridiques (DLPAJ) du ministère de l'Intérieur justifieraient ce choix. « Le pilotage national » (p. 49) reviendrait au CNAPS pour la sécurité privée, et à la DLPAJ pour les polices municipales. Si le rôle de la DLPAJ ne fait aucun doute, celui du CNAPS suscite des interrogations. La confiance accordée à un établissement public dans lequel les professionnels de la sécurité privée sont très présents surprend. Même si le rapport évoque une augmentation du nombre de représentants de l'État dans le collège (p. 114), la formule est-elle adaptée pour aider le secteur privé à gagner en crédibilité ? Un service dédié au sein du ministère de l'Intérieur ne serait-il pas préférable ?

Localement, les députés entendent pallier les inconvénients de l'empilement des structures et des outils de coopération (p. 47). Ils tirent aussi les conséquences de l'autonomie accordée aux commissaires de police et aux commandants de gendarmerie dans le cadre de la police de sécurité du quotidien (p. 43).
Dès lors, la solution préconisée consiste, d'une part, à donner aux autorités de l'État sur le terrain plus de latitude pour fixer les axes des coopérations, plutôt que d'élaborer une doctrine nationale trop rigide. Si le rôle des maires est rappelé en quelques mots brefs, une formule en gras traduit le fil directeur : « l'État est et doit rester le garant de la sécurité globale qui sera ainsi produite » (p. 44.).
Les députés complètent, d'autre part, leur raisonnement en contestant, non sans raison, l'actuelle organisation des circonscriptions de sécurité pour valoriser la notion de bassins de vie. En adéquation avec les réalités de terrain et détachée des limites administratives traditionnelles, leur création permettrait

un pilotage plus flexible grâce à un conseil local unique (p. 47), évidemment présidé par un représentant de l'État. La sécurité privée y participerait (p. 105), ce qui serait un progrès, alors qu'elle est curieusement tenue à l'écart des CLSPD.
À ce stade, malgré ou à cause de possibles ramifications locales, le positionnement de ce conseil par rapport aux CLSPD, (art. L 132-4 CSI) présidés par les maires manque de précision, tout comme l'articulation avec le niveau intercommunal. En outre, le préfet semble plus en retrait, tout comme le Parquet, ce qui se comprend puisque les bassins, à définir, transcenderaient les circonscriptions administratives. En revanche, le rapport affirme « que la déclinaison opérationnelle devra consacrer le rôle prépondérant des cadres de la police et de la gendarmerie nationales » (p. 47). Dans ce but, chaque force se doterait d'un référent de haut niveau qui deviendrait l'interlocuteur des différents partenaires (p. 45).

Les propositions spécifiques

Les polices municipales

En la matière, un relatif classicisme prédomine.
Le texte reprend la thématique des polices municipales intercommunales, tout en soutenant les mutualisations entre polices municipales. Parmi les obstacles, le rapport pointe des réticences financières que compenserait une péréquation pilotée par le préfet (p. 59). Néanmoins, sans mesure plus énergique, la crainte des maires de perdre une nouvelle compétence pourrait

perdurer.
Outre des développements sur la revalorisation des carrières ou la suppression, proposée en 2012, des gardes champêtres (p. 68), ainsi qu'une clarification du statut des Agents de surveillance de la voie publique (p. 69) – ASVP –, les propositions concernent surtout les moyens et les prérogatives destinés à renforcer ces partenaires privilégiés.

Sur les moyens, le rapport prend, d'une part, position en faveur de l'armement de principe (p. 72). Bien que 84 % des policiers municipaux soient déjà armés (44 % d'armes à feu), l'obligation ne fait pas l'unanimité, notamment parmi les maires. Par ailleurs, le rapport n'aborde pas les conditions d'emploi et, en particulier, de l'alignement sur les règles applicables aux forces nationales (art. L 435-1 CSI).
D'autre part, les parlementaires s'inscrivent dans le mouvement bien amorcé d'un meilleur accès aux fichiers et, plus accessoirement, aux réseaux de communication des forces nationales. Après les progrès obtenus sur le fondement du décret n° 2018-387 du 24 mai 2018 (accès direct aux fichiers des permis de conduire et des immatriculations), il s'agirait d'autoriser la consultation du fichier des personnes recherchées et celui des véhicules signalés (p. 73). De plus, en prenant le contre-pied de la Commission nationale de l'informatique et des libertés (CNIL) et des juges administratifs, le rapport soutient l'ouverture de la Lecture Automatisée des Plaques d'Immatriculation aux polices municipales ainsi qu'une réflexion sur l'usage de drones (p. 77). Il n'est pas non plus hostile à la légalisation de dispositifs de signalement dématérialisés du type de celui brièvement

expérimenté à Nice (« Reporty »), avant son interruption à la demande de la CNIL faute de cadre juridique adéquat (p. 83).
De telles perspectives semblent contradictoires avec les prérogatives des polices municipales. Car celles-ci ne seraient pas appelées à substantiellement évoluer, sauf quelques modifications ponctuelles relatives au traitement des ivresses publiques (p. 79) et à la fermeture d'établissements par le maire (p. 82). Si la mission espère une réouverture du débat relatif au contrôle d'identité (p. 83), tout renforcement des prérogatives judiciaires est écartée. Le refus d'exposer les policiers municipaux à des contraintes bureaucratiques qui les éloigneraient du terrain motive ce choix (p. 74). Ceux qui attendaient une vision renouvelée pour atténuer les inégalités territoriales et clarifier les rôles de policiers municipaux seront déçus. Dès lors, chaque commune continuerait d'employer sa police municipale comme elle l'entend, dans le respect du cadre juridique en vigueur.

