Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

CONCOURS D'ENTREE A L'ECOLE DE 2019

CONCOURS INTERNE

1ère épreuve d'admissibilité

DROIT PUBLIC

(durée : cinq heures – coefficient 4)

Une épreuve de droit public consistant en la rédaction d'une note d'analyse
et de propositions à partir d'un dossier.

L'épreuve vise à apprécier les connaissances des candidats dans le domaine du droit public général (droit constitutionnel, droit administratif, droit de l'Union européenne, droit de la Convention européenne des droits de l'homme) ainsi que leur capacité de raisonnement critique et d'analyse juridique.

Il est attendu des candidats qu'ils rédigent une note sur une ou plusieurs questions de droit en examinant les différentes solutions possibles, avec leurs avantages et inconvénients respectifs, et qu'ils fassent des préconisations opérationnelles.

Les candidats répondent à la commande à partir de leurs connaissances juridiques et à l'aide d'un dossier composé d'un ensemble de documents (textes normatifs, jurisprudence, extraits de rapports publics, articles de doctrine, etc.) destinés à nourrir leur réflexion. Ce dossier ne dépasse pas vingt-cinq pages.

SUJET

En votre qualité de chef de bureau au sein de la direction des libertés publiques et des affaires juridiques du ministère de l'Intérieur, il vous est demandé de rédiger une note d'analyse et de propositions sur le traitement des données de connexion au regard de l'impératif de sécurité intérieure.

Conseil Constitutionnel, décision n° 2015-478 QPC, *Association French Data Network et autres,* 24 juillet 2015 (extraits). **Document n° 1**

Le Conseil constitutionnel a été saisi le 5 juin 2015 par le Conseil d'État (décision n° 388134 du même jour), dans les conditions prévues à l'article 61-1 de la Constitution, d'une question prioritaire de constitutionnalité posée pour les associations French Data Network, La Quadrature du Net et Fédération des fournisseurs d'accès à internet associatifs, par la SCP Spinosi et Sureau, avocat au Conseil d'État et à la Cour de cassation, relative à la conformité aux droits et libertés que la Constitution garantit des articles L. 246-1 à L. 246-5 du code de la sécurité intérieure, enregistrée au secrétariat général du Conseil constitutionnel sous le n° 2015-478 QPC.

[…]

1. Considérant qu'aux termes de l'article L. 246-1 du code de la sécurité intérieure dans sa rédaction résultant de la loi du 18 décembre 2013 susvisée : « Pour les finalités énumérées à l'article L. 241-2, peut être autorisé le recueil, auprès des opérateurs de communications électroniques et des personnes mentionnées à l'article L. 34-1 du code des postes et des communications électroniques ainsi que des personnes mentionnées aux 1 et 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, des informations ou documents traités ou conservés par leurs réseaux ou services de communications électroniques, y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications. » ;

2. Considérant qu'aux termes de l'article L. 246-2 du même code, dans sa rédaction résultant de la loi du 18 décembre 2013 :
« I. - Les informations ou documents mentionnés à l'article L. 246-1 sont sollicités par les agents individuellement désignés et dûment habilités des services relevant des ministres chargés de la sécurité intérieure, de la défense, de l'économie et du budget, chargés des missions prévues à l'article L. 241-2.
« II. - Les demandes des agents sont motivées et soumises à la décision d'une personnalité qualifiée placée auprès du Premier ministre. Cette personnalité est désignée pour une durée de trois ans renouvelable par la Commission nationale de contrôle des interceptions de sécurité, sur proposition du Premier ministre qui lui présente une liste d'au moins trois noms. Des adjoints pouvant la suppléer sont désignés dans les mêmes conditions. La personnalité qualifiée établit un rapport d'activité annuel adressé à la Commission nationale de contrôle des interceptions de sécurité. Ces décisions, accompagnées de leur motif, font l'objet d'un enregistrement et sont communiquées à la Commission nationale de contrôle des interceptions de sécurité. » ;

3. Considérant qu'aux termes de l'article L. 246-3 du même code, dans sa rédaction résultant de la loi du 18 décembre 2013 :
« Pour les finalités énumérées à l'article L. 241-2, les informations ou documents mentionnés à l'article L. 246-1 peuvent être recueillis sur sollicitation du réseau et transmis en temps réel par les opérateurs aux agents mentionnés au I de l'article L. 246-2.
« L'autorisation de recueil de ces informations ou documents est accordée, sur demande écrite et motivée des ministres de la sécurité intérieure, de la défense, de l'économie et du budget ou des personnes que chacun d'eux a spécialement désignées, par décision écrite du Premier ministre ou des personnes spécialement désignées par lui, pour une durée maximale de trente jours. Elle peut être renouvelée, dans les mêmes conditions de forme et de durée. Elle est communiquée dans un délai de quarante-huit heures au président de la Commission nationale de contrôle des interceptions de sécurité.

« Si celui-ci estime que la légalité de cette autorisation au regard des dispositions du présent titre n'est pas certaine, il réunit la commission, qui statue dans les sept jours suivant la réception par son président de la communication mentionnée au deuxième alinéa.
« Au cas où la commission estime que le recueil d'une donnée de connexion a été autorisé en méconnaissance des dispositions du présent titre, elle adresse au Premier ministre une recommandation tendant à ce qu'il y soit mis fin.
« Elle porte également cette recommandation à la connaissance du ministre ayant proposé le recueil de ces données et du ministre chargé des communications électroniques. » ;

4. Considérant qu'aux termes de l'article L. 246-4 du même code, dans sa rédaction résultant de la loi du 18 décembre 2013 :
« La Commission nationale de contrôle des interceptions de sécurité dispose d'un accès permanent au dispositif de recueil des informations ou documents mis en œuvre en vertu du présent chapitre, afin de procéder à des contrôles visant à s'assurer du respect des conditions fixées aux articles L. 246-1 à L. 246-3. En cas de manquement, elle adresse une recommandation au Premier ministre. Celui-ci fait connaître à la commission, dans un délai de quinze jours, les mesures prises pour remédier au manquement constaté.
« Les modalités d'application du présent article sont fixées par décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés et de la Commission nationale de contrôle des interceptions de sécurité, qui précise notamment la procédure de suivi des demandes et les conditions et durée de conservation des informations ou documents transmis. » ;

