La veille juridique

N°65, février 2018

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

Edito

Le Conseil constitutionnel devrait rendre, le 21 mars 2018, sa décision QPC relative à l'article 434-15-2 du Code pénal qui incrimine « toute personne » qui ne remet pas aux autorités judiciaires la clef de déchiffrement relative à un document pouvant avoir servi à la préparation ou à la commission d'une infraction. Cette décision va sans doute consister en une déclaration de constitutionnalité sous réserve : le texte ne s'appliquerait pas aux auteurs coauteurs ou complices en vertu du droit de se taire et de ne pas s'auto-incriminer. Il demeurerait applicable aux tiers, fournisseurs de clefs de chiffrement.

Cette QPC appelle plusieurs remarques :
L'article a été introduit dans le Code pénal par la loi du 15 novembre 2001. On sait combien elle fut influencée par l'émotion due aux attentats du 11 septembre. Fruit d'un amendement, l'article a été voté sans véritable débat, ce qui rend difficile

(Suite page 2)

EDITORIAL

l'interprétation de la volonté du législateur. Il est aujourd'hui soumis à l'examen des Sages, plus de 16 ans après sa promulgation. Durant cette période, il a été mis en application, y compris à l'égard d'auteurs, de coauteurs ou de complices. C'est dire l'incertitude juridique qui pèse sur un texte qui n'a pas été « blanchi » par voie d'action. Faudrait-il modifier le droit constitutionnel en prévoyant une saisine obligatoire du Conseil dès lors qu'il s'agit de vérifier la constitutionnalité d'un texte modifiant le droit ou la procédure pénale ou de tout autre texte de nature à porter atteinte à une liberté publique ? La responsabilité du législateur perdrait ce que gagnerait la stabilité juridique.

Les QPC portées devant le Conseil constitutionnel mettent souvent en balance les exigences de sécurité et celles de liberté. Les Sages apportent une réponse qui vérifie si une atteinte à la seconde par la première est nécessaire, adaptée et proportionnée à l'intérêt social poursuivi. Cet équilibre est d'ailleurs celui sur lequel repose la notion d'ordre public. Parfois les commentaires relatifs à la décision sont critiques et font état d'une démobilisation, d'une entrave à l'action des forces en charge de la sécurité au profit de la reconnaissance de droits aux délinquants. Cette opinion est fausse et dangereuse. Fausse, car le Conseil constitutionnel comme la Cour de cassation disent le droit, tout le droit, rien que le droit. Ce droit est souvent influencé par des règles conventionnelles qui l'encadrent. Dangereuse, car elle laisse accroire qu'il n'y a pas de limite à l'action, dès lors que l'on combat un adversaire, voire un ennemi de la société. Sans barrière, toutes les dérives sont possibles, au nom d'une cause certes légitime mais qui se dénature dans l'action. C'est le rôle des juges d'éviter que la machine ne s'emballe. Le droit doit évoluer, s'adapter mais avec une recherche d'équilibre, de « sang-froid juridique ». Ce principe de modération peut entraîner pour les démocraties la perte d'une « bataille » mais il assure la « victoire finale ». C'est un sujet permanent de réflexion pour le gendarme « soldat de la loi ».

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

VEILLE JURIDIQUE DE LA GENDARMERIE NATIONALE

Sommaire

Déontologie et sécurité

Par M. Frédéric Debove

Trois personnes peuvent garder un secret, si deux d'entre elles sont mortes (Benjamin Franklin)

Comme le disait avec humour Guy Bedos, « *la célébrité n'est pas facile à assumer, je ne vois rien de pire, si peut-être, l'anonymat !* ». Or, c'est précisément l'anonymat qui se trouve au cœur de l'arrêt de la Chambre criminelle de la Cour de cassation en date du 12 décembre 2017 (pourvoi n°17-80821, à paraître au bulletin). Dans cette décision, la Haute juridiction s'est prononcée sur les contours d'une incrimination pénale qui intéresse de près les forces de l'ordre puisqu'il s'agit du délit inscrit à l'article 39 sexies (sic !) de la loi du 29 juillet 1881 sur la liberté de la presse. Dans sa rédaction issue de la loi n°2009-971 du 3 août 2009 relative à la gendarmerie nationale, l'incrimination punit d'une amende de 15 000 euros le fait de « révéler, par quelques moyen d'expression que ce soit, l'identité des fonctionnaires de la police nationale, de militaires, de personnels civils du ministère de la défense ou d'agents des douanes appartenant à des services ou unités désignés par arrêté du ministre intéressé (singulièrement les arrêtés du 7 avril 2011 et du 20 novembre 1995) et dont les missions exigent, pour des raisons de sécurité, le respect de l'anonymat ».
En l'occurrence, un fonctionnaire de police appartenant au Groupe de sécurité de la présidence de la République (GSPR), désigné par arrêté du 7 avril 2011 comme devant bénéficier de l'anonymat pour des raisons de sécurité, avait déposé plainte auprès du procureur de la République de Paris, du chef de l'infraction prévue et réprimée par l'article 39 sexies de la loi du 29 juillet 1881. Sa plainte faisait suite à la publication, dans le journal *Closer* du 13 au 26 février 2015, d'un article contenant diverses informations qui auraient permis de l'identifier. Plus précisément, les informations litigieuses se rapportaient à la publication de plusieurs photographies accompagnées d'un texte faisant état de la « protection régulièrement assurée par "M"... "fonctionnaire à la petite cinquantaine"... "premier des " sièges du Président au sein du GSPR (Groupe de sécurité de la présidence de la République) "... " issu de l'ex-service de protection des hautes personnalités (devenu le Service

de la protection)" ».

Souvent juges varient, bien fol qui s'y fie

En première instance, devant le tribunal correctionnel de Paris, le directeur de publication du magasine *Closer* avait été renvoyé des fins de la poursuite. Le ministère public ayant relevé appel de cette décision, la chambre des appels correctionnels de la Cour d'appel de Paris confirmait par la suite cette première décision dans un arrêt en date du 12 janvier 2017. Pour écarter la prévention, les juges d'appel fondaient alors leur décision de relaxe sur une double série de considérations. En premier lieu, le délit de l'article 39 sexies de la loi du 29 juillet 1881 ne prohiberait en effet que la seule révélation de l'état civil des fonctionnaires concernés. Partant, l'interdiction ne saurait être interprétée comme pouvant s'appliquer à tout élément susceptible d'en permettre l'identification, voire à la diffusion de leur image. En second lieu, l'élément de révélation supposerait que cette identité n'ait pas été précédemment révélée ; or, dans le cas de l'espèce, le magasine *Closer* n'était pas à l'origine de la révélation initiale.
Dans son arrêt en date du 12 décembre 2017, la Chambre criminelle de la Cour de cassation censure cette interprétation jugée par trop restrictive de l'article 39 sexies de la loi du 29 juillet 1881. Dans un attendu de principe aussi ferme que péremptoire, la Haute juridiction considère en effet « qu'en statuant ainsi, sans mieux rechercher si les éléments fournis par le journal "Closer" au sujet de ce policier permettaient de l'identifier, et alors que la diffusion de précédentes informations relatives à l'intéressé ne faisait pas obstacle à la caractérisation de l'infraction, la cour d'appel a méconnu » le texte de l'article 39 sexies de la loi du 29 juillet 1881 et le principe selon lequel tout arrêt doit comporter les motifs propres à justifier la décision (toute insuffisance ou contradiction de motifs étant équivalente à une absence de motifs).
Rendu dans un domaine vierge de toute jurisprudence notable depuis la création de l'incrimination litigieuse, cet arrêt de la Chambre criminelle de la Cour cassation est riche d'enseignements, s'agissant de la portée

du délit inscrit à l'article 39 sexies de la loi du 29 juillet 1881. *L'apport le plus notable (et sans nul doute le plus douteux) de l'arrêt est de considérer que l'interdiction formulée par la loi sur la presse n'est pas limitée à la révélation des noms et prénoms des personnes concernées mais s'applique à la diffusion d'informations qui en permettent l'identification. Autant dire, l'identification d'une personne est dorénavant assimilée à son identité au regard de la répression de la révélation. Mutatis mutandis*, il est permis de considérer que cette jurisprudence extensive n'est pas cantonnée au seul droit de la presse mais doit s'appliquer à d'autres Codes protecteurs de l'anonymat des forces de l'ordre, comme le Code de procédure pénale. En considération d'un tel raisonnement, le délit de révélation de l'identité d'un agent infiltré (art. 706-84 C. pr. pén.) devrait à l'avenir pouvoir être caractérisé non seulement dans l'hypothèse de la révélation des noms et prénoms des agents concernés mais également dans des circonstances où sont diffusées des informations permettant l'identification des intéressés.

Poenalia sunt restringenda

En même temps que l'on peut aisément comprendre l'intérêt pratique d'une telle solution jurisprudentielle (singulièrement en termes de protection des forces de l'ordre), l'interprétation analogique sur laquelle elle repose n'est pas à l'abri de la critique. En effet, toute la matière pénale est gouvernée par la règle aussi ferme que traditionnelle selon laquelle la loi pénale est d'interprétation stricte (art. 111-4 C. pén.). *Poenalia sunt restringenda*, mais la question se déplace : qu'est-ce qu'une interprétation stricte ?
Interprétation stricte ne signifie pas interprétation littérale ou grammaticale. Le principe en est l'attachement à la lettre du texte à l'égard duquel l'interprète professe un respect quasi religieux. Présumée parfaite, la loi pénale doit être lue comme le hiéroglyphe que déchiffre l'égyptologue. En ce qu'elle s'adonne à un véritable culte de la loi, la méthode littérale ou « judaïque » s'inscrit *a priori* dans le prolongement du principe de légalité. Bonne en soi, cette méthode présente cependant des inconvénients en certaines circonstances. Si, par

exemple, une contradiction apparaît entre ce qu'a voulu le législateur et ce qu'il a écrit, c'est le texte de la loi qui doit nécessairement l'emporter. Une telle conclusion n'est pas satisfaisante, tant s'en faut. C'est pourquoi, la jurisprudence criminelle n'hésite pas à rectifier la portée d'un texte dont la lettre trahit la pensée de ses rédacteurs.

En règle générale, l'interprétation stricte n'est pas davantage synonyme de celle qui s'opère par analogie ou induction. À la vérité, la méthode analogique est plus qu'une technique d'interprétation, puisqu'elle consiste à étendre la solution énoncée pour un cas à des cas semblables pour lesquels la loi est muette. Dans le silence du législateur, le juge est ainsi conduit à appliquer au comportement qui lui est soumis la règle prévue pour un cas voisin mais différent. Admis en d'autres matières, l'argument d'analogie (*a pari*) est en principe rejeté en droit pénal car, à vouloir trop étirer le texte, on finit par condamner sans texte. En raisonnant par analogie, le juge pénal pourrait par exemple réprimer l'abus de biens sociaux commis dans une société de personnes, alors que la loi n'envisage ce délit que pour certaines sociétés de capitaux. Pareillement, le raisonnement analogique permettrait d'assimiler la simple consultation de sites pédophiles à de la détention d'images de mineurs à caractère pornographique (or consulter n'est pas détenir), de la même manière qu'une comptabilité irrégulière pourrait être considérée comme une comptabilité totalement fictive. Prohibée lorsqu'elle est défavorable au prévenu (*in malam partem*), l'interprétation par analogie est en revanche admise dès lors qu'elle lui profite (*in favorem*). La solution est traditionnelle en jurisprudence. À bien y regarder, l'interprétation stricte prend souvent la forme, en jurisprudence, de l'interprétation téléologique ou déclarative. Derrière la lettre du texte, il y a la volonté du législateur. La méthode téléologique s'attache essentiellement à découvrir l'esprit qui a animé la genèse du texte. Non pas la volonté désuète d'un lointain législateur, mais l'intention hypothétique du législateur actuel. Autrement dit, le juge pénal est souvent conduit à rechercher (en s'appuyant, le cas échéant, sur les travaux préparatoires - exposés des motifs des projets de lois, rapports des commissions, débats parlementaires - du texte à interpréter) quelle serait la volonté probable du législateur si celui-ci avait à régler la difficulté d'interprétation. Une telle démarche est couramment suivie lorsqu'il s'agit de délimiter les contours d'une notion incertaine au contenu non

défini : ainsi, la notion de soustraction dans le vol, celle de manœuvres frauduleuses dans l'escroquerie ou encore celle de victime (autrui) dans l'homicide involontaire. Mais la méthode téléologique est également très utile lorsqu'il s'agit d'adapter un texte à des nécessités nouvelles que le législateur de l'époque ne pouvait prévoir. C'est ainsi que l'envoi de SMS ou de textes agressifs a pu être qualifié d'appels téléphoniques malveillants ou d'agressions sonores (Crim., 30 septembre 2009). En ce qu'elle retarde le vieillissement des textes, la méthode téléologique présente un avantage évident. Mais, en prêtant au législateur des intentions qu'il n'a parfois jamais eues, la méthode conduit à déformer l'incrimination, ce qui maltraite assurément la liberté individuelle.

