La veille juridique

N°51, octobre 2016

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

## Edito

*Frédéric Debove et Xavier Latour portent leur regard sur deux acteurs qui prennent une place croissante dans la sécurité. L'année 1983 a marqué un tournant dans la perception de l'insécurité : les élections municipales ont été les premières élections politiques influencées par l'augmentation sensible de la délinquance ; la loi du 12 juillet 1983 est venue clarifier le rôle des entreprises de sécurité privée. Depuis, la constante augmentation de la délinquance a créé un « gap » entre l'offre de sécurité régalienne et la demande des citoyens. La nature ayant horreur du vide, polices municipales et sécurité privée ont investi un champ libre, bordé toutefois par une jurisprudence du Conseil constitutionnel qui reste ferme sur les principes de monopole de la puissance publique sur la voie publique et de subordination de la police judiciaire à l'autorité judiciaire. Il n'empêche que ces deux acteurs* *(Suite en page 2)*




## EDITORIAL

**Par le G^al^ d'armée (2S) Marc WATIN-AUGOUARD**

n'ont pas achevé leur montée en puissance. Quel sera le détenteur futur des pouvoirs de police générale du maire ? Le président de l'EPCI ? Dans ce cas, il faudrait profondément changer le mode d'élection de son président, ce qui remettrait en cause une des premières décisions de l'Assemblée constituante faisant des maires les responsables de la sécurité publique. Quant aux services privés de sécurité, l'émergence du risque cyber leur ouvre un terrain beaucoup plus large que celui qui leur est réservé dans le monde réel.

Avec Claudia Ghica-Lemarchand, nous nous intéressons à la preuve douanière. Les douanes ont aussi pris une place croissante dans la lutte contre les grands trafics. Administration fiscale, certes, mais aussi acteur de la sécurité intérieure. Les douaniers peuvent agir depuis 1999 dans le cadre de la procédure pénale (douanes judiciaires), mais avec un souci constant de ne pas mélanger les règles qui ressortissent du Code des douanes et du Code de procédure pénale. L'arrêt commenté est un exemple intéressant de concours d'infraction pénale et douanière qui ne saurait modifier la valeur juridique du procès-verbal établi dans le cadre d'une procédure pénale.

Enfin, Ludovic Guinamant nous donne un premier aperçu du contrôle effectué par le Conseil d'État sur la mise en œuvre des techniques de renseignement. Ce premier bilan est très intéressant car, si le texte a son importance, son application en a tout autant. La loi du 24 juillet 2015 relative au renseignement fait l'objet d'un regard attentif du Conseil constitutionnel qui vient de déclarer un de ses articles relatif aux communications hertziennes contraire à la Constitution.

Pour en savoir plus, adressez-vous… aux renseignements... ou lisez ce numéro d'octobre de la veille juridique du CREOGN.

# VEILLE JURIDIQUE DE LA GENDARMERIE NATIONALE



## Sommaire





## Déontologie et sécurité

Par M. Frédéric DEBOVE

### Des détectives ... privés d'enquête ?

#### Une profession en quête de respectabilité

Dans son remarquable ouvrage consacré à l'histoire des détectives privés (éd. Nouveau monde, 2007), Dominique Kalifa retrace avec une plume brillante la genèse de l'enquête privée en France et à l'étranger. Alimentée par une galerie de portraits au passé souvent sulfureux et de figures tutélaires comme François-Eugène Vidocq ou bien encore Allan Pinkerton, la profession de détective (ou d'enquêteur de droit privé ou encore d'agent privé de recherches) plie sous le poids d'images déplorables ou ridicules. En dépit du triomphe du roman policier et du récit d'enquête (que l'on songe par exemple à Sherlock Holmes), le professionnel du renseignement apparaît largement disqualifié : son activité reste suspecte, entachée de malversations et de pratiques douteuses. L'opinion publique étant toujours prompte à la caricature, les écarts individuels de certains détectives indélicats sont érigés en règle générale et font porter la réprobation et la responsabilité sur tous les membres de la profession. En bref, la pratique du métier de détective est recouverte d'un voile de représentations désastreuses qui ont eu pour effet d'en altérer durablement l'image. Certaines sentences empruntées à L'Argus policier des années 1920 résument assez bien le sentiment général : « *l'agent d'affaires privées appartient à la grande famille des déclassés* », « *une agence de renseignement n'est jamais qu'une étape dans un long processus de dépravation morale et de déclassement social* », « *fréquemment démuni, le détective est un rapiat, avide et âpre au gain ; plus riche, c'est un rapace, qui ne lâche ses victimes qu'une fois pressurées ; le monde social n'existe pour lui que dans un rapport vénal, qu'il lui appartient de dominer dès les premiers instants* ».
Aussi, les pouvoirs publics se sont-ils efforcés depuis plusieurs décennies de moraliser la profession, d'en réguler l'accès et d'en garantir le sérieux, notamment par l'édiction de règles déontologiques, d'en épurer les rangs de ses brebis galeuses, d'en écarter les personnes d'une mo-

ralité douteuse, de pourchasser les pratiques compromettantes et les basses manoeuvres, d'en rendre les fonctions honorables et dignes d'être recherchées par des praticiens recommandables par leur capacité, leur expertise et leur honorabilité. La voie de la rédemption est jalonnée de plusieurs étapes essentielles. Après avoir été érigée en une activité de sécurité privée (loi n°95-73 du 21 janvier 1995), la profession devient vraiment réglementée en application de la loi n°2003-239 pour la sécurité intérieure du 18 mars 2003. Outre la surveillance institutionnelle de la profession par les commissaires de police et les officiers de la gendarmerie nationale, sont ainsi institués des critères rigoureux d'honorabilité, un agrément par l'État des dirigeants et enquêteurs libéraux, une autorisation administrative préalable à toute ouverture d'un établissement principal ou secondaire, une obligation de qualification professionnelle. À la faveur de la loi n°2011-267 du 14 mars 2011 appelée également « LOPPSI 2 », la profession d'enquêteur de droit privé est soumise au contrôle du Conseil National des Activités Privées de Sécurité (CNAPS), établissement public administratif chargé notamment de la délivrance et du renouvellement des agréments et des autorisations d'exercice. Depuis l'entrée en vigueur de l'ordonnance n°2012-351 du 12 mars 2012, la profession est insérée dans le Code de la sécurité intérieure qui la définit sobrement comme « une activité libérale consistant, pour une personne à recueillir, même sans faire état de sa qualité ni révéler l'objet de sa mission, des informations ou renseignements destinés à des tiers, en vue de la défense de leurs intérêts » (livre VI - activités privées de sécurité, titre II-activités des agences de recherches privées). Enfin, en application du décret n°2012-870 du 10 juillet 2012, la profession de détective est soumise, à l'instar de toutes les autres activités privées de sécurité, à un code de déontologie. En une trentaine d'articles, ce code décrit la science des devoirs devant irriguer l'action quotidienne de celles et ceux qui ont décidé de consacrer leur vie à la vérité (Vitam impendere Vero), pour emprunter une devise chère à Jean -Jacques Rousseau : respect impératif du droit, obligation de sobriété, interdiction de se départir de sa dignité, probité, discernement, professionnalisme, respect, loyauté, confidentialité, honnêteté des démarches commerciales, transparence sur la réalité de l'activité antérieure, refus de prestations illégales, obligation de conseil, respect des intérêts fondamentaux de la Nation et du secret des affaires, etc.



## Un malade imaginaire en quête d'allocations

La moisson jurisprudentielle en lien avec les détectives privés est suffisamment rare pour que toute décision de justice appelle en soi une attention spécifique. Ce qui est vrai des juridictions nationales vaut *a fortiori* pour des juridictions supranationales. Aussi, **l'arrêt rendu par la Cour européenne des droits de l'Homme le 18 octobre 2016 dans l'affaire Vukota-Bojic contre Suisse** appelle-t-il un éclairage particulier car les solutions dégagées par les juges strasbourgeois sont riches d'enseignements pour les pratiques professionnelles et déontologiques des détectives français : une surveillance secrète d'un assuré social, quand bien même serait-elle limitée à des lieux publics, peut être en effet constitutive d'une violation du droit au respect de la vie privée, dès l'instant où l'enquête litigieuse entraîne la collecte d'informations de manière systématique et n'est pas suffisamment réglementée dans ses modalités (durée de la surveillance, périodes où elle peut s'exercer, modalités de stockage et de consultation des informations recueillies au cours de l'enquête). En outre, dans l'hypothèse où les éléments d'information recueillis au cours de l'enquête seraient les seules preuves produites dans le cadre du procès, la violation du droit au respect de la vie privée pourrait, le cas échéant, se doubler d'une violation du droit au procès équitable.

La requérante, Savjeta Vukota-Bojić, est une ressortissante suisse née en 1954 et habitant à Opfikon (Suisse). En août 1995, elle fut heurtée par une moto et tomba sur le dos. On diagnostiqua initialement chez elle un traumatisme cérébral et un éventuel traumatisme crânien, et elle passa plusieurs examens médicaux qui se soldèrent par des conclusions contradictoires sur son aptitude au travail.
Sur la base de ces rapports, l'assureur de Mme Vukota-Bojić estima que le droit de celle-ci à des allocations journalières devait prendre fin dès le mois d'avril 1997. Cette décision fut annulée par le tribunal des assurances sociales de Zurich, qui ordonna la conduite d'une enquête complémentaire. Les rapports qui en résultèrent conclurent que Mme Vukota-Bojić souffrait d'un dysfonctionnement cérébral qui avait été causé par son accident. Parallèlement, le 21 mars 2002, l'autorité locale

en matière d'assurance sociale lui avait accordé une pension d'invalidité complète. Le 14 janvier 2005, l'assureur décida à nouveau que l'assurance n'octroierait plus aucune allocation à Mme Vukota-Bojić. Le tribunal des assurances sociales invalida là encore cette décision, à la suite de quoi l'assureur invita Mme Vukota-Bojić à passer un nouvel examen médical, ce qu'elle refusa.
L'assureur décida dès lors de la faire surveiller en secret par des détectives privés, afin de faire la lumière sur son état de santé. La surveillance fut conduite à quatre dates différentes et dura à chaque fois plusieurs heures. Les détectives suivirent Mme Vukota-Bojić dans des lieux publics sur de longues distances. Un rapport de surveillance fut dressé.
Sur la base de ce rapport, l'assureur confirma sa décision que l'assurance n'octroierait plus aucune allocation à Mme Vukota-Bojić. En avril 2007, un neurologue désigné par lui, le Dr H., rédigea un avis d'expert anonyme qui concluait qu'elle n'était invalide qu'à 10 %. L'assureur décida d'accorder à Mme Vukota-Bojić des allocations journalières et une pension à hauteur de ce taux. Mme Vukota-Bojić forma un recours contre les décisions de l'assureur mais, dans un arrêt du 29 mars 2010, le tribunal fédéral estima que l'assureur avait été fondé à demander à Mme Vukota-Bojić un nouvel examen médical, que la surveillance était légale et que l'avis du Dr H. était convaincant sur la question du droit de cette dernière à des allocations. Mme Vukota-Bojić demanda des clarifications à cette juridiction, mais en vain.
Dans sa requête introduite devant la Cour de Strasbourg le 14 octobre 2010, Mme Vukota-Bojić voyait dans l'enquête conduite par des détectives privés une violation de son droit à la vie privée garanti par l'article 8 de la Convention européenne des droits de l'Homme. Sur le terrain de l'article 6 § 1 (droit à un procès équitable en matière civile), elle estimait également que les décisions par lesquelles le tribunal fédéral avait statué en décidant d'admettre et de mettre en avant l'avis d'expert du Dr H. et les preuves recueillies au moyen de la surveillance étaient contraires à son droit à un procès équitable.