5. Considérant qu'aux termes de l'article L. 246-5 du même code, dans sa rédaction résultant de la loi du 18 décembre 2013 : « Les surcoûts identifiables et spécifiques éventuellement exposés par les opérateurs et personnes mentionnées à l'article L. 246-1 pour répondre à ces demandes font l'objet d'une compensation financière de la part de l'Etat. » ;

6. Considérant que les associations requérantes soutiennent, d'une part, qu'en instituant par les dispositions contestées une procédure de réquisition administrative des données de connexion sans définir précisément le type de données pouvant être collectées par l'autorité administrative et les conditions de leur collecte lorsqu'elles sont transmises en temps réel à l'autorité administrative et, d'autre part, qu'en ne prévoyant dans le cadre de cette procédure aucune garantie spécifique pour protéger le secret professionnel des avocats et des journalistes, le législateur a méconnu l'étendue de sa compétence ;

7. Considérant que la question prioritaire de constitutionnalité porte sur les articles L. 246-1 et L. 246-3 du code de la sécurité intérieure ;

- Sur le grief tiré de l'incompétence négative résultant de la définition insuffisante des données de connexion et des conditions de leur collecte en cas de transmission en temps réel :

8. Considérant que les associations requérantes soutiennent, d'une part, qu'en employant les termes d'« informations ou documents » et ceux d'« opérateur de communications électroniques » à l'article L. 246-1 du code de la sécurité intérieure, le législateur n'a pas défini de façon suffisamment précise les données de connexion pouvant être collectées par l'autorité administrative sur réquisition et, d'autre part, qu'en employant les termes de « sollicitation du réseau » à l'article L. 246-3 du même code, il n'a pas exclu la possibilité pour cette autorité d'accéder directement aux données de connexion détenues par les opérateurs de communications électroniques dans le cadre de cette même procédure ; qu'il en résulterait une méconnaissance par le législateur de l'étendue de sa compétence dans des conditions portant atteinte au droit au respect de la vie privée ;

9. Considérant que la méconnaissance par le législateur de sa propre compétence ne peut être invoquée à l'appui d'une question prioritaire de constitutionnalité que dans le cas où cette méconnaissance affecte par elle-même un droit ou une liberté que la Constitution garantit ;

10. Considérant qu'aux termes de l'article 34 de la Constitution : « La loi fixe les règles concernant… les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques » ; que la méconnaissance par le législateur de sa compétence, dans la détermination de ces garanties dans le cadre d'une procédure de réquisition administrative de données de connexion, affecte par elle-même le droit au respect de la vie privée ;

11. Considérant, en premier lieu, d'une part, qu'en vertu de l'article L. 246-1 du code de la sécurité intérieure, la procédure de recueil des données de connexion sur réquisition administrative peut s'exercer auprès des opérateurs de communications électroniques et des personnes mentionnées à l'article L. 34-1 du code des postes et des communications électroniques ainsi que des personnes mentionnées aux 1 et 2 du paragraphe I de l'article 6 de la loi du 21 juin 2004 susvisée ; que l'article L. 32 du code des postes et des communications électroniques définit dans son 1° les communications électroniques comme « les émissions, transmissions ou réceptions de signes, de signaux, d'écrits, d'images ou de sons, par voie électromagnétique » et dans son 15° l'opérateur comme « toute personne physique ou morale exploitant un réseau de communications électroniques ouvert au public ou fournissant au public un service de communications électroniques » ; que le paragraphe II de l'article L. 34-1 du même code prévoit son application aux opérateurs de communications électroniques, et notamment aux personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, et aux personnes qui fournissent au public des services de communications électroniques, ainsi qu'aux personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau ; que les personnes mentionnées aux 1 et 2 du paragraphe I de l'article 6 de la loi du 21 juin 2004 sont celles dont l'activité est d'offrir un accès à des services de communication au public en ligne et celles qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services ;

12. Considérant, d'autre part, qu'en vertu du même article L. 246-1, peuvent être recueillis par l'autorité administrative les informations ou documents traités ou conservés par les réseaux ou services de communications électroniques des personnes susmentionnées ; que, selon les dispositions du VI de l'article L. 34-1 du code des postes et des communications électroniques, les données conservées et traitées portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation des équipements terminaux et ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications ; que selon le paragraphe II de l'article 6 de la loi du 21 juin 2004, les données conservées sont celles de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires ; qu'ainsi, le législateur a suffisamment défini les données de connexion, qui ne peuvent porter sur le contenu de correspondances ou les informations consultées ;

13. Considérant, en second lieu, qu'il résulte de l'article L. 246-1 que les données de connexion requises sont transmises par les opérateurs aux autorités administratives compétentes ; que selon l'article L. 246-3, lorsque les données de connexion sont transmises en temps réel à l'autorité administrative, celles-ci ne peuvent être recueillies qu'après « sollicitation » de son réseau par l'opérateur ; que, par suite, les autorités administratives ne peuvent accéder directement au réseau des opérateurs dans le cadre de la procédure prévue aux articles L. 246-1 et L. 246-3 ;

14. Considérant qu'il résulte de ce qui précède que le grief tiré de ce que le législateur, en ne définissant pas précisément la procédure de réquisition administrative des données de connexion détenues et traitées par les opérateurs de communications électroniques, a méconnu l'étendue de sa compétence dans des conditions affectant le droit au respect de la vie privée, doit être écarté ;

- Sur le grief tiré de l’incompétence négative résultant de l’absence de garanties de nature à protéger le secret professionnel des avocats et des journalistes :

15. Considérant que les associations requérantes soutiennent que le législateur, en ne prévoyant pas des garanties spécifiques de nature à protéger l'accès aux données de connexion des avocats et des journalistes, a méconnu l'étendue de sa compétence dans des conditions portant atteinte au droit au respect de la vie privée, à la liberté d'expression et de communication, ainsi qu'aux droits de la défense et au droit à un procès équitable, au droit au secret des échanges et correspondances des avocats et au droit au secret des sources des journalistes ;