Les policiers municipaux sont des partenaires privilégiés, mais au service des forces nationales. En plus de leur confier la coordination des polices municipales dans un bassin de vie (p. 60), les communes devraient systématiquement leur transmettre les images de dispositifs de vidéoprotection qu'elles financement largement (p. 61). Parallèlement, comment seraient financés les Centres de supervision urbains communs aux forces nationales et aux polices municipales (p. 61), ou les hôtels de police partagés (p. 62) ? Certains maires ne verront-ils pas une forme d'étatisation indirecte, doublée d'un transfert de charges ? D'autant plus que, même en matière de contrôle, leur rôle serait moindre si l'avis préalable de la Commission consultative des

polices municipales (art. L 513-1 CSI) venait à disparaître (p. 84).

La sécurité privée

Les progrès de la coproduction passent par une meilleure fiabilité du secteur.

Pour y parvenir, les préconisations reprennent plusieurs idées avancées par la profession. Parmi les plus significatives, le vœu d'une amélioration de l'encadrement intermédiaire est à nouveau formé. La formation et la pédagogie (p. 93) suffiront-elles ? Afin d'écarter les entreprises fragiles, une garantie financière serait instaurée (p. 94), ce qui ne devrait pas rassurer les petits entrepreneurs. De plus, pour lutter contre une sous-traitance dévastatrice pour la qualité des prestations, les députés ont tourné leur regard vers l'Espagne pour limiter la pratique à un seul niveau, tout en définissant les parts de marché à sous-traiter (p. 95). Avec lucidité, le travail pointe aussi la responsabilité des donneurs d'ordre, y compris publics, à la recherche du moins-disant (p. 96), et qui devraient être solidairement responsables des prestataires. La recherche de crédibilité justifierait, par ailleurs, l'instauration d'une certification pour accomplir certaines activités (p. 98), dans le prolongement de ce qui existe pour la protection embarquée à bord des navires.

Pour davantage de fiabilité, les contrôles du CNAPS seraient étendus et approfondis. L'extension passerait par l'inclusion, parfois tentée, dans le Livre 6 CSI, de nouveaux domaines (installation de dispositifs de sécurité électronique, conseil en

sécurité-sûreté, société de service de défense). Malgré le bien-fondé de la suggestion, la réalisation s'annonce délicate. Les rapporteurs envisagent même une extension à tous les salariés des sociétés privées de sécurité, ce qui paraît un peu excessif et difficile à mettre en œuvre (p. 121). Par ailleurs, les formateurs entreraient dans le champ du Titre II bis du Livre 6 CSI (p. 89). Il est vrai que rien ne justifie leur mise à l'écart. La volonté d'associer des agents du CNAPS ou de l'État aux jurys de délivrance des cartes professionnelles retient également l'attention, en dépit de l'importance des moyens à mobiliser.
La délivrance des cartes professionnelles (sécurisées) serait plus rigoureuse pour tenir compte des critiques de la Cour des comptes (p. 87). Elle supposerait, notamment, un accès renforcé aux fichiers de police (p. 116). Afin de gagner en cohérence, la délivrance et le retrait des autorisations seraient retirés aux Commissions locales d'agrément et de contrôle pour être attribués au directeur du CNAPS. La proposition d'énumérer les condamnations incompatibles avec l'exercice de la profession pourrait, cependant, restreindre à l'excès la marge d'appréciation d'un dossier.
En outre, le CNAPS bénéficierait d'un renforcement de ses équipes, tandis que l'assermentation consoliderait utilement les inspections conduites (p. 116). La procédure disciplinaire serait, elle aussi, améliorée (p. 119), en particulier pour prévenir les conflits d'intérêts grâce à un dépaysement bienvenu des affaires.

Un partenaire rendu plus crédible participerait à des « collaborations nouvelles » (p. 86). Dans cet esprit, les agents (en tenue standardisée) seraient mieux protégés. En droit, cela

supposerait la reconnaissance de garanties particulières (circonstances aggravantes) dont l'inexistence persistante est incompréhensible (p. 100). En fait, la mission ouvre, non sans audace, la piste de l'utilisation de pistolets à impulsion électrique (p. 102), malgré les critiques à leur égard.
Certaines collaborations évoquées s'inscrivent dans le prolongement d'expérimentations amorcées (gardes statiques, transport de scellés), ou d'innovations prudentes (transfert de détenus non dangereux hospitalisés, de personnes en état d'ivresse vers les hôpitaux par exemple). Le contrôle par les forces de l'État serait systématique, conformément à la jurisprudence du Conseil constitutionnel. Deux pistes retiennent davantage l'attention. La première concerne l'association aux activités de sécurité routière (p. 110), malgré les incertitudes juridiques relatives aux véhicules-radar pilotés par des opérateurs privés. L'autre consisterait à les associer, sur le fondement de l'assermentation, à des procédures simplifiées pour des petits délits (préjudice de 200 euros maximum).

En définitive, l'État doit désormais convaincre ses partenaires du bien-fondé d'une sécurité globale délicate à organiser. En exprimant sa volonté d'engager rapidement les concertations, le Premier ministre semble décidé à progresser. Jusqu'où ?

Directeur de publication :	Colonel Dominique SCHOENHER
Rédacteur en chef :	G[al] d'armée (2S) Marc WATIN-AUGOUARD
Rédacteurs :	G[al] d'armée (2S) Marc WATIN-AUGOUARD Frédéric DEBOVE Claudia GHICA-LEMARCHAND Xavier LATOUR Ludovic GUINAMANT
Equipe éditoriale :	Odile NETZER