Le triomphe de l'analogie *in malam partem*

En considération de l'impérieuse nécessité de garantir l'anonymat des fonctionnaires de police ou des militaires de la gendarmerie, l'on comprend aisément que la révélation d'éléments permettant l'identification d'un membre soit aussi périlleuse que la révélation de l'identité des éléments de l'identité civile (noms et prénoms). Toutefois, au regard des règles traditionnelles gouvernant l'interprétation de la loi pénale, cette assimilation est juridiquement nettement plus contestable. Pour se convaincre de l'orthodoxie douteuse de l'interprétation dégagée par la Chambre criminelle dans son arrêt en date du 12 décembre 2017, il suffit de parcourir certaines autres dispositions de la loi du 29 juillet 1881 dont l'objet consiste également à protéger l'anonymat de certains protagonistes. Ainsi, lorsqu'il s'agit de protéger un mineur qui s'est suicidé ou bien encore un mineur victime d'une infraction (comme la petite Maëlys par exemple), la loi pénale réprime *expressis verbis* le fait de diffuser, de quelque manière que ce soit, des informations *relatives à l'identité ou permettant l'identification du mineur* (art. 39 bis, L. 29 juillet 1881). Pareillement, pour préserver l'anonymat d'une victime (mineure ou majeure d'une infraction sexuelle), il est interdit de diffuser des renseignements concernant son identité ou l'image de cette victime lorsqu'elle est identifiable (art. 39 quinquies, L. 29 juillet 1881). L'argument *a contrario* qui fragilise très sensiblement le raisonnement

de la Cour de cassation se retrouve à l'identique dans le Code de procédure pénale. Afin de protéger davantage encore l'anonymat du témoin dont la vie ou l'intégrité physique (ou celles de ses proches) est en danger, la loi n°2016-731 du 3 juin 2016 punit ainsi d'une peine de cinq ans d'emprisonnement et de 75 000 euros d'amende « le fait de révéler l'identité d'un témoin ayant bénéficié de l'anonymat ou de diffuser des informations permettant son identification ou sa localisation » (art. 706-62-1 C. pr. pén.). En d'autres termes, et pour reprendre la belle expression de Jérémy Bentham, les paroles de la loi doivent se peser comme des diamants, si bien que l'identité et l'identification ne doivent être assimilées que dans la seule mesure où le législateur en a décidé ainsi expressément. Déformer délibérément les contours d'une incrimination claire et précise pour les besoins de la répression, c'est ériger la jurisprudence en légisprudence en méconnaissant ostensiblement la séparation des pouvoirs.

Quand une erreur utile est jugée préférable à une vérité nuisible

En même temps qu'il n'est pas à l'abri de la critique en assimilant les concepts « d'identité » et « d'identification », l'arrêt du 12 décembre 2017 ne convainc pas davantage lorsqu'il affirme péremptoirement que « la diffusion de précédentes informations relatives à l'intéressé ne fait pas obstacle à la caractérisation du délit inscrit à l'article 39 sexies de la loi du 29 juillet 1881 sur la presse ». Là encore, la formule a belle allure et donne l'impression de l'inévitable, comme une coulée de lave. L'impression est voulue : l'affirmation entend clore la discussion en offrant le moins de prise possible à sa réouverture : elle se présente comme un oeuf, plein et lisse. Dans le charabia du médecin de Molière, il n'y avait de clair que le constat. Ici, la conclusion est claire mais dans le même temps orpheline de toute justification. Dans l'arrêt du 12 décembre 2017, le comment et le pourquoi se perdent dans les ténèbres. Une ténébreuse affaire, comme l'aurait dit Balzac … essayons d'y voir plus clair !

L'article 39 sexies de la loi du 29 juillet 1881 s'attache à réprimer « la

révélation » de l'identité d'un agent des forces de l'ordre autorisé, de par ses missions et son service de rattachement, à bénéficier de l'anonymat. La consultation d'un dictionnaire s'impose : emprunté au latin *revelare* (XII^{e} siècle), le verbe « révéler » signifie mettre à nu, dévoiler, faire connaître ou faire savoir ce qui était inconnu ou secret. Un secret, une vérité ou bien encore une religion peuvent ainsi être révélés. Mais peut-on encore révéler ce qui est déjà connu de tous en ayant été rendu public ? Une réponse négative semble devoir s'imposer ici, si les mots ont encore un sens. Telle n'est pourtant pas la position de la Cour de cassation qui transpose au délit de l'article 39 sexies de la loi du 29 juillet 1881 sa jurisprudence traditionnelle en matière de diffamation. Pourtant, là encore, cette transposition est largement contestable. En effet, alors que l'article 39 sexies de la loi de 1881 ne réprime que « la révélation », l'article 29 de la même loi se rapportant au délit de diffamation réprime autant « la publication directe » que « la reproduction de l'allégation » attentatoire à l'honneur ou à la considération. Reproduire une allégation diffamatoire caractérise donc parfaitement un délit (en ce sens, Crim. 6 octobre 1992). Pareillement, diffuser des informations relatives à l'identité d'un mineur victime d'une infraction (ou qui s'est suicidé) est constitutif d'un délit quand bien même la diffusion litigieuse ne ferait-elle que reprendre des éléments déjà publiés par d'autres organes de presse sans qu'aucune poursuite n'ait d'ailleurs besoin d'avoir été exercée à leur encontre (en ce sens, Crim., 4 juin 1998, pourvoi n° 97-80577).

En revanche, lorsque la loi ne réprime que la seule « révélation », toute diffusion d'une information déjà connue devrait logiquement échapper aux foudres de la répression. Ainsi le commande le principe de légalité criminelle. Sans préjuger d'une éventuelle saisine de la Cour européenne des droits de l'Homme sur le fondement de l'article 7 CEDH, cet arrêt de la Chambre criminelle de la Cour de cassation invite - par-delà son extrême bienveillance à l'égard de l'anonymat - à une prompte réécriture des dispositions de l'article 39 sexies de la loi du 29 juillet 1881, afin d'éviter que l'opportunisme du présent ne devienne rapidement l'embarras ou la condamnation du lendemain.

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

LÉGISLATION

Loi n° 2018-133 du 26 février 2018 transposant la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016

La loi du 26 février 2018 contient des dispositions transposant la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016. Ce texte, dit directive « *Network and Information Security*-NIS », rassemble des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information au sein de l'Union. Selon l'article 114 du Traité sur le fonctionnement de l'Union européenne, celle-ci est habilitée à adopter des mesures destinées à établir ou assurer le fonctionnement du marché intérieur. La résilience des réseaux et systèmes informatiques joue un rôle tel qu'une harmonisation de la cybersécurité entre les États membres s'impose.
L'objectif poursuivi est donc de renforcer la capacité de surmonter une cyberattaque et d'assurer la continuité du fonctionnement des réseaux et des infrastructures. Il s'agit de garantir la sécurité à l'égard des incidents et des risques qui affectent certaines entreprises stratégiques. La loi transpose donc les mesures concernant les opérateurs fournissant des « services essentiels » (OSE) à la continuité des activités économiques et sociales critiques de la nation ainsi que les « fournisseurs de services numériques » (FSN), services eux-mêmes utilisés par les opérateurs de services essentiels.
Son premier article porte sur la définition des « réseaux et systèmes d'information ».

I. La définition des « réseaux et systèmes d'information »

Reprenant les termes de la directive, la loi (article 1[er]) définit ce qu'il faut entendre par « réseaux et systèmes d'information », lesquels n'étaient

pas jusqu'alors précisés dans le droit positif français. Le Sénat avait envisagé une définition des systèmes de traitement automatisé de données, lors de l'écriture du nouveau Code pénal : « *Tout ensemble composé d'une ou plusieurs unités de traitement, de mémoire, de logiciel, de données, d'organes d'entrées-sorties et de liaisons, qui concourent à un résultat déterminé, cet ensemble étant protégé par des dispositifs de sécurité* ». Mais cette précision n'avait pas été retenue pour éviter de lier le droit à une technologie pouvant évoluer. Jacques Godfrain, auteur de la loi éponyme a rappelé, lors du 5[e] Forum international de la cybersécurité (Lille 2013), quelle fut alors la recherche d'équilibre entre un texte suffisamment précis et un texte « ouvert » aux mutations technologiques. L'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les autorités administratives définit le système d'information comme « *tout ensemble de moyens destinés à élaborer, traiter, stocker ou transmettre des informations faisant l'objet d'échanges par voie électronique entre autorités administratives et usagers ainsi qu'entre autorités administratives* ». Mais ce texte, comme l'a souligné le sénateur Philippe Bonnecarrère lors des travaux parlementaires, n'a qu'une portée limitée à son objet. Suivant l'avis du Conseil d'État[1], le législateur a repris la définition posée par la directive qui dépasse le seul cadre des systèmes de traitement automatisé de données (STAD) et est suffisamment large pour demeurer pertinente en fonction de l'évolution des techniques.
Est donc qualifié de réseau ou de système d'information, tout réseau de communications électroniques défini au 2° de l'article L. 32 du Code des postes et des communications électroniques, c'est-à-dire « *toute installation ou tout ensemble d'installations de transport ou de diffusion ainsi que, le cas échéant, les autres moyens assurant l'acheminement de communications électroniques, notamment ceux de commutation et de routage* ». Sont ainsi considérés comme des réseaux de communications électroniques « *les réseaux satellitaires, les réseaux terrestres, les systèmes utilisant le réseau électrique pour autant qu'ils servent à l'acheminement de communications électroniques et les réseaux assurant la diffusion ou utilisés pour la distribution de services de communication audiovisuelle* ». Entre également dans la définition

1. Conseil d'État, avis n° 393665 du 14 novembre 2017.

« tout dispositif ou tout ensemble de dispositifs interconnectés ou apparentés dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données numériques ».
Plus novatrice est l'incorporation des « données numériques stockées, traitées, récupérées ou transmises » par les systèmes ci-dessus évoqués, en vue de leur fonctionnement, utilisation, protection et maintenance. C'est une manière de prendre en compte le caractère stratégique de la donnée dans la transformation numérique.
La définition très générique devrait survivre à des nouvelles ruptures technologiques. Elle couvre les trois « couches » de l'espace numérique : la couche matérielle (le *hardware*), la couche logique (le *software*) et la couche sémantique.
La sécurité des réseaux et systèmes d'information consiste, selon le même article, en leur capacité de résister, à un niveau de confiance donné, à des actions qui compromettent la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement, et des services connexes que ces réseaux et systèmes d'information offrent ou rendent accessibles. Rien de bien nouveau en revanche au regard de la définition de la Sécurité des systèmes d'information (SSI) retenue notamment par l'Agence nationale de sécurité des systèmes d'information (ANSSI).

II. La cybersécurité des opérateurs de services essentiels (OSE)

La loi définit la notion de service essentiel et précise les réseaux concernés par des obligations imposées aux opérateurs.

A. La notion de service essentiel

L'article 5 reprend les critères posés par la directive NIS (art 5) : « *est un opérateur de services essentiels (OSE) celui dont l'activité inclut la fourniture de services essentiels au fonctionnement de la société et de l'économie et dont la prestation de service repose sur l'utilisation de réseaux et systèmes d'information. Un incident les visant aurait un effet*

disruptif important sur la fourniture de ces services ».
Il est prévu, dans un premier temps, conformément à l'annexe II de la directive, de mieux protéger l'énergie, les transports, les banques, les infrastructures de marchés financiers, la santé, la fourniture et la distribution d'eau potable et les infrastructures numériques. S'agissant de ces dernières, la directive vise les fournisseurs de services DNS (*Domain Name Service*), les IXP (*Internet Exchange Point*) et les registres de noms de domaine de haut niveau.
Le gouvernement envisage toutefois, comme il le précise dans l'étude d'impact, de procéder à une extension au tourisme, à l'agroalimentaire, aux assurances, aux affaires sociales et à la construction automobile.

