LA VEILLE JURIDIQUE

Centre de Recherche de l'Ecole des Officiers de la Gendarmerie Nationale

N° 89 | Septembre 2020

EDITO

Voici venue la rentrée et, avec elle, la reprise de la Veille juridique du CREOGN. Une nouveauté : la publication sur notre site des veilles thématiques, reprenant la totalité des articles de l'année précédente. Merci à l'équipe de rédaction qui a entrepris ce travail. Sont déjà publiées les veilles thématiques « Déontologie de la sécurité », « Droit des collectivités territoriales et de la sécurité privée » et « Droit de l'espace numérique ». Les deux autres thèmes devraient être bientôt accessibles sur le site. Une fois encore je redis combien ces documents peuvent être utiles aux candidats aux concours.

Notre rédactrice de la rubrique « Police administrative », Elisabeth Rolin, a été nommée, le 1er

(Suite page 2)

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

Edito

août, au cabinet du directeur général de la gendarmerie nationale comme cheffe du pôle juridique et judiciaire. Nous lui présentons des vœux de réussite dans ses nouvelles fonctions et la remercions d'accepter de poursuivre la mission auprès du CREOGN, malgré le poids de ses nouvelles attributions.

La rentrée est aussi celle de la Covid qui ne manque pas d'affecter toutes les activités, notamment celles consacrées à l'enseignement. La distanciation sociale dans une école comme l'EOGN, où le « collectif » l'emporte sur la solitude de la distanciation, n'est pas un exercice simple. Il nous oblige à nous adapter, comme nous l'avons fait avec l'équipe de Paris 2 derrière Frédéric Debove, à l'occasion de la soutenance des mémoires des élèves civils et militaires du Master 2 « Droit et stratégies de la sécurité ». Quel que soit le niveau de notre « agilité », nous devons être conscients de la durée de la pandémie et de ses multiples conséquences sur la vie politique, économique et sociale. Bien évidemment, la gendarmerie est directement concernée, non seulement parce que ses personnels et leurs familles sont aussi victimes de la Covid, mais aussi en raison de son impact sur le service à rendre aux citoyens. Malgré cela la vie doit continuer. La nouvelle stratégie « Répondre présent » définie par le général d'armée Rodriguez n'est pas une option conjoncturelle mais va s'inscrire dans la durée, ouvrant un vaste chantier pour la réflexion et l'action.

Cette période inédite soulève de nombreuses difficultés d'ordre juridique, sociologique ou moral : comment préserver la primauté du « politique » sur « l'expertise », concilier les libertés, notamment celles d'aller et de venir, de manifester ou de se rassembler, avec un virus qui n'aime guère les concentrations de personnes, même si elles ne sont pas les plus vulnérables ? Comment articuler les

Edito

réponses entre autorités déconcentrées et autorités décentralisées ? Comment organiser dans la durée un télétravail qui se « massifie » et présente des caractéristiques peu explorées par le droit du travail ? Comment équilibrer la préservation de la santé et les exigences de l'économie ?

Il nous faut aussi porter un regard sur la violence qui semble se banaliser depuis la levée du confinement et vise souvent les détenteurs de l'autorité, les maires en première ligne. Notre société est malade, de la Covid mais aussi des conséquences d'une forte détérioration du « vivre ensemble », de la remise ne cause du « pacte républicain ». Comment imaginer sa résilience si elle aborde l'adversité désunie ? Autant de thématiques qui ne manqueront pas d'animer les débats, la recherche. L'époque est riche en sujets inédits pour les docteurs et doctorants de la gendarmerie, dont la communauté s'accroît.

Je ne peux oublier de mentionner – spécialité oblige – un événement peu repris par les médias mais qui constitue incontestablement une rupture dans la cybercriminalité : la mort d'une patiente lors d'une cyberattaque de l'hôpital de Düsseldorf, le 15 septembre dernier. C'est la première fois qu'une cyberattaque, en dehors de l'hypothèse d'un conflit armé, fait une victime. Certes, cette mort n'était pas intentionnelle, mais elle montre que la mise en danger d'autrui, via l'espace numérique, est désormais une réalité. Qu'en sera-t-il dans le monde hyperconnecté qui s'annonce, avec son cortège de risques systémiques ?

Le débat sur la 5G illustre l'inquiétude que suscite la transformation numérique. S'il faut refuser les prises de positions des rétrogrades (déjà exprimées lors de l'avènement du chemin de fer ou de l'automobile), il convient de reconnaître que toute

Edito

innovation ne peut se satisfaire d'une réponse technique et juridique ; elle doit être portée par une acceptation sociale qui repose avant tout sur la confiance dans les prescripteurs. La confiance, un mot clé qui va dominer notre société. Sans elle, rien ne peut se construire.
Bonne lecture de la Veille juridique !

Par le général d'armée (2S) Marc WATIN-AUGOUARD

SOMMAIRE

Déontologie et sécurité

Fréderic DEBOVE

De la Covid-19 au maintien de l'ordre : le temps des mutants !

Alors que les scientifiques et le pouvoir politique s'opposent vertement sur l'hypothèse d'une mutation – voire d'une surmutation – du Sars-CoV-2, la fin de l'été 2020 semble sonner le glas de pratiques policières souvent vilipendées, en ouvrant la voie à une autre mutation, plus tangible et attendue, celle du maintien de l'ordre à la française. Un maintien de l'ordre plus respectueux du droit, de la déontologie et des libertés fondamentales, tel était le souhait exprimé par le Défenseur des droit à travers sa décision-cadre n° 2020-131 portant recommandations générales sur les pratiques du maintien de l'ordre au regard des règles de déontologie. Dans le prolongement de cette décision-cadre du 9 juillet 2020, et alors que le mouvement des « gilets jaunes » connaît de nouveau quelques frémissements après une période d'assoupissement, le ministre de l'Intérieur Gérald Darmanin vient de dévoiler les grands axes du schéma national du maintien de l'ordre (SNMO). Avant de scruter les principales innovations de cette nouvelle doctrine commune à la gendarmerie et à la police nationales, il convient de récapituler les faiblesses et les imperfections de l'ancien dispositif telles qu'elles sont explicitées dans la décision-cadre précitée.

Les maux du MO à la française

Le 9 juillet 2020, le Défenseur des droits a rendu publique une

décision (n° 2020-131) singulière dans le domaine de la déontologie de la sécurité. Détachée de toute saisine particulière, la décision n° 2020-131 prend en effet la forme d'une décision-cadre. Sur un total de 23 pages, cette décision-cadre énonce une série de recommandations générales se rapportant au maintien de l'ordre. Prenant appui sur les très nombreuses saisines enregistrées depuis le début du mouvement des « gilets jaunes » (près de deux cents, réparties selon les griefs suivants : violences physiques (52), usage du LBD (46), usage du gaz lacrymogène (51), usage de grenades (18), mise en œuvre de la pratique des nasses (26), entrave à la prise de vues (12)) ces recommandations sont tantôt inédites, tantôt des reformulations de recommandations précédentes (V. singulièrement le rapport du Défenseur des droits rendu public en janvier 2018 et intitulé *Les conséquences de la doctrine et de la pratique du maintien de l'ordre en France par les forces de l'ordre au regard des règles de déontologie qui s'imposent à elles*). Quand bien même deux obligations déontologiques – l'obligation de discernement ; l'obligation de protection de l'intégrité physique des manifestants et des forces de sécurité – imprègnent très largement la décision-cadre, cette dernière est jalonnée de multiples préconisations destinées à alimenter la conception d'un nouveau schéma national de maintien de l'ordre.

Une première série de recommandations a trait à la liberté fondamentale d'aller et venir qui se trouve régulièrement malmenée au contact de certaines pratiques policières comme les contrôles d'identité délocalisés, les interpellations préventives, les pratiques d'encagement ou bien encore les interpellations massives. **S'agissant des contrôles d'identité délocalisés**, le

Déontologie et sécurité

Défenseur des droits tient à réitérer sa position selon laquelle, en dehors des conditions posées par l'article 78-3 du Code de procédure pénale (refus ou impossibilité de justifier son identité), de telles pratiques sont dépourvues de toute base légale. En ce qu'ils ont pour effet de transporter une personne et de la priver temporairement de liberté, le plus souvent en dehors de tout contrôle de l'autorité judiciaire, les contrôles d'identité délocalisés sont corrélativement source de responsabilité pénale et disciplinaire pour le militaire de la gendarmerie ou le fonctionnaire de police qui l'ordonne ou l'exécute (décision n° 2019-246 du 10 décembre 2019). Pareil constat vaut également pour **certaines interpellations préventives**. Sans préjuger des décisions que le Défenseur des droits sera appelé à rendre dans le cadre de saisines individuelles en cours d'instruction, les interpellations en amont ou aux abords des manifestations ne sont pas sans soulever de délicates interrogations lorsque le seul motif sur lequel elles sont fondées est la détention d'objets qui en eux-mêmes ne sont ni dangereux ni illicites (gilets jaunes, lunettes de piscine, masques de protection, sérum physiologique, etc.). Malgré les avancées de la loi dite « anti-casseurs » n° 2019-290 du 10 avril 2019 (avec l'institution du nouveau délit de dissimulation du visage, l'extension de la peine complémentaire d'interdiction de manifester, l'extension aux délits d'attroupements illicites des procédures rapides de jugement, la faculté pour le procureur de la République de délivrer des réquisitions écrites au fins de visites de véhicules, d'inspections visuelles des bagages et de leur fouille sur les lieux d'une manifestation et à ses abords immédiats), aucune disposition juridique ne permet aujourd'hui d'interpeller des

manifestants qui n'enfreignent pas la loi en considération de leur comportement (visage dissimulé par exemple) ou des objets qu'ils détiennent (arme, stupéfiants par exemple). De surcroît, les inspections visuelles des bagages et leur fouille, ainsi que les visites des véhicules, ne peuvent conduire à une immobilisation de la personne concernée que le temps strictement nécessaire à leur réalisation. Ces opérations policières ne sauraient avoir, par elles-mêmes, pour effet de restreindre l'accès à une manifestation, ni d'en empêcher le déroulement (Cons. Const., déc. n° 2019-780 DC du 4 avril 2019). En complément de ces interpellations préventives – même si les deux opérations peuvent être en pratique dissociées –, **se pose également la question de la légalité des confiscations** se rapportant à ces objets qui ne sont en eux-mêmes ni illicites, ni dangereux pour autrui (cf *supra*, p. 8). Quand bien même certaines confiscations ont-elles pu s'effectuer en application d'arrêtés préfectoraux ou de réquisitions judiciaires, le Défenseur des droits exprime ses plus grandes réserves à l'égard de ces mesures préventives au regard de la valeur constitutionnelle de la liberté de manifester et des modalités très aléatoires de restitution des objets confisqués.

De la même manière qu'elle condamne les contrôles d'identité délocalisés ainsi que les interpellations et confiscations préventives, la décision-cadre n° 2020-131 stigmatise la pratique policière consistant à priver plusieurs personnes de leur liberté de se mouvoir au sein d'une manifestation au moyen d'un encerclement par les forces de l'ordre. Souvent accompagnée d'usage de gaz lacrymogène, **cette technique dite de l'encagement** présente sans doute une certaine utilité pratique au

moment d'isoler et de neutraliser une nébuleuse violente. Toutefois, en l'absence de cadre juridique en limitant l'usage et en considération des difficultés pratiques de s'extraire de la nasse, le Défenseur des droits réclame qu'il soit mis fin à cette technique de maintien de l'ordre.

Sans condamner le principe même des interpellations en nombre à l'occasion de manifestations, le Défenseur des droits insiste dans sa décision-cadre sur plusieurs difficultés au regard des libertés fondamentales. Une première difficulté a trait à la difficile conciliation entre les garanties procédurales offertes aux personnes gardées à vue et l'allongement inévitable des délais inhérents au caractère collectif de l'interpellation (une interpellation massive de manifestants pouvant ainsi conduire à priver un mineur d'un examen médical dans un délai raisonnable). Une deuxième difficulté se rapporte aux conditions de rétention des personnes concernées par l'interpellation collective. Sans même évoquer certaines pratiques policières très singulières (manifestants agenouillés au sol avec les mains positionnées derrière la tête), le maintien plusieurs heures dans un car de police ou sur un parking d'un commissariat sans pouvoir se déshydrater ou accéder aux toilettes interroge légitimement sur la préservation de la dignité des personnes interpellées. Une troisième difficulté – qui dépasse d'ailleurs largement la seule hypothèse des interpellations collectives – a trait à la difficile conciliation du maintien de l'ordre avec la liberté d'informer. Sur cette question, la position du Défenseur des droits est sans aucune ambiguïté : l'usage de la force à l'encontre d'un journaliste ou d'un observateur issus de la société civile (comme la Ligue des droits de l'Homme),

clairement identifiables, caractérise une violence illégitime en même temps qu'une atteinte à la liberté d'expression. En outre, si les forces de l'ordre bénéficient comme tout citoyen du droit au respect de la vie privée, elles ne peuvent faire obstacle à l'enregistrement ou à la diffusion publique d'images ou de paroles à l'occasion de l'exercice de leur fonction (V. en ce sens les termes de la circulaire n° 2008-8433-D du 23 décembre 2008).

Alors que certaines recommandations du Défenseur des droits concernent la liberté de manifester en général, d'autres sont plus spécifiques et concernent tout particulièrement l'usage de la force.

Pourtant encadré par le Code pénal (art. 431-3) et le Code de la sécurité intérieure (art. L. 211-9 et R. 434-18), l'usage de la force en maintien de l'ordre ne correspondrait pas toujours à une nécessité absolue, à s'en tenir à l'appréciation même du Défenseur des droits. Par respect des libertés publiques et de l'intégrité physique des manifestants, le Défenseur des droits recommande en conséquence le retrait ou l'évaluation approfondie de l'usage de plusieurs armes qu'il juge inadaptées aux opérations de maintien de l'ordre. S'agissant du lanceur de balles de défense LBD 40x46, c'est l'interdiction qui l'emporte et, à titre subsidiaire, la traçabilité systématique des tirs de LBD si l'usage de cette arme devait perdurer. En ce qui concerne la grenade GLI-F4 et sa remplaçante – sans explosif ni effet de souffle – la grenade GM2L, une réflexion approfondie est sollicitée sur la dotation de cette arme de force intermédiaire dans le cadre d'opérations de maintien de l'ordre. En lien avec le constat de l'usage inapproprié de la force, le Défenseur des droits renouvelle en outre ses recommandations (déjà

formulées dans le rapport de janvier 2018) se rapportant à l'action des unités non dédiées au maintien de l'ordre (comme les BAC). Fondées sur des initiatives individuelles dépourvues de coordination d'ensemble, les pratiques de ces unités sont très souvent éloignées de la doctrine de la police administrative d'accompagnement de la liberté de manifestation. Autant sources de tensions avec les manifestants que périlleuses pour les fonctionnaires affectés dans ces unités, ces pratiques sont douteuses en termes de transparence de l'action policière, singulièrement lorsque les personnels considérés interviennent en civil, sans aucun signe distinctif et parfois même en se dissimulant le visage (avec un casque intégral ou une cagoule). Par la désorganisation qu'elles créent dans le maintien de l'ordre, ces pratiques méritent d'être repensées.