## Trop de surveillance tue la surveillance

S'agissant du grief fondé sur une prétendue violation de l'article 8 de la Convention européenne des droits de l'Homme, la Cour estime que la surveillance mise en place par l'assureur s'analyse en une violation du droit à la vie privée de Mme Vukota-Bojić. Elle constate tout d'abord que, l'assureur étant un acteur d'un régime d'assurance public, considéré en droit interne comme une entité publique, son action est imputable à l'État.
De plus, bien que la surveillance ait été seulement conduite dans des lieux publics, l'article 8 § 1 était applicable étant donné que les enquêteurs ont agi de manière systématique, qu'ils ont compilé des données permanentes sur Mme Vukota-Bojić et que celles-ci ont été sollicitées afin de régler un litige en matière d'assurance. Il y a donc eu ingérence dans la vie privée de Mme Vukota-Bojić.
De plus, cette ingérence n'était pas « prévue par la loi » comme le prescrit l'article 8 § 2. Si la législation suisse permettait bien aux compagnies d'assurances de prendre les « mesures d'enquête nécessaires » et de recueillir les « informations nécessaires » en cas de réticence d'un assuré à livrer des informations, ces dispositions étaient insuffisamment précises. En particulier, elles n'indiquaient pas à quel moment et pendant quelle durée la surveillance pouvait être conduite ni ne prévoyaient des garanties contre les abus, par exemple des procédures à suivre lorsque les compagnies stockent, consultent, examinent, utilisent, communiquent ou détruisent des informations. Il en avait résulté un risque d'accès et de divulgation non autorisé d'informations. La surveillance de Mme Vukota-Bojić était donc contraire à l'article 8.

S'agissant du grief fondé sur la prétendue violation du droit au procès équitable, la Cour de Strasbourg juge que la production au prétoire des preuves recueillies au moyen de la surveillance, ainsi que de l'avis d'expert du Dr H. fondé sur ces pièces, n'était pas contraire à l'article 6. Considérée dans son ensemble, la procédure a été conduite équitablement. Mme Vukota-Bojić a eu la possibilité de contester l'admissibilité du rapport de surveillance et des preuves y associées et le tribunal fédéral a motivé sa décision autorisant leur admission. De plus, les données recueillies au moyen de la surveillance et l'avis du Dr H. n'étaient

## Déontologie et sécurité

pas les seules preuves sur lesquelles la décision du tribunal fédéral était fondée, celui-ci ayant également souligné l'existence d'autres rapports médicaux contradictoires.



## Droit de l'espace numérique

**Par le G[al] d'armée (2S) Marc WATIN-AUGOUARD**

### DROIT PÉNAL

### Loi du 7 octobre 2016 pour une République numérique – Incrimination du « revenge porn »

L'incrimination de la vengeance pornographique (*revenge porn*) résulte de la loi du 7 octobre 2016 pour une République numérique qui modifie l'article 226-1 du Code pénal. Est puni de deux ans d'emprisonnement et de 60 000 euros d'amende le fait de transmettre ou de diffuser sans le consentement exprès de la personne l'image ou la voix de celle-ci, prise dans un lieu public ou privé, dès lors qu'elle présente un caractère sexuel. La diffusion d'images intimes d'un(e) « ex » sur les réseaux sociaux est une « cyberviolence » devenue un mode de vengeance d'autant plus attentatoire à l'image que la diffusion en cascade est très difficile à maîtriser. Comme cela a été rappelé lors des débats parlementaires, 90% des victimes sont des femmes qui évoquent souvent un viol virtuel.

Cette modification du Code pénal était nécessaire. En effet, l'arrêt de la Cour de cassation du 16 mars 2016[1], s'appuyant sur le droit antérieur, a cassé un arrêt de la Cour d'appel de Montpellier. En l'espèce, cette juridiction avait confirmé une condamnation en première instance d'une personne qui avait diffusé, sur Internet, une photographie de son ex-compagne, prise par lui, à l'époque de leur vie commune, la représentant nue alors qu'elle était enceinte. Pour la Cour de cassation, n'est pas pénalement réprimé le fait de diffuser, sans son accord, l'image d'une personne réalisée dans un lieu privé avec son consentement[2]. La modification du Code comble un vide. Indifférente au consentement

1. Cass.crim, 16 mars 2016, n°15-82.676
2. « Attendu que, pour confirmer cette décision, l'arrêt énonce que le fait, pour la partie civile, d'avoir accepté d'être photographiée ne signifie pas, compte tenu du caractère intime de la photographie, qu'elle avait donné son accord pour que celle-ci soit diffusée ; Mais attendu qu'en se déterminant ainsi, alors que n'est pas pénalement réprimé le fait de diffuser, sans son accord, l'image d'une personne réalisée dans un lieu privé avec son consentement, la Cour d'appel a méconnu les textes susvisés et le principe ci-dessus énoncé ».

à la prise de photographie, elle rend possible une condamnation, dès lors que c'est la diffusion sans consentement exprès qui est incriminée.

**Art. 226-2-1. du Code pénal (*créé par la loi pour la République numérique –art.67*)**

**Lorsque les délits prévus aux articles 226-1 et 226-2 portent sur des paroles ou des images présentant un caractère sexuel prises dans un lieu public ou privé, les peines sont portées à deux ans d'emprisonnement et à 60 000 € d'amende.**
**Est puni des mêmes peines le fait, en l'absence d'accord de la personne pour la diffusion, de porter à la connaissance du public ou d'un tiers tout enregistrement ou tout document portant sur des paroles ou des images présentant un caractère sexuel, obtenu, avec le consentement exprès ou présumé de la personne ou par elle-même, à l'aide de l'un des actes prévus à l'article 226-1.**

## Attaque par déni de service distribué (DDoS) - Article 323-2 du Code pénal

L'attaque « 10-21 » qui a fortement perturbé le fonctionnement d'un certain nombre de services en ligne, le 21 octobre 2016, marque un tournant dans l'histoire des cyberattaques par déni de service distribué.
L'utilisation d'un *botnet* s'appuyant sur des objets connectés souligne leur fragilité au moment où leur nombre croît de manière exponentielle (20 à 30 milliards en 2020, près de 1000 milliards au cours de la prochaine décennie).
L'article 323-2 du Code pénal réprime le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données. L'entrave au fonctionnement d'un système de traitement automatisé de données peut être constituée par l'injection d'un *malware,* d'une *bombe logique* ou par une attaque par déni de service (*Distributed Denial off*



*Service* DDoS) par un *botnet*[3] qui met en action plusieurs milliers d'ordinateurs « zombies », dont l'attaquant a pris le contrôle pour adresser à la cible autant de requêtes simultanées qui saturent le système. Le déni de service peut résulter d'une attaque par réflexion. Des ordinateurs « réflecteurs » sont utilisés pour envoyer des requêtes sur la cible. Ces réflecteurs, leurrés par l'attaquant qui usurpe l'adresse IP de la cible, lui répondent et génèrent ainsi un trafic qui la sature. D'autres attaques, dites volumétriques, augmentent l'occupation de la bande passante et saturent ainsi les ressources de traitement de la cible. Constitue, par exemple, une entrave au fonctionnement d'un système de traitement automatisé de données, le fait de procéder à une attaque par « *mailbombing* » adressant simultanément 12 000 messages identiques[4] qui vont ralentir ou bloquer le fonctionnement par saturation.

La généralisation de l'Internet des objets a, bien évidemment, des conséquences en termes de sécurité. Selon Ben Johnson, cofondateur de Carbon Black et ex-hacker de la NSA, « *Internet continue de reposer sur des protocoles et une infrastructure conçus avant que la cybersécurité ne soit un problème* ».
Les objets connectés sont généralement moins protégés et sont donc vulnérables[5]. Inquiétante également l'existence de *Shodan*, moteur de recherche qui repère les objets connectés à Internet, donc favorise leur détournement. « *Google fouille les sites web, je fouille les objets* », dit John Matherly, son fondateur[6] . Dans un rapport[7], le sénateur américain Edward-J Markey avertit des dangers relatifs à la voiture intelligente. 250 millions devraient circuler en 2020, avec des risques de cyberat-

3. Sur le *botnet,* on se référera à la thèse fondatrice d'Eric Freyssinet : *« Lutte contre les botnets : analyse et stratégie »*, Thèse de doctorat en informatique de l'Université Pierre et Marie Curie, novembre 2015.
4. Tribunal de grande instance de Nanterre, n°0613971065 du 8 juin 2006, Société Amen/ Michel M.
5. Au Defcon de Las Vegas, en août 2016, des chercheurs ont montré comment prendre le contrôle d'un vibromasseur connecté. Standard innovation, le fabricant canadien, aurait collecté des données personnelles intimes…
6. www.shodanhq.com Le moteur recense la localisation de tous les appareils connectés à Internet.
7. Edward-J Markey, Tracing&Hacking, février 2015, www.markey.senate.gov/imo/media .

taque car « *les constructeurs automobiles sont nouveaux dans le monde des logiciels et manquent d'expérience dans les programmes malveillants et de piratage* ». En 2013, la DARPA avait déjà averti des dangers[8].

Pour s'en convaincre, il suffit d'observer les faits qui vont *crescendo*. La société Proofpoint, spécialisée dans les passerelles de messagerie sécurisées, a mis en évidence une cyberattaque ayant eu lieu, entre le 23 décembre 2013 et le 6 janvier 2014, via l'Internet des objets : 750 000 courriers électroniques frauduleux auraient été adressés vers des entreprises ou des particuliers par plus de 100 000 équipements connectés, parmi eux des téléviseurs et des appareils ménagers, dont au moins un réfrigérateur. En septembre 2016, l'attaque du blog KrebsOnSecurity.com est attribuée au *botnet Mirai*. Selon le cabinet d'analyse Flashpoint, le malware *Mirai* semble à l'origine de cette attaque, dont l'auteur se vante de disposer de 380 000 objets connectés piratés utilisant le protocole telnet. *Mirai* scanne le réseau à la recherche des objets connectés vulnérables. Cette attaque par DDoS est suivie par celle du serveur OVH par 145 607 caméras IP compromises. Le trafic dépasse alors 1 térabit/s de trafic par seconde[9]. Cet événement marque une inflexion dans l'ampleur des attaques DDoS par objets connectés. Outre leur fragilité liée aux failles introduites dès leur conception, ces objets appartiennent souvent à des réseaux domestiques connectés à Internet via les FAI. Ceux-ci peuvent attribuer des adresses IP « dynamiques » qui changent régulièrement, ce qui rend plus difficile la traçabilité et donc l'attribution de l'attaque.

Plus spectaculaire encore, car touchant de très nombreux internautes, le service DNS Dyn[10] est victime, le 21 octobre 2016, pendant plusieurs heures, d'une attaque massive, en deux vagues, avec des

8.Charlie Miller & Chris Valasek Adventures in Automotive Networks and Control Units, DARPA, 2013, http://illmatics.com/car_hacking.pdf .

9. L'attaque par DdOS dont a été victime le blogueur Brian Krebs, le 22 septembre 2016, est de 620 gigabits par seconde.

10. Dyn est une des entreprises privées qui, par délégation de l'ICANN (ICANN- Accredited Registrars), gère des annuaires DNS faisant le lien entre une adresse IP et une URL par son service DynDNS.



charges de 1,6 terabit/s, par l'intermédiaire d'objets connectés (caméras de surveillance, babyphones, machines à café, réfrigérateurs, montres, etc.). La société Dyn redirige les flux Internet vers les hébergeurs. Elle a notamment pour clients Amazon, Twitter, Paypal, eBay, Airbnb, CNN, Spotify, Reddit, GitHub, le New York Times, Netflix, Financial Times, The Guardian… au total, une trentaine de sites. Ceux-ci, contrairement à d'autres, ne dépendent que d'un fournisseur de service DNS, d'où leur fragilité. Cette fois encore, *Mirai* est mis en cause. Le fabricant de caméras de surveillance, Hangzhou XiongMai Technology, est obligé de rappeler des modèles vendus aux États-Unis qui présentent une faible sécurité et offrent des mots de passe par défaut. Le code source de *Mirai* ayant été mis en *open source*, on peut s'attendre à de nombreuses répliques.