B. Le champ d'application de la loi

La loi s'applique aux réseaux et systèmes d'information des opérateurs de services essentiels, dont la liste est arrêtée par le Premier ministre (article 5).
La loi ne s'applique pas dans certains cas prévus par son article 2, lorsque des dispositions sont déjà en vigueur : sont ainsi exclus de son périmètre, *pour les seules activités d'exploitation de réseaux et de fourniture de services de communications électroniques*, les opérateurs mentionnés au 15° de l'article L. 32 du Code des postes et des communications électroniques, c'est-à-dire toute personne physique ou morale exploitant un réseau de communications électroniques ouvert au public ou fournissant au public un service de communications électroniques.
La loi ne s'applique pas non plus aux acteurs déjà soumis à des normes européennes sectorielles créant des obligations au moins équivalentes portant sur leurs réseaux et systèmes d'information. Il en est ainsi des prestataires de confiance, régis par le règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 relatif à l'identification électronique et des services de confiance pour les transactions électroniques au sein du marché intérieur.
Mais ces exclusions ne concernent pas les réseaux et systèmes qui sont nécessaires à la fourniture de services essentiels ou de service numérique et ne sont pas couverts par des dispositions spécifiques.
L'article 5 opère une distinction claire entre OSE et OIV. Ces derniers

sont des opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation. Les articles L. 1332-1 et L. 1332-2 du Code de la défense leur imposent des règles plus rigoureuses en matière de cybersécurité. Comme le souligne cependant le rapporteur de la loi devant l'Assemblée nationale, certaines entreprises sont susceptibles de répondre à la fois à la définition d'OIV et à celle d'OSE en fonction des systèmes d'information concernés. Il cite les propos de l'ANSSI au sujet de la SNCF, laquelle a recours à des systèmes d'information de sensibilités différentes : le système d'aiguillage est d'importance vitale puisqu'un important dysfonctionnement serait susceptible de mettre en danger des vies humaines ; le système de billetterie est un service essentiel puisqu'un dysfonctionnement conséquent répond aux critères de l'OSE. Le site d'information générale et de promotion de la SNCF, quant à lui, ne relève d'aucune des deux catégories, car il n'a pas de caractère stratégique.
La loi, on le voit bien, ne vient pas surajouter des obligations mais elle élève le niveau de cybersécurité d'acteurs non déjà concernés ou de certaines de leurs activités non visées par les règles imposées aux OIV.

C. Les obligations pesant sur les OSE

Les règles qui s'imposent aux OSE doivent garantir un niveau de sécurité « adapté au risque existant, compte tenu de l'état des connaissances » (art 6). Elles sont fixées par le Premier ministre qui se voit ainsi confier une nouvelle police administrative spéciale. Elles concernent chacun des domaines suivants :

1° La gouvernance de la sécurité des réseaux et systèmes d'information ;
2° La protection des réseaux et systèmes d'information ;
3° La défense des réseaux et systèmes d'information ;
4° La résilience des activités.

Ces règles, assorties de sanctions pénales[2] (art.9), peuvent notamment prescrire que les opérateurs recourent à des dispositifs matériels ou logiciels ou à des services informatiques dont la sécurité a été certifiée.

Les OSE doivent déclarer à l'ANSSI, sans délai après en avoir pris connaissance, les incidents affectant leurs réseaux et systèmes d'information, dès lors qu'ils concernent des réseaux et systèmes d'information nécessaires à la fourniture de services essentiels (art.7) et ont ou peuvent avoir un impact significatif du fait d'une perturbation grave. La gravité est analysée *in concreto* mais la directive NIS offre une liste de critères : le nombre d'utilisateurs, la dépendance d'autres secteurs essentiels par rapport au service affecté, les conséquences que des incidents pourraient avoir, en termes de degré et de durée, sur les fonctions économiques, sociétales ou sur la sûreté publique, la part de marché de l'opérateur concerné, la portée géographique de l'incident, l'importance que revêt l'opérateur pour garantir un niveau suffisant de service dans le secteur ou le sous-secteur concerné, compte tenu de la disponibilité de solutions de rechange pour la fourniture de ce service. L'obligation de signalement rappelle celle imposée aux OIV ou celle imposée auprès de la CNIL, en cas de compromission de données à caractère personnel.

S'agissant des contrôles sur pièce et sur place (art.8), ils relèvent de l'ANSSI mais peuvent cependant être effectués par un prestataire de service qualifié par le Premier ministre. L'ANSSI ou le prestataire de service qualifié chargé du contrôle est autorisé à accéder aux réseaux

2. Est puni de 100 000 € d'amende le fait, pour les dirigeants des opérateurs mentionnés à l'article 5, de ne pas se conformer aux règles de sécurité mentionnées à l'article 6 à l'issue du délai fixé par la mise en demeure qui leur a été adressée en application de l'article 8.
Est puni de 75 000 € d'amende le fait, pour les mêmes personnes, de ne pas satisfaire à l'obligation de déclaration d'incident.
Est puni de 125 000 € d'amende le fait, pour les mêmes personnes, de faire obstacle aux opérations de contrôle mentionnées à l'article 8.
Ces sanctions sont plus faibles que celles prévues pour les OIV (150 000 euros). Dans les deux cas, ce sont les personnes physiques qui sont pénalement responsables.
On regrettera une fois de plus que ces dispositions pénales ne soient pas codifiées.

et systèmes d'information de l'OSE concerné pour effectuer des analyses et des relevés d'informations techniques. En cas de manquement, l'ANSSI peut mettre en demeure l'opérateur de se conformer aux obligations qui lui incombent.
L'Agence reçoit les notifications d'incidents et, après consultation de l'opérateur (notamment en raison de la confidentialité de certaines informations), peut informer le public, lorsque cette information est nécessaire pour prévenir ou traiter un incident. Cette information peut être étendue à d'autres États membres de l'UE en cas d'impact transfrontalier.

III. La sécurité des réseaux et systèmes d'information des fournisseurs de service numérique (FSN)

La loi définit la notion de fournisseurs de service numérique et fixe les règles qui leur sont applicables. Les contraintes qui pèsent sur les FSN sont moins exigeantes que celles qui concernent les OSE.

A. La définition des fournisseurs de service numérique

La loi (art.10) reprend la définition des services numériques et fournisseurs de tels services figurant à l'article 4 de la directive :
« Est un service numérique tout service fourni normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire de services ».
Un fournisseur de service numérique (FSN) est une personne morale qui fournit l'un des services suivants :

a) place de marché en ligne, à savoir un service numérique qui permet à des consommateurs ou à des professionnels, au sens du dernier alinéa de l'article liminaire du Code de la consommation, de conclure des contrats de vente ou de service en ligne avec des professionnels, soit sur le site Internet de la place de marché en ligne, soit sur le site Internet d'un professionnel qui utilise les services informatiques fournis

par la place de marché en ligne ;
b) moteur de recherche en ligne, service numérique qui permet aux utilisateurs d'effectuer des recherches sur, en principe, tous les sites Internet ou sur les sites Internet dans une langue donnée, sur la base d'une requête lancée sur n'importe quel sujet sous la forme d'un mot clé, d'une phrase ou d'une autre entrée, et qui renvoie des liens à partir desquels il est possible de trouver des informations en rapport avec le contenu demandé ;
c) service d'informatique en nuage (*cloud*), service numérique qui permet l'accès à un ensemble modulable et variable de ressources informatiques pouvant être partagées.

À défaut d'une liste nominative prévue pour les OSE, cette définition s'appuie sur les opérations effectuées, permettant ainsi aux fournisseurs de service numérique de s'assurer qu'ils entrent bien dans le champ de la loi.

B. Les règles applicables aux fournisseurs de services numériques

Conformément à la directive, la loi ne s'applique pas aux entreprises qui emploient moins de cinquante salariés et dont le chiffre d'affaires annuel n'excède pas 10 millions d'euros (art.11).

1. Les règles de compétence des États membres

Les fournisseurs de service numérique, établis hors de l'UE mais offrant des services sur le territoire national, doivent désigner un représentant auprès de l'ANSSI, sauf s'ils ont accompli cette formalité auprès d'un autre État membre (art.11). En application de la directive, « *le fournisseur de service numérique est considéré comme relevant de la compétence de l'État membre dans lequel le représentant est établi* », ceci pour éviter la redondance ou un vide juridique. On notera toutefois, comme l'a souligné le sénateur Bonnecarrère, qu'il n'existe, d'une part, aucun mécanisme juridique permettant aux États membres de s'assurer que les FSN établis hors de l'UE se sont bien déclarés

dans un autre État membre et, d'autre part, définissant l'autorité judiciaire compétente chargée de poursuivre et de sanctionner les fournisseurs qui ne respecteraient pas cette obligation de déclaration. La loi française est donc applicable aux FSN qui ont établi leur siège social en France ou qui, établis hors de l'Union, ont désigné un représentant sur le territoire national, faute de l'avoir fait dans un autre État membre.

2. La garantie d'un niveau de sécurité adapté aux risques

Les fournisseurs de service numérique doivent garantir « compte tenu de l'état des connaissances », un niveau de sécurité des réseaux et des systèmes d'information nécessaires à la fourniture de leurs services adapté aux risques existants. L'article 12 de la loi précise les domaines pour lesquels des obligations leur sont imposées :

1° la sécurité des systèmes et des installations ;
2° la gestion des incidents ;
3° la gestion de la continuité des activités ;
4° le suivi, l'audit et le contrôle ;
5° le respect des normes internationales.

Le régime des fournisseurs de service numérique est moins contraignant que celui des OSE, car ils offrent déjà un niveau de sécurité élevé. Les OSE doivent respecter des règles fixées par le Premier ministre, alors que, conformément à la directive, les FSN sont libres de définir les mesures de sécurité adaptées aux risques auxquels ils sont confrontés. C'est à eux « *d'identifier les risques qui menacent la sécurité de ces réseaux et systèmes d'information et de prendre des mesures techniques et organisationnelles nécessaires et proportionnées pour gérer ces risques, pour éviter les incidents de nature à porter atteinte à ces réseaux et systèmes d'information ainsi que pour en réduire au minimum l'impact, de manière à garantir la continuité de leurs services* ».
Les FSN (art.13) doivent également communiquer à l'ANSSI les incidents dont ils sont victimes, mais seulement ceux ayant un impact

significatif sur la fourniture de leurs services. Mais les OSE doivent aussi signaler ceux qui seraient « susceptibles » d'en avoir un, ce qui souligne, là encore, une plus forte contrainte pour ces opérateurs.
L'article 13 est cependant plus précis s'agissant des critères permettant de qualifier le caractère significatif de l'impact : outre le nombre d'utilisateurs, la zone géographique et la durée, sont en revanche ajoutés la gravité de la perturbation du fonctionnement du service et son ampleur. Comme pour les OSE, l'ANSSI peut informer le public et d'autres États membres.

3. Des contrôles assortis de sanctions pénales

Le Premier ministre peut confier à l'ANSSI ou à des prestataires de service qu'il a qualifiés le soin de procéder à des contrôles sur pièce et sur place chez un fournisseur de services qui ne satisferait pas à ses obligations (art.14). Les manquements peuvent faire l'objet d'une mise en demeure assortie d'un délai. Les sanctions pénales[3] sont similaires mais inférieures, s'agissant du quantum quant à celles pouvant être infligées aux dirigeants des OSE.

***

Le corpus juridique relatif à la cybersécurité s'enrichit avec la loi du 26 février 2018. Le renforcement du dispositif législatif devrait se poursuivre avec la future Loi de programmation militaire (LPM) dont l'examen vient de débuter au Parlement. Les dispositions de la directive ne sont pas toutes de nature législative. Ainsi, le décret n°2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes

3. Est puni de 75 000 € d'amende le fait, pour les dirigeants des fournisseurs de service numérique mentionnés à l'article 11, de ne pas se conformer aux mesures de sécurité mentionnées à l'article 12, à l'issue du délai fixé par la mise en demeure qui leur a été adressée en application de l'article 14.
Est puni de 50 000 € d'amende le fait, pour les mêmes personnes, de ne pas satisfaire aux obligations de déclaration d'incident ou d'information du public prévues à l'article 13.
Est puni de 100 000 € d'amende le fait, pour les mêmes personnes, de faire obstacle aux opérations de contrôle mentionnées à l'article 14.

d'information » sera modifié pour tenir compte des nouvelles missions de l'ANSSI. La loi augmente, en effet, ses attributions en matière de contrôle, de notification des incidents et d'information du public ou des Etats membres.

JURISPRUDENCE JUDICIAIRE

Cour de cassation, 1ère chambre civile, (17-10.499) Google/M. Thierry X., 14 février 2018

La juridiction saisie d'une demande de déréférencement ne peut ordonner au moteur de recherche une mesure d'injonction d'ordre général et doit mettre en balance les intérêts en présence.