La parabole biblique du bon grain et de l'ivraie transposée au MO

Après avoir plongé la France en état de choc et mis en berne le drapeau tricolore, les attentats terroristes de l'année 2015 avaient donné naissance à un nouveau schéma national d'intervention (SNI). Le contexte de mobilisation des « gilets jaunes », la radicalisation de la contestation, l'infiltration des cortèges pacifiques par des groupuscules organisés, violents et mobiles, le rejet du cadre codifié des manifestations, comme les recommandations récentes du Défenseur des droits, ont précipité pour leur part l'élaboration d'un nouveau schéma national du maintien de l'ordre (SNMO). Esquissé dès le printemps 2019 par le ministre de l'Intérieur de l'époque, Christophe Castaner, ce

nouveau cadre d'exercice du maintien de l'ordre vient d'être dévoilé (16 septembre 2020) dans ses grands lignes par son successeur place Beauvau, Gérald Darmanin. Loin de faire table rase du passé, ce schéma conserve la philosophie générale du maintien de l'ordre à la française tout en y apportant des évolutions notables en termes de mobilité des forces de l'ordre, de capacités d'action et de communication avec les manifestants. **Synthétisé dans un document de 29 pages, le SNMO est conçu comme *« le premier document de doctrine en la matière commun à l'ensemble des forces de la police et de la gendarmerie nationales »***. Le cadre d'exercice est délibérément global en ce qu'il a vocation à couvrir toutes les configurations possibles de manifestations rencontrées sur le territoire national (pacifiques, violentes, urbaines, rurales). Le schéma est destiné à recevoir une large publicité (par le biais de supports pédagogiques) afin de diffuser une culture partagée sur les règles gouvernant les manifestations, les sommations ou bien encore l'usage des armes.
Ferme à l'égard des auteurs de violences tout en étant pleinement respectueux de la liberté d'expression collective à l'égard des manifestants, tel est l'esprit du schéma national du maintien de l'ordre. Après une première partie consacrée à un rappel des règles juridiques gouvernant les manifestations (régime de déclaration préalable, possibilités d'interdictions, etc.), **le SNMO érige la communication avec les organisateurs et les manifestants en une priorité dans la gestion de l'ordre public**. Pour développer plus en avant cette interaction, le SNMO préconise de dédier une équipe au dialogue, à la liaison et à l'information avec les organisateurs et les manifestants. Dans une

logique d'apaisement, cette mission – placée sous l'autorité du directeur du service d'ordre – sera exclusive de toute autre lors du maintien de l'ordre, du rassemblement jusqu'à la dispersion. Pour accompagner cette nouvelle mission jugée prioritaire, de nouveaux équipements (haut-parleurs de forte puissance, panneaux à message variable, envoi de SMS groupés, etc.) seront mis à disposition des forces de l'ordre.

Afin de mieux concilier la liberté fondamentale d'information et les impératifs du maintien de l'ordre, le SNMO préconise la désignation d'un officier référent au sein des forces de l'ordre ainsi que la mise en place d'un canal d'échange dédié. Cet esprit de conciliation a toutefois ses limites : de façon sans doute un peu péremptoire (au regard de la jurisprudence européenne), le SNMO énonce en effet que *« le délit constitué par le fait de se maintenir dans un attroupement après sommation ne comporte aucune exception, y compris au profit des journalistes ou de membres d'associations. Dès lors qu'ils sont au cœur d'un attroupement, ils doivent, comme n'importe quel citoyen, obtempérer aux injonctions des représentants des forces de l'ordre en se positionnant en dehors des manifestants appelés à se disperser »*.

Dans sa partie centrale, le SNMO rappelle quelques vérités d'évidence et, singulièrement, l'importance des mesures préventives (anticipation des risques par l'engagement des services de renseignement dans le suivi des individus les plus radicalisés, limitation des opportunités d'exaction par des mesures de prévention situationnelle, détection de l'intrusion d'objets dangereux par le jeu de réquisitions judiciaires, etc.) **ou bien encore le professionnalisme des unités spécialisées** (dont les effectifs seront sensiblement augmentés : + 215 ETP pour les compagnies

républicaines de sécurité, + 300 ETP pour les escadrons de gendarmerie mobile, + 88 ETP pour les compagnies d'intervention de la préfecture de police de Paris). Pour autant, le SNMO n'écarte pas le recours à des unités plus généralistes et territoriales, à la condition qu'elles soient équipées en conséquence. De même, en situations d'urgence ou exceptionnelles, et aux fins de disposer de l'ensemble des forces disponibles, l'assistance mutuelle est préconisée entre les effectifs de la police et de la gendarmerie nationales ; des effectifs sur lesquels peuvent utilement se greffer des équipes des services d'incendie et de secours.

En termes de doctrine, le SNMO privilégie le maintien à distance de la foule, à tout le moins en l'absence de risques de troubles à l'ordre public. Dans le cas contraire, l'adaptation au plus près du dispositif doit intervenir sans délai aux fins de permettre l'interpellation des fauteurs de troubles, le respect du parcours et la préservation de la liberté de manifestation. Lorsque des troubles à l'ordre public surgissent et que la dispersion de la manifestation s'impose, le SNMO préconise le recours à des sommations plus intelligibles à destination des manifestants. En somme, l'illégalité du rassemblement doit être immédiatement perceptible par celles et ceux auxquels s'adressent les sommations dont la formulation pourrait à l'avenir s'articuler autour des annonces suivantes : *« Attention ! Attention ! Vous participez à un attroupement. Vous devez vous disperser et quitter les lieux »*, *« Première sommation : nous allons faire usage de la force. Quittez immédiatement les lieux »*, *« Dernière sommation : nous allons faire usage de la force. Quittez immédiatement les lieux »*.

Par-delà l'intelligibilité de l'action policière, le SNMO met l'accent sur l'impérieuse exigence de transparence des

opérations de maintien de l'ordre. Dans cette perspective, le SNMO rappelle l'interdiction du port de la cagoule pour les personnels relevant d'unités spécialisées, le caractère obligatoire du port du RIO sur les tenues de maintien de l'ordre et annonce la prochaine généralisation du marquage dans le dos des personnels relevant d'unités spécialisées.

Enfin, symboliquement, les derniers développements du SNMO sont consacrés à l'action des forces de l'ordre contre les auteurs d'exactions. Afin de discriminer le bon grain (le manifestant paisible) de l'ivraie (le fauteur de trouble), **le SNMO insiste sur la double exigence de réactivité et de mobilité qui doit guider l'action des forces de l'ordre**. En complément de certaines formations spécialisées déjà existantes (comme les BRAV de la Préfecture de police de Paris ou bien encore les pelotons d'intervention), le SNMO encourage la création d'unités mobiles composées d'effectifs territoriaux qui présentent l'avantage de maîtriser la topographie de la zone considérée. Sous réserve de toujours laisser une issue aux manifestants, le SNMO s'écarte des préconisations du Défenseur des droits en ne condamnant pas la technique de l'encagement dont la pertinence est saluée en certaines circonstances. Pareillement, plutôt que d'émettre des réserves sur le phénomène contemporain de judiciarisation du maintien de l'ordre (comme le fait le Défenseur des droits), **le SNMO préconise de mieux intégrer la dimension judiciaire du maintien de l'ordre dans les dispositifs mis en place**. Des équipes judiciaires de constatation devront à l'avenir être intégrées au sein des opérations. Ces procéduriers devront pouvoir accéder en temps utile à tous les moyens de preuve de la police technique et scientifique (et singulièrement les exploitations de vidéos ou

d'images captées par des caméras de vidéo-protection, des drones ou des hélicoptères) pour caractériser les infractions et identifier leurs auteurs. Mieux associés au dispositif, en amont jusqu'en aval, et présents le cas échéant sur les lieux de la manifestation, les magistrats du Parquet seront plus à même d'orienter les procédures en mettant en œuvre les modes de poursuites rapides éventuellement assortis d'un déferrement.

Enfin, comme par pudeur, le SNMO consacre ses derniers développements à l'emploi de la force en maintien de l'ordre. Après avoir rappelé le chapelet des exigences s'y rapportant (absolue nécessité, proportionnalité, graduation, traçabilité), le SNMO préconise quelques évolutions en termes d'emploi des moyens de forces intermédiaires afin de les rendre moins vulnérables. En même temps qu'il confirme l'abandon de la grenade GLI-F4 au profit du modèle GM2L, le SNMO définit une nouvelle doctrine d'emploi du LBD 40 à l'occasion d'opérations de maintien de l'ordre. Sans préjudice des situations de légitime défense, tout tir de LBD – tracé par une caméra – relèvera à l'avenir de la responsabilité d'un binôme (tireur, superviseur), le superviseur étant chargé *« d'évaluer la situation d'ensemble et les mouvements des manifestants, de s'assurer de la compréhension des ordres par le tireur et de désigner l'objectif »*. En somme, il s'agit d'éviter les initiatives individuelles intempestives et malheureuses en sécurisant autant qu'il est possible l'usage des armes dans un contexte dégradé. Enfin, puisque rien ne dure vraiment, le SNMO s'achève en précisant que ses préconisations ne sont pas gravées dans le marbre : à l'échéance d'une année, un bilan sera réalisé avec les directions opérationnelles, étant observé que ce bilan n'est pas exclusif de bilans partiels et de la mise en œuvre de processus

d'amélioration continue … Il est décidément bien loin le temps où l'on pouvait écrire fièrement sur les cadrans des Palais de justice la célèbre formule latine *Hora fugit stat jus* !

Droit de l'espace numérique

Général d'armée (2S) Marc WATIN-AUGOUARD

CJUE (grande chambre), 16 juillet 2020 (affaire C-311/18), Data Protection Commissioner/ Facebook Ireland Ltd, Maximillian Schrems

Le transfert de données à caractère personnel vers des pays tiers et à des fins commerciales peut s'effectuer sur la base de clauses types de protection (CTP) qui ne sont pas, en elles-mêmes, contraires à la Charte de l'Union. Il doit être remis en cause par « l'exportateur » ou l'autorité nationale de contrôle, dès lors que la législation de « l'importateur » n'en respecte pas les principes, notamment en n'offrant pas de recours devant un juge indépendant. Le Bouclier de protection de données (*Privacy Shield*), quant à lui, n'est pas valide au regard de la Charte, eu égard à l'insuffisant encadrement des mesures de surveillance prises par les autorités américaines.

Du *Safe Harbor* au *Privacy Shield*

La Cour de justice de l'Union européenne (CJUE) a été saisie d'une demande de questions préjudicielles relatives à un litige opposant le *Data Protection Commissionner* (DPC – CNIL irlandaise) à Facebook Ireland Ltd et à M. Maximilian Schrems au sujet d'une plainte introduite par celui-ci concernant le transfert de ses données à caractère personnel par Facebook Ireland vers Facebook Inc., société établie aux États-Unis.
Maximilian Schrems, citoyen autrichien, est déjà connu pour être à l'origine de l'invalidation par la CJUE du *Safe Harbor*, premier

accord sur les données à caractère personnel entre l'Union et les États-Unis. Cet étudiant autrichien est un utilisateur de Facebook qui a signé un contrat habituel avec Facebook Ireland, filiale de Facebook Inc., lequel stipule que les données à caractère personnel des utilisateurs de Facebook résidant sur le territoire de l'Union sont, en tout ou en partie, transférées vers des serveurs appartenant à Facebook Inc., situés sur le territoire des États-Unis, où elles font l'objet d'un traitement.

Le 25 juin 2013, il a saisi le DPC afin d'interdire à Facebook « d'exporter » ses données vers les États-Unis. L'affaire Snowden venait d'éclater, mettant en évidence les pratiques de surveillance généralisée de la part des services américains. Mais l'autorité de contrôle irlandaise a rejeté sa plainte au motif que la Commission européenne avait constaté, par sa décision 2000/520/CE du 26 juillet 2000, dite *Safe Harbor*, que les États-Unis assuraient un niveau adéquat de protection. Sur son recours, la Haute Cour d'Irlande a saisi la CJUE d'une demande de décision préjudicielle relative à la validité de cette décision. Par l'arrêt du 6 octobre 2015[1], la Cour a censuré la décision de la Commission.

Commencent alors des négociations devant aboutir à un nouvel accord. La décision d'exécution (UE) 2016/1250, Bouclier de protection des données (BPD – plus communément dénommé *Privacy Shield*) est adoptée par le Conseil, le 12 juillet 2016, après approbation du Parlement européen. Son article premier constate que *« les États-Unis assurent un niveau adéquat de protection des données à caractère personnel transférées depuis l'Union vers des*

1. CJUE Data Protection Commissioner/Maximillian Schrems, 6 octobre 2015 (C-362/14).

organisations établies aux États-Unis ». Le Bouclier de protection des données se compose des principes publiés par le ministère américain du commerce, le 7 juillet 2016, et des observations et engagements officiels, l'ensemble figurant dans les annexes de la décision. En vertu des dispositions du BPD, les données à caractère personnel des Européens sont transférées depuis l'Union vers des organisations établies aux États-Unis. Ce sont donc les autorités américaines qui établissent une liste d'entités qui s'autocertifient[2]…

Le G29 (aujourd'hui Comité européen de la protection des données – CEPD) souligne, dès la publication de la décision, les dangers que les lois américaines relatives à la surveillance font peser sur les données des Européens. Mais la Commission considère que toute ingérence des autorités publiques américaines dans l'exercice des droits fondamentaux des personnes pour les besoins de la sécurité nationale, de l'intérêt public ou du respect des lois et, partant, les restrictions imposées aux organisations autocertifiées en ce qui concerne leur respect des principes, sont limitées à ce qui est strictement nécessaire pour atteindre l'objectif légitime visé et qu'il existe une protection juridictionnelle effective contre des ingérences de cette nature.

Le BPD fait l'objet chaque année d'une évaluation. Le dernier rapport du 23 octobre 2019[3] est très favorable, si l'on en croit les propos de la commissaire européenne Věra Jourová : « *Avec*

2. Elles figurent sur la liste des organisations adhérant au Bouclier de protection des données, tenue à jour et publiée par le ministère américain du commerce (DoC), ce qui témoigne de leur « indépendance ».

3. Rapport COM(2019) 495 final de la Commission au Parlement et au Conseil sur la troisième évaluation annuelle du *Privacy Shield* du 23 octobre 2019.

quelque 5 000 sociétés participantes, le bouclier de protection des données est une réussite. L'examen annuel nous permet de vérifier que tout fonctionne correctement. Nous poursuivrons le dialogue sur la diplomatie numérique avec nos homologues américains afin de rendre le bouclier plus solide, notamment en matière de contrôle, d'application de la législation et, à plus long terme, pour améliorer la convergence de nos systèmes ».