Cette cyberattaque du «10-21 », ajoutée à celle qui a frappé Yahoo avec la compromission massive de données personnelles de 500 millions de ses utilisateurs, semble donner raison à Bruce Schneier, cryptologue invité du FIC 2016, qui, le 13 septembre 2016, annonçait que « quelqu'un apprend comment détruire Internet[11]». Dans son blog, il évoque l'action d'un État, compte tenu de la puissance des actions menées pour tester la défense des systèmes. Selon lui, la Chine pourrait être derrière ces attaques. D'autres pensent à la Russie qui est entrée dans une seconde « Guerre froide » avec l'Occident. La coïncidence avec les élections américaines n'est sans doute pas fortuite. Les victimes sont principalement situées aux États-Unis, mais l'attaque a aussi été ressentie par des Européens. Wikileaks voit dans cette action un soutien à Julian Assange, réfugié dans l'ambassade d'Équateur à Londres et dont l'accès à Internet a été coupé. Quant à Damien Bancal[12] , il affirme être entré en contact avec le groupe S.O.X, groupe de pirates russes et bulgares. Ce groupe prétend disposer de 1,7 milliard d'IP disponibles et ajoute que ce n'est qu'un début et qu'il prépare quelque chose de grand…

Face à une attaque d'une telle ampleur, on comprend que la lutte contre la cybercriminalité ne puisse à elle seule résoudre le problème. Il s'agit bien de cybercriminalité car aucune preuve de l'implication d'un

11. Bruce Schneier, *« Someone is learning how to take down internet »*, 13 septembre 2016, lawfareblog.com

12. Journaliste spécialisé dans la cybersécurité, blog www. zataz.com, 26 octobre 2016.

État n'est avancée. Tant que le droit des conflits armés ne peut être invoqué, le droit commun s'applique et avec lui la loi Godfrain, dont notamment l'article 323-2 du Code pénal. D'où l'importance du renfort de la cyberdéfense qui protège notamment les opérateurs d'importance vitale. Face à ce type d'attaque, le développement en amont de protections intelligentes ayant en particulier recours au Big data (Threat Intelligence) est un mode de prévention qui devra être généralisé, sauf à remettre en cause le développement massif de l'Internet des objets.

## JURISPRUDENCE CONSTITUTIONNELLE

### Décision n°2016-590 QPC du 21 octobre 2016

L'article L. 811-5 du Code de la sécurité intérieure, relatif à la surveillance et au contrôle des transmissions par voie hertzienne, est déclaré contraire à la Constitution.

Avant d'étudier l'article en cause, un point sur la compétence de la CNCTR s'impose.

#### La compétence de la CNCTR

La loi du 24 juillet 2015 relative au renseignement a institué une Commission Nationale de Contrôle des Techniques de Renseignement (CNCTR), autorité administrative indépendante qui, sauf cas particuliers, donne un avis préalable à toute autorisation délivrée par le Premier ministre pour l'usage, sur le territoire national, des techniques de renseignement. À chaque étape de la procédure, elle a un droit d'accès permanent, complet et direct à l'information recueillie ainsi qu'aux locaux où sont centralisés les renseignements (Art. L. 833-2 CSI) et à ceux dans lesquels sont mises en œuvre des techniques de recueil du renseignement (Art. L. 871-4 CSI).
La commission a un pouvoir de recommandation pouvant conduire à l'interruption de la mise en œuvre d'une technique et à la destruction des données recueillies. Elle est composée de 9 membres (2 députés -



- 2 sénateurs - 2 membres du Conseil d'État - 2 membres de la Cour de Cassation – 1 personne qualifiée en matière de communications électroniques). Son président, nommé par le Président de la République, est un des membres du Conseil d'État ou de la Cour de cassation. Elle se réunit en séance plénière ou en séance restreinte (sans les parlementaires). Le président ou trois de ses membres peuvent saisir le Conseil d'État en cas de litige. La demande écrite et motivée (Art. L.821 -2) émane d'un ministre (ministre de la Défense, de l'Intérieur, ministre en charge de l'Économie, du budget ou des douanes). Elle est communiquée au président de la CNCTR qui rend un avis dans les 24 heures (72 heures si l'avis est donné en commission plénière ou restreinte). Le Premier ministre intervient alors dans la procédure d'autorisation. S'il passe outre l'avis de la CNCTR, le Conseil d'État peut être saisi.
Cette procédure connaît deux inflexions :

- En cas d'urgence absolue (Art. L.821-5), le Premier ministre peut accorder l'autorisation sans avis préalable de la CNCTR. Mais il ne peut le faire que si sont en cause l'indépendance nationale, l'intégrité du territoire et la défense nationale, la prévention du terrorisme et la prévention des atteintes à la forme républicaine des institutions. Les parlementaires, magistrats, avocats et journalistes ne peuvent être concernés par cette dérogation. La CNCTR est informée dans les 24 heures ;

- Les demandes d'accès administratif aux données de connexion (Art. L.821-1) sont directement adressées par les services à la CNCTR et non par l'intermédiaire d'un ministre.

Seule entorse à la procédure, les dispositions de l'article L.811-5 du CSI qui excluent, aux seules fins de la défense des intérêts nationaux (notion plus large que celle des intérêts fondamentaux de la Nation[13]**),** la surveillance et le contrôle des transmissions par voie hertzienne, rattachables ou non au territoire national, du champ du contrôle par la CNCTR. Tel est l'objet de la QPC transmise au Conseil constitutionnel

13. La notion est, en effet, plus large que celle que recouvrent les finalités des techniques de renseignement précisées par l'article L.813-1 du CSI. Elle sort du champ des intérêts fondamentaux de la Nation (art. 410-1 du Code pénal).

par le Conseil d'État, suite à un recours pour excès de pouvoir exercé par la Quadrature du Net, French Data Network, la Fédération des fournisseurs d'accès à Internet associatifs et igwan.net.

**L'inconstitutionnalité de l'article L. 811-5 du CSI**

L'article contesté résulte de l'incorporation dans le CSI, par l'ordonnance du 12 mars 2012, de l'article 20 de la loi du 10 juillet 1991 relative au secret des correspondances (Art. L .241-3 devenu L.811-5 par la loi du 24 juillet 2015). À l'origine, le législateur avait exclu l'article 20 du dispositif de contrôle car les opérations consistaient, selon lui, en une surveillance générale du domaine radioélectrique et non une mesure ciblée, individualisée et localisée. L'article L.871-2 du CSI précise la procédure suivie « *Pour l'exécution de ces mesures, le ministre de la Défense ou le ministre de l'Intérieur peuvent requérir, auprès des personnes physiques ou morales exploitant des réseaux de communications électroniques ou fournisseurs de services de communications électroniques, les informations ou documents qui leur sont nécessaires pour la réalisation et l'exploitation des interceptions autorisées par la loi* ».
Pour le Premier ministre[14], l'article incriminé correspond à des « *mesures de police des ondes, pour vérifier que des fréquences radioélectriques ne font pas l'objet d'un piratage, que ce soit des fréquences affectées à la police ou des fréquences maritimes dédiées aux urgences. [Cet article]* – poursuit-il – *couvre également l'activité des capteurs hertziens des armées, parfois installés sur le territoire national, dont l'objet est de recueillir des signaux techniques et des transmissions électromagnétiques émis depuis l'étranger, par exemple ceux engendrés par des mouvements de troupes, d'aéronefs ou de navires dans une zone donnée* ». Et d'ajouter le caractère aléatoire, non individualisé et très faiblement intrusif dans la vie privée de ces mesures.
Mais le Conseil constitutionnel, qui ne s'était pas prononcé sur l'article L.811-5[15], déclare cet article contraire à la Constitution car, « *faute de*

14. Observations présentées par le Premier ministre en réponse aux arguments des auteurs de la QPC.
15. Décision n°2015-713 DC du 23 juillet 2015 sur la loi relative au renseignement.



*garanties appropriées, les dispositions contestées portent une atteinte manifestement disproportionnée au respect de la vie privée et au secret des correspondances résultant de l'article 2 de la Déclaration des droits de l'Homme et du citoyen de 1789* ». Les associations à l'origine de la QPC soutenaient que le législateur n'avait pas exercé pleinement la compétence qu'il détient de l'article 34 en ne définissant pas les conditions de collecte, d'exploitation, de conservation et de destruction des renseignements recueillis et en ne prévoyant pas de dispositif de contrôle de ces mesures.
Pour le Conseil constitutionnel, « *Dès lors qu'elles permettent aux pouvoirs publics de prendre des mesures de surveillance et de contrôle de toute transmission empruntant la voie hertzienne, sans exclure que puissent être interceptées des communications ou recueillies des données individualisables, les dispositions contestées portent atteinte au droit au respect de la vie privée et au secret des correspondances* ».
L'article L.871-2 susvisé évoque bien d'ailleurs des interceptions.
Compte tenu des conséquences manifestement excessives d'une abrogation immédiate de l'article L. 811-5, le Conseil constitutionnel reporte la date au 31 décembre 2017 pour permettre au législateur d'apporter les corrections nécessaires. Toutefois, pendant cette période de sursis, les dispositions de l'article L. 811-5 ne peuvent servir de fondement à des mesures d'interception de correspondances, de recueil de données de connexion ou de captation des données informatiques qui doivent être soumises à autorisation. La CNCTR doit être régulièrement informée sur le champ et la nature des mesures prises en application de l'article invalidé.
On notera que c'est le quatrième article de la loi du 24 juillet qui fait l'objet d'une censure par le Conseil constitutionnel :

- A été jugé non conforme à la Constitution l'article L. 821-6 CSI qui instituait une procédure « d'urgence opérationnelle » permettant aux services, en cas de menace imminente, de mettre en œuvre des techniques de renseignement, sans information du ministre concerné, sans autorisation du Premier ministre et sans avis préalable de la Commission Nationale de Contrôle des Techniques de Renseignement (CNCTR). La menace imminente ne justifiait pas une telle disproportion par rapport au respect de

la vie privée et au secret des correspondances ;

- A été également censuré l'article L. 854-1 CSI relatif aux surveillances des communications émises ou reçues à l'étranger. Le Conseil reprochait à la loi de n'avoir pas défini les règles concernant les garanties fondamentales. Le renvoi à un décret en Conseil d'État des conditions d'exploitation, de conservation et de destruction des renseignements, ainsi que des modalités d'exercice du contrôle par la CNCTR, méconnaissait l'article 34 de la Constitution qui définit le domaine de la loi. Cet article a été rétabli par la loi du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales jugée conforme à la Constitution ;

- Enfin, une censure plus technique a affecté les dispositions de l'article L.832-4 relatives au budget de la CNCTR qui devaient relever d'une loi de finances.

## JURISPRUDENCE JUDICIAIRE

### Cour de Justice de l'Union européenne – Arrêt C-582/14 du 19 octobre 2016, Patrick Breyer contre Bundesrepublik Deutschland

Une adresse Internet Protocol « dynamique » peut être une donnée à caractère personnel.

#### La saisine de la CJUE

Patrick Breyer, citoyen allemand, reprochait aux autorités de son pays d'enregistrer et de conserver son adresse Internet Protocol (IP) lorsqu'il consulte les sites Internet fédéraux. Ces derniers enregistrent les données de consultation, notamment l'adresse IP, pour se prémunir des malveillances et engager le cas échéant des poursuites pénales. Après un rejet de sa demande en première instance, la Cour d'appel a partiel-



lement réformé le jugement, ce qui bien sûr n'a pas satisfait les deux parties qui ont engagé un recours en révision devant le Bundesgerichtshof. C'est dans ce cadre que la Cour fédérale de justice allemande a adressé à la CJUE une demande de décision préjudicielle, au titre de l'article 267 TFUE. Cette demande portait sur l'interprétation de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
Une adresse IP « dynamique » est-elle une donnée à caractère personnel ? Telle était l'une des questions soulevées. Il existe, en effet, deux types d'adresse IP : la première « fixe » est affectée en permanence à la « machine » connectée. La seconde est temporaire et attribuée par le fournisseur d'accès lors de chaque session. Elle peut donc changer, ce qui rend sa traçabilité plus complexe mais non impossible. Pour identifier la machine origine, il faut combiner l'action du FAI et celle du site consulté. Dans son arrêt du 24 novembre 2011[16], la CJUE avait déjà pris position sur les adresses IP, dont elle avait reconnu la qualité de donnée à caractère personnel dans le point 51 : les adresses IP fixes sont « des données protégées à caractère personnel, car elles permettent l'identification précise desdits utilisateurs ». Mais, dans cette affaire, il s'agissait de la relation directe entre le FAI et l'internaute.
L'arrêt du 19 octobre 2016 clarifie d'une manière définitive le lien entre l'adresse IP et la notion de données à caractère personnel. Il met un terme aux hésitations jurisprudentielles.