16. Considérant qu'il incombe au législateur d'assurer la conciliation entre, d'une part, la prévention des atteintes à l'ordre public et des infractions, nécessaire à la sauvegarde de droits et de principes de valeur constitutionnelle, et, d'autre part, l'exercice des droits et des libertés constitutionnellement garantis ; qu'au nombre de ces derniers figurent le droit au respect de la vie privée et le secret des correspondances, la liberté d'expression, les droits de la défense et le droit à un procès équitable, protégés par les articles 2, 4, 11 et 16 de la Déclaration des droits de l'homme et du citoyen de 1789 ; qu'en revanche, aucune disposition constitutionnelle ne consacre spécifiquement un droit au secret des échanges et correspondances des avocats et un droit au secret des sources des journalistes ;

17. Considérant, en premier lieu, que les dispositions contestées instituent une procédure de réquisition administrative de données de connexion excluant l'accès au contenu des correspondances ; que, par suite, elles ne sauraient méconnaître le droit au secret des correspondances et la liberté d'expression ;

18. Considérant, en second lieu, qu'outre qu'elle ne peut porter sur le contenu de correspondances, la procédure de réquisition administrative résultant des dispositions contestées est autorisée uniquement aux fins de recueillir des renseignements intéressant la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France ou la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous ; qu'elle est mise en œuvre par des agents spécialement habilités ; qu'elle est subordonnée à l'accord préalable d'une personnalité qualifiée, placée auprès du Premier ministre, désignée par la commission nationale de contrôle des interceptions de sécurité ; que, si l'autorisation de recueil des données en temps réel est délivrée par le Premier ministre, cette autorisation est soumise au contrôle de la commission nationale de contrôle des interceptions de sécurité ; que cette dernière dispose d'un accès permanent au dispositif de recueil des informations ou documents et adresse des recommandations au ministre de l'intérieur ou au Premier ministre lorsqu'elle constate un manquement aux règles édictées ou une atteinte aux droits et libertés ; qu'enfin, aux termes de l'article 226-13 du code pénal : « La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15 000 euros d'amende » ;

19. Considérant qu'il résulte de ce qui précède que le législateur a prévu des garanties suffisantes afin qu'il ne résulte pas de la procédure prévue aux articles L. 246-1 et L. 246-3 du code de la sécurité intérieure une atteinte disproportionnée au droit au respect de la vie privée, aux droits de la défense, au droit à un procès équitable, y compris pour les avocats et journalistes ; que le grief tiré de ce que le législateur aurait insuffisamment exercé sa compétence en ne prévoyant pas des garanties spécifiques pour protéger le secret professionnel des avocats et journalistes doit être écarté ;

20. Considérant qu'il résulte de tout ce qui précède que les dispositions contestées, qui ne sont contraires à aucun autre droit ou liberté que la Constitution garantit, doivent être déclarées conformes à la Constitution.

[…]

Observations de la Commission nationale de l'informatique et des libertés (CNIL) sur le projet de loi renforçant la sécurité intérieure et la lutte contre le terrorisme, 11 juillet 2017 (extraits). **Document n° 2**

[…]

Les points de vigilance de la CNIL sur le projet de loi

Sur le fond, la CNIL suit toujours, dans l'examen des textes en matière de sécurité, une démarche constructive recherchant **une juste conciliation entre la prévention des atteintes à l'ordre public et le droit au respect de la protection des données personnelles**.

A cet égard, une vigilance particulière s'impose sur les mesures du projet de loi qui affectent le droit de chacun à la protection de ses données personnelles. Si la Commission relève que des garanties sont prévues pour encadrer les mesures les plus intrusives, en ce qui concerne en particulier les conditions de placement sous surveillance électronique, les modalités de saisie et d'exploitation de données informatiques dans le cadre des visites ou la surveillance des communications hertziennes, elle estime que ces garanties devraient être renforcées.

Tout d'abord, sur l'obligation de déclarer les numéros d'abonnement et les identifiants des moyens de communication électronique prévue dans certaines hypothèses. A la demande du Conseil d'Etat, les mots de passe ont été exclus de la liste des éléments à déclarer. Cependant, la Commission relève que cette obligation est susceptible de concerner un champ très large de services de communication, tels que la téléphonie fixe ou mobile, la transmission vocale sur internet, les SMS, les courriels, les messageries instantanées, etc. Ce champ n'est pas précisé ni limité par le projet de loi. Le texte ne prévoit pas davantage les finalités et les conditions d'utilisation de ces numéros et identifiants. Des précisions devront être apportées sur ce point pour clarifier les finalités et garantir la proportionnalité de telles mesures.

Une grande vigilance devra par ailleurs être observée sur les données PNR (Passenger Name Record[1]). Il s'agit là d'un type de traitement de grande ampleur, susceptible d'avoir une incidence majeure sur le droit au respect de la vie privée. Le projet de loi supprime le caractère expérimental de celui-ci conformément à la directive européenne n° 2016/681. Pour autant, cette pérennisation n'ôte rien à l'exigence d'évaluation. La CNIL rappelle que la directive prévoit une clause de réexamen de l'ensemble du dispositif, sur la base des informations communiquées par les États membres. Le traitement mis en œuvre au niveau national est en outre plus étendu que ce que prévoit la directive, dans la mesure où il peut être utilisé, par les services de renseignement, à des fins de prévention des atteintes aux intérêts fondamentaux de la nation. Il faudra donc, dans les conditions fixées par la loi et le règlement, prévoir une rigoureuse évaluation du dispositif national, et notamment de l'effectivité des garanties prévues pour les personnes concernées.
[…]

Le nécessaire contrôle des fichiers de renseignement

Le projet de loi renforce en outre, par plusieurs de ses dispositions, le rôle et le contenu des fichiers des services de renseignement. En effet, d'une part, les mesures individuelles de surveillance que le ministre peut prescrire ou les visites et saisies auxquelles le préfet peut faire procéder reposeront nécessairement sur l'identification préalable, au sein des fichiers mis en œuvre ou utilisés par les services de renseignement, des personnes remplissant certains critères. D'autre part, le projet prévoit

[1] Note du jury : stockage de données personnelles des utilisateurs de transports aériens.

et encadre, à la suite de la censure par le Conseil constitutionnel d'une partie d'un précédent texte, l'interception des communications électroniques par voie hertzienne.