L'arrêt du 13 mai 2014 (C-131/12, Google Spain et Google) a considéré que l'activité d'un moteur de recherche consistant à trouver des informations publiées ou placées sur Internet par des tiers, à les indexer de manière automatique, à les stocker temporairement et, enfin, à les mettre à la disposition des internautes selon un ordre de préférence donné doit être qualifiée de « traitement de données à caractère personnel ». Le moteur de recherche est alors qualifié de responsable dudit traitement. L'arrêt Google Spain a également interprété la directive 95/46 (bientôt remplacée par le Règlement Général sur la Protection des Données - RGPD) en précisant que l'exploitant d'un moteur de recherche « *est obligé de supprimer de la liste de résultats, affichée à la suite d'une recherche effectuée à partir du nom d'une personne, des liens vers des pages web, publiées par des tiers et contenant des informations relatives à cette personne, également dans l'hypothèse où ce nom ou ces informations ne sont pas effacés préalablement ou simultanément de ces pages web, et ce, le cas échéant, même lorsque leur publication en elle-même sur lesdites pages est licite* ». Mais l'arrêt apporte une restriction : le droit à la suppression n'est pas absolu et n'est pas opposable *« s'il apparaissait, pour des raisons particulières, telles que le rôle joué par ladite personne dans la vie publique, que*

l'ingérence dans ses droits fondamentaux est justifiée par l'intérêt prépondérant dudit public à avoir, du fait de cette inclusion, accès à l'information en question ». Le juge saisi en cas de demande de déréférencement doit porter une appréciation sur son bien-fondé et procéder, *in concreto*, à la mise en balance des intérêts en présence. Il ne peut ordonner une mesure d'injonction d'ordre général conférant un caractère automatique à la suppression de la liste de résultats, affichée à la suite d'une recherche effectuée à partir du nom d'une personne, des liens vers des pages Internet contenant des informations relatives à cette personne.

Tel est le sens de l'arrêt de la Cour de cassation du 14 février 2018. Celui-ci casse l'arrêt n°15/13987 du 15 septembre 2016 de la Cour d'appel d'Aix-en-Provence. Celui-ci avait réformé partiellement une ordonnance de référé du 9 juillet 2015 du TGI de Nice qui enjoignait Google France et Google. Inc à supprimer des liens référencés en lien avec les données à caractère strictement privé et personnel du requérant concernant son ascendance, ses enfants et certaines unions. La demande de suppression étant trop large, la Cour avait limité ce droit aux deux « *seuls liens identifiés et signalés* ». Mais la Cour de cassation relève « *qu'après avoir ordonné à la société Google Inc. de supprimer les liens qui conduisent, lors de recherches opérées sur le moteur Google.fr incluant les nom et prénom de M. X., aux deux adresses URL précisées en son dispositif, l'arrêt enjoint à cette société de supprimer les liens qui conduisent, lors de recherches opérées dans les mêmes conditions, à toute adresse URL identifiée et signalée par M. X. comme portant atteinte à sa vie privée, dans un délai de sept jours à compter de la réception de ce signalement. Qu'en prononçant ainsi une injonction d'ordre général et sans procéder, comme il le lui incombait, à la mise en balance des intérêts en présence, la cour d'appel a violé les textes susvisés* ».

Cour de Cassation, Chambre criminelle (16-87.168), M.R.M. 16 janvier 2018

L'atteinte à un système de traitement automatisé de données est indifférente au mobile. L'installation d'un keylogger caractérise la mauvaise foi de l'auteur qui se rend également coupable de détention d'équipement dès lors qu'il n'est pas habilité à assurer la maintenance et la sécurité d'un parc informatique.

Le 12 novembre 2013, le service informatique du CHU de Nice découvre la présence d'un keylogger matériel (câble entre le port du clavier et le clavier) sur les ordinateurs de deux médecins du centre. L'enquête s'oriente vers un médecin contractuel en conflit devant l'Ordre des médecins. Ce praticien fait l'objet d'une perquisition à son domicile qui permet de découvrir un keylogger et des captures d'écran en provenance des deux ordinateurs espionnés, stockées sur clef USB et sur ordinateur portable. L'auteur des faits, tout en reconnaissant avoir acquis ce matériel sur Internet, déclare avoir agi ainsi pour récupérer des éléments pouvant aider sa défense dans un litige professionnel porté par un professeur devant l'Ordre des médecins.
La Cour d'appel d'Aix-en-Provence (5e chambre), dans un arrêt du 8 novembre 2016, le condamne à quatre mois de prison avec sursis et à la confiscation de son matériel pour atteinte à un système de traitement automatisé de données (STAD), infraction prévue et réprimée par l'article 323-1 du Code pénal, et pour détention sans motif légitime d'équipement, d'instrument de programme ou données conçus et adaptés pour commettre une telle atteinte, infraction prévue et réprimée par l'article 323-3-1 du Code pénal.
Le prévenu avait alors déclaré pour sa défense que le keylogger ne permettait pas l'accès aux données contenues dans les ordinateurs visés mais seulement de visualiser les caractères frappés sur le clavier de deux ordinateurs à la disposition de tous les personnels du service. Mais il avait aussi reconnu que c'est par ce biais qu'il avait obtenu le code d'accès à la messagerie des deux médecins et donc de prendre connaissance des courriels qu'ils échangeaient. L'interception de ces

courriels avait pour objectif, selon lui, d'obtenir de bonne foi et pour un motif légitime, des éléments pour sa défense contre un professeur cherchant à l'évincer de son poste.
La Cour de cassation écarte bien sûr de tels moyens pour retenir l'infraction d'atteinte au STAD. Les motifs avancés par le prévenu pour justifier son action délictueuse sont des mobiles indifférents à la caractérisation de l'infraction. L'installation d'un keylogger à l'insu des victimes et l'interception de leurs courriels témoignent de la mauvaise foi de l'intéressé. En conséquence, le délit est bien constitué. La Cour de cassation confirme ainsi un raisonnement déjà soutenu lors d'un précédent arrêt (Cass.crim, n°16-81822, M. Jerry X., 10 mai 2017). En l'espèce, un avocat en cours de divorce avait installé un keylogger sur l'ordinateur de son épouse ; la Cour avait précisé que la définition de l'incrimination étant d'interprétation stricte, les fins que poursuit le titulaire du droit d'accès sont indifférentes.
S'agissant de l'infraction d'acquisition, de détention d'un équipement permettant de réaliser une atteinte à un STAD, la Cour de cassation retient la culpabilité du médecin puisque, selon l'article 323-3-1, l'autorisation se limite aux seules personnes habilitées à assurer la maintenance et la sécurité d'un parc informatique. Dans l'affaire Jerry X., l'auteur était en droit de mettre en place un keylogger en qualité d'administrateur réseau du système informatique du cabinet et donc de sa sécurité. C'est le détournement de la finalité du keylogger qui avait été constitutive de l'infraction de maintien frauduleux dans le STAD de son épouse.

Cour d'appel de Toulouse, 4ème chambre – Sec. 2, Mme X. / Autour du bain, 2 février 2018

Est une faute grave le fait de laisser volontairement ouverte une session Facebook comprenant des injures à l'égard de son employeur et de ses collègues.

Une salariée est licenciée pour avoir échangé sur Facebook des propos

insultants et dénigrants sur son entreprise, sa supérieure hiérarchique, certaines de ses collègues. Ces propos ont été tenus alors qu'elle était en congé de maladie. Elle avait pendant ce temps laissé sa session volontairement ouverte pour que les personnes visées en prennent connaissance. Ainsi, l'ensemble des salariés pouvait en prendre connaissance.
Considérant qu'un tel agissement avait rompu le lien de confiance et généré une souffrance pour l'ensemble des salariés, la Cour d'appel confirme le bien-fondé du licenciement pour faute grave.

Par Mme Claudia Ghica-Lemarchand

DISPOSITIF DE SONORISATION

Crim. 6 février 2018, n° 17-85301

L'article 706-96 du Code pénal donne compétence au juge des libertés et de la détention, à la requête du procureur de la République, d'autoriser les officiers et agents de police judiciaire à mettre en place un dispositif technique ayant pour objet, sans le consentement des intéressés, la captation, la fixation, la transmission et l'enregistrement de paroles prononcées par une ou plusieurs personnes à titre privé ou confidentiel, dans des lieux ou véhicules privés ou publics, ou de l'image d'une ou de plusieurs personnes se trouvant dans un lieu privé. En vue de mettre en place le dispositif technique, le juge des libertés et de la détention peut autoriser l'introduction dans un véhicule ou un lieu privé, y compris hors des heures prévues légales, à l'insu ou sans le consentement du propriétaire ou du possesseur du véhicule ou de l'occupant des lieux ou de toute personne titulaire d'un droit sur ceux-ci. Ces opérations, qui ne peuvent avoir d'autre fin que la mise en place du dispositif technique, sont effectuées sous son contrôle. Le texte prévoit un parfait parallélisme, puisque les mêmes garanties sont appliquées en cas de désinstallation du dispositif. Cette procédure dérogatoire étant hautement attentatoire à la vie privée, elle est limitée aux infractions de criminalité organisée prévues aux articles 706-73 et 706-73-1. Si l'article apporte des précisions quant aux lieux pouvant faire l'objet de ce mécanisme et exclut les lieux professionnels protégés en matière de perquisitions (cabinets d'avocats, locaux de presse, cabinet d'un médecin, d'un notaire ou d'un huissier, les locaux d'une juridiction ou au domicile d'une personne exerçant des fonctions juridictionnelles), nulle précision n'est apportée quant aux personnes pouvant faire des contestations de cette procédure.
La Chambre criminelle a été saisie d'une question prioritaire de constitutionnalité rédigée de la manière suivante : « *Les dispositions des articles 706-96 dans leurs rédactions issues des lois n°2005-1549 du 12 décembre 2005 et n°2015-993 du 17 août 2015, 171 et 802 du*

Code de procédure pénale, telles qu'interprétées de façon constante par la jurisprudence de la chambre criminelle, en ce qu'elles privent la personne mise en examen, qui ne dispose d'aucun droit sur le véhicule ou le lieu sonorisé et dont les propos n'ont pas été captés, de la possibilité de dénoncer la violation des règles applicables en matière de sonorisation, portent-elles atteinte aux droits et libertés que la Constitution garantit et plus exactement au principe d'égalité des justiciables, aux droits de la défense ainsi qu'au droit à un recours effectif devant une juridiction, garantis par les articles 6 et 16 de la Déclaration des droits de l'homme et du citoyen de 1789 ? ». Sans surprise, la Chambre criminelle refuse de transmettre la QPC au Conseil constitutionnel puisqu'elle n'est pas nouvelle et porte sur « la portée effective de l'interprétation jurisprudentielle constante de cette disposition législative », mais elle saisit l'occasion pour préciser le dispositif.

Les juges ont soumis la recevabilité du moyen de nullité pris de l'irrégularité de la mise en œuvre de sonorisations à la condition que le requérant dispose « d'un droit ou d'un titre sur les lieux ou véhicules privés ou publics ou que ses paroles ou son image aient été captées ». Cette position représente une interprétation conforme aux textes du Code de procédure pénale tels qu'ils ont été remaniés par les lois successives et rend compte de la volonté du législateur, prolongée par le juge pénal, d'opérer « une conciliation équilibrée entre, d'une part, les droits de la défense au stade de l'instruction préparatoire, d'autre part, les principes de valeur constitutionnelle de prévention des atteintes à l'ordre public et de recherche des auteurs d'infractions en matière de criminalité organisée ». Mais cette limitation de la recevabilité de la contestation du procédé mis en œuvre cède devant trois situations qui produisent une inversion de cet équilibre.

D'une part, « le recours par les autorités publiques à un procédé déloyal » libère les moyens de remise en cause pour faire constater ce contournement de l'esprit de la procédure pénale. L'esprit de loyauté de la recherche de la preuve prime sur toute considération formelle imposée par les textes. D'autre part, dans l'hypothèse où cette personne serait renvoyée devant une juridiction de jugement « il lui est loisible, dans le cadre du débat contradictoire, de contester la force probante des indices et des éléments de preuve qui seraient éventuellement retenus à charge à partir de sonorisations concernant des tiers ».