#### L'adresse IP au cœur de controverses

La définition des données à caractère personnel est énoncée par l'article 2 a) de la directive 95/46/CE. Elle est reprise dans une forme plus littéraire par l'article 2 de la loi du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés :
*« Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directe-*

16. CJUE, affaire C-70/10 Scarlet Extended SA c/Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM).

*ment ou indirectement, par référence à un numéro d'identification ou un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne ».*
Cette définition est très ouverte pour éviter tout enfermement dans des critères liés notamment aux évolutions technologiques. On observera que l'identification peut être indirecte grâce au résultat de la combinaison de l'ensemble des moyens dont on dispose (notamment de plusieurs données).
La nature de l'adresse IP a fait l'objet de prises de position contradictoires.
Dès 2000, pour le G29 [17], « *on peut parler sans l'ombre d'un doute de données à caractère personnel* » au sens de l'article 2, point a) de la directive. Le G29 considère, en effet, que « *les fournisseurs d'accès à Internet et les gestionnaires de réseaux locaux peuvent, en utilisant des moyens raisonnables, identifier les utilisateurs Internet auxquels ils ont attribué des adresses IP, du fait qu'ils enregistrent systématiquement dans un fichier les date, heure, durée et adresse dynamique IP données à l'utilisateur d'Internet* ». Le 2 août 2007[18], la CNIL et le G29 soutiennent que l'adresse IP est une donnée à caractère personnel. La CNIL réagit à deux arrêts de la Cour d'appel de Paris relatifs au téléchargement d'œuvres musicales. Le premier, en date du 27 avril 2007[19], refuse d'admettre que l'adresse IP est une donnée à caractère personnel en considérant que celle-ci « *ne permet pas d'identifier le* (sic) *ou les personnes qui ont utilisé cet ordinateur puisque seule l'autorité légitime pour poursuivre l'enquête (police ou gendarmerie) peut obtenir du fournisseur l'accès d'identité de l'utilisateur* ». Quelques jours plus tard, le 15 mai 2007[20], elle affirme que « *le relevé de l'adresse IP de l'ordinateur ayant servi à l'infraction entre dans le constat de sa ma-*

17. G 29, avis du 21 novembre 2000, « *Le respect de la vie privée sur Internet- une approche européenne intégrée sur la protection des données en ligne* ».
www.ec.europa.eu/justice/policies/privacy/docs/wpdocs/2000/wp37fr.pdf
18.http:/www.cnil.fr/linstitution/actualité/article/article/ladresse-ip-est-une-donnee-a-caractere-personnel-pour lensemble-des-cnil-europeennes.
19. CA. Paris, 13e chambre, Anthony G./SCPP, 27 avril 2007.
20. CA Paris, 13e chambre, Henri S/SCPP, 15 mai 2007.



térialité et pas dans l'identification de son auteur ». Elle ajoute « *que cette série de chiffres en effet ne constitue en rien une donnée indirectement nominative relative à la personne dans la mesure où elle ne se rapporte qu'à une machine et non à l'individu qui utilise l'ordinateur* ».
Le 6 septembre 2007, en revanche, le TGI de Saint-Brieuc[21] reconnaît que l'adresse IP est bien une donnée à caractère personnel : « *L'adresse IP est, au sens strict, un identifiant d'une machine lorsque celle-ci se connecte sur l'Internet et non d'une personne. Mais, au même titre qu'un numéro de téléphone n'est, au sens strict, que celui d'une ligne déterminée mais pour laquelle un abonnement a été souscrit par une personne déterminée, un numéro IP associé à un fournisseur d'accès […] constitue un ensemble de moyens permettant de connaître le nom de l'utilisateur* ».
En 2009, c'est au tour de la Cour de cassation d'accentuer l'incertitude : l'arrêt du 13 janvier[22] considère que l'adresse IP n'est pas une donnée personnelle dont le traitement relèverait de la loi du 6 janvier 1978. Dans cette droite ligne, la Cour d'appel de Rennes, par un arrêt du 28 avril 2015[23], confirme que « *le seul relevé d'une adresse IP aux fins de localiser un fournisseur d'accès ne constitue pas un traitement de données à caractère personnel au sens des articles 2, 9 et 25 de la loi informatique et libertés du 6 janvier 1978. L'adresse IP est constituée d'une série de chiffres, n'est pas une donnée, même indirectement nominative, alors qu'elle se rapporte à un ordinateur et non à l'utilisateur* ». Mais, récemment, le tribunal de grande instance de Meaux, par ordonnance de référé du 10 août 2016[24], reconnaît que la recherche d'une adresse IP est un traitement de donnée à caractère personnel.
Dans ce contexte, l'arrêt de la CJUE est le bienvenu car il met un terme à une certaine insécurité juridique et à une divergence d'appréciation entre les autorités nationales chargées de la protection des données et certaines juridictions.

21. TGI de Saint-Brieuc, 6 septembre 2007, Ministère public, SCPP, SACEM c/J.P.
22. Cass. crim, n°08-84.088, 13 janvier 2009.
23. CA. Rennes, ch. Com., n°14/05708, 2 avril 2015.
24. France sécurité/ NC. Numéricable. Voir veille juridique du CREOGN - septembre 2016.

## Droit de l'espace numérique

### La solution de la CJUE

Dans le cas d'espèce, seul le FAI peut connaître directement l'identité de la personne (ou plus exactement de la machine), puisqu'il a attribué l'adresse IP. L'opérateur des sites Internet ne dispose pas d'informations précises permettant cette opération, sauf si l'internaute s'est identifié au cours de la session.
L'adresse IP dynamique ne constitue pas donc à elle seule, pour le fournisseur de services en ligne, une information se rapportant à une personne physique identifiée, mais elle peut être qualifiée d'information se rapportant à une personne physique identifiable si des informations supplémentaires sont détenues par le FAI. Comme l'a souligné l'avocat général, M. Campos Sánchez-Bordona, la conjugaison n'est pas irréalisable en pratique car elle n'implique pas un effort démesuré en termes de temps, de coût et de main-d'œuvre.
Pour la CJUE, une adresse de protocole Internet dynamique, enregistrée par un fournisseur de services de médias en ligne à l'occasion de la consultation par une personne d'un site Internet que ce fournisseur rend accessible au public, constitue, à l'égard dudit fournisseur, une donnée à caractère personnel lorsqu'il dispose des moyens légaux lui permettant de faire identifier la personne concernée grâce aux informations supplémentaires dont dispose le fournisseur d'accès à Internet de cette personne.
La Cour répond également à la Bundesgerichtshof sur le droit des services fédéraux à conserver les données. L'article 7 f) de la directive 95/46 autorise la conservation des données issues des consultations des sites, non seulement pour des motifs de facturation, comme le prévoit la loi fédérale, mais également « pour la réalisation de l'intérêt légitime poursuivi par le responsable du traitement » en garantissant l'utilisation des médias et la continuité de leur fonctionnement.
Par arrêt du 3 novembre 2016 (Cass.civ. n°15-22.595), la Cour de cassation a fait une stricte application de l'arrêt de la CJUE. Elle a reconnu la qualité de donnée à caractère personnel à l'adresse IP en cassant l'arrêt de la Cour d'appel de Rennes du 28 avril 2015 précité. Nouvelle démonstration de l'impact du droit européen sur le droit interne.



## Actualité pénale

**Par Mme Claudia GHICA-LEMARCHAND**

### Escroquerie – application à un immeuble

***Crim. 28 septembre 2016, n° 15-84485, publication Bull. à venir***

L'arrêt rendu par la Chambre criminelle le 28 septembre 2016 constitue un véritable revirement de jurisprudence étendant le champ d'application de l'escroquerie aux immeubles.
Un individu a créé avec son épouse, qui n'était qu'un prête-nom, une société commerciale dont les fonds ont été utilisés pour ses besoins personnels. Par ailleurs, il a établi un faux testament présentant sa mère comme l'unique ayant droit de son oncle défunt, permettant ainsi à celle-ci d'hériter de ce dernier - outre des sommes versées sur une assurance-vie -, d'une villa localisée à Porticcio, dont elle a fait donation de la nue-propriété au demandeur. Il est renvoyé devant le tribunal correctionnel des chefs d'abus de biens sociaux, faits commis entre 2006 et 2008 et de recel d'escroquerie. En revanche, la qualification de l'infraction d'origine d'escroquerie n'est pas retenue car prescrite, les faits ayant été commis en 2001 et découverts en 2008.
L'infraction de recel étant une infraction continue, les poursuites sont possibles et couvrent un champ temporel plus large. Le tribunal correctionnel l'a condamné à deux ans d'emprisonnement dont un an avec sursis, 50 000 euros d'amende et cinq ans d'interdiction de gérer, décision confirmée par la Cour d'appel. Si la qualification de l'abus de biens sociaux n'appelle pas de commentaire particulier, tel n'est pas le cas du recel d'escroquerie portant sur un immeuble. Les décisions de renvoi et de condamnation mettent l'accent sur l'élément matériel large du recel (« le recel peut porter sur toute chose », y compris un bien immeuble), ainsi que sur son caractère continu (« si les faits d'escroquerie dont provient le recel poursuivi ont été commis plus de trois années avant le déclenchement de l'enquête, tel n'est pas le cas de la possession de manière directe ou indirecte dans des conditions qu'il maîtrise, ou de l'utilisation du bien recelé »).
Il forme un pourvoi en cassation à moyen unique, dont seule la première branche sera étudiée. Il soutient que « le recel ne peut pas porter

sur un immeuble, dès lors que celui-ci ne peut pas être l'objet de l'infraction originaire » et qu'il y a violation de l'article 313-1 du Code pénal puisque la remise d'immeuble ne rentre pas dans les prévisions légales du texte. La Cour de cassation rejette le pourvoi et affirme dans un attendu clair à portée générale : « l'escroquerie peut porter sur un immeuble, lequel constitue un bien au sens de l'article 313-1 du Code pénal ».

L'article 313-1 du Code pénal punit l'escroquerie définie comme « le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge ». Si la jurisprudence a régulièrement étendu les manœuvres frauduleuses afin d'englober des comportements divers au sein de l'incrimination, la notion de remise de bien est restée relativement stable. La remise couvre toute forme de remise, indépendamment de la forme, directe ou indirecte, de courte ou longue durée. Le nouveau Code pénal a modifié la liste sur laquelle peut porter la remise pour tomber sous le coup de la loi pénale. L'ancien article 405 du Code pénal visait « des fonds, des meubles ou des obligations, dispositions, billets, promesses, quittances ou décharges, (…) la totalité ou partie de la fortune d'autrui ». La doctrine traditionnelle a toujours considéré que le champ d'application de l'escroquerie excluait les immeubles pour deux raisons. D'une part, la remise ne peut porter sur un immeuble, bien insusceptible de transfert matériel. Ainsi, l'escroquerie peut porter sur l'instrumentum, l'acte en lui-même, mais pas sur le negotium, le contenu de l'acte visant l'immeuble. D'autre part, le droit pénal réserve sa protection aux biens meubles moins bien protégés par le droit civil qui réserve une protection spécifique forte et formalisée aux immeubles. Il est possible de remarquer que la liste limitative de l'ancien article 405 n'exclut pas expressément les immeubles puisque si les meubles sont spécifiquement visés, les immeubles peuvent faire « partie de la fortune d'autrui ».

L'article 313-1 du Code pénal introduit une nouvelle liste de biens sur lesquels peut porter le comportement interdit : « des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge ». Si en vertu du principe d'interprétation stricte de la loi pénale, la liste est limitative, l'énumération porte sur des éléments ayant un caractère large, ce qui lui assure une application largement ouverte. Si la dématérialisation de l'escroquerie était légalement admise par la référence explicite aux « services », après avoir été admise par la jurisprudence dans le cadre des actes « opérant obligation ou décharge », à l'instar des rondelles métalliques dépourvues de toute valeur introduites dans des horodateurs et permettant d'obtenir du temps de stationnement gratuit, la question de l'exclusion des immeubles ne semblait nullement contestable. En effet, la définition légale repose sur le fait que la tromperie détermine « à son préjudice ou au préjudice d'un tiers, à remettre » les susdits biens. Le transfert matériel exigé par la remise reste un des éléments constitutifs de l'escroquerie et semble donc faire obstacle à l'élargissement de l'infraction aux immeubles.