Le texte s'inscrit ainsi dans la continuité des dispositions issues de la loi relative au renseignement de 2015, qui avait déjà **massivement élargi les possibilités de collecte** de données par les services compétents, par le biais notamment de mesures intrusives de contrôle et de surveillance des personnes. Plus généralement, dans les années récentes, le législateur a, soit décidé la création de nouveaux fichiers en lien avec la lutte contre le terrorisme, soit étendu les cas d'enregistrement de données dans ces fichiers, **ces deux tendances appelant des garanties fortes pour les citoyens.**

Si ces garanties ont considérablement progressé, il leur manque selon la Commission une composante essentielle : un contrôle indépendant et global de la gestion de ces fichiers.

Certes, le code de la sécurité intérieure prévoit un encadrement strict de la collecte de données par des techniques intrusives mises en œuvre par les services de renseignement, seulement après intervention de la Commission nationale de contrôle des techniques de renseignement (CNCTR) et autorisation du Premier ministre. Le législateur a par ailleurs prévu un « droit d'accès indirect », par lequel une personne peut obtenir qu'un membre de la CNIL s'assure de la régularité des données enregistrées, le cas échéant, dans l'un de ces fichiers. De même, la formation spécialisée du Conseil d'Etat est compétente pour connaître de requêtes individuelles concernant le recours aux techniques de recueil de renseignement ou le droit d'accès indirect aux fichiers mis en œuvre par les services spécialisés.

Cependant, au-delà de ces contrôles ponctuels, à la demande d'une personne, il n'existe pas aujourd'hui de dispositif de contrôle global des fichiers de renseignement eux-mêmes. Les textes qui les ont créés les ont en effet soustraits, dans la plupart des cas, au contrôle a posteriori de la CNIL. Il en résulte une situation paradoxale : les fichiers constitués à partir des données ainsi collectées sont pleinement soumis aux principes de la loi Informatique et Libertés (principe de finalité, proportionnalité des données collectées, exigence d'exactitude et de mise à jour, etc.), mais aucun contrôleur externe n'est désigné pour en assurer, de manière générale, le respect.

Comme la Commission l'a déjà indiqué, pour être acceptable d'un point de vue juridique, éthique et sociétal, le déplacement éventuel du curseur vers des mesures de sécurité plus intrusives doit nécessairement s'accompagner d'un renforcement des garanties qui encadrent l'action des services de sécurité. Prévoir un tel contrôle est une garantie qu'appelle l'état de droit.

[…]

Cour de justice de l'Union européenne, 21 décembre 2016, *Tele2 Sverige AB c/ Post-och telestyrelsen,* n° C-203/15, *et Secretary of State for the Home Department c/ Tom Watson, Peter Brice, Geoffrey Lewis,* n° C-698/15 (affaires jointes), (extraits). **Document n° 3**

[…]

72. Certes, les mesures législatives visées à l'article 15, paragraphe 1, de la directive 2002/58 se rapportent à des activités propres aux États ou aux autorités étatiques, étrangères aux domaines d'activité des particuliers (voir, en ce sens, arrêt du 29 janvier 2008, Promusicae, C-275/06, EU:C:2008:54, point 51). En outre, les finalités auxquelles, en vertu de cette disposition, de telles mesures doivent répondre, en l'occurrence la sauvegarde de la sécurité nationale, de la défense et de la sécurité publique ainsi que la mise en œuvre de la prévention, de la recherche, de la détection et de la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, recoupent substantiellement les finalités poursuivies par les activités visées à l'article 1er, paragraphe 3, de cette directive.

73. Toutefois, eu égard à l'économie générale de la directive 2002/58, les éléments relevés au point précédent du présent arrêt n'autorisent pas à conclure que les mesures législatives visées à l'article 15, paragraphe 1, de la directive 2002/58 seraient exclues du champ d'application de cette directive, sauf à priver cette disposition de tout effet utile. (…)

[…]

97. S'agissant de la question de savoir si une réglementation nationale, telle que celle en cause dans l'affaire C-203/15, satisfait à ces conditions, il convient de relever que celle-ci prévoit une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique, et qu'elle oblige les fournisseurs de services de communications électroniques à conserver ces données de manière systématique et continue, et ce sans aucune exception. Ainsi qu'il ressort de la décision de renvoi, les catégories de données visées par cette réglementation correspondent, en substance, à celles dont la conservation était prévue par la directive 2006/24.

98. Les données que doivent ainsi conserver les fournisseurs de services de communications électroniques permettent de retrouver et d'identifier la source d'une communication et la destination de celle-ci, de déterminer la date, l'heure, la durée et le type d'une communication, le matériel de communication des utilisateurs, ainsi que de localiser le matériel de communication mobile. Au nombre de ces données figurent, notamment, le nom et l'adresse de l'abonné ou de l'utilisateur inscrit, le numéro de téléphone de l'appelant et le numéro appelé ainsi qu'une adresse IP[2] pour les services Internet. Ces données permettent, en particulier, de savoir quelle est la personne avec laquelle un abonné ou un utilisateur inscrit a communiqué et par quel moyen, tout comme de déterminer le temps de la communication ainsi que l'endroit à partir duquel celle-ci a eu lieu. En outre, elles permettent de connaître la fréquence des communications de l'abonné ou de l'utilisateur inscrit avec certaines personnes pendant une période donnée (…).

99. Prises dans leur ensemble, ces données sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci (…). En particulier, ces données fournissent les moyens d'établir,

[2] Internet Protocole (numéro d'identification attribué à un périphérique informatique).

ainsi que l'a relevé M. l'avocat général aux points 253, 254 et 257 à 259 de ses conclusions, le profil des personnes concernées, information tout aussi sensible, au regard du droit au respect de la vie privée, que le contenu même des communications.

100. L'ingérence que comporte une telle réglementation dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte s'avère d'une vaste ampleur et doit être considérée comme particulièrement grave. La circonstance que la conservation des données est effectuée sans que les utilisateurs des services de communications électroniques en soient informés est susceptible de générer dans l'esprit des personnes concernées le sentiment que leur vie privée fait l'objet d'une surveillance constante (…).