L'invalidation du *Privacy Shield*

À la suite du premier arrêt Schrems invalidant le *Safe Harbor*, la Haute Cour demande à Maximillian Schrems de reformuler sa demande, considérant qu'une grande partie de ses données sont transférées, comme le reconnaît Facebook inc., sur le fondement des 12 clauses types de protection des données figurant en annexe de la décision 2010/87/UE de la Commission du 5 février 2010, dite décision CPT[4]. Ces clauses types, lorsqu'elles sont respectées, sont considérées comme offrant des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants. Elles autorisent le transfert de données, indépendamment d'une décision d'adéquation. Les clauses doivent permettre aux autorités de contrôle de soumettre les importateurs de données et les sous-traitants ultérieurs à des vérifications et,

4. Décision CPT, relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46, modifiée par la décision d'exécution (UE) 2016/2297 de la Commission, du 16 décembre 2016 adoptée à la suite de l'arrêt du 6 octobre 2015, Schrems (C-362/14), invalidant le *Safe Harbor*.

lorsque cela se révèle approprié, de prendre des décisions auxquelles ces derniers devront se plier.
Maximillian Schrems souligne le fait que le droit américain impose à Facebook Inc. de mettre les données à caractère personnel qui lui sont transférées à la disposition des autorités américaines, telles que la *National Security Agency* (NSA) et le *Federal Bureau of Investigation* (FBI). De ce fait, ses données étant utilisées dans le cadre de différents programmes de surveillance, leur transfert serait incompatible avec les articles 7, 8 et 47 de la Charte. C'est l'avis énoncé par le Commissaire dans son « projet de décision » du 24 mai 2016. Le 31 mai, celui-ci saisit la *High Court* (Haute Cour) qui, par décision du 4 mai 2018, adresse à la CJUE un renvoi préjudiciel. À son renvoi est annexé un arrêt, qu'elle a prononcé le 3 octobre 2017, qui présente le résultat de l'examen des preuves produites devant elle, auquel le gouvernement américain a participé de manière contradictoire.

L'action des services de renseignement américains mise en cause par la *High Court*

L'arrêt du 3 octobre 2017 de la *High Court* met en exergue les textes en vigueur aux États-Unis qui permettent aux services de renseignement américains d'accéder aux données à caractère personnel transférées outre-Atlantique : le FISA et l'*Executive Order* n° 12333.

Le FISA

Il s'agit tout d'abord du Foreign Intelligence Surveillance Act (FISA),

du 25 octobre 1978 qui, sous le contrôle de l'*United States Foreign Intelligence Surveillance Court* (FISC), autorise les programmes de surveillance de type PRISM ou UPSTREAM, certifiés chaque année par l'*Attorney General* et le Directeur du renseignement national (DNI). Comme le souligne la *High Court*, le programme PRISM oblige les fournisseurs de service Internet à fournir à la NSA toutes les communications envoyées et reçues par un « sélecteur », une partie d'entre elles étant également transmise au FBI et à la *Central Intelligence Agency* (CIA) (agence centrale de renseignement). En ce qui concerne le programme UPSTREAM, les entreprises de télécommunications exploitant la « dorsale » de l'Internet (réseau de câbles sous-marins, terrestres, commutateurs et routeurs) doivent autoriser la NSA à copier et à filtrer les flux de trafic Internet pour recueillir des communications envoyées par un ressortissant non américain visé par un « sélecteur », reçues par lui ou le concernant. Ces flux concernent aussi bien les métadonnées que les contenus.

L'*Executive Order* n° 12333

L'E.O. 12333 permet à la NSA d'accéder à des données « en transit » vers les États-Unis, en accédant aux câbles sous-marins (notamment ceux qui relient l'Europe aux États-Unis), de les recueillir et de les conserver avant qu'elles n'arrivent aux États-Unis, échappant ainsi aux règles de contrôle du FISA. Les activités fondées sur l'E.O. 12333 ne sont pas régies par la loi. Alors que les ressortissants de l'Union européenne disposent de voies de recours dans le cadre du FISA, lorsqu'ils ont fait l'objet d'une surveillance électronique illégale à des fins de sécurité nationale, il n'en est pas

ainsi dans le cadre de l'E.O. 12333.
Pour la *High Court*, les activités de la NSA fondées sur l'E.O. 12333 ne font pas l'objet d'une surveillance judiciaire et ne sont pas susceptibles de recours juridictionnels. La juridiction estime par ailleurs que le médiateur institué dans le cadre du Bouclier de protection de données ne constitue pas un tribunal, au sens de l'article 47 de la Charte. De ce fait, les citoyens de l'Union n'ont pas accès aux mêmes recours que ceux dont disposent les ressortissants américains contre les traitements de données à caractère personnel par les autorités américaines. Le droit américain ne leur assure pas un niveau de protection substantiellement équivalent à celui garanti par le droit fondamental consacré à cet article.
La *High Court* souligne que la directive stratégique présidentielle n° 28 (*Presidential Policy directive* 28-PPD28), publiée le 17 janvier 2014, relative au contrôle des activités de services de renseignement intéressant les étrangers (donc les Européens) ne confère pas aux personnes concernées des droits opposables aux autorités américaines devant les tribunaux.

La décision CJUE

Conformément aux conclusions de l'avocat général, Henrik Saugmandsgaard, la CJUE ne remet pas en cause la décision de la Commission relative aux clauses contractuelles types (CPT), mais elle invalide la décision BPD (*Privacy Shield*).
Tout d'abord, la Cour considère que les questions préjudicielles qui lui sont transmises se réfèrent aux dispositions de la directive

95/46. Toutefois, il est établi que le commissaire n'avait pas encore adopté de décision finale sur cette plainte lorsque cette directive a été abrogée et remplacée par le Règlement général sur la protection des données (RGPD), avec effet au 25 mai 2018. En conséquence, il y a lieu d'y répondre au regard des dispositions du RGPD, et non de celles de la directive 95/46.
La Cour écarte l'objection relative aux dérogations offertes par le RGPD. La possibilité que les données à caractère personnel transférées entre deux opérateurs économiques à des fins commerciales subissent, au cours ou à la suite du transfert, un traitement à des fins de sécurité publique, de défense et de sûreté de l'État par les autorités du pays tiers concerné, ne saurait exclure ledit transfert du champ d'application du RGPD. L'article 2[5] du Règlement ne s'applique, en effet, qu'aux États de l'Union.
La Cour va examiner la décision CPT puis la décision Bouclier de protection de données (BPD), deux voies offertes pour exporter les données. Ces deux modes de transfert sont prévus respectivement par les articles 46 et 45 du RGPD.

S'agissant de la décision CPT, la Cour souligne que les clauses contractuelles ne lient pas les États tiers puisqu'ils ne sont pas parties au contrat, ce qui n'est pas le cas de la décision d'adéquation qui est le fruit d'un accord entre un État tiers et l'UE. Elles doivent faire bénéficier d'un niveau de protection

5. *« Le présent règlement ne s'applique pas au traitement de données à caractère personnel effectué : par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre des menaces pour la sécurité publique et la prévention de telles menaces. […] ».*

substantiellement équivalent à celui garanti au sein de l'Union par le RGPD, lu à la lumière de la Charte. Le niveau de protection assuré doit être évalué en fonction de l'accès aux données exportées par les autorités du pays tiers et de la pertinence du son système juridique. Il appartient à l'autorité de contrôle (CNIL en France) d'exercer ses pouvoirs, notamment en suspendant ou en interdisant un transfert de données à caractère personnel, dès lors qu'elle constate que ce transfert est effectué en violation de la législation de l'Union européenne (en particulier les articles 45 et 46 du RGPD ainsi que la Charte) ou de l'État membre en matière de protection des données. La CJUE renvoie donc le responsable du traitement ou son sous-traitant établis dans l'Union et l'autorité de contrôle vers leurs responsabilités. L'examen de la décision 2010/87/UE de la Commission, du 5 février 2010[6], au regard des articles 7, 8 et 47 de la Charte des droits fondamentaux, ne révèle aucun élément de nature à affecter la validité de cette décision. Ce n'est pas le texte qui doit être censuré mais, le cas échéant, son application.

Il en va autrement en ce qui concerne la décision BPD. La Commission a accepté que l'adhésion aux principes du Bouclier de protection des données puisse être limitée par *« les exigences relatives à la sécurité nationale, l'intérêt public et le respect de la législation »*. Elle a consacré la primauté du droit américain, selon

6. Décision 2010/87/UE de la Commission, du 5 février 2010, relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement européen et du Conseil, modifiée par la décision d'exécution (UE) 2016/2297 de la Commission, du 16 décembre 2016 (pour tenir compte du RGPD).

lequel les organisations américaines autocertifiées, recevant des données à caractère personnel depuis l'Union, sont tenues d'écarter, sans limitation, ces principes lorsque ces derniers entrent en conflit avec lesdites exigences. La Commission n'a pas soulevé le problème de l'analyse des flux par les autorités américaines, considérant que les garanties offertes par le médiateur étaient suffisantes. La CJUE relève que les activités de la NSA fondées sur l'E.O. 12333 ne font pas l'objet d'une surveillance judiciaire et ne sont pas susceptibles de recours juridictionnels. Elle estime que le médiateur du Bouclier de protection de données ne constitue pas un tribunal, au sens de l'article 47 de la Charte. Le droit américain n'assure pas aux citoyens de l'Union un niveau de protection substantiellement équivalent à celui garanti par le droit fondamental consacré par cet article. Pour ces raisons, elle constate l'invalidité de la décision BPD au regard du droit de l'Union et en particulier de la Charte.

La CJUE ne craint pas d'instaurer un vide juridique. Selon elle, l'article 49 du RGPD établit, de manière précise, les conditions dans lesquelles des transferts de données à caractère personnel vers des pays tiers peuvent avoir lieu en l'absence d'une décision d'adéquation en vertu de l'article 45 dudit Règlement ou de garanties appropriées au titre de l'article 46 du même Règlement.
Mais les motifs de l'invalidation du *Privacy Shield*, combinés aux exigences relatives aux transferts sur la base des clauses types, vont poser des difficultés aux entreprises qui utilisent cette voie. Elles seront, en effet, contraintes de constater que l'activité des services américains est de nature à entraîner la suspension des

transferts. Les organismes de contrôle, telle la CNIl, auront la même obligation. En attendant la conclusion d'un troisième accord d'adéquation (qui suppose une réforme de la législation américaine), seul le transfert de données anonymisées (donc sortant du champ du RGPD) peut se concevoir.
L'après-Brexit ne manquera pas de poser la question du transfert des données vers le Royaume-Uni, celui-ci sortant du champ du RGPD le 31 décembre 2020 et procédant également à des actions de surveillance qui n'offrent pas non plus de garanties pour les citoyens européens.

JURISPRUDENCE ADMINISTRATIVE

Conseil d'État (10ème et 9ème chambres réunies), arrêt n° 430810 du 19 juin 2020, Google LLC/ CNIL

En l'absence d'une autorité chef de file au sens du Règlement général sur la protection des données (RGPD), la Commission nationale de l'informatique et des libertés (CNIL) est compétente pour infliger à Google une amende de 50 millions d'euros pour défaut de transparence, information insatisfaisante et absence de consentement valable pour la personnalisation de la publicité à l'égard des utilisateurs d'Android.
Par délibération du 21 janvier 2019 (n° SAN-2019-001), la formation restreinte de la CNIL a prononcé à son encontre une sanction pécuniaire d'un montant de 50 000 000 d'euros et

décidé de rendre publique sa délibération, qui sera anonymisée à l'expiration d'un délai de deux ans à compter de sa publication.

La saisine du Conseil d'État

En mai 2018, les associations None of Your Business (dont Maximilian Schrems est un des principaux animateurs) et La Quadrature du Net ont saisi la CNIL de deux plaintes collectives déposées en application de l'article 80 du RGPD (représentation de plaignants par une association). En cause, la conformité à la loi du 6 janvier 1978 et au RGPD des traitements opérés par Google LLC à partir des données personnelles des utilisateurs du système d'exploitation Android.
À la suite d'un contrôle effectué par la CNIL, le 21 septembre, la présidente a engagé une procédure de sanction qui a abouti à la délibération constatant les manquements aux articles 6, 12 et 13 du RGPD.
Cette délibération est contestée devant le Conseil d'État.

Les motifs évoqués par Google

Google conteste tout d'abord la régularité de la saisine de la CNIL en soulignant que, l'établissement principal de Google étant situé en Irlande, c'est l'autorité de contrôle de ce pays qui aurait dû être saisie en vertu du principe de l'autorité chef de file prévu par le RGPD. La CNIL n'aurait pas correctement appliqué les procédures de coopération et de cohérence prévues par le chapitre VII du RGPD lorsque plusieurs pays de l'Union sont concernés par un traitement de données à caractère personnel.

Google reproche également à la CNIL une erreur de droit pour avoir retenu que le consentement pour les traitements aux fins de personnalisation de la publicité n'était pas valablement recueilli et pour avoir lui avoir reproché un manquement aux obligations de transparence et d'information telles que prévues par les articles 12 et 13 du RGPD.

La décision du Conseil d'État

S'agissant de la compétence de la CNIL, le RGPD dispose que, lors d'un traitement transfrontalier de données à caractère personnel opéré au sein de l'Union européenne, l'autorité de contrôle de l'établissement principal dans l'Union du responsable de ce traitement est, en tant qu'autorité chef de file, compétente pour contrôler le respect des exigences du RGPD. La société Google Ireland Limited ne pouvait être considérée comme son établissement principal au sein de l'Union européenne. À la date de la délibération de la CNIL, la société Google Ireland n'exerçait pas un pouvoir de direction ou de contrôle, quant aux finalités et aux moyens des traitements litigieux, sur les autres filiales européennes de la société Google LLC de nature à la regarder comme une administration centrale au sens du RGPD. L'autorité de régulation irlandaise a confirmé cette analyse par un droit de réponse exercé le 27 août 2018 dans le quotidien *Irish Times*. La société Google LLC qui, seule, déterminait leurs finalités et moyens, ne disposait pas, à la date de la sanction attaquée, d'établissement principal au sein de l'Union européenne. Comme le souligne le Conseil d'État, la CNIL a soumis les plaintes dont elle était saisie à ses homologues européens via le système européen d'échange

d'information en vue de la désignation d'une éventuelle autorité chef de file. Aucune autorité de contrôle européenne n'a alors décidé de saisir le comité européen de la protection des données ni fait part d'une appréciation divergente de celle de la CNIL quant à l'absence d'établissement principal de Google LLC en Europe. La CNIL était donc compétente. Il en irait différemment aujourd'hui, le *Data Protection Commissioner* (autorité de régulation irlandaise) serait compétent.

Le mécanisme prévu aux articles 60 à 62 du RGPD, afin d'encourager la coopération entre les différentes autorités européennes de contrôle de protection des données et d'assurer une application cohérente du Règlement dans l'ensemble de l'Union, ne s'applique qu'en cas de désignation d'une autorité chef de file ou d'opérations conjointes des autorités de contrôle. Tel n'est pas le cas en l'espèce.

Sur les griefs relatifs au consentement et à la transparence, Google avance pour sa défense un dispositif à plusieurs niveaux, avec un premier « étage » relatif aux règles de confidentialité et conditions d'utilisations d'où part une arborescence par lien hypertexte qui apporte des précisions. Pour le Conseil d'État, le premier niveau d'information proposé aux utilisateurs apparaît excessivement général eu égard à l'ampleur des traitements opérés par la société, au degré d'intrusion dans la vie privée qu'ils impliquent et au volume et à la nature des données collectées. Les informations essentielles relatives à certains traitements ne sont accessibles qu'à la suite de nombreuses actions, ou ne le sont qu'à partir de liens hypertextes eux-mêmes difficilement accessibles. Par l'éparpillement de l'information qu'elle organise, l'arborescence apparaît de nature à nuire à l'accessibilité et à la clarté de celle-ci

pour les utilisateurs.