Pour contourner cette difficulté, les juges instructeurs et du fond saisis de l'espèce ne se sont pas placés sur le terrain de l'escroquerie, l'infraction d'origine, mais sur le terrain du recel. Une ambiguïté peut être relevée à cet égard. L'article 321-1 du Code pénal punit deux types de recel différents. D'une part, l'alinéa 1 punit le recel-détention qui « est le fait de dissimuler, de détenir ou de transmettre une chose, ou de faire office d'intermédiaire afin de la transmettre, en sachant que cette chose provient d'un crime ou d'un délit ». D'autre part, le recel-profit est « le fait, en connaissance de cause, de bénéficier, par tout moyen, du produit d'un crime ou d'un délit ». Si le recel-détention doit être nécessairement matérialisé et ne peut porter sur un immeuble, une telle limitation n'est pas imposée au recel-profit qui est très large et englobe tout type de biens, meubles ou immeubles. Si l'arrêt vise l'article 321-1 sans préciser l'alinéa, l'hésitation est permise. L'utilisation du recel-profit rendrait l'application du recel-profit indiscutable, mais l'arrêt rappelle « que c'est en parfaite adéquation avec la loi pénale, qui prévoit que le recel peut porter sur toute chose, que le magistrat instructeur a retenu un bien immeuble », renvoyant indirectement au recel-détention. La Chambre criminelle de la Cour de cassation ne cherche pas la facilité et choisit de donner une portée générale à son arrêt, se plaçant directement sur le terrain de l'escroquerie et pas du recel. En effet, le pourvoi critique les juges de l'avoir déclaré « coupable d'avoir

recelé une maison d'habitation provenant d'une escroquerie, lorsque le recel ne peut pas porter sur un immeuble, dès lors que celui-ci ne peut pas être l'objet de l'infraction originaire » qui ne rentre pas dans les prévisions de l'article 313-1 du Code pénal.
La Cour de cassation affirme dès lors que « l'escroquerie peut porter sur un immeuble, lequel constitue un bien au sens de l'article 313-1 du Code pénal ». L'affirmation de la Cour de cassation est incontestable. Au sens des grandes classifications opérées par le droit civil, les biens sont meubles et immeubles. Le nouveau Code pénal a fait le choix de renoncer au renvoi « aux meubles » expressément désignés dans l'ancien Code pénal et de les remplacer par la référence aux « biens » englobant les immeubles. La méthode d'interprétation téléologique plaide en faveur de cette nouvelle interprétation. Néanmoins, une question reste possible. Comment concilier les composantes de l'escroquerie ? L'escroquerie est une infraction complexe puisque son élément matériel est composé d'éléments de nature diverse – la tromperie, le bien, le préjudice et la remise. Si les trois premiers sont parfaitement compatibles avec l'incorporation de l'immeuble au champ d'application de l'escroquerie, le dernier soulève une question de logique. Comment réaliser la remise d'un immeuble ? Il convient de retenir une définition purement juridique de la remise qui se détache de son caractère matériel. Si dans le cadre du vol, la soustraction avait été élargie dans le sens d'une atteinte juridique à la possession et était devenue compatible avec la remise, l'escroquerie effectue le chemin inverse. Elle se traduit par une atteinte à la possession et, de manière plus large, à la propriété sous une forme de remise juridique portant atteinte aux droits du véritable propriétaire, sans qu'elle soit matérialisée par une remise matérielle qui nuirait exclusivement aux droits du possesseur. Cette évolution de la jurisprudence est dès lors parfaitement compatible avec l'admission de la remise indirecte déjà opérée par la jurisprudence.
Cet arrêt important de la Chambre criminelle assure un champ d'application plus large à l'escroquerie et constitue un revirement remarquable dans le sens d'une répression plus forte des comportements portant atteinte aux biens. La question reste ouverte à l'égard de l'application de l'abus de confiance qui connaît la même restriction aux immeubles.



## Association de malfaiteurs terroriste criminelle

***Crim. 7 octobre 2016, n° 16-84597, publication Bull. à venir***

L'arrêt du 7 octobre 2016 reprend les mises en examen effectuées dans le cadre de l'affaire Merah, en l'absence de l'auteur principal, à l'égard de son frère et de la personne ayant fourni les moyens de commettre les infractions. En mars 2012, le terroriste islamiste Mohamed Merah tue sept personnes, trois militaires et quatre civils en raison de leur appartenance à une ethnie et à la religion juive, dont trois enfants. Il est abattu au cours de la tentative d'interpellation.
Son frère est mis en examen des chefs d'association de malfaiteurs terroriste criminelle, de complicité d'assassinats et de tentatives d'assassinats, de vol en réunion. Il conteste à la fois les éléments de preuve et les qualifications retenues. En premier lieu, la qualification de complicité serait injustifiée. En effet, la complicité doit respecter trois conditions pour être punissable – se traduire par des actes positifs, antérieurs ou concomitants et commis en toute connaissance de cause. Si le caractère antérieur n'est nullement contesté, les deux autres conditions sont discutées. D'une part, le pourvoi soutient que les juges ont retenu « une simple abstention qui, à la supposer avérée, est inopérante » car ils se sont contentés de constater qu'il n'avait pas « cherché à décourager son frère de commettre les actions qu'il sentait venir ». D'autre part, « la chambre de l'instruction qui n'a pas dit en quoi le mis en examen avait intentionnellement commis les faits reprochés ou adhéré aux projets délictueux commis par son frère, le simple rapprochement des deux hommes à une époque contemporaine des faits étant radicalement indifférente à établir la participation du mis en examen aux infractions poursuivies ». Ensuite, le pourvoi conteste la responsabilité pénale de l'accusé en rappelant le principe selon lequel « nul n'est responsable que de son propre fait ». Ainsi, les juges ne pouvaient pas « se contenter de souligner le radicalisme religieux du mis en examen et l'emprise prétendue exercée sur son frère, pour le renvoyer devant la Cour d'assises, sans lui imputer, de manière personnelle et certaine, la commission de faits précis ». Enfin, les éléments de preuve retenus par les juges seraient, selon le pourvoi, hypothétiques et entachés de par-

tialité pour certains. La Cour de cassation rejette toutes ces critiques en validant à la fois les qualifications pénales retenues, ainsi que l'implication de l'accusé dans les faits en qualité de complice, et rappelle « les juridictions d'instruction apprécient souverainement si les faits retenus à la charge de la personne mise en examen sont constitutifs d'une infraction, la Cour de cassation n'ayant d'autre pouvoir que de vérifier si, à supposer ces faits établis, la qualification justifie la saisine de la juridiction de jugement ».

Le deuxième individu est renvoyé devant la Cour d'assises spécialement composée sous la prévention de délits connexes d'infractions à la législation sur les armes en relation avec une entreprise terroriste et de participation à un groupement formé ou une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, de l'un des actes de terrorisme prévus à l'article 421-1 du Code pénal. Le ministère public a requis la requalification de l'association de malfaiteurs en crime réprimé par l'article 421-6 du Code pénal en invoquant, notamment, la fourniture par celui-ci à Mohamed Mérah d'armes destinées à être utilisées par celui-ci dans son entreprise terroriste ayant pour objet de commettre des assassinats. La chambre de l'instruction a refusé la requalification en considérant qu'aucun élément de la procédure ne permettait d'établir que la personne poursuivie avait été avertie des projets criminels de Merah ou qu'il avait « une connaissance indubitable des projets concrets du futur assassin » et considérant qu'il était « connu en tant que "commercial" du quartier, [et] fournissait "un peu tout ce qu'on lui demandait sans perdre son temps à s'interroger sur l'utilisation qui serait faite du matériel qu'il mettait à disposition" des délinquants ». Cependant, les juges retiennent « l'existence de charges de s'être associé à une entreprise terroriste, en fournissant des armes et munitions, un gilet pare-balles et des fonds à Mohamed Mérah dont il n'ignorait pas sa capacité à commettre des actes en lien avec son idéologie radicale djihadiste ». Pour cette raison, les juges ont retenu à son encontre la participation à un groupement formé ou une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, de l'un des actes de terrorisme prévus à l'article 421-1 du Code pénal et refusé de retenir la circonstance aggravante de l'article 421-6 en l'absence de « la démonstration de la connaissance précise et concrète » du projet criminel.



La Chambre criminelle de la Cour de cassation casse l'arrêt en considérant que la chambre de l'instruction a méconnu le sens et la portée du texte, mais saisit l'occasion pour rendre un attendu de principe précisant le champ d'application de la circonstance aggravante de l'article 421-6 1° du Code pénal, dans le cadre d'une lecture combinée avec les articles 421-1 et 421-2-1. « Est punissable en tant que crime la participation à un groupement formé ou une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'un acte de terrorisme, dès lors qu'il a pour objet de porter volontairement atteinte à la vie ou à l'intégrité de la personne. » Le dispositif mis en place par le législateur trouve une cohérence interne au-delà des réformes successives et fréquentes. L'article 421-1 définit les actes de terrorisme qui sont composés des infractions de droit commun auxquelles se joint un dol spécial – « lorsqu'elles sont intentionnellement en relation avec une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur ». L'article 421-2-1 assimile aux actes de terrorisme « le fait de participer à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'un des actes de terrorisme mentionnés aux articles précédents ». L'article 421-6 définit une circonstance aggravante qui permet de relever la peine criminelle à trente ans, visant au premier titre les infractions contre les personnes figurant à l'article 421-1 1°. La chambre de l'instruction a donc retenu la participation à un acte terroriste, par combinaison des articles 421-1 et 421-2-1 mais a refusé l'aggravation de l'article 421-6 du Code pénal. Son raisonnement est invalidé par la Cour de cassation pour deux raisons. La première raison est pratique et porte sur la qualification. Il ne semble pas logique de retenir les infractions contre les personnes projetées comme élément constitutif de la qualification retenue et de refuser d'en tenir compte dans le cadre de sa répression. La deuxième raison est juridique et tient à la jurisprudence traditionnelle applicable à la complicité et transposée aux incriminations reposant sur la participation à une infraction. Pour que la responsabilité pénale soit retenue, la participation doit nécessairement être intentionnelle, la seule question qui se pose est de savoir si l'intention doit être déterminée (la personne doit-elle manifester la volonté de participer à une infraction commise dans des conditions connues et déterminées à l'avance ?) ou si une intention

indéterminée suffit (la personne se joint à un projet criminel sans en connaître les détails précis d'exécution). De longue date, la jurisprudence se contente d'une intention indéterminée dans le cadre de la complicité et utilise ce même mécanisme dans le cadre des infractions de participation à une entreprise criminelle. Ainsi, l'intention indéterminée est suffisante pour caractériser l'infraction de l'article 421-1 ou 421-2-1. Dès lors, la Cour de cassation opère encore plus facilement l'extension à la circonstance aggravante, alors même qu'elle repose sur un des éléments constitutifs de l'infraction de l'article 421-1. L'intention indéterminée de participer à un groupement terroriste « dès lors qu'il a pour objet de porter volontairement atteinte à la vie ou à l'intégrité de la personne », traduit par le fait de se procurer des armes, sans ignorer sa « capacité à commettre des actes en lien avec son idéologie radicale djihadiste », est un motif d'aggravation de la répression.