101. Même si une telle réglementation n'autorise pas la conservation du contenu d'une communication et, partant, n'est pas de nature à porter atteinte au contenu essentiel desdits droits (…), la conservation des données relatives au trafic et des données de localisation pourrait toutefois avoir une incidence sur l'utilisation des moyens de communication électronique et, en conséquence, sur l'exercice par les utilisateurs de ces moyens de leur liberté d'expression, garantie à l'article 11 de la Charte (…).

102. Eu égard à la gravité de l'ingérence dans les droits fondamentaux en cause que constitue une réglementation nationale prévoyant, aux fins de la lutte contre la criminalité, la conservation de données relatives au trafic et de données de localisation, seule la lutte contre la criminalité grave est susceptible de justifier une telle mesure (…).

103. En outre, si l'efficacité de la lutte contre la criminalité grave, notamment contre la criminalité organisée et le terrorisme, peut dépendre dans une large mesure de l'utilisation des techniques modernes d'enquête, un tel objectif d'intérêt général, pour fondamental qu'il soit, ne saurait à lui seul justifier qu'une réglementation nationale prévoyant la conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation soit considérée comme nécessaire aux fins de ladite lutte (…).

104. À cet égard, il convient de relever, d'une part, qu'une telle réglementation a pour effet, eu égard à ses caractéristiques décrites au point 97 du présent arrêt, que la conservation des données relatives au trafic et des données de localisation est la règle, alors que le système mis en place par la directive 2002/58 exige que cette conservation des données soit l'exception.

105. D'autre part, une réglementation nationale telle que celle en cause au principal, qui couvre de manière généralisée tous les abonnés et utilisateurs inscrits et vise tous les moyens de communication électronique ainsi que l'ensemble des données relatives au trafic, ne prévoit aucune différenciation, limitation ou exception en fonction de l'objectif poursuivi. Elle concerne de manière globale l'ensemble des personnes faisant usage de services de communications électroniques, sans que ces personnes se trouvent, même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales. Elle s'applique donc même à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec des infractions pénales graves. En outre, elle ne prévoit aucune exception, de telle sorte qu'elle s'applique même à des personnes dont les communications sont soumises, selon les règles du droit national, au secret professionnel (…).

106. Une telle réglementation ne requiert aucune relation entre les données dont la conservation est prévue et une menace pour la sécurité publique. Notamment, elle n'est pas limitée à une conservation portant soit sur des données afférentes à une période temporelle et/ou une zone géographique et/ou sur un cercle de personnes susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave, soit sur des personnes qui pourraient, pour d'autres motifs, contribuer, par la conservation de leurs données, à la lutte contre la criminalité (…).

107. Une réglementation nationale telle que celle en cause au principal excède donc les limites du strict nécessaire et ne saurait être considérée comme étant justifiée, dans une société démocratique, ainsi que l'exige l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte.

108. En revanche, l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, ne s'oppose pas à ce qu'un État membre adopte une réglementation permettant, à titre préventif, la conservation ciblée des données relatives au trafic et des données de localisation, à des fins de lutte contre la criminalité grave, à condition que la conservation des données soit, en ce qui concerne les catégories de données à conserver, les moyens de communication visés, les personnes concernées ainsi que la durée de conservation retenue, limitée au strict nécessaire.

109. Pour satisfaire aux exigences énoncées au point précédent du présent arrêt, cette réglementation nationale doit, en premier lieu, prévoir des règles claires et précises régissant la portée et l'application d'une telle mesure de conservation des données et imposant un minimum d'exigences, de telle sorte que les personnes dont les données ont été conservées disposent de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus. Elle doit en particulier indiquer en quelles circonstances et sous quelles conditions une mesure de conservation des données peut, à titre préventif, être prise, garantissant ainsi qu'une telle mesure soit limitée au strict nécessaire (…).

110. En second lieu, s'agissant des conditions matérielles auxquelles doit satisfaire une réglementation nationale permettant, dans le cadre de la lutte contre la criminalité, la conservation, à titre préventif, des données relatives au trafic et des données de localisation, afin de garantir qu'elle soit limitée au strict nécessaire, il convient de relever que, si ces conditions peuvent varier en fonction des mesures prises aux fins de la prévention, de la recherche, de la détection et de la poursuite de la criminalité grave, la conservation des données n'en doit pas moins toujours répondre à des critères objectifs, établissant un rapport entre les données à conserver et l'objectif poursuivi. En particulier, de telles conditions doivent s'avérer, en pratique, de nature à délimiter effectivement l'ampleur de la mesure et, par suite, le public concerné.

111. S'agissant de la délimitation d'une telle mesure quant au public et aux situations potentiellement concernés, la réglementation nationale doit être fondée sur des éléments objectifs permettant de viser un public dont les données sont susceptibles de révéler un lien, au moins indirect, avec des actes de criminalité grave, de contribuer d'une manière ou d'une autre à la lutte contre la criminalité grave ou de prévenir un risque grave pour la sécurité publique. Une telle délimitation peut être assurée au moyen d'un critère géographique lorsque les autorités nationales compétentes considèrent, sur la base d'éléments objectifs, qu'il existe, dans une ou plusieurs zones géographiques, un risque élevé de préparation ou de commission de tels actes.

[…]

Cour de justice des Communautés européennes, **11 janvier 2000,** ***Tanja Kreil c/ Bundesrepublik Deutschland*****, n° C-285/98 (extrait).** **Document n° 4**

[…]

15. Tout d'abord, ainsi que l'a relevé la Cour au point 15 de l'arrêt du 26 octobre 1999, Sirdar (C-273/97, non encore publié au Recueil), il appartient aux États membres, qui ont à arrêter les mesures propres à assurer leur sécurité intérieure et extérieure, de prendre les décisions relatives à l'organisation de leurs forces armées. Il n'en résulte pas, cependant, que de telles décisions doivent échapper totalement à l'application du droit communautaire.