Pour appuyer sa démonstration, le Conseil d'État relève que pour *« obtenir l'ensemble des informations pertinentes relatives au traitement personnalisé des annonces, un utilisateur doit d'abord effectuer trois actions à partir du premier niveau d'information, avant de revenir au document initial et d'effectuer deux nouvelles actions, soit un total de cinq actions, tandis que six actions sont nécessaires pour obtenir une information exhaustive quant à la géolocalisation. Les informations relatives à la durée de conservation des données, qui doivent être obligatoirement fournies en vertu du a) du 2° de l'article 13 du RGPD, ne sont accessibles qu'à partir d'un lien hypertexte disponible à la soixante-huitième page du document "Règles de confidentialités" »*.

Enfin, un consentement donné au moyen d'une case cochée par défaut n'implique pas un comportement actif de la part de l'utilisateur et ne peut dès lors être considéré comme procédant d'un acte positif clair permettant valablement le recueil du consentement.

ACTUALITÉ NUMÉRIQUE

L'Union européenne inflige ses premières sanctions à la suite de cyberattaques

Le 30 juillet 2020, un peu plus d'un an après leur publication, le Conseil de l'UE vient de mettre en application la décision-cadre et le règlement en date du 17 mai 2019 permettant d'infliger des

mesures restrictives visant les personnes physiques ou morales, entités ou organismes qui sont responsables de cyberattaques ou de tentatives de cyberattaques. Ces mesures concernent six personnes physiques et trois personnes morales.

Les textes mis en application

Le 19 juin 2017, le Conseil européen a adopté les conclusions relatives à un cadre pour une réponse diplomatique conjointe face aux actes de cybermalveillance. La « boîte à outils cyberdiplomatique » répond à la nécessité de protéger l'Union, ses États membres et leurs citoyens à l'égard des acteurs étatiques et non étatiques qui mènent des cyberattaques. Elle concourt à la prévention des conflits, à la coopération et à la stabilité dans le cyberespace en précisant les mesures pouvant être décidées dans le cadre de la Politique étrangère et de sécurité commune (PESC), y compris les mesures restrictives, pour prévenir les actes de cybermalveillance et y répondre.

Lors du sommet numérique de Tallinn (29 septembre 2017), Jean-Claude Juncker, alors président de la Commission européenne, a déclaré que *« les cyberattaques ne connaissent pas de frontières, pourtant, nos capacités de réaction varient fortement d'un pays à l'autre, ce qui crée des failles et des vulnérabilités qui favorisent les cyberattaques. L'UE doit se doter de structures plus robustes et plus efficaces pour améliorer sa cyber-résilience et réagir aux cyberattaques »*. Il ajoutait : *« Nous ne voulons pas être le maillon faible de la lutte contre cette menace mondiale »*.

Les 19 et 20 octobre 2017, toujours à Tallinn, le Conseil européen a demandé une approche commune de la cybersécurité au sein de

l'UE qui s'est traduite par le *Cybersecurity Act*, approuvé par le Parlement européen, le 12 mars 2019 (voir Veille juridique du CREOGN n° 78 , mai 2019, p. 20-24).

Le 17 mai 2019, le Conseil de l'Union européenne a pris une décision-cadre et un règlement qui s'inscrivent dans la logique de la « boite à outil cyberdiplomatique ».

La décision (PESC) 2019/797 du Conseil, du 17 mai 2019, concerne les mesures restrictives contre les auteurs des cyberattaques qui menacent l'Union ou ses États membres. Pour le Conseil, *« les mesures relevant de la politique étrangère et de sécurité commune (PESC), y compris, si nécessaire, les mesures restrictives, adoptées dans le cadre des dispositions pertinentes des traités, conviennent à un cadre pour une réponse diplomatique conjointe de l'Union face aux actes de cybermalveillance, le but étant d'encourager la coopération, de faciliter la réduction des menaces immédiates et à long terme, et d'influencer le comportement d'agresseurs potentiels à long terme »*.

Ces mesures ont pour but de dissuader et contrer les cyberattaques qui ont une origine externe au territoire de l'Union et visent l'Union ou ses États membres (la cybercriminalité interne n'est donc pas concernée). Mais elles peuvent aussi être mises en œuvre, si cela est jugé nécessaire, pour réaliser les objectifs de la PESC figurant dans les dispositions pertinentes de l'article 21 du traité sur l'Union européenne, lorsque les cyberattaques visent des pays tiers ou des organisations internationales.

Les mesures restrictives fixées par la décision portent sur l'interdiction d'entrée ou de passage en transit sur le territoire des États membres et sur le gel des fonds et ressources économiques appartenant aux personnes physiques ou morales, entités ou

organismes qui sont responsables de cyberattaques ou de tentatives de cyberattaques. S'agissant du gel des fonds et ressources, le règlement (UE) du Conseil du 17 mai 2019, concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres, apporte les précisions relatives à sa mise en œuvre.
Comme le précise la décision-cadre, les mesures ciblées doivent être distinguées de l'imputation à des tiers de la responsabilité des cyberattaques, décision politique souveraine prise au cas par cas. Chaque État membre demeure libre d'apprécier l'implication d'un État tiers.

Les décisions du 30 juillet 2020

Le 16 avril 2018, le Conseil a fermement condamné les cyberattaques, connues sous le nom de « WannaCry » et de « NotPetya », qui ont causé des dommages et des pertes économiques importants dans l'Union. Rançongiciel pour la première, destruction de données pour la seconde, ces cyberattaques constituent des références par leur ampleur et leurs conséquences. NotPetya, visant principalement l'Ukraine, a eu des effets collatéraux importants, notamment en France (Saint-Gobain, SNCF, Auchan, BNP).
Le 4 octobre 2018, les présidents du Conseil européen et de la Commission européenne et la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité ont ensemble condamné une tentative de cyberattaque visant l'Organisation pour l'interdiction des armes chimiques (OIAC) aux Pays-Bas. Dans une déclaration au nom de l'Union le 12 avril 2019, la haute

représentante a exhorté les acteurs à cesser d'entreprendre des cyberactivités malveillantes qui visent à saper l'intégrité, la sécurité et la compétitivité économique de l'Union, y compris les actes d'espionnage portant atteinte à la propriété intellectuelle. Ces « vols cybernétiques » sont notamment ceux commis par le groupe dénommé « APT10 » (« Advanced Persistent Threat 10 »), impliqué dans l'opération « Cloud Hopper » qui a visé les entreprises via le cloud. Pour le Conseil, *« l'opération Cloud Hopper a ciblé les systèmes d'information de sociétés multinationales sur six continents, y compris des entreprises situées dans l'Union, et a obtenu un accès non autorisé à des données commercialement sensibles, entraînant des pertes économiques importantes »*.

Les sanctions imposées comprennent une interdiction de pénétrer sur le territoire de l'UE et un gel des avoirs. En outre, il est interdit aux personnes et aux entités de l'UE de mettre des fonds à la disposition des personnes et entités inscrites sur la liste.

Les six personnes physiques et les trois personnes morales sont inscrites sur la liste des personnes physiques et morales, entités et organismes figurant à l'annexe I de la décision (PESC) 2020/1127 et du règlement (UE) 2019/796 et jusqu'alors vierge. Deux Chinois et quatre Russes sont visés ainsi que trois organismes : l'un chinois, l'un nord-coréen, l'un russe. On notera que l'UE n'hésite pas à sanctionner des organes liés aux Etats (Russie en particulier).

Ci-après sont reproduits deux extraits qui illustrent la forme que prend cette annexe.

Droit de l'espace numérique

Nom	Données d'identification	Les raisons
GAO Qiang	Lieu de naissance: province du Shandong, Chine Adresse : Salle 1102, Manoir de Guanfu, 46 Xinkai Road, Hedong District, Tianjin, Chine Nationalité: chinoise Genre masculin	Gao Qiang est impliqué dans « l'opération Cloud Hopper », une série de cyberattaques à effet significatif provenant de l'extérieur de l'Union et constituant une menace externe pour l'Union ou ses États membres et de cyberattaques ayant un effet significatif contre des États tiers. L'opération « Cloud Hopper» a ciblé les systèmes d'information de sociétés multinationales sur six continents, y compris des entreprises situées dans l'Union, et a obtenu un accès non autorisé à des données commercialement sensibles, entraînant des pertes économiques importantes. L'acteur connu publiquement sous le nom de « APT10 » (« Advanced Persistent Threat 10 ») (alias « Red Apollo », « CVNX », « Stone Panda », « MenuPass » et «Potassium ») a réalisé «Operation Cloud Hopper». Gao Qiang peut être lié à APT10, notamment grâce à son association avec l'infrastructure de commande et de contrôle APT10. De plus, Huaying Haitai, une entité désignée pour fournir un soutien et faciliter « l'opération Cloud Hopper », a employé Gao Qiang. Il a des liens avec Zhang Shilong, qui est également désigné dans le cadre de « l'opération Cloud Hopper ». Gao Qiang est donc associé à la fois à Huaying Haitai et à Zhang Shilong.

Droit de l'espace numérique

Nom	Données d'identification	Les raisons
Centre principal des technologies spéciales (GTsST) de la Direction principale de l'état-major général des forces armées de la Fédération de Russie (GU / GRU)	Adresse : 22 Kirova Street, Moscou, Fédération de Russie	Le Centre principal pour les technologies spéciales (GTsST) de la Direction principale de l'état-major général des forces armées de la Fédération de Russie (GU / GRU), également connu sous son numéro de poste sur le terrain 74455, est responsable de cyber-attaques avec un effet significatif provenant de l'extérieur de l'Union et constituant une menace extérieure pour l'Union ou ses États membres et pour les cyberattaques ayant un effet significatif contre des États tiers, y compris les cyberattaques publiquement connues sous le nom «NotPetya» ou «EternalPetya» en juin 2017 et le cyberattaques dirigées contre un réseau électrique ukrainien à l'hiver 2015 et 2016. « NotPetya » ou « EternalPetya » a rendu les données inaccessibles dans un certain nombre d'entreprises de l'Union, de l'Europe au sens large et du monde entier, en ciblant les ordinateurs avec des ransomwares et en bloquant l'accès aux données, entraînant entre autres des pertes économiques importantes. La cyberattaque contre un réseau électrique ukrainien a entraîné la désactivation de certaines parties de celui-ci pendant l'hiver. L'acteur, connu publiquement sous

		Les raisons (suite)
		le nom de « Sandworm » (alias « Sandworm Team », « BlackEnergy Group», «Voodoo Bear», «Quedagh», «Olympic Destroyer» et «Telebots»), est également à l'origine de l'attaque du réseau électrique ukrainien , « NotPetya » ou « EternalPetya ». Le Centre principal des technologies spéciales de la Direction principale de l'état-major général des forces armées de la Fédération de Russie joue un rôle actif dans les cyber-activités entreprises par Sandworm et peut être lié à Sandworm.« Sandworm Team », « BlackEnergy Group», «Voodoo Bear », « Quedagh », « Olympic Destroyer » et « Telebots »), est également à l'origine de l'attaque du réseau électrique ukrainien , « NotPetya » ou « EternalPetya ». Le Centre principal des technologies spéciales de la Direction principale de l'état-major général des forces armées de la Fédération de Russie joue un rôle actif dans les cyber-activités entreprises par Sandworm et peut être lié à Sandworm.

Droit de l'espace numérique

Encrochat, une enquête exemplaire

EncroChat : le plus gros dossier traité depuis 12 ans par Europol. Le chiffrement de bout en bout au service des criminels mis au clair

Le 2 juillet 2020, lors d'une conférence de presse conjointe d'Europol et d'Eurojust, la gendarmerie nationale et la police néerlandaise ont annoncé avoir mis un terme à l'action de réseaux criminels grâce à la « neutralisation » du chiffrement de bout en bout du réseau téléphonique EncroChat, le « Whatsapp des gangsters », que ces derniers utilisaient. Au-delà de la prouesse technique, cette action a permis l'arrestation de plus de mille personnes, Français, Néerlandais ou Britanniques, la saisie de drogues (10 tonnes de cocaïne et 1 200 kilos de méthamphétamine, plusieurs centaines de kilos de cannabis), le démantèlement de 19 laboratoires de drogues synthétiques, la saisie de dizaines d'armes automatiques, de montres de luxe, de 80 voitures haut de gamme, dont certaines à compartiments cachés, et près de 20 millions d'euros en espèces. Sept conteneurs transformés en chambres de torture ont été découverts aux Pays-Bas.

Plus de 300 enquêtes, également en Espagne, en Allemagne, en Norvège, pourraient être concernées par rebonds. Si le résultat est impressionnant, c'est la technique d'enquête qui mérite un regard particulier.

EncroChat est une entreprise néerlandaise qui offre des services téléphoniques chiffrés, moyennant un abonnement de plus de 2 000 euros par an. Elle a environ 60 000 clients, 90 % d'entre eux

étant liés aux milieux criminels. Les modifications apportées par l'entreprise aux smartphones BQ Aquaris X2 ont pour objectif d'empêcher toute traçabilité des conversations et de permettre d'effacer les données en cas « d'urgence ». Les téléphones fournis sont entièrement modifiés, dépouillés de leurs caméra, micro, système GPS ou port USB. Ils sont alors équipés d'un logiciel de messagerie instantanée chiffrée, couplé à une infrastructure sécurisée. Un code PIN spécial permet la destruction immédiate de toutes les données et un effacement du terminal en cas de saisies consécutives d'un mot de passe erroné. La suppression automatique des messages sur les appareils des destinataires faisait également partie des « garanties » offertes. De ce fait, les intentions d'EncroChat sont manifestes quant à la clientèle servie par cooptation et aux messages d'alerte envoyés pour prévenir les utilisateurs d'une intervention d'autorités gouvernementales.

L'entreprise agissant depuis la France, dans la région de Lille, au profit d'une clientèle mondiale, la gendarmerie nationale a été saisie des faits. Sous le contrôle des magistrats de la Juridiction interrégionale spécialisée de Lille (JIRS), les militaires de la gendarmerie du Centre de lutte contre les criminalités numériques (C3N), du Département sciences de la donnée (DSD), du Service central de renseignement criminel (SCRC), du Bureau des systèmes d'informations et d'investigations (BSII) et du Laboratoire informatique électronique (INL) de l'Institut de recherche criminelle de la gendarmerie nationale (IRCGN) ont été autorisés à mettre en œuvre un « dispositif technique » (couvert par le secret de la défense nationale), destiné à intercepter et à comprendre les conversations téléphoniques sécurisées d'EncroChat.

Les enquêteurs ont eu accès en temps réel aux communications d'environ 60 000 utilisateurs. Près de 120 millions de messages et images, presque tous liés à de la criminalité organisée de haut niveau, ont été interceptés, sans que la captation soit détectée. Les travaux de recherche (projet CEREBUS), menés par le SCRC et l'INL de l'IRCGN, ont été facilités grâce à des financements européens.
De cette enquête exemplaire, plusieurs enseignements peuvent être tirés :

• La criminalité organisée utilise tous les moyens numériques, notamment les plus sophistiqués. Les investigations dans l'espace numérique sont désormais au cœur des pratiques professionnelles des enquêteurs. La preuve numérique est, aujourd'hui, la « reine des preuves » ;

• La coopération européenne est une réalité qui se manifeste au travers des équipes communes d'enquête coordonnées par Eurojust et prévues par l'article 13 de la Convention relative à l'entraide judiciaire en matière pénale (29 mai 2000) et par la contribution au financement des recherches techniques. S'il est un domaine qui devrait tempérer les ardeurs des Eurosceptiques, c'est bien celui de la coopération et de la collaboration en matière de lutte contre la cybercriminalité ;

• Le chiffrement de bout en bout est souvent présenté comme un obstacle aux investigations numériques ; dans le cas d'espèce, la démonstration est faite que la meilleure parade réside dans la compétence scientifique et technique des enquêteurs. La gendarmerie nationale a fait un choix stratégique, dont elle perçoit les fruits aujourd'hui. Après avoir démantelé le botnet gênant Retadup (été 2019), elle offre une nouvelle illustration de son

savoir-faire. L'augmentation du recrutement « scientifique », notamment à l'École des officiers de la gendarmerie nationale (EOGN), est annonciateur d'une accélération de la mutation de cette institution militaire chargée d'une mission de sécurité.