## Procès-verbaux douaniers

***Crim. 28 septembre 2016, n° 15-84383, Publication Bull. à venir***

Si la législation récente a constamment accru les pouvoirs d'investigation des douaniers, les procès-verbaux dressés par les agents des douanes ont une force particulière pour les infractions douanières mais pas pour les infractions de droit commun.
La brigade des douanes a mis en place un dispositif de surveillance dans un port lui permettant de voir un déchargement de sacs d'une yole à destination d'un individu à terre. Si la yole a réussi à prendre la fuite, les agents ont interpellé à très grande proximité un individu essoufflé en sueur, caché sous une yole, que les douaniers ont formellement reconnu comme l'individu ayant réceptionné les sacs contenant de la cocaïne. Ils ont dressé un procès-verbal sur la foi duquel l'individu a été déclaré coupable de transport, détention et acquisition de manière illicite de stupéfiants (infraction punie par le Code pénal) et importation, sans déclaration préalable, de manière illicite, d'une substance classée comme stupéfiant (infraction punie par le Code des douanes), retenant comme base de la condamnation à la fois des articles du Code pénal et



du Code des douanes. Le pourvoi critique l'arrêt en considérant que les preuves obtenues par les douaniers n'étaient pas suffisantes dans le cadre de la procédure pénale. Si les procès-verbaux douaniers ont une force particulière, puisqu'en vertu de l'article 336 du Code des douanes, « les procès-verbaux de douane rédigés par deux agents des douanes ou de toute autre administration font foi jusqu'à inscription de faux des constatations matérielles qu'ils relatent », néanmoins, il faut voir ici une exception au droit commun, puisqu'en procédure pénale, l'article 430 du Code de procédure pénale « sauf dans le cas où la loi en dispose autrement, les procès-verbaux et les rapports constatant les délits ne valent qu'à titre de simples renseignements ». La liberté de la preuve étant le principe, tout mode de preuve permet de contredire les constatations contenues dans le procès-verbal, alors qu'en matière douanière, seule la procédure exceptionnelle de l'inscription en faux permet de les renverser. Or, les juges du fond avaient étendu la force probante exceptionnelle des procès-verbaux douaniers en matière pénale, retenant la culpabilité du prévenu sur cette même base pour les infractions punies par le Code pénal, tout comme pour les infractions punies par le Code des douanes. La Cour de cassation censure la décision au motif que « le procès-verbal de constatation ne valait qu'à titre de simple renseignement pour les délits de droit commun ». La liberté de la preuve reprend sa force en droit pénal et, si les juges peuvent fonder leur conviction sur le procès-verbal établi par les agents des douanes, ils doivent motiver leur décision et la fonder sur l'appréciation des différents éléments de preuve soumis à la discussion des parties, sans privilégier le procès-verbal douanier, simple renseignement, à mettre en balance avec les autres éléments de preuve. Même s'il s'agit d'une exigence principalement juridique, tant il paraît difficile en pratique de s'extraire de ce mode de preuve prépondérant, il convient de la respecter du point de vue du formalisme procédural. Néanmoins, la Cour de cassation ne suit pas le raisonnement suggéré par le pourvoi jusqu'à son terme. En effet, les faits de l'espèce relèvent d'un concours idéal de qualifications pénale et douanière. Le pourvoi suggère que « la valeur de procès-verbaux ne saurait varier lorsque les infractions poursuivies relèvent des mêmes faits, sans méconnaître l'article 6 de la Convention européenne des droits de l'Homme ». Ce serait une nouvelle conséquence procédurale indirecte du principe « ne bis in idem » appliqué à la

preuve. La Cour de cassation ne répond pas à cette critique, à juste titre, en application de sa jurisprudence traditionnelle dite « Ben Haddadi ». Lorsque les qualifications en concours portent atteinte à des valeurs sociales différentes, le cumul d'infractions est autorisé. En l'espèce, la qualification d'infraction relative à la législation sur les stupéfiants protège la santé publique, alors que l'infraction douanière poursuit comme but la réglementation de la circulation des marchandises. Si la valeur des moyens de preuve peut être affectée par la particularité de la matière traitée, cette dernière n'invalide pas les modes de preuve traditionnels de la procédure pénale.

## Garde à vue - Accès limité au dossier de la procédure

***Crim. 4 octobre 2016, n° 16-82309, publication Bull. à venir***

Dans son arrêt du 4 octobre 2016, la Chambre criminelle examine la conformité du régime de la garde à vue, notamment de l'accès aux différentes pièces du dossier, par rapport à différents textes européens. À l'issue d'un arrêt long, complexe et technique, elle valide le dispositif français actuel. Dans le cadre d'une affaire de vente de manuscrits précieux sous une forme inhabituelle pouvant constituer des pratiques commerciales trompeuses, la Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes (DGCCRF) a saisi le ministère public. La brigade de la délinquance économique a procédé à plusieurs gardes à vue, dont une à l'égard d'un professeur de droit. Une information a été ouverte des chefs de pratiques commerciales trompeuses, escroqueries en bande organisée, abus de biens sociaux et abus de confiance, blanchiment en bande organisée et l'intéressé a déposé une requête en annulation des pièces de la procédure qui a été rejetée. Il a formé un pourvoi en cassation contenant trois moyens.
Le premier moyen du pourvoi conteste la régularité de la procédure par rapport à l'article 6 de la Convention de sauvegarde des droits de l'Homme garantissant le droit au procès équitable. Plusieurs actes de la procédure font état d'une note du parquet contenant certains éléments de la procédure et de l'échange avec la DGCCRF, note qui ne lui a pas



été communiquée lors de sa garde à vue, ce qui lui aurait causé grief. La Chambre criminelle rejette le moyen car les références faites à la note du parquet par les autres pièces déterminent suffisamment le cadre de la procédure.
Le deuxième moyen du pourvoi soutient la violation de l'article 6 de la directive 2012/13/UE relative au droit à l'information dans le cadre des procédures pénales (le droit d'être informé de l'accusation portée contre soi) et de l'article 5-2 de la CEDH et critique une information insuffisante sur les qualifications retenues sans que les faits reprochés soient détaillés. La Chambre criminelle écarte la critique en considérant que « l'information délivrée au requérant à travers les qualifications des infractions, la période et le lieu, lui a permis de prendre connaissance des motifs de son placement en garde à vue dans le respect de ses droits et d'exercer normalement sa défense ; que les juges ajoutent que le requérant était parfaitement à même de discerner les contours du secret professionnel qui s'imposait à lui en sa qualité d'avocat et les hypothèses où les nécessités de sa propre défense pouvaient l'en délier et qu'il avait également été dûment informé de son droit au silence s'il craignait de manquer aux devoirs de son état ». Il est intéressant de remarquer qu'elle reprend à son compte l'analyse de la chambre de l'instruction sur les objectifs de la directive relative au droit à l'information qui est celle d'une nécessaire gradation des droits garantis en fonction du stade de la procédure auquel ils interviennent : « l'article 6, § 2, de la directive impose, en cas d'arrestation, la délivrance d'une information sur les motifs de l'arrestation, y compris de l'acte pénalement sanctionné imputé, tandis que l'article 6, § 3, impose une information détaillée au stade du jugement ». Ainsi, « l'article 63-1 du Code de procédure pénale constitue une transposition complète et conforme de l'article 6, § 2, de la directive en ce qu'il prévoit une information pour le gardé à vue sur les "motifs de l'acte pénalement sanctionné" transposés comme créant un droit à l'information sur la qualification, la date et le lieu présumés de l'infraction », ce qui correspond aussi aux exigences conventionnelles en la matière.
Ainsi, dans un attendu général et global, la Chambre criminelle fond les deux systèmes européens pour doublement valider le droit positif français : « d'une part, les dispositions de l'article 5, § 2, de la Convention européenne des droits de l'Homme ont pour seul objet d'aviser la per-

sonne arrêtée des raisons de sa privation de liberté afin qu'elle puisse en discuter la légalité devant un tribunal, d'autre part, l'article 6 de la directive du 22 mai 2012, dont le préambule précise qu'elle s'appuie sur les droits énoncés dans la Charte des droits fondamentaux de l'Union européenne en développant les articles 5 et 6 de la Convention européenne des droits de l'Homme tels qu'ils sont interprétés par la Cour européenne des droits de l'Homme, prescrit aux États membres de veiller à ce que les personnes arrêtées soient informées de l'acte pénalement sanctionné qu'elles sont soupçonnées d'avoir commis mais précise que les informations détaillées sur l'accusation, notamment sur la nature de leur participation, doivent être communiquées au plus tard au moment où la juridiction est appelée à se prononcer sur le bien-fondé de l'accusation et non pas nécessairement dès le stade de l'arrestation, ce dont il résulte que l'article 63-1 du Code de procédure pénale constitue une transposition complète de l'article 6 de ladite directive ».

Le troisième moyen critique l'article 63-4-1 du Code de procédure pénale qui prévoit une liste des pièces de procédure qui peuvent être consultées par l'avocat assistant la personne lors de la garde à vue, mais qui ne permet pas la transmission de la totalité des pièces comme étant contraire à l'article 7 de la directive 2012/13 UE relative au droit à l'information dans le cadre des procédures pénales, « alors que le principe du contradictoire, le respect des droits de la défense et l'équilibre des droits des parties imposent l'accès à l'entier dossier de la procédure dès le stade du placement en garde à vue ». La chambre de l'instruction avait rejeté cette critique en considérant que l'accès limité à certaines pièces du dossier était justifié « en ce qu'il introduit le droit pour le gardé à vue et son avocat de contrôler uniquement la légalité de la mesure de garde à vue, qui s'entend comme un contrôle sur le motif de la garde à vue qui doit être la suspicion d'une infraction criminelle ou délictuelle punie d'une peine d'emprisonnement, sur le déroulement régulier de la mesure avec notamment la notification de tous les droits et la vérification de leur mise en œuvre effective et sur la compatibilité de la mesure avec l'état de santé du gardé à vue ». De leur propre initiative, les juges d'instruction procèdent aussi à l'examen de conventionnalité et constatent que « l'absence de communication de l'ensemble des pièces du dossier, à ce stade de la procédure, n'étant pas de nature à priver la personne d'un droit effectif et concret à un procès équitable, l'accès à



ces pièces étant garanti devant les juridictions d'instruction et de jugement », adoptant ainsi une position conforme à la jurisprudence de la Cour de cassation qui s'était déjà prononcée sur cette question. Dès lors, la chambre criminelle valide aussi l'article 64-3-1 du Code de procédure pénale en constatant à la fois sa conventionnalité (la CEDH « n'exige, à tous les stades de la procédure, qu'un accès aux documents relatifs à l'affaire en question détenus par les autorités compétentes qui sont essentiels pour contester de manière effective la légalité de l'arrestation ou de la détention ») et sa conformité au droit de l'Union européenne (puisque la directive laisse la faculté aux États membres de n'ouvrir l'accès à l'intégralité des pièces du dossier que lors de la phase juridictionnelle du procès pénal).

## BRÈVES

### Constatation visuelle dans un parking sur autorisation

***Crim. 5 octobre 2016, n° 16-81843***

Le syndic d'une copropriété a autorisé les policiers à accéder à l'ensemble des espaces communs intérieurs. Les policiers ont pénétré dans le parking souterrain et effectué des constatations sur un véhicule volé et faussement immatriculé. La personne concernée a demandé la nullité des preuves, considérant qu'il s'agissait d'une perquisition et que les policiers devaient nécessairement avoir l'assentiment de la personne pour y procéder. En effet, se plaçant dans le cadre d'une enquête préliminaire, l'article 76 du Code de procédure pénale est applicable. « Les perquisitions, visites domiciliaires et saisies de pièces à conviction ou de biens dont la confiscation est prévue à l'article 131-21 du Code pénal ne peuvent être effectuées sans l'assentiment exprès de la personne chez laquelle l'opération a lieu ». La chambre de l'instruction a écarté la demande et a relevé « que les surveillances litigieuses opérées par les enquêteurs dans ledit parking n'étaient que de simples constatations visuelles, et que l'autorisation donnée préalablement par le syndic aux policiers, agissant en enquête préliminaire, leur permettait

de pénétrer dans le parking ». Le mis en examen a formé un pourvoi en cassation à moyen unique en deux branches. D'une part, le moyen d'investigation est critiqué car « la pénétration des enquêteurs dans un immeuble privé doit être qualifiée de perquisition, quand bien même elle ne donnerait lieu à aucune saisie » puisque la perquisition « se définit comme la recherche, à l'intérieur d'un lieu normalement clos, des indices permettant d'établir l'existence d'une infraction ou d'en déterminer l'auteur ». D'autre part, la perquisition est entachée de nullité puisque l'autorisation du syndic ne remplit pas les conditions de l'article 76, seule l'autorisation de la majorité des copropriétaires correspondant à la condition légale. La Chambre criminelle rejette expressément les deux critiques, en inversant l'ordre. D'une part, « les policiers, agissant en enquête préliminaire, ont été spécialement autorisés, en connaissance de cause, par le syndic de copropriété à pénétrer dans les parties communes d'une résidence ». D'autre part, les policiers « n'ont procédé, sur ledit véhicule volé en stationnement dans le parking, qu'à de simples constatations visuelles, lesquelles, n'entrant pas dans les prévisions de l'article 76 du Code de procédure pénale, ne sont pas assimilables à une perquisition ». La solution arrêtée par la Chambre criminelle est classique en reprenant des solutions récentes importantes. Un arrêt rendu par la Chambre criminelle le 27 mai 2009 (Bull. n° 108) analyse les parties communes d'un immeuble comme étant un lieu privé et les soumet, de fait, à une autorisation de pénétration de la part de la personne compétente. La Cour de cassation interprète très largement ce pouvoir puisque l'autorisation peut être donnée par le syndic, représentant la volonté générale de la copropriété, mais aussi par un résident, raison pour laquelle l'arrêt commenté rappelle que la personne concernée par la procédure pénale, locataire de l'immeuble, avait aussi un droit sur son appartement et les dépendances. Une fois qu'ils pénètrent sur autorisation dans l'immeuble, les policiers ne peuvent pas procéder à tous actes. Par conséquent, la Chambre criminelle rappelle que les policiers n'ont procédé qu'à de simples constatations visuelles qui ne sont pas assimilables à une perquisition et ne sont donc pas soumises aux exigences de l'article 76 du Code de procédure pénale. Dans deux arrêts allant dans le même sens (Crim. 2 octobre 2013 n° 12-87976 et Crim. 23 octobre 2013 n° 13-82762), elle dessinait une ligne de séparation entre les deux types d'investigation reposant sur l'absence d'acte



de coercition, ce qui lui permettait de conclure à la conventionnalité du procédé au regard de l'article 8 de la CEDH. L'arrêt du 5 octobre 2016 s'inscrit dans cette lignée, reprenant l'analyse retenue dans un arrêt rendu par la Cour de cassation le 14 octobre 2015 n° 15-81765, pérennisant de fait la solution.