16. En effet, ainsi que la Cour l'a déjà constaté, le traité ne prévoit des dérogations applicables en cas de situations susceptibles de mettre en cause la sécurité publique que dans ses articles 36, 48, 56, 223 (devenus, après modification, articles 30 CE, 39 CE, 46 CE et 296 CE) et 224 (devenu article 297 CE), qui concernent des hypothèses exceptionnelles bien délimitées. Il ne saurait en être déduit qu'il existerait une réserve générale, inhérente au traité, excluant du champ d'application du droit communautaire toute mesure prise au titre de la sécurité publique. Reconnaître l'existence d'une telle réserve, en dehors des conditions spécifiques des dispositions du traité, risquerait de porter atteinte au caractère contraignant et à l'application uniforme du droit communautaire (voir, en ce sens, arrêts du 15 mai 1986, Johnston, 222/84, Rec. p. 1651, point 26, et Sirdar, précité, point 16).

[…]

Charte des droits fondamentaux de l'Union européenne, article 8 (extrait). **Document n° 5**

[…]

Article 8 : Protection des données à caractère personnel

1. Toute personne a droit à la protection des données à caractère personnel la concernant.

2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.

3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante.

[…]

Conseil d'Etat, 26 juillet 2018*, Quadrature du Net, French Data Network et la Fédération des fournisseurs d'accès à internet associatifs,* n° 394922, *Association Igwan.net,* n° 397844,
***Quadrature du Net, French Data Network et la Fédération des fournisseurs d'accès à internet associatifs,* n° 397851 (extraits).**

Document n° 6

[…]

Considérant ce qui suit :

1. Par trois requêtes, La Quadrature du Net, French Data Network et la Fédération des fournisseurs d'accès à internet associatifs demandent l'annulation pour excès de pouvoir, sous le numéro 394922 du décret du 28 septembre 2015 portant désignation des services spécialisés de renseignement, sous le numéro 394925 du décret du 1er octobre 2015 relatif au contentieux de la mise en œuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'Etat, et sous le numéro 397851 du décret du 29 janvier 2016 relatif aux techniques de recueil de renseignement. L'association Igwan.net, sous le numéro 397844, demande l'annulation du décret du 11 décembre 2015 relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure, pris en application de l'article L. 811-4 du code de la sécurité intérieure. Ces requêtes présentent à juger les mêmes questions. Il y a lieu de les joindre pour statuer par une seule décision.

Sur les moyens de légalité externe :

[…].

Sur les moyens de légalité interne :

En ce qui concerne le moyen tiré de la méconnaissance de l'article L. 851-1 du code de la sécurité intérieure par le décret du 29 janvier 2016 relatif aux techniques de recueil de renseignement :

3. Les dispositions de l'article R. 851-5 du code de la sécurité intérieure créées par le décret du 29 janvier 2016 relatif aux techniques de recueil de renseignement qui définissent les données de connexion susceptibles d'être recueillies auprès des opérateurs de communications électroniques excluent des données ainsi recueillies le contenu des correspondances échangées ou des informations consultées. En outre, ces dispositions réservent le recueil de certaines de ces données aux seules techniques de renseignement prévues aux articles L. 851-2 et L. 851-3 du code de la sécurité intérieure, lesquelles ne sont mises en œuvre que pour les seuls besoins de la prévention du terrorisme. Ce faisant, contrairement à ce que soutiennent les associations requérantes, ces dispositions réglementaires ne méconnaissent pas les dispositions de l'article L. 851-1 du même code pour l'application desquelles elles ont été prises.

En ce qui concerne les moyens invoqués par la voie de l'exception :

4. A l'appui de leurs conclusions, les requérants soulèvent des moyens, par la voie de l'exception, à l'encontre de l'ensemble des dispositions du livre VIII du code de la sécurité intérieure, de celles du chapitre III bis du titre VII du livre VII du code de justice administrative et de celles de l'article 323-8 du code pénal.

[…]

S'agissant des moyens tirés de la méconnaissance de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales :

7. En premier lieu, les associations requérantes soutiennent que les décrets attaqués ont été pris sur le fondement ou pour l'application de dispositions législatives qui méconnaissent le droit à un recours effectif garanti notamment par l'article 13 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, en raison des atteintes portées au droit au recours, aux droits de la défense et au principe du contradictoire dans le cadre du contentieux de la mise en œuvre des techniques de renseignement.

8. Les dispositions des articles L. 841-1 et L. 841-2 du code de la sécurité intérieure prévoient les conditions dans lesquelles le Conseil d'Etat est compétent pour connaître des requêtes concernant la mise en œuvre des techniques de renseignement soumises à autorisation. Il peut être saisi soit par toute personne souhaitant vérifier qu'aucune technique de renseignement n'est irrégulièrement mise en œuvre et justifiant d'avoir au préalable saisi la Commission nationale de contrôle des techniques de renseignement sur le fondement de l'article L. 833-4 du même code, soit par le président de cette commission, ou trois de ses membres, lorsque le Premier ministre ne donne pas suite aux avis ou aux recommandations de la commission ou que les suites qui y sont données sont estimées insuffisantes. S'agissant des mesures de surveillance des communications électroniques internationales encadrées par le chapitre IV du titre V du livre VIII du code de la sécurité intérieure, si la personne qui pense faire l'objet d'une telle mesure de surveillance ne peut directement saisir un juge pour en contester la régularité, elle peut en revanche, sur le fondement des dispositions de l'article L. 854-9 de ce code, former une réclamation à cette fin auprès de la Commission nationale de contrôle des techniques de renseignement. Or, ce même article prévoit que lorsque la commission identifie un manquement, de sa propre initiative ou à la suite d'une telle réclamation, elle adresse au Premier ministre une recommandation tendant à ce qu'il y soit mis fin et que les renseignements collectés soient, le cas échéant, détruits. Elle peut également saisir le Conseil d'Etat.