EncroChat sera assurément au cœur des débats lors du FIC 2021. Un exemple vivant de cybersécurité « collective et collaborative » !

Les décisions de justice accessibles librement en ligne

La loi Lemaire du 7 octobre 2016 a fixé les bases de l'*open data*, c'est-à-dire de la fourniture gratuite sous un format numérique des données, non protégées par le secret, issues des administrations publiques. Les décisions de justice figurent parmi ces informations. Seules les plus significatives étaient jusqu'à présent accessibles, l'essentiel ne pouvant être obtenu qu'à titre onéreux, par le biais notamment de Legaltech. Sont désormais disponibles les décisions rendues publiquement et accessibles à toute personne sans autorisation préalable. Il n'en est pas de même des décisions non définitives, des décisions rendues par les juridictions d'instruction ou de l'application des peines et des décisions rendues par les juridictions pour mineurs ou après des débats tenus à huis clos.
Le décret n° 2020-797 du 29 juin 2020, relatif à la mise à la disposition du public des décisions des juridictions judiciaires et administratives, ouvre de nouvelles perspectives. Le Conseil d'État et la Cour de cassation sont désormais responsables de la mise en ligne dans un délai de 2 mois (décisions du juge administratif) ou de

6 mois (juge judiciaire).
Une des conditions de cette « libération » est l'anonymisation. Celle-ci concerne les auteurs, les victimes et peut porter sur tout autre élément d'identification, dès lors que des considérations de sécurité et de vie privée de tiers ou de leur entourage justifient une occultation.
S'agissant du pénal intéressant davantage les officiers de police judiciaire (OPJ) et les agents de police judiciaire (APJ), sont accessibles les arrêts de la Cour de cassation, les décisions des juridictions de jugement du premier ou du second degré, lorsqu'elles sont définitives et ont été rendues publiquement à la suite d'un débat public. Le Parquet peut s'y opposer s'il s'agit d'une condamnation effacée par l'amnistie, la réhabilitation ou la révision ou si la condamnation est prescrite. Il en est de même s'il apparaît que la copie est demandée dans l'intention de nuire.
Les décisions seront accessibles via un portail Internet mis en œuvre par le ministère de la Justice. Le traitement massif de données (à l'aide de l'intelligence artificielle) pourrait permettre de mieux mettre en exergue les circonstances de droit et de fait qui fondent une jurisprudence plus homogène. Mais la loi du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice interdit d'effectuer des profilages en utilisant les données d'identité des magistrats et des membres du greffe en vue *« d'évaluer, d'analyser, de comparer ou de prédire leurs pratiques professionnelles réelles ou supposées ».* De même, toute décision à caractère pénal doit tenir compte des circonstances des faits et de la personnalité de l'auteur, conditions constitutionnelles de l'application d'une peine. L'*open data* devra éclairer, mais en aucun cas

contraindre la décision par un *« enfermement algorithmique »*.

Le « dossier pénal numérique »

Le décret n° 2020-767 du 23 juin 2020 crée un traitement de données à caractère personnel dénommé « dossier pénal numérique » mis en œuvre dans chaque juridiction. Prévu par la loi du 20 mars 2019, il a pour finalités de faciliter et d'améliorer le traitement des dossiers pénaux par les magistrats, les greffiers et les personnes habilitées à les assister. Il permettra le recours, pour la conduite de la procédure pénale, au dossier de procédure numérique ainsi qu'à la copie numérisée du dossier, au dossier unique de personnalité relatif aux mineurs et aux minutes dématérialisées. Par ailleurs, le dossier facilitera les échanges d'informations, au sein des juridictions et entre juridictions, avec les avocats et les parties. Entreront notamment dans la composition du dossier les procès-verbaux et rapports dressés par les officiers ou agents de police judiciaire et les fonctionnaires et agents chargés de certaines fonctions de police judiciaire, les actes d'experts ou de personnes requises. Le décret fixe la liste des données pouvant être enregistrées. Il précise que les données, visées à l'article 6 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, ne peuvent être traitées qui dans la stricte mesure où ces données sont nécessaires à la poursuite des finalités : il s'agit des données à caractère personnel qui révèlent la prétendue origine raciale ou l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne physique, les données

génétiques, les données biométriques aux fins d'identifier une personne physique de manière unique, les données concernant la santé ou les données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique. Sur ces données « sensibles », le Conseil d'État aura prochainement à trancher.

Droit de l'espace numérique

Lieutenant Océane GERRIET

Bref rappel sur le contrôle des accès au lieu de travail

La Commission nationale de l'informatique et des libertés (CNIL) a annoncé avoir mis en demeure plusieurs organismes privés et publics *« de mettre leurs dispositifs de contrôle des horaires en conformité avec le RGPD »* à la suite de plusieurs plaintes reçues[1]. Ces derniers utilisaient en effet un système de badge qui intègre également la prise d'une photo systématique à chaque pointage. Voici l'occasion de faire un bref rappel sur les règles entourant le contrôle des accès au travail.

D'emblée, il convient de rappeler qu'il est tout à fait légitime de vouloir contrôler les accès de son entreprise ou de son administration. Sur ce point, la CNIL avait d'ailleurs rédigé une norme simplifiée sur ce type de traitement récurrent. La base légale communément admise est l'obligation légale, notamment l'obligation de sécurité à laquelle est tenu l'employeur (article L. 4121-1 du Code du travail)) et/ou l'intérêt légitime de ce dernier, notamment, d'assurer l'intégrité de ses locaux, voire de préserver la discrétion nécessaire à ses activités.

Toutefois, ce type de traitement doit bien évidemment respecter les principes inhérents à la protection des données personnelles. Si

1. CNIL, Badgeuses photo : mise en demeure de plusieurs employeurs pour collecte excessive de données, *cnil.fr*, 27 août 2020. Disponible sur : https://www.cnil.fr/fr/badgeuses-photo-mise-en-demeure-de-plusieurs-employeurs-pour-collecte-excessive-de-donnees

l'entreprise ou l'administration n'a plus à réaliser de déclaration préalable auprès de la CNIL, elle doit néanmoins faire preuve de responsabilité en entreprenant des démarches de conformité « par défaut », notamment, la tenue d'un registre[2], voire une analyse de risque en cas de risque élevé pour les données[3].

Après avoir rappelé les finalités poursuivies, l'organisme devra s'attacher à justifier chacune des données qu'il entend collecter, le tout dans le strict respect du principe de minimisation des données et c'est précisément sur ce point que la CNIL a effectué une mise en garde. L'article 5.1.c du Règlement général sur la protection des données (RGPD) rappelle que les données traitées doivent être *« adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités [du traitement] »*. Dans le cas d'espèce, il s'agit essentiellement de permettre l'accès aux locaux professionnels aux seules personnes autorisées et/ou de contrôler leurs horaires de travail, de sorte que l'on comprend aisément que les données

2. L'article 30 du RGPD exige que *« chaque responsable du traitement [RT] (…) [tienne] un registre des activités de traitement effectuées sous [sa] responsabilité »*. Ce registre comporte les informations suivantes : nom et coordonnées du RT, les finalités du traitement, la description des catégories de personnes concernées et des catégories de données à caractère personnel, les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales, les éventuels transferts de données, la durée de conservation des données et une description générale des mesures de sécurité techniques et organisationnelles mises en place.

3. Le Comité européen de la protection des données a émis des lignes directrices (WP 248) fixant une liste de 9 critères (indépendants les uns des autres) caractérisant la présence d'un risque pour les données.

relatives à leur identité sont importantes : le nom, le prénom, le genre, la date de naissance (permettant éventuellement de comparer avec une autre pièce d'identité) et une photographie. Cette dernière permet de s'assurer de la correspondance entre le porteur de la carte et le badge qu'il présente. Toutefois, les organismes soumis à une mise en demeure sont allés (beaucoup) trop loin en prenant systématiquement leurs employés en photo dès qu'ils passaient leur badge. La CNIL opère alors l'analyse de la nécessité des moyens mis en place au regard de la finalité. D'une part, elle souligne que la simple utilisation du badge suffisait à remplir les finalités poursuivies par le traitement puisqu'elle permet d'assurer le contrôle des accès et des horaires. D'autre part, elle remarque que les photographies réalisées à chaque passage étaient très rarement (voire pas du tout) utilisées par les services de sécurité. Partant, elle ne pouvait que conclure à **l'excessivité** de cette collecte et a ordonné aux organismes concernés de se conformer au RGPD dans un délai de 3 mois.

Cette décision ne surprend pas mais elle ne signifie pas pour autant que des mesures plus strictes ne peuvent pas être prises mais qu'elles doivent être *« dûment justifiées »*. Il est intéressant de souligner que nombre d'entreprises dans des secteurs sensibles peuvent être amenées à utiliser, par exemple, des données biométriques[4] aux fins de renforcer la sécurité de leurs accès. Par

4. Définition de l'article 4 du RGPD : *« les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques ».*

principe, et conformément à l'article 9 du RGPD, le traitement de ces données sensibles est prohibé mais comprend, comme tout principe, des exceptions limitativement énumérées dont deux peuvent être évoquées, car adéquates à une telle finalité. D'une part, le traitement est possible lorsqu'il est nécessaire pour des motifs d'intérêt public importants. Il est permis de penser que la protection des sites d'intérêts vitaux de l'État pourrait rentrer dans ce cadre, au regard de la sensibilité du lieu et des risque encourus pour la sûreté de l'État. D'autre part, le traitement est possible lorsqu'il est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée. À titre d'exemple, on pourrait imaginer le cas où l'entreprise manipule des produits chimiques dangereux, de sorte que seules les personnes habilitées et compétentes doivent accéder aux locaux. Dans une délibération du 10 janvier 2019, la CNIL rappelle les règles inhérentes au traitement de telles données dans le cadre du contrôle des accès. Ainsi, le responsable de traitement doit démontrer que le recours à ces données sensibles est justifié **par l'insuffisance des autres moyens d'identification ou par *« des mesures organisationnelles et techniques de protection »* qui ne permettent pas d'atteindre le niveau de sécurité exigé**. À ce titre, elle exige du responsable de traitement qu'il *« détaille (…) le contexte spécifique »* rendant nécessaire ce haut niveau de protection et les raisons du recours à cette technologie dans un document **exhaustif**. Par conséquent, et sans que cela n'étonne, l'autorité de contrôle est particulièrement exigeante vis-à-vis de la mise en œuvre d'un tel traitement.

En tous les cas, ces mises en demeure rappellent que **le principe de**

minimisation des données est primordial dans toute démarche de conformité. Cela a, par ailleurs, déjà été rappelé par les hautes juridictions françaises. En effet, la CNIL évoque une jurisprudence de la Cour de cassation[5] et une du Conseil d'Etat[6] ayant eu à apprécier l'opportunité de la mise en place de la géolocalisation pour contrôler le temps de travail des employés. À l'unisson, les magistrats ont estimé que la collecte d'une telle donnée était excessive eu égard à la finalité qui pouvait être accomplie par d'autres moyens, même *« moins efficaces »*.

Force est de constater que ces jurisprudences et ce rappel de la CNIL doivent être mis en perspective avec l'essence même du droit de la protection des données. Pour mémoire, le RGPD a consacré ce droit comme *« un droit fondamental »*. Son premier considérant souligne également qu'un traitement de données à caractère personnel *« devrait être conçu pour servir l'humanité »*. En ce sens, la CNIL émet une incise intéressante dans sa publication puisqu'elle rappelle aux managers leur rôle essentiel : l'encadrement de leurs employés. Or, cet objectif peut être poursuivi par tout autre moyen et n'a pas besoin de *« reposer sur des technologies intrusives »*. Ainsi, les nouvelles technologies ne doivent pas apparaître comme une fin en soi mais devraient rester des « outils » et ne pas se substituer aux tâches et aux missions qui relèvent de l'Homme intrinsèquement et du manager ou du chef de surcroît. Une badgeuse, visant à contrôler notamment l'arrivée et le départ de l'employé, ne saurait remplacer l'action du manager qui doit passer

5. Soc., 19 décembre 2018, n° 17-14.631.
6. CE, 15 décembre 2017, n° 403776.

voir ses équipes chaque matin pour dire bonjour et s'assurer de leur départ chaque soir. Un tableau de suivi (très utile) ne suffit pas et ne doit pas remplacer les réunions de service (y compris à distance en période de crise sanitaire) qui permettent de faciliter les échanges et de créer / renforcer les liens dans l'équipe. Les applications de messagerie utiles pour communiquer et échanger en tout temps et en tout lieu ne doivent jamais se substituer aux contacts humains et préserver l'oralité. Bref, si les nouvelles technologies s'immiscent chaque jour un peu plus dans notre quotidien, peut-être que le défi de demain sera d'être plus « humain » et non « transhumain »[6] comme l'a rappelé l'édition 2020 du Forum international de la cybersécurité dont le thème était : *« replacer l'humain au cœur [de la cybersécurité] »*.[7]

6. Alain Damasio, Michel Lévy-Provençal, Demain, serons-nous très humains plutôt que transhumains ?, *huffingtonpost.fr*, 5 avril 2015, mise à jour le 5 octobre 2016 [Consulté le 8 septembre 2020]. Disponible sur : https://www.huffingtonpost.fr/alain-damasio/humanisme-transhumanisme_b_6998646.html

7. ObservatoireFIC.com. Disponible sur : https://observatoire-fic.com/fic-2020-replacer-lhumain-au-coeur-de-la-cybersecurite/

Actualité pénale

Claudia GHICA-LEMARCHAND

La question des mesures de sûreté à l'encontre des auteurs d'infractions terroristes à l'issue de leur peine

Loi n° 2020-1023 du 10 août 2020 instaurant des mesures de sûreté à l'encontre des auteurs d'infractions terroristes à l'issue de leur peine, JO n° 196, 11 août 2020

Conseil constitutionnel, Décision 2020-805 DC du 7 août 2020 (loi instaurant des mesures de sûreté à l'encontre des auteurs d'infractions terroristes à l'issue de leur peine)

Empruntant à William Shakespeare cette appréciation, car il est difficile de s'élever à la hauteur de son talent, le devenir de cette loi rappelle sa célèbre pièce *Beaucoup de bruit pour rien*. Le 10 mars 2020, peu de temps avant la décision du confinement général pour cause de pandémie mondiale, une proposition de loi a été enregistrée à l'Assemblée nationale, proposition ayant pour objet d'instaurer des mesures de sûreté à l'encontre des auteurs d'infractions terroristes et à l'issue de leur peine. L'objet du texte, présenté sobrement sur le site du Parlement, s'inscrit dans le cadre de la lutte anti-terroriste, priorité absolue du Gouvernement, et vise *« à renforcer le suivi et à prévenir la récidive des personnes condamnées pour des faits de terrorisme et arrivant en fin de peine. Elle instaure la possibilité d'ordonner des mesures de sûreté à leur encontre »*. Elle est justifiée par un constat chiffré qui n'appelle pas plus de commentaires car, *« d'ici la fin de l'année 2022, 154 des 534 personnes actuellement détenues pour des* actes *de terrorisme en*

lien avec la mouvance islamiste (TIS) seront libérées, dont 42 en 2020, 62 en 2021 et 50 en 2022 ». La *ratio legis*, l'objectif visé par le législateur est incontestable et indiscutable, mais sa mise en œuvre a soulevé une polémique ayant abouti à une neutralisation du dispositif voté.