## Preuve des contraventions

***Crim. 20 septembre 2016, n° 16-80148, publication Bull. à venir***

Une personne a été condamnée par le juge de proximité sur la foi d'un procès-verbal mentionnant « changement de direction sans avertissement préalable ». Elle a contesté la décision car le procès-verbal ne comportait pas de précision sur les circonstances dans lesquels les faits reprochés ont été commis. La juridiction d'appel a considéré que le procès-verbal était régulier en la forme et que le prévenu n'apportait pas de preuve contraire, donc a confirmé la décision de condamnation. La Chambre criminelle rejette les deux branches du pourvoi, apportant des précisions de fond et de forme. D'une part, les constatations de l'agent verbalisateur « suffisent à établir la matérialité de l'infraction relevée ». D'autre part, le prévenu n'a pas contesté la connaissance des faits lors de son interpellation immédiate.

En premier lieu, les règles de preuve applicables aux contraventions sont particulières. Selon l'article 537 du Code de procédure pénale, en matière contraventionnelle, les procès-verbaux font foi jusqu'à preuve contraire, qui ne peut être apportée que par écrit ou témoins. L'article 429 définit les conditions de validité de ces modes de preuves : « Tout procès-verbal ou rapport n'a de valeur probante que s'il est régulier en la forme, si son auteur a agi dans l'exercice de ses fonctions et a rapporté sur une matière de sa compétence ce qu'il a vu, entendu ou constaté personnellement ». La Cour de cassation relève ainsi, dans le sillage des juges du fond, que selon « les constatations de l'agent verbalisateur, le véhicule conduit par … a opéré, au lieu indiqué, un changement de direction sans avertissement préalable » et rajoutent que ces remarques « suffisent à établir la matérialité de l'infraction relevée ». En

effet, la contravention reste la seule infraction matérielle depuis l'entrée en vigueur du nouveau Code pénal. Cela ne signifie nullement que l'élément moral n'est pas requis dans le cadre de la qualification, mais que sa preuve n'est pas exigée. La seule constatation matérielle des faits emporte qualification pénale.
En deuxième lieu, l'exigence de la rédaction dans le procès-verbal des circonstances exactes de l'infraction pouvait renvoyer aussi à la violation du droit à l'information de la personne mise en cause. La Chambre criminelle prend la précaution de relever que cet élément n'est nullement contesté lors de l'interpellation immédiate de la personne.



**Par M. Ludovic GUINAMANT**

## Premier bilan du contrôle des techniques de renseignement et de l'utilisation des fichiers de renseignement par le Conseil d'État

***Conseil d'État, 19 octobre 2016, formation de jugement spécialisée, n°396503, n°396505, n°396512, n°396518, n°396521, n°396524, n°396558, n°396561, n°396635, n°396958, n°397623, n°398654, n° 398658, n°400658, n°401976.***

***Décret n°2016-1337 du 7 octobre 2016 portant changement d'appellation de la direction de la protection et de la sécurité de la défense***

***Projet de loi relatif au statut de Paris et à l'aménagement métropolitain***

La loi n° 2015-912 du 24 juillet 2015 a profondément renouvelé le contrôle par le juge des techniques et des fichiers de renseignement. Elle a donné au Conseil d'État compétence pour juger directement des recours concernant la mise en œuvre des techniques de renseignement (articles L. 841-1 du Code de la sécurité intérieure). En outre, la loi a donné compétence au Conseil d'État pour juger des requêtes concernant la mise en œuvre de l'article 41 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, pour les traitements ou parties de traitements intéressant la sûreté de l'État (article L. 841-2 du Code de la sécurité intérieure).

Le Conseil d'État peut ainsi être saisi par toute personne souhaitant vérifier qu'aucune technique de renseignement n'est irrégulièrement mise en œuvre à son égard ainsi que par la Commission nationale de contrôle des techniques de renseignement. Il peut également être saisi des décisions de la CNIL lorsqu'elle effectue des vérifications dans les fichiers intéressant la sûreté de l'État.

## Police administrative

Le Conseil d'État peut également être saisi d'une question par un juge judiciaire ou administratif lorsque celui-ci s'interroge, dans le cadre d'un dossier qu'il traite, sur la régularité d'une ou de plusieurs techniques de recueil de renseignement.

Pour examiner ces recours relatifs aux techniques de renseignement et aux fichiers informatiques intéressant la sûreté de l'État, la loi a créé au sein du Conseil d'État une formation de jugement spécialisée composée de cinq membres et de deux rapporteurs publics, tous habilités au secret de la défense nationale. Les décisions rendues par la formation spécialisée sont publiques mais elles ne peuvent en aucun cas révéler des éléments couverts par le secret et protégés par la loi.

Lorsque la formation spécialisée constate qu'aucune illégalité n'a été commise en matière de technique de renseignement ou d'inscription dans un fichier informatique intéressant la sûreté de l'Etat, soit que la personne ne fasse l'objet d'aucune technique de renseignement ou d'aucune inscription dans un fichier, soit qu'elle en fasse l'objet mais dans des conditions régulières, la décision de la formation spécialisée se contente d'indiquer qu'aucune illégalité n'a été commise. Elle ne confirme pas, et n'infirme pas non plus, la mise en œuvre d'une technique et ne révèle pas si le requérant figure ou non dans le fichier. En dire davantage reviendrait en effet à trahir le secret protégé par la loi.

En revanche, lorsque la formation spécialisée constate une illégalité, elle peut annuler l'autorisation de recourir à la technique de renseignement, ordonner la destruction des renseignements collectés, ordonner la rectification ou l'effacement des données contenues dans un fichier et indemniser un préjudice. En ce cas sa décision mentionne l'illégalité, mais sans faire état d'aucun élément protégé par le secret de la défense nationale.

La formation spécialisée a rendu le 19 octobre 2016 ses 15 premières décisions et un premier bilan peut être effectué au regard de ces décisions rendues par la cour suprême de l'ordre administratif.



## Police administrative

### Un contrôle des techniques de renseignement limité en ce qui concerne les communications électroniques internationales

Cinq décisions concernent directement des particuliers qui ont souhaité faire vérifier qu'aucune technique de renseignement n'avait été irrégulièrement mise en œuvre à leur égard et, le cas échéant, de faire constater que les techniques utilisées étaient illégales.

Parmi ces cinq dernières décisions, le Conseil d'État a informé quatre requérants qu'il avait procédé aux vérifications nécessaires et les a informés que celles-ci n'appelaient aucune mesure de sa part.

En revanche, dans sa décision n°397623, M. A, requérante, sollicitait le Conseil d'État afin de vérifier si des techniques de renseignement ont été mises en œuvre pour surveiller ses communications électroniques internationales. Néanmoins, le Conseil d'État rejette la requête comme étant irrecevable en précisant que lorsqu'elle *« constate qu'un manquement a été commis dans la mise en œuvre d'une mesure de surveillance internationale, la Commission adresse au Premier ministre une recommandation tendant à ce que le manquement cesse et que les renseignements collectés soient, le cas échéant, détruits. Si le Premier ministre n'a pas donné suite ou a insuffisamment donné suite à cette recommandation, le président de la Commission ou trois de ses membres peuvent saisir le Conseil d'État d'une requête. Alors même que la personne faisant l'objet d'une mesure de surveillance internationale ne peut saisir un juge pour contester la régularité de cette mesure, le législateur a assuré une conciliation qui n'est pas manifestement disproportionnée entre le droit à un recours juridictionnel effectif et le secret de la défense nationale en prévoyant que la Commission peut former un recours à l'encontre d'une mesure de surveillance internationale, ainsi que l'a jugé le Conseil constitutionnel dans sa décision n° 2015- 722 DC du 26 novembre 2015 ».*

Le Conseil d'État, conformément à la loi du 24 juillet 2015, distingue donc bien le contrôle des techniques de renseignement lorsqu'elles sont effectuées en France, des techniques de renseignement spéci-

fiques, prévues à l'article L. 851-4 du Code la sécurité intérieure et suivants, applicables aux mesures de surveillance des communications électroniques internationales. Dans ce dernier cas, il est constant que le degré de contrôle du Conseil d'État est moindre dès lors que seul le président de la Commission Nationale de Contrôle des Techniques de Renseignement (CNCTR), autorité administrative indépendante prévue par les articles L. 831-1 du Code de la sécurité intérieure, a la possibilité de saisir le Conseil d'État dans le cadre du contrôle des techniques de renseignement des communications électroniques internationales.

### Un contrôle des décisions de la CNIL systématiquement validé par le Conseil d'État

Pour les dix autres décisions, les requérants sollicitaient l'annulation des décisions de la CNIL relatives à des fichiers gérés par le ministère de la Défense. Cinq requérants demandaient des informations contenues dans le fichier de la Direction Générale de la Sécurité Extérieure (DGSE), cinq dans le fichier de la Direction de la Protection et de la Sécurité de la Défense (DPSD, devenue par décret n°2016-1337 du 7 octobre 2016 la Direction du Renseignement et de la Sécurité de la Défense – DRSD), et un dans celui de la Direction du Renseignement Militaire (DRM). L'ensemble des requêtes a fait l'objet d'un renvoi sans motivation.

L'article R. 841-2 du Code de la sécurité intérieure prévoit l'ensemble des traitements automatisés qui peuvent être contrôlés par le Conseil d'État au titre de la loi du 24 juillet 2015. En effet, cette disposition réglementaire évoque de manière exhaustive : le fichier CRISTINA créé au profit de la Direction Générale de la Sécurité Intérieure (DGSI), les fichiers mis en œuvre par la DGSE et la DRM, celui nommé SIREX mis en œuvre par la DPSD (DRSD depuis le 7 octobre 2016), le FSPRT, le FPR (Fichier des Personnes Recherchées) en ce qui concerne les seules données intéressant la sûreté de l'État, le fichier STARTRAC de TRACFIN (Traitement du Renseignement et Action contre les Circuits Financiers Clandestins), le SIS (Système d'Information Schengen) en ce qui concerne la prévention d'une menace grave émanant de l'intéressé ou d'autres menaces graves pour la sûreté intérieure et extérieure de l'État et le BCR-DNRED de la direction générale des douanes et des droits indirects.



### Un contrôle indirect des décisions préfectorales prises en matière de police administrative de la prévention du terrorisme

Par ailleurs, il convient de préciser qu'une des requêtes (n°396503) intervenait, indirectement, dans le cadre d'une décision du préfet délégué à la sécurité des plateformes aéroportuaires de Roissy-Charles-de-Gaulle et du Bourget, en délégation de signature du préfet de Seine-Saint-Denis, refusant de renouveler une habilitation d'accès aux zones de sûreté aéroportuaire qui se fondait sur le fichier de la DGSE.