L'appréciation de la recevabilité de la contestation ne repose plus sur le moyen objectif du procédé utilisé, mais sur le critère subjectif de prise en compte de la personne. Enfin, « la différence de situation entre la personne justifiant soit d'un droit ou d'un titre sur les lieux ou véhicules privés ou publics objet d'une sonorisation, soit de la captation de ses paroles ou de son image, et celle qui n'établit aucune de ces circonstances, justifie la différence de traitement résultant de la rédaction de l'article 706-96 du code de procédure pénale et de l'interprétation constante que la Cour de cassation fait de cet article combiné aux articles 171 et 802 du code de procédure pénale, au stade de l'instruction préparatoire et qui est en rapport direct avec l'objet de la loi ». La Chambre criminelle ne peut opérer un contrôle de constitutionnalité, mais applique les exigences formulées par le Conseil constitutionnel. En effet, les juges considèrent qu'il peut y avoir des différences de traitement, même si elles dérogent au principe d'égalité qui ne s'oppose ni à ce que le législateur règle de façon différente des situations différentes, ni à ce qu'il déroge à l'égalité pour des raisons d'intérêt général, pourvu que, dans l'un et l'autre cas, la différence de traitement qui en résulte soit en rapport direct avec l'objet de la loi qui l'établit. Or, en l'espèce, la limitation de la recevabilité des actions contestant les procédés dérogatoires résulte des textes et de leur mise en œuvre jurisprudentielle dans le cadre de la lutte renforcée contre la criminalité organisée menée par différentes réformes en la matière depuis la loi du 9 mars 2004.

AUTORITÉ DE LA CHOSE JUGÉE AU PÉNAL

Conseil d'État, 16 février 2018, n° 395371

Les rapports entre le droit pénal et les autres disciplines juridiques sont complexes. Si le juge pénal revendique son autonomie à l'égard des autres branches du droit, la place centrale que la matière occupe lui assure aussi une certaine prééminence. Ainsi, deux adages ont forgé la primauté du droit pénal. D'une part, « le criminel tient le civil en l'état » a été considérablement réduit par la loi du 5 mars 2007 donnant une nouvelle rédaction à l'article 4 du Code de procédure pénale et limitant

considérablement son champ d'application. D'autre part, « l'autorité de la chose jugée au pénal » s'impose aux autres juridictions, qu'elles appartiennent à l'ordre judiciaire ou administratif. Si les illustrations des conflits du premier type sont plus fréquentes, ses répercussions devant les juridictions administratives sont plus rares et méritent d'être soulignées. C'est dans ce contexte que s'inscrit l'arrêt rendu par le Conseil d'État le 16 février 2018.

En l'espèce, une personne a constitué une société de location de villas sur la Côte d'Azur domiciliée au Royaume-Uni. Elle est associée majoritaire et gérante de cette personne morale. Néanmoins, elle ne déclare pas la totalité des revenus que ces activités lui procurent. Elle subit deux procédures distinctes – la première est menée devant les juridictions administratives, alors que la seconde est engagée devant les juridictions pénales.

L'administration fiscale procède à un examen contradictoire de sa situation fiscale personnelle et lui impose des impositions supplémentaires au titre des revenus distribués correspondant aux bénéfices et à des pénalités. Le tribunal administratif, confirmé par la Cour d'appel administrative, rejette la demande de décharge des impositions supplémentaires. Pour justifier leur décision, les juges ont considéré que la société disposait en France d'un établissement stable au sens des stipulations précitées de la convention franco-britannique du 22 mai 1968 qui pose deux conditions alternatives : pour être regardée comme ayant un établissement stable en France, une société résidente du Royaume-Uni doit, soit disposer d'une installation fixe d'affaires par laquelle elle exerce tout ou partie de son activité, soit avoir recours à une personne non indépendante exerçant habituellement en France des pouvoirs lui permettant de l'engager dans une relation commerciale ayant trait aux opérations constituant ses activités propres. En l'espèce, les juges constatent que les deux conditions sont remplies. D'une part, la société disposait en France de locaux permanents, au sein desquels elle déployait « le matériel informatique nécessaire à cette activité et bénéficiait des moyens de communication utiles ». D'autre part, la personne physique poursuivie disposait « des compétences pour négocier avec les propriétaires des biens, les clients et divers partenaires commerciaux » et possédait « des procurations sur les comptes bancaires de la société » permettant de déduire qu'elle « assurait la

gestion administrative, commerciale et financière pleine et entière ». Elle était « maître de l'affaire » et représentait la société personne morale en étant pourvue de la compétence, de l'autorité et des moyens nécessaires.

Mais elle est aussi poursuivie des chefs de soustraction frauduleuse à l'établissement et au paiement, d'une part, de taxe sur la valeur ajoutée et, d'autre part, d'impôt sur les sociétés comme associée majoritaire et gérante d'une société domiciliée au Royaume-Uni. La Cour d'appel prononce une relaxe au motif que « les éléments du dossier sont insuffisants pour caractériser une véritable exploitation en France d'une activité pour le compte d'une société X, au sens de la loi française ou l'installation d'un établissement stable au sens de la convention fiscale franco-anglaise ». Pour expliquer leur décision, les juges retiennent, d'une part, que « les actes décisionnels de la société sont tous pris au Royaume-Uni lors d'assemblées générales réunissant les divers associés » et que « les principaux moyens de communication de la société […] auprès de sa clientèle, à savoir téléphone, télécopie, e mail et site internet, sont tous localisés au Royaume-Uni » et d'autre part, que la mission de la personne poursuivie « était d'exercer une activité exclusivement préparatoire ou auxiliaire au seul profit de l'entreprise britannique et qu'elle ne pouvait jamais conclure un contrat, au nom et pour le compte de la société mère, toute activité commerciale lui étant interdite » pour en déduire qu'elle « n'avait aucun pouvoir pour engager contractuellement en son seul nom la société ». Les juges judiciaires écartent ainsi la culpabilité, car il n'y a pas d'éléments factuels suffisants, mais aussi parce qu'elle n'a pas la qualité juridique de représentant de la société et ne peut se voir reprocher des actes commis au nom de la société.

Il est important de noter que la Chambre des appels correctionnels, instance judiciaire, s'est prononcée après la Cour administrative d'appel. Pourtant, la personne se pourvoit en cassation devant le Conseil d'État, qui, tout en donnant raison aux juges administratifs sur le fond, décide d'annuler leur décision, ce qui peut paraître paradoxal, à première vue, mais est totalement justifié, du point de vue des principes généraux du droit.

En premier lieu, le Conseil d'État considère que la Cour administrative d'appel n'a « ni dénaturé les pièces du dossier qui lui était soumis, ni

entaché son arrêt d'erreur de droit en écartant le moyen inopérant tiré de ce que la procédure d'imposition avait été irrégulièrement conduite ». Ensuite, nonobstant l'appréciation exacte faite par les juges administratifs, le Conseil d'État annule leur décision et dispense une véritable leçon de … droit pénal en précisant l'étendue et les effets de l'autorité de la chose jugée au pénal.

L'autorité de la chose jugée au pénal est un principe majeur de l'organisation des juridictions et revêt un caractère d'ordre public. À ce titre, il peut être invoqué en premier lieu devant le juge de cassation et, même si le Conseil d'État ne le rappelle pas, doit être relevé d'office par les juges, indépendamment de la juridiction à laquelle ils appartiennent. Mais surtout, l'autorité de la chose jugée présente « un caractère absolu » et produit des effets « même si le jugement pénal est intervenu postérieurement à la décision de la juridiction administrative frappée de pourvoi devant le Conseil d'État ». Mais le Conseil d'État rappelle aussi l'étendue du principe. Elle s'attache aux décisions des juges répressifs devenues définitives et porte sur « la constatation matérielle des faits mentionnés dans le jugement et qui sont le support nécessaire du dispositif » mais « ne saurait, en revanche, s'attacher aux motifs d'un jugement de relaxe tirés de ce que les faits reprochés ne sont pas établis ou de ce qu'un doute subsiste sur leur réalité ». En l'espèce, le Conseil d'État souligne que les constatations de fait des juges répressifs sont en contradiction avec celles retenues par les juges administratifs. Par conséquent, le principe de l'autorité de la chose jugée au pénal fait obstacle au maintien de la décision contraire des juges administratifs.

L'arrêt rendu par le Conseil d'État rappelle opportunément l'importance de l'autorité de la chose jugée au pénal sur le civil et sur l'administratif, mais l'encadre dans des limites matérielles strictes. Son caractère absolu et d'ordre public est mis en avant, mais son étendue est limitée à l'objet de la saisine, de la décision et des constatations qui en sont le support. Cela n'est pas sans rappeler la jurisprudence de la Cour de cassation qui avait ainsi limité l'autorité des décisions du Conseil constitutionnel afin de s'en affranchir dans certains cas (voir notamment la jurisprudence sur le statut pénal du chef de l'État).

GARDE À VUE EN CAS D'ENTRÉE IRRÉGULIÈRE SUR LE TERRITOIRE – REFUS

Cass. 1re civ., 7 févr. 2018, n° 17-10.338, publ. Bull. à venir

Un ressortissant colombien est interpellé à bord d'un bus venant d'Espagne à destination de Paris. Il présente un passeport dont le visa a expiré. Il est placé en garde à vue pour entrée irrégulière sur le territoire français. Il fait l'objet d'un arrêté préfectoral portant obligation de quitter le territoire et est placé en rétention administrative. Le premier président de la Cour d'appel de Toulouse prolonge la mesure et valide la garde à vue, car les policiers disposaient des éléments leur permettant de soupçonner que l'intéressé avait commis le délit d'entrée irrégulière en France, puni d'un an d'emprisonnement. L'individu visé par cette mesure forme un pourvoi en cassation.

La première chambre civile rend un arrêt de cassation : « en cas de flagrant délit, le placement en garde à vue n'est possible, en vertu des articles 63 et 67 du code de procédure pénale, qu'à l'occasion d'enquêtes sur les délits punis d'emprisonnement ; qu'il s'ensuit que le ressortissant d'un pays tiers, entré en France irrégulièrement, par une frontière intérieure à l'espace Schengen, qui n'encourt pas l'emprisonnement prévu à l'article L. 621-2 du CESEDA dès lors que la procédure de retour organisée par la directive 2008/115/CE n'a pas encore été menée à son terme, ne peut être placé en garde à vue à l'occasion d'une procédure de flagrant délit diligentée du seul chef d'entrée irrégulière ».

La Cour de cassation commence par rappeler les conditions de droit commun du placement en garde à vue et, plus particulièrement, la règle de l'article 67 du Code de procédure pénale qui exige que seuls les délits punis de peines d'emprisonnement puissent en faire l'objet. Mais elle choisit d'inscrire résolument sa décision dans les pas de la jurisprudence de la Cour de justice de l'Union européenne (CJUE). Cette dernière fait primer l'effet utile de la directive dite retour 2008/115/CE sur le droit interne des États membres. Un premier pas a été franchi avec les arrêts El Dridi (CJUE, 28 avr. 2011, aff. C-61/11, El Dridi *)* et Achughbabian (CJUE, 6 déc. 2011, aff. C-329/11, Achughbabian*)* qui

ont considéré que l'article L 621-1 du CESEDA (Code de l'entrée et du séjour des étrangers et du droit d'asile), prévoyant une peine d'un an d'emprisonnement pour l'entrée ou le séjour irréguliers d'étrangers sur le territoire français, était contraire au droit de l'UE, conduisant le législateur à l'abroger en 2013. La loi n° 2012-1560 du 31 décembre 2012 relative à la retenue pour vérification du droit au séjour et modifiant le délit d'aide au séjour irrégulier pour en exclure les actions humanitaires et désintéressées a introduit l'article L 621-2 dans le CESEDA qui distingue nettement la situation des ressortissants de l'UE de celle des autres. Le délit d'entrée irrégulière sur le territoire n'est pas supprimé, mais la mise en œuvre de l'action publique est limitée aux cas de flagrance (le dernier alinéa exige la réunion des conditions de l'article 53 du Code de procédure pénale). Mais la CJUE, dans son arrêt Sélina AFFUM (CJUE, 7 juin 2016, aff. C-47/15, Sélina Affum contre Préfet du Pas-de-Calais), a décidé que la directive 2008/115/CE doit être interprétée « en ce sens qu'un ressortissant d'un pays tiers se trouve en séjour irrégulier sur le territoire d'un État membre et relève, à ce titre, du champ d'application de cette directive, lorsque, sans remplir les conditions d'entrée, de séjour ou de résidence, il transite par cet État membre en tant que passager d'un autobus, en provenance d'un autre État membre, faisant partie de l'espace Schengen, et à destination d'un troisième État membre se trouvant en dehors de cet espace », opérant une assimilation entre les personnes relevant de la directive et son territoire d'application. Mais la CJUE est allée encore plus loin en considérant que « la directive 2008/115 doit être interprétée en ce sens qu'elle s'oppose à une réglementation d'un État membre permettant du seul fait de l'entrée irrégulière par une frontière intérieure, conduisant au séjour irrégulier, l'emprisonnement d'un ressortissant d'un pays tiers, pour lequel la procédure de retour établie par cette directive n'a pas encore été menée à son terme ».
La Cour de cassation se place dans le sillage de la jurisprudence Sélina AFFUM et considère que le ressortissant d'un pays hors Union européenne ne peut être placé en garde à vue pour l'infraction d'entrée irrégulière sur le territoire puisque cette infraction n'est pas susceptible de peine d'emprisonnement, selon la CJUE. La solution apparaissait déjà dans un arrêt rendu le 9 novembre 2016 (Cass. 1re civ., 9 nov. 2016, n° 13-28.349) dans des termes identiques, reflétant le conflit

persistant entre l'interprétation européenne et la position interne. De ce point de vue, la solution est parfaitement justifiée juridiquement. Si l'infraction ne peut être assortie d'emprisonnement, elle ne peut conduire au placement en garde à vue qui devient une privation de liberté arbitraire, car dénuée de fondement. Il peut être utilement remarqué que la loi du 31 décembre 2012 a aussi créé, à l'article L 611-1-1 CESEDA, une procédure de rétention « aux fins de vérification de son droit de circulation ou de séjour sur le territoire français » pour une durée maximale de 16 heures. Cette procédure spéciale a vocation à se substituer à la procédure de droit commun qui repose sur la garde à vue.