La proposition de loi introduit un régime *ad hoc* de sûreté qui viendrait s'appliquer alors que tous les autres dispositifs de ce type se révèlent insuffisants, les conditions de nécessité et de subsidiarité sont rappelées expressément. Son article unique prévoit d'introduire une nouvelle section dans le Code de procédure pénale. Composée de l'article 706-25-15, elle donne la compétence du tribunal d'application des peines, après avis préalable de la commission pluridisciplinaire des mesures de sûreté, selon la procédure habituelle d'évaluation, de prononcer des mesures de sûreté : obligation de répondre aux convocations du juge d'application des peines, établir sa résidence en un lieu déterminé, obtenir une autorisation avant tout changement d'emploi ou de résidence ainsi que pour tout déplacement à l'étranger, obligation de présentation périodique, interdiction d'entrer en relation et de paraître dans certains lieux, placement sous surveillance électronique mobile. Ces mesures seraient ordonnées pour une durée d'un an, renouvelable dans une limite de dix ans en matière correctionnelle et vingt ans en matière criminelle. Toutes les garanties de procédure pénale s'appliqueraient à ces mesures. La violation des obligations et interdictions imposées par les mesures de sûreté serait passible de trois ans d'emprisonnement et 45 000 euros d'amende. Le Gouvernement a déclaré la procédure d'urgence sur ce texte le 11

juin 2020.

L'Assemblée nationale a adopté le texte en lui apportant peu de modifications quantitatives, mais importantes sur le fond. Dans le cadre des mesures de sûreté pouvant être prononcées, le texte prévoit la nécessité de *« respecter les conditions d'une prise en charge sanitaire, sociale, éducative ou psychologique, destinée à permettre sa réinsertion et l'acquisition des valeurs de la citoyenneté ; cette prise en charge peut, le cas échéant, intervenir au sein d'un établissement d'accueil adapté dans lequel le condamné est tenu de résider »*. La durée de renouvellement des mesures est abaissée car elles sont limitées à cinq ans, sauf lorsque les faits commis par le condamné constituent un crime ou un délit puni de dix ans d'emprisonnement. Pour un mineur, les durées sont ramenées respectivement à trois ans et cinq ans. L'Assemblée nationale prévoit expressément que ces nouvelles mesures de sûreté ne peuvent pas être ordonnées à l'encontre des personnes libérées avant la promulgation de la loi. La proposition adoptée s'enrichit d'un nouvel article modifiant le Code pénal. L'article 421-8, créé par 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 procédure pénale, prévoit que les personnes condamnées pour des infractions terroristes *« peuvent également être condamnées à un suivi socio-judiciaire »*, selon les modalités de droit commun prévues aux articles 131-36-1 à 131-36-13. La nouvelle rédaction retenue par l'Assemblée nationale prévoit que, désormais, les condamnés pour terrorisme « sont » également soumis au suivi socio-judiciaire. En contrepartie, afin de préserver le principe constitutionnel d'individualisation de

la peine, l'article s'enrichit d'un second alinéa qui permet à la juridiction, par une décision spécialement motivée, de ne pas prononcer cette peine, en considération des circonstances de l'infraction et de la personnalité de son auteur. Il est possible de constater que le suivi socio-judiciaire est de droit et la dispense est l'exception, puisque l'article commence par « toutefois ».

Si le Sénat considérait comme bienvenue la création d'une mesure de sûreté dédiée aux terroristes, il attirait l'attention sur la constitutionnalité du dispositif. Si les mesures de sûreté ne sont pas exclues, par principe, *« dès lors qu'elles visent à protéger la société contre la commission de nouveaux crimes ou délits graves »*, elles sont soumises à des exigences fortes, notamment au regard de l'article 9 de la Déclaration des droits de l'Homme et du citoyen qui prohibe les atteintes à la liberté qui ne constitueraient pas *« une rigueur nécessaire »*. C'est la raison pour laquelle la commission des lois a porté une attention particulière *« à garantir un équilibre entre opérationnalité de la mesure, efficacité de la lutte contre le terrorisme et garantie des droits et libertés constitutionnels ».* À cette fin, elle s'est attachée à mieux définir les critères de dangerosité permettant de la prononcer. Si le risque très élevé de récidive est une constante, il est complété par *« l'adhésion persistante à une idéologie ou à des thèses incitant à commettre des actes de terrorisme »*. La mesure de sûreté adoptée par l'Assemblée Nationale contenait deux obligations qui ont été complétées par deux obligations complémentaires venant renforcer le volet « surveillance » – l'interdiction de se livrer à l'activité à l'occasion de laquelle a été commise l'infraction et l'interdiction de détenir ou de porter une arme. En même temps, le

volet réinsertion a aussi été enrichi de la mise en œuvre d'un suivi par les services pénitentiaires d'insertion et de probation et l'obligation d'exercer une activité professionnelle ou de suivre une formation. Le Sénat a adopté ce nouveau dispositif en modifiant notamment la proposition adoptée par l'Assemblée sur deux points. D'une part, la durée de la mesure a été élevée et portée à deux ans afin de mieux évaluer l'insertion. D'autre part, certaines obligations prononcées dans le cadre de la nouvelle mesure de sûreté étaient susceptibles d'être inscrites au fichier des personnes recherchées par une modification de l'article 230-19 du Code de procédure pénale.

Si la commission mixte paritaire a trouvé un accord retenant ces apports successifs du travail parlementaire, texte adopté par le Sénat le 23 juillet 2020 et définitivement par l'Assemblée nationale le 27 juillet, le Conseil constitutionnel a été saisi par le Président de l'Assemblée nationale et par un groupe de députés et de sénateurs afin d'examiner la constitutionnalité du texte. Si les obligations et interdictions sont restées stables, la juridiction décidant de la mesure de sûreté est la juridiction régionale des mesures de sûreté. La durée de la mesure de sûreté est d'un an, renouvelable jusqu'à cinq ou dix ans, donc les maxima les plus faibles ont été conservés.
Trois griefs étaient développés contre ce texte. D'une part, l'article 9 de la Déclaration des droits de l'Homme et du citoyen garantit la présomption d'innocence, s'opposant à la prise de mesure en l'absence de commission d'infraction. D'autre part, cette nouvelle mesure de sûreté vise *« la liberté personnelle par une rigueur non nécessaire et porterai(en)t à la liberté individuelle, à la liberté d'aller et de venir et au droit au respect de la vie privée une atteinte qui ne*

serait ni nécessaire, ni adaptée, ni proportionnée à l'objectif poursuivi par le législateur ». Enfin, le principe de légalité des délits et des peines serait méconnu en raison de la subjectivité de l'appréciation de la dangerosité d'une personne. Le Conseil constitutionnel prononce l'inconstitutionnalité du nouveau dispositif, même s'il n'en invalide pas le principe d'existence. Le raisonnement du Conseil, en réponse aux différents griefs, doit être séparé en deux étapes. En premier lieu, le législateur peut adopter des mesures de sûreté et la nouvelle loi est, de ce point de vue, conforme à la Constitution. En second lieu, les mesures de sûreté doivent remplir certaines conditions et respecter une certaine proportionnalité, ce qui n'est pas le cas du nouveau dispositif.

En premier lieu, le Conseil constitutionnel valide la qualification légale de mesure de sûreté retenue par le Parlement. Cela paraît élémentaire, mais l'analyse de sa nature est complexe juridiquement et entraîne des effets majeurs. Le Conseil constitutionnel constate que *« cette mesure n'est ni une peine ni une sanction ayant le caractère d'une punition »*. Sans jamais prononcer le qualificatif de mesure de sûreté, cette formule indique que le dispositif appartient à cette catégorie juridique. Pour ce faire, le Conseil rappelle les critères essentiels : la mesure succède à l'accomplissement de la peine, elle n'est pas décidée par la juridiction de jugement mais par la juridiction régionale de la mesure de sûreté et, surtout, elle repose sur *« la particulière dangerosité de la personne »* et pas sur sa culpabilité. Cette qualification juridique appelle deux remarques. D'une part, les mesures de sûreté font partie des sanctions pénales, en complément des peines. À ce titre, elles doivent remplir des

garanties juridiques essentielles, à l'instar de la légalité pénale, telles que les principes de nécessité, de subsidiarité, de rigueur, le respect de la dignité humaine, pour n'en citer que quelques-uns. D'autre part, il existe une différence majeure entre les peines et les mesures de sûreté et elle porte sur leur application dans le temps. Si les peines sont soumises au principe de non-rétroactivité, les mesures de sûreté y échappent et s'appliquent à des infractions commises ou à des condamnations prononcées avant leur entrée en vigueur. Il convient de préciser que le nouveau texte précisait à cet égard que la nouvelle mesure n'était pas susceptible de s'appliquer aux personnes déjà libérées, mais qu'elle s'appliquerait aux personnes condamnées avant sa création et libérées après. Après avoir examiné la nature du nouveau dispositif, le Conseil s'attache à en examiner la conformité aux exigences constitutionnelles.

Dans un second temps, le Conseil rappelle que *« bien que dépourvue de caractère punitif, elle doit respecter le principe, résultant des articles 2, 4 et 9 de la Déclaration de 1789, selon lequel la liberté personnelle ne saurait être entravée par une rigueur qui ne soit nécessaire »*. Le législateur assure la conciliation entre la prévention des atteintes à l'ordre public et l'exercice des droits et libertés constitutionnellement garantis. La mesure de sûreté après exécution de la peine pour les infractions terroristes commises s'inscrit dans le cadre de la lutte contre le terrorisme et participe à l'objectif constitutionnel de prévention des atteintes à l'ordre public, car elle répond à deux conditions : elle vient s'ajouter à d'autres mesures judiciaires ou administratives poursuivant cet objectif, mais répond au besoin particulier de prévenir le risque de

récidive d'une personne qui *« persiste à adhérer, à l'issue de sa peine, à une idéologie ou à des thèses incitant à la commission d'actes de terrorisme »*. Ainsi, le principe de son existence respecte la Constitution, mais cela ne suffit pas, car il convient qu'elle réponde aussi aux exigences constitutionnelles de qualité de la norme pénale. Le Conseil constitutionnel rappelle le principe de subsidiarité de ces mesures, qui ne peuvent intervenir *« qu'à condition qu'aucune mesure moins attentatoire aux droits et libertés constitutionnellement garantis ne soit suffisante pour prévenir la commission de ces actes »*. À cela s'ajoute un contrôle de proportionnalité, car il faut que *« les conditions de mise en œuvre de ces mesures et leur durée soient adaptées et proportionnées à l'objectif poursuivi »*, conditions renforcées lorsque la personne a déjà purgé sa peine.

Le Conseil examine l'ensemble des obligations et leur régime juridique afin d'en déterminer « la rigueur » nécessaire. Il relève cinq points de friction :

• les différentes obligations et interdictions prévues par la mesure de sûreté et pouvant être utilisées de manière cumulative sont susceptibles de porter atteinte *« à la liberté d'aller et de venir, au droit au respect de la vie privée et au droit de mener une vie familiale normale »* ;

• la durée de la mesure est limitée à un an, mais peut être renouvelée jusqu'à dix ans et est déterminée en fonction de la peine encourue, pas de la peine prononcée par la juridiction de jugement ;

• la mesure est limitée aux infractions terroristes, mais ne tient pas compte des sursis éventuellement prononcés ;

• si le critère de la mesure de sûreté est la dangerosité, le dispositif n'exige pas *« que la personne ait pu, pendant l'exécution de cette peine, bénéficier de mesures de nature à favoriser sa réinsertion »* ;

• les décisions de renouvellement de la mesure de sûreté se prennent dans les mêmes conditions que la décision initiale, sans exiger de nouveaux éléments ou des éléments complémentaires.

Ces points permettent au Conseil constitutionnel de considérer que la mesure de sûreté porte atteinte aux droits et libertés constitutionnellement garantis, car dépassant la rigueur nécessaire. Le texte se voit amputé, on pourrait dire plutôt décapité, car tous les articles sont invalidés, sauf la modification de l'article 421-8 du Code pénal disposant que le suivi socio-judiciaire est prononcé pour les infractions terroristes et n'est plus une simple faculté laissée au juge pénal.

La décision du 7 août 2020 fera date en droit pénal. Si elle rappelle très fortement sa décision du 21 février 2008, elle va plus loin dans l'alignement du régime juridique des sanctions pénales. La décision du 21 février 2008 portait sur la loi du 25 février 2008 relative à la rétention de sûreté et à la déclaration d'irresponsabilité pénale pour cause de trouble mental qui a créé deux nouvelles mesures de sûreté – la surveillance de sûreté et la rétention de sûreté. Si le Conseil constitutionnel a approuvé leur nature juridique de mesures de sûreté, *« ne constituant ni une peine, ni une sanction ayant le caractère d'une punition »*, il a introduit une distinction du point de vue de leur régime juridique. Ainsi, la surveillance de sûreté, composée d'obligations et interdictions diverses, rappelant

celles de la loi du 10 août 2020, pouvait s'appliquer rétroactivement à des condamnations prononcées avant son entrée en vigueur. Tel ne fut pas le cas de la rétention de sûreté qui, d'une rigueur excessive, car restreignant la liberté d'aller et venir, s'est trouvée soumise au principe de non-rétroactivité caractérisant normalement les peines. Cette décision a introduit une instabilité d'analyse et a donné naissance à une catégorie hybride de sanctions pénales que les commentateurs appellent les mesures-peines. La décision du Conseil constitutionnel était, cependant, en parfait accord avec la jurisprudence de la Cour européenne des droits de l'Homme qui soumet les mesures de sûreté privatives de liberté à la non-rétroactivité, alors que les mesures de sûreté restrictives de droits peuvent rétroagir et s'appliquer à des condamnations antérieures à leur création.

Le Conseil constitutionnel semble franchir une étape dans sa décision du 7 août 2020, une étape que l'on aurait pu qualifier d'élévation des standards devant la Cour européenne des droits de l'Homme. En effet, les contraintes imposées au législateur sont alourdies, ce qui conduit à un élargissement de la protection des libertés individuelles. Les critères utilisés par le Conseil constitutionnel pour déclarer la mesure de sûreté appellent plusieurs remarques.

En premier lieu, le contenu même des obligations et interdictions composant la mesure de sûreté, ainsi que le fait de les prononcer cumulativement, sont de facture classique et trouvent leur inspiration dans d'autres mécanismes comme le sursis probatoire, le suivi socio-judiciaire, la surveillance de sûreté. Il ne semble pas que le Conseil constitutionnel mette en cause leur existence, mais

plutôt leur utilisation complémentaire post-peine dans le cadre dessiné par la nouvelle loi.