9. Saisie de conclusions tendant à ce qu'elle s'assure qu'aucune technique de renseignement n'est irrégulièrement mise en œuvre à l'égard du requérant ou de la personne concernée, il appartient à la formation spécialisée, créée par l'article L. 773-2 du code de justice administrative, de vérifier, au vu des éléments qui lui ont été communiqués hors la procédure contradictoire, si le requérant fait ou non l'objet d'une telle technique. Dans l'affirmative, il lui appartient d'apprécier si cette technique est mise en œuvre dans le respect du livre VIII du code de la sécurité intérieure. Lorsqu'il apparaît soit qu'aucune technique de renseignement n'est mise en œuvre à l'égard du requérant, soit que cette mise en œuvre n'est entachée d'aucune illégalité, la formation de jugement informe le requérant de l'accomplissement de ces vérifications et qu'aucune illégalité n'a été commise, sans autre précision. Dans le cas où une technique de renseignement est mise en œuvre dans des conditions qui apparaissent entachées d'illégalité, elle en informe le requérant, sans faire état d'aucun élément protégé par le secret de la défense nationale. En pareil cas, par une décision distincte dont seule l'administration compétente et la Commission nationale de contrôle des techniques de renseignement sont destinataires, la formation spécialisée annule le cas échéant l'autorisation et ordonne la destruction des renseignements irrégulièrement collectés.

10. La dérogation apportée, par les dispositions contestées du code de justice administrative, au caractère contradictoire de la procédure juridictionnelle, qui a pour seul objet de porter à la connaissance des juges des éléments couverts par le secret de la défense nationale et qui ne peuvent, dès lors, être communiqués au requérant, permet à la formation spécialisée, qui entend les parties, de statuer en toute connaissance de cause. Les pouvoirs dont elle est investie, pour instruire les requêtes, relever d'office toutes les illégalités qu'elle constate et enjoindre à l'administration de prendre toutes mesures utiles afin de remédier aux illégalités constatées garantissent l'effectivité du contrôle juridictionnel qu'elle exerce.

11. Il s'ensuit que ni les conditions dans lesquelles la formation spécialisée peut être saisie ni celles dans lesquelles elle remplit son office juridictionnel ne méconnaissent, contrairement à ce qui est soutenu, le droit au recours effectif des personnes qui la saisissent, garanti notamment par l'article 13 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.

12. En second lieu, les associations requérantes soutiennent que les décrets attaqués ont été pris sur le fondement ou pour l'application de dispositions législatives qui méconnaissent le droit au respect de la vie privée garanti notamment par l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, en raison de l'absence de notification des mesures de surveillance aux personnes concernées après qu'elles ont été levées.

13. Eu égard, d'une part, aux attributions de la Commission nationale de contrôle des techniques de renseignement, autorité administrative indépendante à laquelle il appartient de vérifier, sous le contrôle du juge, que les techniques de recueil de renseignement sont mises en œuvre, sur le territoire national, conformément aux exigences découlant du code de la sécurité intérieure, et, d'autre part, au recours effectif ouvert, dans les conditions décrites aux points précédents, devant la formation spécialisée du Conseil d'Etat, la circonstance que les dispositions législatives contestées ne prévoient pas la notification aux personnes concernées des mesures de surveillance dont elles ont fait l'objet, une fois ces dernières levées, ne caractérise pas, par elle-même, une atteinte excessive portée au droit au respect de la vie privée.

14. Il résulte de ce qui précède que les moyens tirés de la contrariété des dispositions législatives contestées aux articles 8 et 13 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales doivent, en tout état de cause, être écartés.

S'agissant du moyen tiré de la méconnaissance de la directive du 8 juin 2000 :

15. Les dispositions de l'article L. 851-3 du code de la sécurité intérieure permettent d'imposer aux opérateurs de communications électroniques et aux prestataires techniques " la mise en œuvre sur leurs réseaux de traitements automatisées destinés, en fonction de paramètres précisés dans l'autorisation, à détecter des connexions susceptibles de révéler une menace terroriste ". Cette technique vise uniquement à recueillir pendant une durée limitée, parmi l'ensemble des données de connexion traitées par ces personnes, celles de ces données qui pourraient présenter un lien avec une telle infraction grave. Dans ces conditions, ces dispositions, qui n'imposent pas une obligation générale de surveillance active, ne méconnaissent pas les dispositions claires de l'article 15 de la directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur, qui prévoient que " Les Etats membres ne doivent pas imposer aux prestataires, pour la fourniture des services de simple transport, de stockage et d'hébergement une obligation générale de surveiller les informations qu'ils transmettent ou stockent, ou une obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites ". Il s'ensuit qu'en tout état de cause, le moyen tiré de la méconnaissance de la directive du 8 juin 2000 doit être écarté.

S'agissant des moyens tirés de la méconnaissance de la directive du 12 juillet 2002 et de la Charte des droits fondamentaux de l'Union européenne :

16. D'une part, aux termes de l'article 4 du Traité sur l'Union européenne, l'Union " respecte les fonctions essentielles de l'Etat, notamment celles qui ont pour objet d'assurer son intégrité territoriale, de maintenir l'ordre public et de sauvegarder la sécurité nationale. En particulier, la sécurité nationale reste de la seule responsabilité de chaque Etat membre ". L'article 51 de la Charte des droits fondamentaux de l'Union européenne prévoit que " 1. Les dispositions de la présente Charte s'adressent aux institutions, organes et organismes de l'Union dans le respect du principe de subsidiarité, ainsi qu'aux Etats membres uniquement lorsqu'ils mettent en œuvre le droit de l'Union.

(...) 2. La présente Charte n'étend pas le champ d'application du droit de l'Union au-delà des compétences de l'Union, ni ne crée aucune compétence ni aucune tâche nouvelles pour l'Union et ne modifie pas les compétences et tâches définies dans les traités ". Aux termes de son article 54 : " Aucune des dispositions de la présente Charte ne doit être interprétée comme impliquant un droit quelconque de se livrer à une activité ou d'accomplir un acte visant à la destruction des droits ou libertés reconnus dans la présente Charte (...) ".