TÉLÉPHONE PORTABLE AU VOLANT

Crim. 23 janvier 2018, n° 17-83077

Un conducteur a été contrôlé alors qu'il faisait usage de son téléphone en étant assis au volant de son véhicule qui stationnait sur la file de droite d'un rond-point avec les feux de détresse allumés, moteur en état de marche. Il est poursuivi devant la juridiction de proximité du chef de téléphone tenu à la main par le conducteur d'un véhicule en circulation. Il sollicite sa relaxe en soutenant que le véhicule n'était pas en circulation, puisqu'il se trouvait à l'arrêt, moteur éteint. Le jugement entre en voie de condamnation, car il avait bien son téléphone en main, alors qu'il était au volant de son véhicule et que celui-ci se trouvait en stationnement sur une voie de circulation. On voit le paradoxe de la situation. Soit le véhicule est en stationnement, soit en circulation. Or, selon les parties, ces deux allégations pouvaient être soutenues. Il convient donc d'apporter une preuve supplémentaire pour emporter la conviction des juges. Cet élément est l'état de marche du véhicule. Le moteur tourne-t-il ou est-il à l'arrêt ? Le prévenu n'apporte aucunement la preuve du fait que le moteur était éteint, alors que le ministère public fait constater par un procès-verbal de renseignement judiciaire que le moteur était en état de marche. Ce dernier emporte donc la conviction des juges qui considèrent que le véhicule était en état de marche. Ils condamnent la personne sur le fondement de l'article R 412-6-1 du

Code de la route qui interdit l'usage d'un téléphone tenu en main par le conducteur d'un véhicule en circulation et le punit d'une amende prévue pour les contraventions de la deuxième classe et du retrait de deux points du permis de conduire. La personne condamnée forme un pourvoi rejeté par la Cour de cassation qui invoque le pouvoir d'appréciation souveraine des éléments de preuves débattus contradictoirement par les juges du fond, mais saisit l'occasion pour dispenser un enseignement juridique.

La Chambre criminelle affirme que « doit être regardé comme toujours en circulation, au sens et pour l'application de l'article R 412-6-1 du code de la route, le véhicule momentanément arrêté sur une voie de circulation pour une cause autre qu'un événement de force majeure ». Si la solution des juges peut être considérée comme sévère, elle est parfaitement fondée au regard des principes du droit. Un véhicule moteur en marche sur une voie de circulation est un véhicule en circulation, puisque les arrêts sont interdits. Un événement de force majeure peut conduire à exonérer la personne de sa responsabilité pénale, mais les raisons de convenance personnelle en sont exclues. La force majeure étant soumise aux conditions cumulatives d'imprévisibilité et d'irrésistibilité, aucun doute n'est permis quant au fait que l'usage du téléphone portable ne les remplisse pas.

ABUS DE CONFIANCE

Crim., 31 janvier 2018, n° 17-80.049

Un notaire a mis en vente aux enchères, par l'intermédiaire de commissaires-priseurs, sur la base d'une estimation comprise entre 400 000 et 500 000 euros, la seule copie intégrale connue des *Mémoires d'outre-tombe* de François-René de Chateaubriand. Le directeur du service du livre et de la lecture au ministère de la Culture a demandé le retrait de la vente du manuscrit, estimant que le notaire n'en était pas propriétaire. Des investigations entreprises, il ressort que, par acte sous seing-privé en date du 22 mars 1836, François-René de Chateaubriand a cédé la propriété littéraire de ses œuvres inédites à son éditeur, agissant en son nom personnel, et pour le compte d'une société en

cours de constitution à l'époque. Cet acte était accompagné de codicilles et d'autres documents précisant les volontés de l'auteur, notamment, les conditions dans lesquelles devaient être publiées, à sa mort, ses œuvres inédites ; qu'il était ainsi prévu qu'un manuscrit restait entre les mains de l'auteur pour y faire les additions et corrections qu'il jugerait nécessaires, qu'un autre, appartenant à la société des acquéreurs, était déposé chez le notaire, le troisième étant remis à l'éditeur. Le manuscrit gardé par l'auteur devant être collationné avec les deux autres avant d'être publié. Un procès-verbal de 1847 constate le remplacement de l'exemplaire resté à l'étude notariale par un autre ; il établit que le gérant de la société d'édition a pris deux parties et a laissé les autres à l'étude notariale qui en était dépositaire. Il y est resté jusqu'à la vente décidée par le notaire qui détenait la totalité des parts de l'étude et avait succédé à son père et arrière- grand-père, lequel était le successeur ayant reçu le manuscrit en dépôt.

Le notaire a été poursuivi pour abus de confiance aggravé pour avoir détourné le manuscrit au préjudice de la succession par un officier public ou ministériel dans ou à l'occasion de ses fonctions. Il a été condamné par les juges du fond, ce qui a été confirmé par la Cour d'appel :

- « le prévenu a mis en vente l'ouvrage alors qu'il avait été informé par le conservateur général aux archives nationales que le répertoire de l'étude aux archives nationales mentionnait un acte de dépôt relatif au manuscrit ; que l'expression "laisser les autres" (portefeuilles) figurant dans l'attestation du 11 mai 1850 ne suffit pas à caractériser une donation » ;

- le contrat d'édition, qui n'était pas limité dans le temps, ne prenait pas fin avec l'achèvement de l'édition des mémoires, le 3 juillet 1850, et ne rendait pas caduc, à cette date, le dépôt du manuscrit dans l'étude notariale ;

- un dépositaire ne peut acquérir par prescription et le notaire ne démontrait pas que le titre en sa possession aurait été interverti.

Actualité pénale

L'absence de revendication de l'ouvrage pendant des décennies est indifférente ;

- le notaire, en sa qualité de notaire et de juriste, ne pouvait vendre l'ouvrage sans avoir effectué les recherches nécessaires et fait appel, le cas échéant, à des généalogistes ;
- il a, notamment dans ses premières déclarations, nettement reconnu ses défaillances à cet égard ;
- se comportant comme le propriétaire de l'ouvrage en le mettant en vente, il a détourné le manuscrit au préjudice des héritiers des ayants droit de la société d'édition devenue A... et Cie, leur occasionnant, à défaut d'un préjudice financier, la vente n'ayant pas abouti, un préjudice moral.

Il forme un pourvoi en cassation, rejeté par la Chambre criminelle qui considère que :

- la nature précaire du contrat en vertu duquel la chose a été remise a été établie par les juges ;
- « l'existence d'un préjudice, qui peut n'être qu'éventuel, se trouve nécessairement incluse dans la constatation du détournement ».

Police administrative

Par M. Ludovic Guinamant

Le Conseil d'État précise la portée de la notion de « grands événements », au sens du Code de la sécurité intérieure

Conseil d'État, 10ème et 9ème chambres réunies, 21 février 2018, n°414827

L'article 53 de la loi n° 2016-731 du 3 juin 2016, renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, a créé un article L. 211-11-1 dans le Code de la sécurité intérieure (CSI).
Ce dernier prévoit notamment que *« les grands événements exposés, par leur ampleur ou leurs circonstances particulières, à un risque exceptionnel de menace terroriste sont désignés par décret. Ce décret désigne également les établissements et les installations qui accueillent ces grands événements ainsi que leur organisateur »*. Il ajoute que l'accès de toute personne, autre que les spectateurs ou participants, à tout ou partie des établissements et installations susmentionnés est soumis à autorisation de l'organisation, prise après avis de l'autorité administrative qui peut consulter certains traitements automatisés de données à caractère personnel relevant de l'article 26 de la loi n° 78-17 du 6 janvier 1978, à l'exception des fichiers d'identification, afin de vérifier que le comportement ou les agissements de la personne ne sont pas de nature à porter atteinte à la sécurité des personnes, à la sécurité publique ou à la sûreté de l'État.

Le décret n°2017-1224 du 3 août 2017 a créé un traitement automatisé de données à caractère personnel dénommé *« Automatisation de la consultation centralisée de renseignements et de données »* (ACCReD) qui a pour objet de faciliter la réalisation des enquêtes administratives prévues, notamment, à l'article L. 211-11-1 du CSI par le Service national des enquêtes administratives de sécurité (SNEAS) de la DGPN et par le Commandement spécialisé pour la sécurité nucléaire (CoSSeN) de la DGGN et d'exploiter les informations recueillies dans

ce cadre.
Néanmoins, la Ligue des droits de l'Homme (LDH) a saisi le Conseil d'État d'une requête en annulation pour excès de pouvoir contre le décret précité et le 4 janvier 2018, au cours de l'instruction du dossier contentieux, elle a déposé une question prioritaire de constitutionnalité contre les dispositions de l'article L. 211-11-1 du CSI.

Dans ce dernier dossier contentieux, la LDH soutient qu'en s'abstenant, d'une part, de prévoir une définition suffisamment précise des notions de *« grands événements »* et *« d'organisateur »* de tels événements, d'autre part, d'assortir les pouvoirs des organisateurs de garanties appropriées et, enfin, d'encadrer les conditions de création et de consultation des traitements automatisés de données à caractère personnel destinés à la réalisation des enquêtes administratives qu'il permet, le législateur a entaché l'article L. 211-11-1 du CSI d'une incompétence négative affectant le droit au respect de la vie privée, la liberté d'aller et venir ainsi que le droit à un recours effectif garantis par les articles 2 et 16 de la Déclaration des droits de l'Homme et du citoyen de 1789.

Toutefois, le Conseil d'État, dans sa décision du 21 février 2018, décide de ne pas transmettre la question prioritaire de constitutionnalité au Conseil constitutionnel en précisant toutefois que « *les dispositions de l'article L. 211-11-1 du code de la sécurité intérieure imposent au pouvoir réglementaire, pour chaque mise en œuvre du régime d'autorisation qu'elles créent, de procéder par décret, sous le contrôle du juge de l'excès de pouvoir, premièrement, à la désignation du grand événement concerné, qui doit être exposé, par son ampleur ou ses circonstances particulières, à un risque exceptionnel de menace terroriste, deuxièmement, à l'identification de la personne physique ou morale, de droit public ou de droit privé, chargée de son organisation et donc de la délivrance des autorisations d'accès, troisièmement, à la délimitation précise de la durée de préparation et de déroulement du grand événement et, quatrièmement, à la désignation des établissements et installations qui accueillent ce grand événement et dont l'accès peut être interdit, à l'exclusion de tout autre local et des voies publiques permettant d'y accéder* ».

Cette dernière incise permet donc de préciser l'étendue du *« grand événement »* comme ne pouvant concerner que des établissements ou des installations précisés dans un décret et excluant les voies publiques d'accès et tout autre local qui n'accueille pas le « *grand événement* ».

Lutte contre la fraude documentaire : le Conseil d'État rappelle le régime de la preuve objective

Conseil d'État, 5ème et 6ème chambres réunies, 14 février 2018, n°407880

M. B. a demandé, le 8 novembre 2013, à la préfecture du Val d'Oise la délivrance d'un permis de conduire français en échange d'un permis de conduire malien. Toutefois, le préfet du Val d'Oise a consulté par la voie diplomatique les autorités maliennes, qui n'ont pas répondu, puis il a saisi un service spécialisé dans la lutte contre la fraude documentaire qui a relevé une anomalie conduisant à douter de l'authenticité du titre. Tirant les conséquences du rapport du service de lutte contre la fraude, le préfet a alors décidé de refuser l'échange de permis sollicité.