Ensuite, le Conseil constitutionnel trouve la durée de la mesure d'une rigueur excessive en utilisant deux arguments. Si le premier peut se comprendre – la mesure de sûreté vient s'ajouter à la peine exécutée –, le second suscite l'étonnement. La durée de renouvellement de la mesure de sûreté considérée comme durée maximale est calculée en fonction de la peine encourue et non de la peine prononcée. Loin d'être un défaut, l'utilisation de ce critère est la garantie d'une bonne justice pénale. En effet, la peine encourue est un critère objectif qui affermit le respect de la légalité pénale. En plus, ce critère garantit mieux l'égalité de tous les citoyens devant la loi pénale.

En troisième lieu, et dans la continuation de la critique précédente, le Conseil reproche à la mesure de sûreté d'être décidée sans prise en considération de l'éventuel sursis assortissant la peine. Mais cette critique ne vaut que si l'on prend en compte la peine prononcée, ce qui est rarement le cas en droit pénal où la référence est la peine encourue, en vertu du principe de légalité pénale.

La quatrième critique formulée par le Conseil retient l'attention, car elle vise indirectement le mécanisme de la mesure de sûreté. Classiquement, la mesure de sûreté repose sur la dangerosité, ce qui permet de la distinguer de la peine qui se fonde sur la culpabilité, donc sur l'infraction commise. En cela, la dangerosité représente un critère subjectif, rattaché à la personne, alors que l'infraction commise représente un critère objectif, fondé sur les faits. Si le fondement même de la dangerosité n'est pas remis en cause, des critiques récurrentes visent son évaluation, par voie de conséquence, sa fiabilité. Le Conseil constitutionnel n'aborde pas

ces querelles juridiques, mais oppose une critique pragmatique. Si la dangerosité expose la personne à la mesure de sûreté, il faut que des moyens soient mis en œuvre afin de la faire baisser. Il faut donc agir en amont, pendant la phase de détention et exiger *« pendant l'exécution de cette peine, de bénéficier de mesures de nature à favoriser sa réinsertion »*. Il semble utile de rappeler que la Cour européenne des droits de l'Homme utilise cette même exigence pour valider les mesures de sûreté.

En dernier lieu, le Conseil constate que le renouvellement de la mesure, pour la même durée d'un an, limité selon la nature de l'infraction, n'est pas soumis à l'exigence que la dangerosité soit corroborée par *« des éléments nouveaux ou complémentaires »*. Il convient de rappeler que la procédure conduisant à la mise en œuvre de cette nouvelle mesure de sûreté suit la procédure dessinée par la loi de 2008. Elle est prise après avis motivé de la commission pluridisciplinaire des mesures de sûreté, chargée d'évaluer la dangerosité de la personne après une phase d'observation et d'analyse de six semaines. Elle est ordonnée, après une phase contradictoire, par la juridiction régionale de la rétention de sûreté de Paris ou, en ce qui concerne les mineurs, par le tribunal pour enfants de Paris, décisions susceptibles de recours. Cela signifie que la commission pluridisciplinaire des mesures de sûreté procède à une évaluation de la dangerosité pendant six semaines avant chaque nouvelle procédure contradictoire susceptible d'aboutir à la mise en œuvre de la mesure de sûreté. Mais si l'on applique la critique du Conseil constitutionnel, cela signifie-t-il qu'il ne suffit plus qu'elle évalue la dangerosité, mais qu'elle trouve de nouveaux éléments ou des éléments complémentaires ? Quid si la personne continue de manifester son

adhésion à des thèses radicales ou violentes ? Cela ne suffirait pas, car ces éléments ne seraient pas nouveaux, ni complémentaires. La dernière critique apportée par le Conseil constitutionnel sape l'inspiration même de cette mesure de sûreté qui reposait sur *« une adhésion persistante à une idéologie ou à des thèses incitant à la commission d'actes de terrorisme »*. La « persistance » ne suffit plus, il faut quelque chose de nouveau ou de plus fort. Cette formule ambiguë devra être éclaircie par le Conseil constitutionnel, au risque de conduire à une remise en cause de la notion même de dangerosité.

La loi du 10 août 2020 a été promulguée totalement vidée de sa substance, inutile juridiquement, peu opportune politiquement. Quels enseignements en tirer ? Que le problème des sorties « sèches » de personnes terroristes continuant de présenter une dangerosité n'est pas réglé. Le Conseil constitutionnel engage un contrôle de proportionnalité des mesures qui semble dépasser le contrôle normal de la sanction de la disproportion relevant de sa compétence. Le dialogue des « juges suprêmes », malgré le fait que le Conseil constitutionnel n'est pas une Cour et que les juges européens ont une dimension extra-territoriale, continue de façonner substantiellement le droit pénal français.

Violations réitérées du confinement

Conseil constitutionnel 2020-846/847/848, QPC du 26 juin 2020

La loi n° 2020-290 du 23 mars 2020 d'urgence pour faire face à l'épidémie de Covid-19 a modifié le Code de la santé publique et a

introduit un système original de sanction de la violation des restrictions de sortie et déplacement. L'article L 3136-1 CSP punit la violation de ces mesures de l'amende prévue pour les contraventions de la quatrième classe, selon la procédure de forfaitisation ramenée à 135 euros. La réitération du comportement appelle une aggravation croissante des sanctions. Lorsque la personne commet une nouvelle violation dans un délai de quinze jours, l'amende qui lui est appliquée est celle prévue pour les contraventions de la cinquième classe. Si ces mêmes violations sont verbalisées à plus de trois reprises dans un délai de trente jours, les faits sont punis de six mois d'emprisonnement et de 3 750 euros d'amende ainsi que de la peine complémentaire de travail d'intérêt général et de la peine complémentaire de suspension, pour une durée de trois ans au plus, du permis de conduire lorsque l'infraction a été commise à l'aide d'un véhicule. Il est permis de constater que la commission de trois violations transforme la nature de l'infraction qui passe d'une qualification contraventionnelle à une qualification délictuelle. Trois questions prioritaires de constitutionnalité critiquent la correctionnalisation de l'infraction, elles sont jointes par le Conseil constitutionnel donnant lieu à une décision unique.

Les QPC formulent trois griefs. D'une part, les questions considèrent qu'il y a méconnaissance du principe de légalité des délits et des peines pour plusieurs raisons – la violation de la répartition des compétences qui aurait permis au pouvoir réglementaire de définir les éléments constitutifs d'un délit, pourtant réservé à la compétence du législateur ; les motifs de sortie seraient *« équivoques »*, notamment *« les besoins familiaux*

et de santé » ne répondant pas à l'exigence de clarté et d'intelligibilité de la loi pénale ; la même sortie non autorisée peut donner lieu à plusieurs verbalisations. D'autre part, le mécanisme comprendrait la violation de la présomption d'innocence, les droits de la défense et le droit à un recours juridictionnel effectif dans la mesure où le délit est automatiquement caractérisé par trois verbalisations, alors qu'il faut attendre ces trois verbalisations pour être présenté au juge pénal. Enfin, la peine de six mois d'emprisonnement serait disproportionnée, d'une part, et présenterait une violation du principe *ne bis in idem*, puisqu'elle sanctionnerait un comportement déjà puni par la peine contraventionnelle.

Le Conseil constitutionnel rejette les trois critiques. En premier lieu, le principe de légalité est respecté autant dans la répartition des compétences, puisque c'est la loi qui a défini les éléments constitutifs du comportement, que dans la définition de l'infraction. La loi du 23 mars 2020 a établi une liste de critères permettant les sorties et ils sont exempts de critiques, mais obéissent à la nécessité d'une définition générale. Ensuite, le tribunal correctionnel apprécie le bien-fondé de la qualification pénale et n'est pas tenu par une qualification automatique des faits. Enfin, les peines instituées ne sont pas disproportionnées, car elles répondent à l'objectif d'assurer *« le respect de mesures prises pour garantir la santé publique durant l'état d'urgence sanitaire qui peut être déclaré en cas de catastrophe sanitaire mettant en péril, par sa nature et sa gravité, la santé de la population »*.

Dès lors, toutes les critiques sont écartées et la loi du 23 mars 2020 est considérée en conformité totale avec la Constitution.

Actualité pénale

Contrôle des mesures d'isolement ou de contention dans le cadre des soins psychiatriques sans consentement

Conseil constitutionnel, décision n° 2020-844 QPC du 19 juin 2020

Le Conseil constitutionnel a été saisi d'une QPC portant sur l'article L 3225-5-1 du Code de la santé publique qui permet de prononcer des mesures d'isolement et de contention dans le cadre des soins psychiatriques, des pratiques de dernier recours, décidées par un psychiatre pour une durée limitée et faisant l'objet d'une mise en œuvre strictement surveillée par l'établissement de santé. Selon les requérants, ces mesures méconnaîtraient l'article 66 de la Constitution qui exige que toute privation de liberté soit placée sous le contrôle de l'autorité judiciaire. Le Conseil constitutionnel considère que le législateur a fixé des conditions de fond et des garanties de procédure propres à assurer que ces mesures soient adaptées, nécessaires et proportionnées à l'état de la personne qui en fait l'objet. De plus, si l'article 66 garantit l'intervention de l'autorité judiciaire, il ne l'impose pas préalablement. De ce point de vue, les dispositions contestées ne sont pas contraires à la Constitution. En revanche, *« la liberté individuelle ne peut être tenue pour sauvegardée que si le juge intervient dans le plus court délai possible »*. Or, l'isolement et la contention sont décidés par un psychiatre, mais le législateur n'a pas prévu d'intervention du juge judiciaire pour contrôler cette mesure et surtout son maintien. Par voie de conséquence, le dispositif est contraire à l'article 66 de la

Constitution mais la date d'effet d'inconstitutionnalité est reportée au 31 décembre 2020, car son effet immédiat entraînerait *« des conséquences manifestement excessives »*.

Condition de paiement préalable pour la contestation des forfaits de post-stationnement

Conseil constitutionnel, Décision 2020-855 QPC du 9 septembre 2020

Le forfait de post-stationnement (FPS) est venu remplacer l'amende unique de première classe en cas de stationnement non payé. D'un montant variant d'une commune à l'autre, il peut être contesté au moyen d'un recours administratif préalable obligatoire et, en cas d'échec de ce dernier, devant la Commission du contentieux du stationnement payant (CCSP). L'article L 2333-87-5 du Code des collectivités territoriales dispose que la recevabilité du recours contentieux contre la décision rendue à l'issue du recours administratif préalable obligatoire et contre le titre exécutoire émis, est subordonnée au paiement préalable du montant de l'avis de paiement du forfait de post-stationnement et de sa majoration, le cas échéant. Le Conseil d'État a transmis une question prioritaire de constitutionnalité reprochant à ce dispositif d'imposer la condition de paiement préalable du FPS et de son éventuelle majoration sans prévoir aucune exception, ce qui méconnaît le droit à un recours juridictionnel effectif.

Si le Conseil constitutionnel valide l'objectif poursuivi par le législateur, car il constate qu'en *« imposant ainsi que le forfait et la*

majoration soient acquittés avant de pouvoir les contester devant le juge, le législateur a entendu, dans un but de bonne administration de la justice, prévenir les recours dilatoires dans un contentieux exclusivement pécuniaire susceptible de concerner un très grand nombre de personnes », il le déclare contraire à la Constitution pour deux raisons. D'une part, la proportionnalité de la sanction n'est pas garantie car, même si *« le montant du forfait de post-stationnement ne peut excéder celui de la redevance due, aucune disposition législative ne garantit que la somme à payer pour contester des forfaits de post-stationnement et leur majoration éventuelle ne soit d'un montant trop élevé »*. D'autre part, l'exigence de paiement préalable est générale et ne connaît aucune exception. Par voie de conséquence, la garantie de paiement préalable du FPS est de nature à porter une atteinte substantielle au droit d'exercer un recours juridictionnel effectif. La déclaration d'inconstitutionnalité est à effet immédiat, donc est applicable à toutes les affaires non jugées définitivement à cette date.

Usage de drogue – Généralisation de l'amende forfaitaire

La loi du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice a prévu l'application d'une amende forfaitaire aux délits d'usage de drogue. À cette fin, l'article L 3352-5 du Code de la santé publique a été complété. Si l'usage de drogue est un délit puni d'un an d'emprisonnement et de 3 750 euros d'amende, selon l'article L 3421-1 du Code de la santé publique, l'action publique peut être éteinte, y compris en cas de récidive, par le versement d'une amende forfaitaire de 200 euros, conformément aux articles

495-17 et suivants du Code de procédure pénale. Le montant de l'amende minorée est de 150 euros, ce qui implique qu'elle soit réglée sous quinze jours, alors qu'au-delà de 45 jours, la personne devra payer 450 euros. En cas d'échec du dispositif, la qualification délictuelle est maintenue. Ce dispositif a été expérimenté, dans un premier temps, à Reims, Rennes, Créteil et Boissy Saint-Léger à partir du 16 juin 2020, et étendu ensuite à Lille et Marseille. Le Premier ministre, Jean Castex, a annoncé, dans son premier discours, la généralisation des amendes forfaitaires pour consommation de drogue à partir du 1er septembre 2020. Le 31 août 2020, un communiqué conjoint des ministres de l'Intérieur et de la Justice souligne la mobilisation conjointe des acteurs de ces deux ministères et la collaboration forte mise au service de la lutte contre ces formes de criminalité qui est une « priorité majeure » du Gouvernement.

Cette généralisation permet d'atteindre le but poursuivi par ce dispositif qui est de désengorger les tribunaux et de permettre une sanction effective, même si elle est moindre, car de nature contraventionnelle à la place de la sanction délictuelle initialement prévue. Cette procédure d'amende forfaitaire alternative se veut rapide, efficace, permettant une meilleure distribution des rôles, la sanction de l'usage de stupéfiants pouvant être traitée par le biais des procès-verbaux électroniques directement par les forces de l'ordre et permettant ainsi aux magistrats de concentrer leurs efforts sur les trafics de drogues et la criminalité qui s'y agrège.

Police administrative

Élisabeth Rolin

Procédure spéciale d'expulsion des gens du voyage et référé « mesures utiles »

CE, 8ème - 3ème chambres réunies, 16 juillet 2020, Département de l'Essonne, n° 437113[1]

Pour protéger le domaine public contre des occupations irrégulières, le référé « mesures utiles » peut trouver à s'appliquer même s'il existe une procédure spéciale d'expulsion des gens du voyage.

Le département de l'Essonne, propriétaire de terrains sur le territoire de la commune de Corbeil-Essonnes, a mandaté un huissier de justice le 14 novembre 2019 qui a relevé, d'une part, la présence de vingt-trois caravanes et de trois véhicules particuliers ou utilitaires, d'autre part, les identités de plusieurs individus.