Le requérant ayant choisi de solliciter la CNIL le 24 janvier 2015 afin d'avoir accès aux informations contenues dans le fichier de la DGSE, par une lettre du 17 novembre 2015, la présidente de la CNIL a informé le requérant qu'il avait été procédé à l'ensemble des vérifications demandées s'agissant de ce fichier et que la procédure était terminée, sans apporter à l'intéressé d'autres informations.

Le requérant a alors saisi le TA de Paris le 19 janvier 2016 en demandant l'annulation de la décision de la CNIL et à ce qu'il soit enjoint au ministre de la défense de lui communiquer les informations, issues du fichier DGSE, qui ont été transmises au préfet délégué à la sécurité des plateformes aéroportuaires de Roissy-Charles-de-Gaulle et du Bourget. Le TA, incompétent au titre de la loi du 27 juillet 2015, a alors transmis la requête au Conseil d'Etat qui a rejeté, après examen des éléments transmis par la CNIL et le ministre de la défense, la requête dans la décision n°396503 du 19 octobre 2016.

On peut se demander ce que le TA de Montreuil, compétent pour les décisions de refus de renouvellement des habilitations à la plateforme de Roissy (Conseil d'État, 2ème et 7ème chambres réunies, 8 juin 2016,

n°398061 et veille juridique N°49 du mois de juin 2016 - pp.46-47), aurait décidé s'il avait été directement saisi de la légalité de cette décision assortie d'un moyen tiré de l'illégalité des informations, dont la source n'est pas uniquement inscrite dans le fichier de la DGSE mais peut provenir de techniques de renseignement, transmises au préfet délégué.

En effet, il nous semble que, dans ces conditions, le TA de Montreuil aurait dû saisir le Conseil d'État, sans passer par la CNIL, au titre de l'article L. 841-1 du Code de la sécurité intérieure qui prévoit que : *« Lorsqu'une juridiction administrative ou une autorité judiciaire est saisie d'une procédure ou d'un litige dont la solution dépend de l'examen de la régularité d'une ou de plusieurs techniques de recueil de renseignement, elle peut, d'office ou sur demande de l'une des parties, saisir le Conseil d'État à titre préjudiciel. Il statue dans le délai d'un mois à compter de sa saisine »*.

Enfin, il convient de préciser que la loi relative au statut de Paris et à l'aménagement métropolitain, dans son article 27, actuellement en cours d'examen devant le Sénat, prévoit que le ressort territorial du préfet de police sera étendu aux emprises aéroportuaires de Seine-et-Marne et du Val-d'Oise, départements dans lesquels les aéroports de Roissy-Charles-de-Gaulle et du Bourget se situent. Cette loi, si elle est adoptée dans les mêmes termes, ne modifiera pas la compétence générale du TA de Montreuil dès lors que les *« litiges relèvent de la compétence du tribunal administratif dans le ressort duquel se trouve le lieu d'exercice de la profession faisant l'objet de la réglementation en cause »*.

Ce premier bilan résultant des premières décisions du Conseil d'État semble montrer qu'il n'y a pas d'utilisation abusive de la police administrative liée aux techniques de renseignement et aux fichiers de renseignement par les autorités administratives.

Le nombre de recours devant le Conseil d'État reste néanmoins encore limité mais devrait connaître une augmentation importante dans les prochains mois, compte tenu de l'augmentation croissante de décisions prises par les autorités administratives se fondant sur des notes



blanches ou sur des données provenant de fichiers de renseignements.

**Par M. Xavier LATOUR**

## Quelle police municipale ?

En septembre 2016, le ministère de l'Intérieur a publié sa feuille de route pour les années à venir. La perspective est celle des années 2030 avec un objectif affirmé dans le titre du document, « L'autorité de l'État au service des Français ».

Malgré un propos essentiellement consacré à l'État central, le document n'ignore pas la dimension territoriale.
Il aborde ainsi brièvement la question des polices municipales.

D'une part, le ministère programme l'évaluation des équipements autorisés. Ce bilan s'impose, en effet, en raison de l'exposition à des menaces accrues des policiers municipaux.
Pour mémoire, des efforts substantiels ont déjà été faits par l'État. L'amélioration de l'interopérabilité des réseaux de communication et une amélioration de l'armement sont des acquis relativement récents. Dès la fin du mois de janvier 2015, le gouvernement annonçait la mise à la disposition des communes de 4000 revolvers pour les policiers municipaux et une aide à l'achat de 8000 gilets pare-balles. Ces orientations ont été mises en application par le décret 2015-496 du 29 avril 2015 qui autorise les agents de police municipale à utiliser, à titre expérimental, des revolvers chambrés pour le calibre 357 magnum. Les autorisations de prélèvements sur le stock étatique semblent cependant être octroyées avec parcimonie.
Apparemment, l'État n'entend pas en rester là. En partie sous la pression des événements et sous celle des syndicats de policiers municipaux, la voie d'un armement plus puissant semble s'entrouvrir. Il reste à déterminer lequel et dans quelles conditions. Pour calmer l'impatience des policiers municipaux, le délégué aux coopérations de sécurité a précisé, le 27 septembre 2016, qu'aucune évolution n'était envisageable à court terme.
En outre, l'accès des policiers municipaux à de nouvelles armes impliquerait nécessairement d'adapter leur formation. Dans un passé pas si



lointain, le Conseil d'État avait été très sourcilleux quant à l'utilisation des pistolets à impulsion électrique. Une vigilance de ce type ne surprendrait pas pour des armes puissantes.
En revanche, le ministère ne répond pas, pour le moment, à une demande forte des syndicats qui revendiquent le droit pour les policiers municipaux de conserver leur arme en dehors de leur service, comme cela est autorisé pour les policiers et les gendarmes nationaux.

D'autre part, le document traite de la question récurrente des partenariats.
L'ambition est alors d'améliorer la définition et la coordination des différents acteurs de la sécurité. Les polices municipales sont appelées à évoluer en raison de la montée en puissance des métropoles et des intercommunalités.
En l'état actuel des choses, les possibilités offertes par le Code de la Sécurité Intérieure (CSI) et le Code Général des Collectivités Territoriales (CGCT) de rationalisation et de mutualisation des polices municipales n'ont pas remporté le succès escompté.
Sans évoquer les mises en commun ponctuelles, le droit positif offre deux possibilités.
La première est celle d'une création par un Établissement Public de Coopération Intercommunale (EPCI) sur le fondement de l'article L 512 -2 CSI. Un EPCI à fiscalité propre peut recruter un ou plusieurs agents de police municipale en vue de les mettre à la disposition de l'ensemble des communes.
La décision est prise à la demande des maires de plusieurs communes. Elle est subordonnée à une délibération des deux tiers au moins des conseils municipaux des communes, représentant plus de la moitié de la population totale de celles-ci, ou de la moitié au moins des conseils municipaux des communes représentant les deux tiers de la population.
La suivante consiste pour les communes à mettre en commun des policiers municipaux (article L 512-1 CSI). Les communes de moins de 20 000 habitants formant un ensemble de moins de 50 000 habitants d'un seul tenant peuvent avoir un ou plusieurs agents de police municipale en commun, compétents sur le territoire de chacune d'entre elles. Une convention conclue entre les communes intéressées précise les moda-

lités de la mise en commun des agents et de leurs équipements. La convention est signée par l'ensemble des maires des communes concernées, après délibération de leurs conseils municipaux, pour une durée minimale d'un an. Cette convention fixe les conditions de son renouvellement ainsi que les conséquences du retrait d'une commune.

Toutefois, le ministre de l'Intérieur a d'ores et déjà annoncé réfléchir à une modification de ces seuils. Sous-évalués, ils ne permettraient pas à de grandes agglomérations de mutualiser leurs effectifs. Une expérimentation lancée en Seine-Saint-Denis pendant cinq ans aidera, selon le ministre, à préciser les besoins.
La multiplication des métropoles, nouvelle forme d'intercommunalité, n'est pas étrangère à cette approche renouvelée. En matière de décentralisation, la volonté politique de réduire les strates et l'éparpillement communal constitue une constante des gouvernements depuis plusieurs années. La métropole répond au souci de constituer des pôles urbains autour de villes suffisamment importantes pour fédérer autour d'elles les énergies. À Lyon, Marseille, Nice, Lille… les compétences sont redistribuées entre les communes membres de la métropole, voire des collectivités territoriales d'un niveau supérieur, comme le département.
Ce mouvement de recomposition territoriale influencera l'exercice des compétences en matière de sécurité. Les polices municipales deviendront-elles des polices métropolitaines ? Les départements et les régions tenteront-ils d'investir le champ de la sécurité au nom d'une efficacité accrue par la taille ou par une spécialisation des missions (dans les établissements scolaires ou les transports par exemple) ?

Parallèlement, les communes essaient, elles aussi, de faire bouger les lignes. Les moyens à leur disposition sont cependant limités.
Par nature régalien, le droit de la sécurité ne laisse qu'une marge de manœuvre limitée aux collectivités territoriales. L'État peut seul déterminer par voie législative à titre principal et par voie réglementaire à titre complémentaire le cadre de fonctionnement, les prérogatives des polices municipales, ainsi que les moyens matériels à leur disposition.

Ces derniers mois, certaines communes se sont interrogées sur le



fonctionnement et l'avenir de leur police municipale.
Beauvais a notamment organisé, en septembre 2015, une consultation locale pour savoir si ses habitants souhaitaient avoir une police municipale armée. La réponse négative a contraint le maire à refuser à ses policiers ce qu'ils demandaient et demandent d'ailleurs encore.
Plus récemment, Nice a lancé une vaste enquête afin de déterminer les attentes de ses administrés. Le questionnaire très détaillé est révélateur des hésitations des maires quant au modèle de police municipale qu'ils veulent.

Initialement pensée pour être une police de proximité, la police municipale s'est transformée jusqu'à devenir très hétérogène. Les 21 000 policiers municipaux répartis dans environ 4000 communes sont souvent très différents les uns des autres. La taille de la police n'est pas la seule explication, pas plus que son armement non obligatoire, mais largement répandu (2/3). La compréhension de la diversité est à rechercher du côté de leurs conditions d'emploi. À cet égard, l'État et les maires ont chacun contribué à en redessiner les contours.

L'État a régulièrement renforcé la dimension pénale des polices municipales. Un nombre croissant d'infractions sont entrées dans leur champ de compétences, même si elles sont quasi exclusivement contraventionnelles. De surcroît, elles dépassent le cadre strict des compétences du maire pour entrer dans des domaines plus généraux, notamment la sécurité routière.
En revanche, l'investigation leur demeure fermée. Les polices municipales restent marquées par une action préventive.

Les maires ont, eux aussi, contribué à l'évolution. Si certains d'entre eux se sont contentés d'avoir une police municipale modeste en nombre et en domaines d'action (sécurité routière, stationnement, présence sur la voie publique…), d'autres ont opté pour une conception plus dynamique et volontariste.
Ils structurent leur police municipale en s'inspirant largement de l'organisation de la police nationale. Ils l'équipent en moyens performants (motos, véhicules…), pour en faire une police prenant une part active dans la lutte contre la délinquance.

## Droit des collectivités territoriales

Le stade de la prévention est dépassé pour celui d'une capacité répressive fondée sur une utilisation a maxima des possibilités offertes par le Code de procédure pénale en matière de flagrant délit de crime ou de délit. Dans l'esprit de certains maires, la prochaine étape serait la recherche d'auteurs de petites infractions. La police municipale entrerait alors dans l'ère de la police judiciaire. Le modèle traditionnel de répartition des compétences en serait inévitablement bouleversé, tout comme la prééminence de l'État en matière de sécurité.

En attendant, les inégalités se creusent sur le territoire selon les capacités financières des communes et leurs choix opérationnels. Une réflexion sur l'avenir des polices municipales a été engagée depuis plusieurs années avec l'ambition de voter une nouvelle loi. La complexité du sujet et le calendrier électoral ne laissent cependant pas augurer un aboutissement à brève échéance.

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