Le tribunal administratif de Cergy a rejeté la requête pour excès de pouvoir déposé par M. B. au motif, notamment, que les quatre attestations d'authenticité délivrées par les autorités maliennes, produites directement dans le cadre de l'instruction contentieuse devant le tribunal par le requérant, n'étaient pas parvenues par la voie diplomatique et, dès lors, ne pouvaient pas être prises en considération par le juge administratif.

Le Conseil d'État considère toutefois que les attestations produites par le requérant, lesquelles émanent des autorités maliennes, présentent néanmoins des garanties suffisantes pour établir l'authenticité du permis et remettre en cause les conclusions du rapport du service spécialisé au vu duquel le préfet avait refusé d'échanger le permis. Dans ces conditions, le Conseil d'État précise que le tribunal

administratif de Cergy, en écartant les preuves apportées par le requérant au motif qu'elles n'avaient pas transité par la voie diplomatique, avait commis une erreur de droit.

Dans cet arrêt, la Cour suprême administrative rappelle donc la mécanique contentieuse qui doit prévaloir dans l'instruction des dossiers de fraudes. Toutes les preuves objectives doivent être examinées et les magistrats doivent les prendre en compte afin de se forger leur intime conviction.

Les mesures individuelles de contrôle administratif validées par le Conseil Constitutionnel

Conseil Constitutionnel, décision n°2017-691 QPC du 16 février 2018

Le Conseil constitutionnel a été saisi, le 4 décembre 2017, par le juge des référés du Conseil d'État d'une question prioritaire de constitutionnalité posée par M. B. portant sur les articles L. 228-1 et suivants du Code de la sécurité intérieure (CSI), dans leur rédaction issue de la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme. Ces dispositions instaurent des mesures individuelles de contrôle administratif et de surveillance que le ministre de l'Intérieur peut prendre, aux fins de prévenir la commission d'actes de terrorisme, à l'encontre de certaines personnes. Quatre types de mesures individuelles de contrôle administratif et de surveillance peuvent être prononcées à l'encontre des personnes entrant dans le champ d'application de l'article L. 228-1 du CSI :

1) la première est l'assignation à résidence définie à l'article L. 228-2 du CSI. Elle peut être prononcée pour une durée maximale de trois mois à compter de la notification de la décision du ministre. Elle peut être renouvelée par décision motivée, pour une durée maximale de trois mois. Au-delà d'une durée cumulée de six mois, chaque renouvellement est subordonné à l'existence d'éléments nouveaux ou

complémentaires ;
2) La deuxième mesure est l'assignation à résidence avec placement sous surveillance électronique mobile. Elle résulte de la combinaison de l'article L. 228-2 précité et de l'article L. 228-3 du CSI ;
3) la troisième mesure est définie à l'article L. 228-4 du CSI. Elle est alternative à l'assignation à résidence. Elle recouvre deux obligations et une interdiction :
– une obligation de déclarer son domicile et tout changement de domicile,
– une obligation de signaler ses déplacements à l'extérieur d'un périmètre déterminé,
– une interdiction de paraître en certains lieux ;
Ces obligations peuvent être prononcées pour une première durée maximale plus longue, de six mois, mais dans la même limite maximale de douze mois.
4) la dernière mesure, prévue à l'article L. 228-5 du CSI, est une interdiction de fréquenter certaines personnes.

D'une manière générale, le Conseil constitutionnel a déclaré conformes à la Constitution les quatre mesures précitées en considérant que « *le législateur, qui a à la fois strictement borné le champ d'application de la mesure qu'il a instaurée et apporté les garanties nécessaires, a assuré une conciliation qui n'est pas manifestement déséquilibrée entre, d'une part, l'objectif de valeur constitutionnelle de prévention des atteintes à l'ordre public et, d'autre part, la liberté d'aller et de venir, le droit au respect de la vie privée, le droit de mener une vie familiale normale et le droit à un recours juridictionnel effectif* ».

Toutefois, les Sages de la rue Montpensier ont censuré les dispositions contentieuses liées au renouvellement de la mesure d'assignation à résidence. Ils indiquent ainsi que « *compte tenu de l'atteinte qu'une telle mesure porte aux droits de l'intéressé, en limitant à un mois le délai dans lequel l'intéressé peut demander l'annulation de cette mesure et en laissant ensuite au juge un délai de deux mois pour statuer, le législateur a opéré une conciliation manifestement déséquilibrée entre les exigences constitutionnelles* ». De la même manière, il précise également que *« le droit à un recours juridictionnel effectif impose que*

le juge administratif soit tenu de statuer sur la demande d'annulation de la mesure dans de brefs délais ».

Le cumul des fonctions de poursuite et de jugement de l'Agence française de lutte contre le dopage (AFLD) méconnaît le principe d'impartialité

Conseil Constitutionnel, décision n°2017-687 QPC du 2 février 2018

Le Conseil constitutionnel a été saisi, le 7 novembre 2017, par le Conseil d'État d'une question prioritaire de constitutionnalité posée par M. N. portant sur le 3° de l'article L. 232-22 du Code du sport, dans sa rédaction résultant de l'ordonnance n° 2015-1207 du 30 septembre 2015 relative aux mesures relevant du domaine de la loi nécessaires pour assurer le respect des principes du Code mondial antidopage.

M. N. a fait l'objet d'un contrôle par l'AFLD à l'occasion de sa participation à une compétition. L'échantillon prélevé ayant révélé la présence de substances dopantes interdites, la fédération française d'équitation a prononcé à son égard une mesure d'interdiction, avec sursis, de participer pendant trois mois aux manifestations organisées ou autorisées par cette fédération, a annulé les résultats qu'il a obtenus et a ordonné la publication de la décision dans un journal spécialisé. L'AFLD s'est saisie d'office de la décision rendue par cette fédération et a aggravé la sanction en portant le délai de la mesure d'interdiction à deux ans et en l'étendant à d'autres organisations sportives.

M. N. soutenait, à l'appui de sa QPC, que le pouvoir de réformation d'office exercé par l'AFLD méconnaissait les principes d'indépendance et d'impartialité qui découlent de l'article 16 de la Déclaration des droits de l'Homme et du citoyen de 1789. Selon lui, en ne désignant pas au sein de l'AFLD, d'une part, l'autorité décidant de la saisine d'office de l'agence et, d'autre part, celle chargée du jugement, le législateur n'avait pas garanti la séparation organique ou fonctionnelle entre ces

pouvoirs.

En application de l'article L. 232-21 du Code du sport, toute personne ayant contrevenu aux dispositions du même Code en matière de lutte contre le dopage encourt des sanctions disciplinaires de la part de la fédération auprès de laquelle elle est licenciée. Les fédérations agréées informent sans délai l'agence française de lutte contre le dopage des décisions prises. En vertu du 3° de l'article L. 232-22 du Code du sport, l'agence peut réformer les décisions prises en application de l'article L. 232-21. Dans ce cas, elle se saisit d'office dans un délai de deux mois à compter de la réception du dossier complet de la décision de la fédération. Conformément à l'article L. 232-23 du Code du sport, l'agence peut ensuite, en cas de condamnation, prononcer un avertissement, une interdiction temporaire ou définitive de participer à une manifestation sportive ou à l'organisation ou au déroulement d'une telle compétition, une interdiction d'exercer certaines fonctions ainsi que des sanctions pécuniaires.

Le Conseil Constitutionnel constate ainsi que les dispositions contestées confient à l'AFLD le pouvoir de se saisir d'office des décisions de sanctions rendues par les fédérations sportives qu'elle envisage de réformer. Ce pouvoir n'est pas attribué à une personne ou à un organe spécifique au sein de l'agence, alors qu'il appartient ensuite à cette dernière de juger les manquements ayant fait l'objet de la décision de la fédération et que, dès lors, elles méconnaissent le principe d'impartialité.

Par M. Xavier Latour

Réflexions récentes sur la sécurité privée

En l'espace de quelques jours, la sécurité privée a plusieurs fois retenu l'attention.
Le 31 janvier 2018, les universités de Paris Descartes et de Nice organisaient un colloque important consacré aux moyens de la sécurité privée. Quelques jours plus tard, le ministre de l'Intérieur ouvrait une nouvelle édition des Assises de la sécurité privée. Puis, le 7 février, la Cour des comptes profitait de son rapport public annuel 2018 pour dresser un constat très critique de la situation de la sécurité privée en France et, plus particulièrement, du fonctionnement du Conseil national des activités privées de sécurité (CNAPS).

Le constat d'une implication croissante de la sécurité privée n'est plus à faire. Son association aux périmètres de protection par la récente loi n° 2017-1510 du 30 octobre 2017 en est une nouvelle expression. Des clients publics (26 % du marché) ou privés sollicitent massivement des moyens humains et matériels. Cela implique de bien cerner les besoins grâce à un haut degré de professionnalisme.
Si le contrat fonde les relations entre un donneur d'ordre et un prestataire, le Code de la sécurité intérieure (CSI) témoigne de son caractère réglementé, et de sa spécificité dans l'environnement économique.

Depuis 1983, l'évolution du droit de la sécurité privée poursuit deux objectifs : déterminer les missions ouvertes ou fermées, tout en encadrant leur accomplissement.
Les entités privées fonctionnent dans le strict respect des obligations légales et réglementaires déterminées par l'État.
Des travaux de ce début d'année, il ressort une sérieuse interrogation : si la sécurité privée est complémentaire de la sécurité publique, comment penser plus efficacement cette complémentarité ? Le ministre de l'Intérieur a démontré sa volonté d'y répondre efficacement en lançant une réflexion sur le continuum des acteurs de la sécurité.
Si la sécurité privée se développe, elle le fait dans un cadre contraint,

voire paradoxal. En effet, ses missions ne cessent pas de se diversifier. Parallèlement, elle suit les évolutions technologiques. Elle s'adapte aux besoins de la société, tout en répondant à l'incapacité des personnes morales de droit public d'y répondre avec leurs seuls moyens. Elle se meut dans un environnement qui la place au premier plan de la prévention des menaces dans leurs formes les plus banales aux plus dramatiques.

Dans ce contexte, le chemin parcouru depuis 1983 est important. Le savoir-faire de la sécurité privée au quotidien comme pendant les grands événements s'est amélioré. Pourtant, des marges de progrès existent.

Les travaux de ce début d'année mettent en évidence d'une part, une mue en profondeur des moyens de la sécurité privée (I), même si, d'autre part, cette mue n'est pas achevée (II).

I. La mue en profondeur de la sécurité privée

Elle concerne, à la fois, les moyens humains (A) et matériels (B).

A. L'humain

Dans cette « industrie de main-d'œuvre », un agent de sécurité agit dans un cadre très contraint, au nom de la préservation de l'ordre public. Personne ne s'en offusquera. Au contraire, les progrès accomplis en matière de moralisation et de professionnalisation favorisent le développement raisonné de la sécurité privée.

Des agents nombreux sont-ils des agents compétents ? La réponse à cette question passe par la compréhension de la formation initiale et continue, désormais encadrée et contrôlée.

Une fois formé, l'agent doit agir. Autant pour ne pas concurrencer les forces publiques que pour ne pas menacer les libertés individuelles,

ses pouvoirs évoluent moins que ses moyens matériels. L'agent de sécurité pratique, au mieux, des palpations et des fouilles, et la plupart du temps sous l'autorité de la force publique. En créant des périmètres de protection gérés par la sécurité publique et la sécurité privée, la loi n° 2017-1510 du 30 octobre 2017 ne déroge pas au cantonnement de la sécurité privée que nul n'entend remettre en cause, tandis que cela stimule de nouvelles formes de partenariat.

L'ensemble du droit applicable à la sécurité privée organise le cantonnement.
L'accomplissement d'une mission dépend de la clarté de l'acte unilatéral ou contractuel applicable. Alors que la loi n° 83-629 du 12 juillet 1983 insistait sur les interdictions, les évolutions législatives portent davantage sur les obligations. Cette réorientation apparaît particulièrement dans les textes relatifs au transport de fonds, à la protection embarquée à bord des navires et à l'usage des armes. Interdictions et obligations sont, ensuite, déclinées sur le terrain.