Le département a alors saisi le juge des référés du tribunal administratif de Versailles d'une demande tendant à ce que celui-ci ordonne, sur le fondement de l'article L. 521-3 du Code la justice administrative (CJA) et sous astreinte, les mesures utiles pour procéder à l'expulsion des individus visés et de celle de toute autre personne qui occuperait ces terrains et n'aurait pu être identifiée, ainsi qu'à l'évacuation des biens des intéressés. Le juge des référés a rejeté sa demande, le 10 décembre 2019, après avoir relevé qu'en raison de l'existence de la procédure spéciale de mise en demeure

1. Sera mentionné aux tables du recueil Lebon.

de quitter les lieux, prévue à l'article 9 de la loi du 5 juillet 2000 relative à l'accueil et à l'habitat des gens du voyage, le département de l'Essonne ne pouvait pas utilement solliciter l'expulsion des occupants de ses terrains en référé en se fondant sur l'article L. 521-3 du CJA.

Le département de l'Essonne s'est pourvu en cassation et a obtenu, le 16 juillet 2020, l'annulation de l'ordonnance du 10 décembre 2019 du juge des référés du tribunal administratif. Par le même arrêt, le Conseil d'État a enjoint aux intéressés et à tout autre occupant de libérer sans délai les terrains occupés sous astreinte de 200 euros par jour de retard à compter de la date de la notification de cette décision.

Cet arrêt du juge de cassation[2] permet de faire un point sur la procédure spéciale d'expulsion des gens du voyage et celle du référé « mesures utiles » prévu à l'article L. 521-3 du CJA qui sont distinctes mais non exclusives. L'intérêt de cet arrêt réside également dans le fait qu'il statue au fond et règle l'affaire au titre de la procédure de référé engagée, en application des dispositions de l'article L. 821-2 du CJA[3], en considérant implicitement que la

2. AJDA 2020, p. 1457obs.Pastor ; JCP A 2020, act.459.

3. S'il prononce l'annulation d'une décision d'une juridiction administrative statuant en dernier ressort, le Conseil d'État peut, soit renvoyer l'affaire devant la même juridiction statuant, sauf impossibilité tenant à la nature de la juridiction, dans une autre formation, soit renvoyer l'affaire devant une autre juridiction de même nature, soit régler l'affaire au fond si l'intérêt d'une bonne administration de la justice le justifie. Lorsque l'affaire fait l'objet d'un second pourvoi en cassation, le Conseil d'État statue définitivement sur cette affaire.

bonne administration de la justice justifiait de ne pas renvoyer cette affaire et de prolonger la durée de l'instance.

Le contentieux du stationnement des résidences mobiles des gens du voyage

La loi n° 2000-614 du 5 juillet 2000 relative à l'accueil et à l'habitat des gens du voyage, modifiée, a organisé une procédure urgente spéciale en cas de stationnement illégal en dehors des aires d'accueil réservées, tant devant le juge administratif que le juge judiciaire. Ce dispositif a été profondément remanié par la loi n° 2007-297 du 5 mars 2007 relative à la prévention de la délinquance. Le maire exerce cette police administrative spéciale en prenant des arrêtés d'interdiction d'occuper certains terrains dans les conditions fixées à l'article 9 de cette même loi.
Le propriétaire ou le titulaire du droit d'usage du terrain occupé peut demander au préfet de mettre en demeure les occupants de quitter les lieux. Le maire de la commune ou le propriétaire du terrain doit ainsi passer par l'intermédiaire du préfet. Mais la mise en demeure ne peut intervenir que si le stationnement est de nature à porter atteinte à la salubrité, la sécurité ou la tranquillité publiques. Elle est assortie d'un délai d'exécution qui ne peut être inférieur à vingt-quatre heures. Elle est notifiée aux occupants et publiée sous forme d'affichage en mairie et sur les lieux. Le cas échéant, elle est notifiée au propriétaire ou titulaire du droit d'usage du terrain. Le fait de ne pas se conformer à l'arrêté municipal est puni de 3 750 euros d'amende.
Aux termes des dispositions du II bis de l'article 9 susmentionné :

Police administrative

« Les personnes destinataires de la décision de mise en demeure prévue au II, ainsi que le propriétaire ou le titulaire du droit d'usage du terrain peuvent, dans le délai fixé par celle-ci, demander son annulation au tribunal administratif. Le recours suspend l'exécution de la décision du préfet à leur égard. Le président du tribunal ou son délégué statue dans ***un délai de quarante-huit heures à compter de sa saisine*** ».

Il s'agit donc d'une procédure d'urgence désignée par les membres des juridictions administratives de *« référé gens du voyage »*, défini à l'article L. 779-1 du CJA et aux articles R. 779-1 à R. 779-8 du même Code. Les décisions rendues par un juge unique, sauf renvoi en formation collégiale, peuvent faire l'objet d'un appel.

Enfin, le même article 9 au IV prévoit aussi une procédure en référé devant le juge judiciaire. En cas d'occupation, en violation de l'arrêté municipal, d'un terrain privé affecté à une activité à caractère économique, et dès lors que cette occupation est de nature à entraver ladite activité, le propriétaire ou le titulaire d'un droit réel d'usage sur le terrain peut saisir le président du tribunal de grande instance aux fins de faire ordonner l'évacuation forcée des résidences mobiles.

Le référé « mesures utiles »

Si le référé « suspension », prévu à l'article L. 521-1 du CJA et le référé « liberté » à l'article L. 521-1 du même Code ont donné lieu à de nombreuses jurisprudences très médiatisées ces derniers mois, notamment dans le cadre de la crise sanitaire, le référé « mesures

utiles » institué par la même loi du 30 juin 2000[4] est resté plus discret.

Aux termes de l'article L. 521-3 du CJA : *« En cas d'urgence et sur simple requête qui sera recevable même en l'absence de décision administrative préalable, le juge des référés peut ordonner toutes autres mesures utiles sans faire obstacle à l'exécution d'aucune décision administrative. »* Saisi sur ce fondement d'une demande qui n'est pas manifestement insusceptible de se rattacher à un litige relevant de la compétence du juge administratif, le juge des référés peut prescrire, à des fins conservatoires ou à titre provisoire, toutes mesures que l'urgence justifie, dont l'expulsion d'occupants sans titre du domaine public, à la condition que ces mesures soient utiles et ne se heurtent à aucune contestation sérieuse.

C'est en se fondant sur cette interprétation de l'article L. 521-3 du CJA que le Conseil d'État censure pour erreur de droit l'ordonnance du juge des référés du tribunal administratif de Versailles qui a rejeté la requête du département de l'Essonne comme irrecevable au regard de l'existence de la procédure spéciale. Mais le Conseil d'État considère que les dispositions de la loi du 5 juillet 2000 relative à l'accueil et à l'habitat des gens du voyage ne font pas obstacle, alors même que les conditions à leur application se trouveraient réunies, à la saisine du juge des référés de conclusions tendant à ce que, sur le fondement de l'article L. 521-3 du CJA,

4. Loi n° 2000-597 du 30 juin 2000 relative au référé devant les juridictions administratives, JORF n° 151 du 1er juillet 2000.

l'expulsion d'occupants sans titre du domaine public soit ordonnée.

Au fond

Le Conseil d'État reprend ensuite l'ensemble des éléments du dossier pour vérifier si la libération des terrains occupés présente un caractère d'utilité et d'urgence au sens des dispositions de l'article L. 521-3 du CJA. Au préalable, il a constaté que la commune de Corbeil-Essonnes est inscrite au schéma départemental d'accueil et d'habitat des gens du voyage de l'Essonne 2019/2024, ce qui exclut l'application de l'article 9-1 de la loi du 5 juillet 2000. De plus, en l'espèce, aucun arrêté municipal n'avait été édicté. En conséquence , le département de l'Essonne pouvait saisir le juge des référés du tribunal administratif.

Ensuite, il relève d'abord qu'il résulte de l'instruction, notamment du constat dressé dès le 14 novembre 2019 par un huissier de justice ainsi que de photographies datées d'avril 2020, que de nombreuses personnes équipées de véhicules et de résidences mobiles ont pris possession, après en avoir brisé les accès, de terrains appartenant au département de l'Essonne et qu'il n'est pas contesté que ces personnes n'ont aucun titre à cette occupation.

Puis, il note que ces personnes alimentent leurs résidences mobiles en électricité à partir d'une armoire électrique qui a été forcée, au moyen de relais et de câbles posés à même le sol. Ils n'ont accès, dans des conditions adéquates, ni au réseau de distribution d'eau potable, ni au réseau d'assainissement, ni à un dispositif de collecte

de déchets. Les seules installations sanitaires qui leur sont accessibles sont situées dans les bâtiments désaffectés implantés sur les terrains concernés, dont la porte a été fracturée. Au surplus, il résulte d'un rapport du président de la commission permanente du département daté du 16 septembre 2019, que cette occupation compromet, d'une part, le projet de commune de Corbeil-Essonnes d'acquérir certains terrains afin d'y construire un parc de stationnement public, d'autre part, le projet du département d'affecter les bâtiments dont elle demeurera propriétaire à des services publics départementaux, dont une maison des solidarités. Cette analyse des faits conduit le Conseil d'État à faire droit à la demande du département de l'Essonne, en enjoignant l'expulsion des terrains occupés sous astreinte de 200 euros par jour de retard à compter de la date à laquelle a été notifié l'arrêt du juge de cassation aux intéressés.

Cette décision qui n'exclut pas la possibilité d'utiliser le référé « mesures utiles » dans de telles circonstances vient compléter l'arsenal juridique de protection du domaine public contre les occupations irrégulières.

Droit des collectivités territoriales et de la sécurité privée

Xavier Latour

Une circulaire pour améliorer l'information des maires

Dans la construction du *continuum* de sécurité entre l'État et les collectivités territoriales, la question de l'information des maires revient régulièrement.

Le Code de la sécurité intérieure (CSI) s'enrichit régulièrement de dispositions censées faciliter le dialogue entre les maires et les représentants de l'État, procureurs comme forces de sécurité intérieure. Les maires sont demandeurs d'éléments leur permettant de mieux cerner l'insécurité sur le territoire de leur commune.
Beaucoup d'entre eux ont pleinement assimilé leur rôle de pivot de la prévention de la délinquance. Ils entendent répondre aux besoins formulés par les administrés, tout en étant certains que les dépenses communales, notamment dans le fonctionnement de polices municipales de plus en plus sollicitées, soient bien employées. Dans leur dialogue avec l'État, en particulier au sein des Conseils locaux de sécurité et prévention de la délinquance (CLSPD), ou lors de la rédaction des conventions de coordination entre la police municipale et la police nationale ou la gendarmerie, ils souhaitent pouvoir mesurer l'ampleur des efforts à fournir ainsi que mieux évaluer la part qui, selon eux, incombe au ministère de l'Intérieur.

Le droit positif en matière d'information

Dans une logique d'équilibre, lorsque le maire signale des crimes ou

des délits en application de l'article 40 du Code de procédure pénale (article L 132-2 CSI), il bénéficie, en retour, d'une information par le procureur sur les suites données.

Surtout, les responsables locaux de la police nationale et de la gendarmerie sont tenus de les informer *« des infractions causant un trouble à l'ordre public »* commises sur le territoire de leur commune (L 132-3 CSI). Une obligation qui connaît, en principe, assez peu de tempéraments, eu égard au caractère particulièrement souple et fluctuant de la notion d'ordre public. À la demande du maire, le procureur de la République doit, pour sa part, communiquer les décisions prises dans le cadre de l'opportunité des poursuites (classement sans suite, alternative), ainsi que les jugements devenus définitifs ou frappés d'appel.
La loi 2019-1461 du 27 décembre 2019 *« engagement et proximité »* a, d'ailleurs, précisé les informations à transmettre à l'élu local. Elle resserre les liens entre les autorités nationales et locales puisque le maire est informé, *« à sa demande »*, des poursuites engagées et des jugements définitifs, ainsi que des suites judiciaires données aux infractions constatées sur le territoire de sa commune par les agents de police municipale.
Le maire a donc la possibilité de collationner toutes les informations d'ordre judiciaire sur l'évolution de la délinquance sur le territoire qu'il administre et, surtout, les décisions rendues à ce sujet. Sa prérogative englobe l'absentéisme scolaire considéré, à tort ou à raison, comme révélateur d'une attitude préludant à l'entrée des mineurs dans la délinquance.

Dans un même ordre d'idées, le législateur a renforcé les moyens d'information globale des nouveaux élus municipaux (article 42) afin de mieux les accompagner dans leur prise de fonctions.

Au sein même des CLSPD (article L 132-5 CSI), des groupes thématiques peuvent traiter des *« questions relatives à l'exécution des peines et à la prévention de la récidive »*, dans le respect de la confidentialité.

De son côté, le préfet de département *« informe régulièrement »* le maire des résultats obtenus en matière de lutte contre l'insécurité (article L 132-10 CSI).

La nécessité d'une circulaire

Rédigée par les services de Madame Belloubet peu avant le changement de gouvernement, la circulaire du 29 juin 2020 (JUSD 2007275 C) traduit une nécessité d'amélioration.

Le texte entend favoriser l'application effective des dispositions de la loi de 2019. De la sorte et d'une part, le législateur a tiré les enseignements de l'existence de polices municipales interventionnistes, et pas uniquement préventives. À la demande des maires, les agents locaux utilisent les potentialités offertes par l'article 21-2 du Code de procédure pénale.
D'autre part, la circulaire rappelle aux procureurs qu'ils sont désormais signataires des conventions de coordination, ce qui motive encore davantage l'existence d'échanges de qualité.

Droit des collectivités territoriales et de la sécurité privée

Dans un environnement administratif complexe, alors que les parties prenantes sont déjà très sollicitées par la gestion du quotidien, l'établissement de nouvelles méthodes de travail ne se fait pas forcément dans la facilité. Des cultures professionnelles différentes constituent peut-être une difficulté supplémentaire.

Pourtant, les pratiques évoluent dans une logique de confiance et de partenariat. La circulaire insiste, à ce propos, sur la nécessité absolue de respecter les règles relatives au secret de *« l'enquête et de l'instruction, conformément aux dispositions de l'article 11 du code de procédure pénale »*. La multiplication des détenteurs d'informations sensibles ne doit pas, en effet, conduire à une remise en cause potentiellement problématique de la confidentialité. Le dialogue est une chose, notamment au sein du CLSPD (ou de son équivalent intercommunal), les fuites en seraient une autre. Cet impératif concerne tout autant les informations communiquées au sein des Groupes locaux de traitement de la délinquance (GLTD).

Tout en ayant le mérite de manifester auprès des procureurs la volonté ministérielle de donner un plein effet aux mesures du CSI, la circulaire ne réglera pas tout.
En ce domaine, la fixation d'obligations juridiques ne peut pas méconnaître les obstacles humains. Seuls les acteurs de la sécurité sont en mesure de s'approprier ces normes et de les faire vivre. En outre, le débat entretenu par certains maires à propos de l'accès à toujours plus d'informations, notamment au fichier des personnes

recherchées, ne retombe pas. Au contraire, les dernières élections municipales lui ont redonné de la vigueur. Pour le moment, l'État ne semble cependant pas prêt à franchir ce cap.

Directeur de publication :	**Colonel Dominique SCHOENHER**
Rédacteur en chef :	**Gal d'armée (2S) Marc WATIN-AUGOUARD**
Rédacteurs :	**Gal d'armée (2S) Marc WATIN-AUGOUARD** **Frédéric DEBOVE** **Claudia GHICA-LEMARCHAND** **Xavier LATOUR** **Elisabeth ROLIN** **Ltn Océane GERRIET**
Équipe éditoriale :	**Odile NETZER**