Par ailleurs, l'agent de sécurité travaille dans un environnement caractérisé par la pluralité et l'interdépendance des intervenants.
Dans le prolongement des pratiques liées à la grande distribution, la circulaire du 5 janvier 2016 (INT/K/16/00290/J) relative aux conventions locales de coopération de sécurité représente une étape utile, en direction d'un dialogue constructif entre la puissance publique et les opérateurs privés. De même, et dans un domaine ponctuel, la circulaire du 20 avril 2017 (INTA1711331J) implique la sécurité privée dans le programme « tourisme et sécurité ».
Au quotidien, la sécurité privée est une source de renseignements à exploiter. Les informations recueillies par les agents privés méritent, sous certaines conditions de filtrage et d'analyse, d'être transmises aux forces publiques.
À l'inverse, les acteurs privés ont impérativement besoin de données précises sur l'état des menaces. En outre, ce dialogue contribue, au moins en théorie, à une meilleure répartition des moyens publics, tout en sécurisant les interventions des uns et des autres.

Si l'humain se situe au cœur de la prestation de sécurité, elle justifie aussi l'emploi de différents matériels.

B. Le matériel

La sécurité des agents privés de plus en plus exposés aux menaces explique une évolution symbolique du droit. Alors que l'ancien état du droit ne bloquait pas complètement les possibilités d'armement, le fondement législatif présente, malgré tout, le mérite de la solidité juridique et politique, en dépit d'un débat parlementaire plus résigné qu'animé.
En faisant prévaloir un critère matériel (la mission), sur un critère organique (personnes privées ou forces publiques), la loi n° 2017-258 du 28 février 2017 assouplit, en théorie, le principe du non-armement de la sécurité privée.
La condition de l'existence de risques exceptionnels en matière de protection physique de personnes et de surveillance renforcée fait cependant planer un doute sur le développement de l'armement dans l'avenir. Une incertitude comparable concerne les agents de surveillance courante, même si aucun risque exceptionnel n'est exigé. Alors que l'État a pris de sérieuses précautions pour encadrer l'armement, rien ne laisse présager *a priori* une appréciation souple par les préfets, sauf si la pression populaire s'en mêle. Parallèlement, les entreprises pourraient hésiter à multiplier les demandes, en raison des régimes de responsabilité et des coûts que l'armement de leurs agents induit.

Par ailleurs, la sophistication technologique bouleverse la sécurité privée en matière de surveillance humaine ; les technologies sont d'autant plus performantes qu'elles sont couplées (reconnaissance faciale couplée à la vidéoprotection, analyse comportementale…). Elles n'en demeurent pas moins hautement sensibles au regard de la protection des données personnelles ou de l'évolution des comportements professionnels.
Comme dans d'autres domaines, la technologie contribue à augmenter les capacités des agents (avec des drones par exemple). Toutefois, l'existence d'une technologie n'implique pas automatiquement son

emploi. Au contraire, le passage de l'utilité théorique à l'utilisation pratique dépend, d'une part, d'un bilan entre les coûts et les avantages économiques et, d'autre part, de l'existence d'un cadre juridique approprié.

Sur tous ces aspects, l'effectivité du droit dépend en grande partie des capacités de contrôle mises en œuvre, et de la doctrine qui les sous-tend. La création du CNAPS marque une étape importante en ce sens. Elle démontre le volontarisme de la puissance publique, tout en l'exposant à plusieurs titres.
D'une part, la possibilité d'une action en responsabilité contre le CNAPS en raison du dysfonctionnement (même pour faute lourde) de ses activités de contrôle est une hypothèse sérieuse. Elle s'appuie sur une jurisprudence bien établie dans d'autres domaines. Si cela venait à se produire, la responsabilité juridique de l'établissement public rejaillirait inévitablement sur l'État, tant sa proximité avec la structure est grande.
D'autre part, l'État a fait le choix de créer un établissement public administratif au fonctionnement duquel les professionnels de la sécurité privée participent. Or, son fonctionnement et ses résultats ont été sévèrement critiqués par la Cour des comptes dans son dernier rapport annuel.

Certes réelle, la mue de la sécurité privée reste inachevée.

II. La mue inachevée de la sécurité privée

Dans un contexte de menaces diverses et évolutives, deux questions persistent : comment poursuivre l'amélioration de l'encadrement de la sécurité privée (A) et mieux coordonner ses actions à celles des forces publiques (B) ?

A. Quel encadrement ?

En dépit de l'encadrement de la formation, beaucoup reste à faire.

L'amélioration de la qualité par la formation est prioritaire. La formation doit être réellement au service de la sécurité privée en valorisant des compétences, et en ouvrant des perspectives d'évolution de carrière.
Or, cela passe par une acceptation du coût par les entreprises, employeurs et donneurs d'ordre, y compris publics. La Cour des comptes a insisté, à juste titre, sur la faiblesse des rémunérations et de l'encadrement intermédiaire d'un côté et, de l'autre, sur une tendance des acheteurs à opter pour le prix le plus bas au risque d'entretenir la spirale malsaine de la sous-traitance.

Des agents efficaces doivent être aussi des agents bien encadrés. Or, au quotidien, l'inégalité des consignes données affaiblit les missions, malgré les obligations du CSI (R 631-16). Au-delà des considérations opérationnelles, quelle est la base juridique la plus adéquate pour améliorer l'efficacité de la sécurité privée ? Conviendrait-il de passer par la loi et le règlement pour imposer aux entreprises des obligations qui s'inspireraient de celles applicables à la prévention de l'incendie ? Autre possibilité, le contrat ne devrait-il pas être privilégié ?
Dans ce cas, la relation entre le donneur d'ordre et le prestataire recèle sans doute des marges de progrès, à condition de penser l'écrit comme une garantie et non comme une contrainte. Par conséquent, entre la loi et la liberté contractuelle, un équilibre devra être trouvé, avec l'objectif essentiel d'améliorer la qualité des prestations.
Parallèlement, la normalisation représente-t-elle une autre solution ? Sa progression ne traduirait-elle pas une forme de privatisation du contrôle qui serait surprenante dans le domaine de la sécurité ?
Plutôt que d'aller dans cette direction, l'affermissement de la puissance publique s'imposerait. Car, si les entreprises n'attachent pas l'importance qu'elles méritent aux consignes, l'État lui-même ne donne pas l'exemple. Sa conception des missions de la sécurité privée manque de rigueur. En d'autres termes, il peine encore à définir une doctrine d'emploi de la sécurité privée, tandis que, parallèlement, le CNAPS est critiqué pour ses insuffisances en matière de police administrative et d'actions disciplinaires. Sur ces points, le rapport de la Cour des comptes brosse un panorama sans concession. Le manque d'implication des représentants de l'État et le poids pris par les professionnels de la sécurité privée fragiliseraient l'ensemble. La

professionnalisation et la moralisation ne seraient pas assez contrôlées, avec seulement un taux de rejet de 8 % des demandes de cartes professionnelles (d'ailleurs non sécurisées) et des sanctions disciplinaires autant insuffisantes que mal appliquées.

Sous un angle technologique, la télésurveillance revêt des formes de plus en plus originales (autosurveillance, par exemple). Plus spécifiquement, les drones attendent encore un cadre juridique adéquat. Les solutions manquent toujours, en particulier en matière de préservation de la vie privée. En effet, les règles applicables à la vidéoprotection fixe ne sont pas transposables à cette forme de surveillance.
Des demandes d'évolutions juridiques accompagneront les progrès technologiques. Les algorithmes couplés au *big data* intéressent au plus haut point la police prédictive. Ces instruments pourraient se généraliser dans les entreprises privées de sécurité, en étant couplés à des fichiers, comme cela se pratique déjà dans les assurances. Des algorithmes sont conçus dans des entreprises privées qui, si elles ne font pas de la surveillance au sens strict, prendront une part essentielle dans l'architecture d'une sécurité dématérialisée. À quels contrôles les soumettre ? Ce pan de la sécurité est encore largement en friche, notamment quant à la détermination des responsabilités et à la garantie de la confiance.
Les industriels voudront trouver un débouché pour leurs produits, lesquels créent le besoin. De leur côté, les professionnels de la sécurité verront probablement le moyen de créer de la valeur ajoutée, tandis que la société angoissée continuera d'accepter des ingérences dans les libertés au nom de la sécurité. Toute la difficulté consistera alors à construire des régimes équilibrés. Mais, à rebours des courants dominants, le politique devra prouver son courage en s'opposant à de possibles dérives, donc à la généralisation de certaines technologies.
La sécurité ne justifie pas tout, tant en termes de transferts (parfois pudiquement appelés partage de missions), que des moyens mobilisés.

Au-delà des technologies, le droit de l'armement évoluera-t-il ? Les critiques adressées par la Cour des comptes incitent à en douter.
Pourtant, un raisonnement par analogie avec les polices municipales

met en évidence une tendance à l'augmentation de la puissance. La survenue de drames relancera sans doute le débat d'une meilleure protection des agents et de la population. À l'inverse, des bavures n'ont jamais conduit à un retour en arrière. Nul ne songe, en général, à désarmer.
Or, le renforcement des moyens pourrait, également, passer par une évolution du droit. À cet égard, le maintien à l'écart des polices municipales de l'article L 435-1-5° CSI (sur la réitération de meurtre ou tentative de meurtre) semble fermer cette perspective, sauf à aligner l'usage des armes de tous les acteurs de la sécurité sur celui de la police nationale et de la gendarmerie. Cette hypothèse demeure, pour le moment improbable, aussi improbable que l'était l'autorisation d'une surveillance armée il y a quelques années.

B. Quelle coordination ?

La coordination s'impose et l'existence d'une délégation dédiée mérite d'être saluée. Pourtant, son positionnement dans l'organisation administrative suscite des interrogations. Le CNAPS est devenu l'interlocuteur privilégié des professionnels, outrepassant son rôle. Il occupe l'espace laissé en partie vacant par le ministère de l'Intérieur. Il n'a pas encore trouvé la façon la plus appropriée d'appréhender les enjeux de la sécurité privée ni institutionnellement ni, sous certains points, juridiquement.

En matière de partage d'informations, le décalage entre le discours et les actes mériterait d'être comblé tant nationalement que localement. Nationalement, des propositions des réformes structurelles existent. Pour autant, le pragmatisme ne justifierait-il pas de commencer localement ? Le mouvement a été enclenché avec les conventions locales de coopération de sécurité.
En droit, le recours à de modestes circulaires, non impératives, pour fonder la coopération et l'échange d'informations, tranche avec l'importance du sujet.
En pratique, des possibilités totalement inexploitées permettraient déjà d'associer la sécurité privée aux instances locales de coordination. Même les communes qui font appel à des prestataires privés ne les

convient pas aux réunions du conseil local de sécurité et de prévention de la délinquance.
Si des démarches volontaires ne suffisent pas à consolider une coopération que nos voisins européens (Italie ou Grande-Bretagne par exemple) appliquent depuis longtemps, alors peut-être conviendrait-il que l'État passe par des voies plus contraignantes.
Deux phénomènes compliquent cependant la situation. D'une part, une forte tendance des acteurs étatiques au cloisonnement perdure. D'autre part, les intervenants privés offrent trop souvent l'image d'une profession hétérogène, et tellement dispersée que l'identification d'interlocuteurs s'avère délicate. La désignation d'un référent local par les organisations représentatives de la sécurité privée (comme cela se fait au sein des commissions locales d'agrément et de contrôle du CNAPS) permettrait, cependant, de contourner l'obstacle. Il dialoguerait avec un référent public (policier ou gendarme) dédié.
D'ailleurs, les pratiques changent. Le 25 janvier 2018, le Club des directeurs de sécurité et sûreté des entreprises (CDSE) et la gendarmerie nationale ont signé une convention qui permet aux gendarmes d'envoyer un officier de liaison dans une structure proche des entreprises.
Au-delà et comme la Cour des comptes (rapport annuel 2018) le met, à juste titre, en évidence, la coordination exige un pilotage de l'État plus étroit.

À cet égard, le contexte ne justifierait-il pas un droit plus volontariste ?
L'une des raisons qui motivent la conclusion obligatoire des conventions de coordination entre les forces nationales et les polices municipales réside dans l'armement de ces dernières. Certes, les polices municipales diffèrent de la sécurité privée.
Pourtant, les textes n'excluent pas l'exercice de l'activité privée dans des transports publics, ou à partir de la voie publique. De plus, la surveillance armée se déploiera dans des espaces exposés à des risques exceptionnels, qui intéresseront aussi les forces publiques. Par conséquent, des conventions de coordination obligatoires pour la surveillance armée compléterait le cadre juridique en vigueur. Cela n'exclurait pas de conserver des conventions facultatives dans les autres domaines, à condition d'en améliorer le modèle et, surtout, de

favoriser l'implication des parties concernées.

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