17. D'autre part, la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, qui a été prise sur le fondement de l'article 95 du traité instituant la Communauté européenne, désormais repris à l'article 114 du traité sur le fonctionnement de l'Union européenne, procède de la volonté de rapprocher les législations des Etats membres afin de permettre l'établissement et le fonctionnement du marché intérieur. Elle a pour objet, ainsi que l'énonce le paragraphe 1 de son article 3, le " traitement des données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux publics de communication dans la Communauté ". Mais, ainsi que le rappelle son article 1er, paragraphe 3, elle " ne s'applique pas aux activités qui ne relèvent pas du traité instituant la Communauté européenne (...) et, en tout état de cause, aux activités concernant la sécurité publique, la défense, la sûreté de l'État (y compris la prospérité économique de l'État lorsqu'il s'agit d'activités liées à la sûreté de l'État) ou aux activités de l'État dans des domaines relevant du droit pénal ". Par ailleurs, son article 15 prévoit que " Les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale - c'est-à-dire la sûreté de l'État - la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe. Toutes les mesures visées dans le présent paragraphe sont prises dans le respect des principes généraux du droit communautaire, y compris ceux visés à l'article 6, paragraphes 1 et 2, du traité sur l'Union européenne ". Les Etats membres sont ainsi autorisés, pour des motifs tenant à la sûreté de l'Etat ou à la lutte contre les infractions pénales, à déroger, notamment, à l'obligation de confidentialité des données à caractère personnel, ainsi que de confidentialité des données relatives au trafic y afférentes, qui découlent de l'article 5, paragraphe 1, de la directive.

Quant au champ d'application de l'article 15, paragraphe 1, de la directive du 12 juillet 2002 :

18. Il résulte des dispositions précitées de la directive du 12 juillet 2002, ainsi que l'a dit pour droit la Cour de justice de l'Union européenne par son arrêt Tele2 Sverige AB c/ Post-och telestyrelsen et Secretary of State for the Home Department c/ Tom Watson et autres (C-203/15 et C-698/15), du 21 décembre 2016, qu'elle " doit être regardée comme régissant les activités des fournisseurs [de services de communications électroniques] ". Les dispositions imposant des obligations à ces fournisseurs, telles que la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation de leurs utilisateurs et abonnés, aux fins mentionnées à l'article 15, paragraphe 1, de la directive du 12 juillet 2002, parmi lesquelles figure la sauvegarde de la sécurité nationale, de la défense et de la sécurité publique relèvent dès lors du champ d'application de cette directive dans la mesure où, ainsi que l'a dit pour droit la Cour de justice, elles régissent leur activité. Par ailleurs, ainsi que l'a également dit pour droit la Cour, la circonstance que de telles obligations n'interviennent qu'aux seules fins de rendre accessibles aux autorités nationales compétentes les données personnelles qu'elles concernent, implique que la réglementation nationale encadrant l'accès et l'utilisation de ces données relève également du champ d'application de la directive du

12 juillet 2002. En revanche, les dispositions nationales qui portent sur des techniques de recueil de renseignement directement mises en œuvre par l'Etat sans régir les activités des fournisseurs de services de communications électroniques en leur imposant des obligations spécifiques ne relèvent pas du champ d'application de cette directive.

19. L'article L. 851-1 du code de la sécurité intérieure dispose que : " Dans les conditions prévues au chapitre Ier du titre II du présent livre, peut être autorisé le recueil, auprès des opérateurs de communications électroniques et des personnes mentionnées à l'article L. 34-1 du code des postes et des communications électroniques ainsi que des personnes mentionnées aux 1 et 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, des informations ou documents traités ou conservés par leurs réseaux ou services de communications électroniques, y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications (...) ". Les articles L. 851-2 et L. 851-4 du code de la sécurité intérieure organisent, pour des finalités et selon des modalités différentes, des accès administratifs en temps réel aux données de connexion ainsi conservées.

20. Il résulte clairement de ce qui précède, eu égard au champ d'application de l'article 15, paragraphe 1, de la directive du 12 juillet 2002 tel qu'interprété par la Cour de justice de l'Union européenne, qu'en relèvent tant l'obligation de conservation induite par les dispositions précitées de l'article L 851-1 du code de la sécurité intérieure que les accès administratifs aux données de connexion, y compris en temps réel, qui la justifient, prévus aux articles L. 851-1, L. 851-2 et L. 851-4 de ce code. Il en va de même des dispositions de l'article L. 851-3 du code de la sécurité intérieure qui, si elles ne font pas peser sur les opérateurs et personnes concernés une obligation préalable de conservation, leur imposent cependant de mettre en œuvre sur leurs réseaux des traitements automatisés destinés à détecter des connexions susceptibles de révéler une menace terroriste.

21. En revanche, il résulte clairement de la directive du 12 juillet 2002 que ne relèvent pas de son champ les dispositions des articles L. 851-5 et L. 851-6, ainsi que celles des chapitres II, III et IV du titre V du livre VIII du code de la sécurité intérieure, dès lors qu'elles portent sur des techniques de recueil de renseignement qui sont directement mises en œuvre par l'Etat sans régir les activités des fournisseurs de services de communications électroniques en leur imposant des obligations spécifiques. Dès lors, ces dispositions ne sauraient être regardées comme mettant en œuvre le droit de l'Union européenne et, par suite, les moyens tirés de la méconnaissance de la directive du 12 juillet 2002 interprétée à la lumière de la Charte des droits fondamentaux de l'Union européenne ne peuvent être utilement invoqués à leur encontre.

Quant à l'obligation de conservation généralisée et indifférenciée :

22. Par son arrêt du 21 décembre 2016, la Cour de justice de l'Union européenne a dit pour droit que l'article 15, paragraphe 1, de cette directive, " lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale prévoyant, à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique ".

23. D'une part, il est constant qu'une telle conservation préventive et indifférenciée permet aux services de renseignement d'accéder aux données relatives aux communications qu'un individu a effectuées avant que soient identifiées les raisons de penser qu'il présente une menace pour la sécurité publique, la défense ou la sûreté de l'Etat. Dans un contexte marqué par des menaces graves et

persistantes pour la sécurité nationale, tenant en particulier au risque terroriste, une telle conservation présente une utilité sans équivalent par rapport au recueil de ces mêmes données à partir seulement du moment où l'individu en cause aurait été identifié comme susceptible de présenter une menace pour la sécurité publique, la défense ou la sûreté de l'Etat.

24. D'autre part, ainsi que l'a relevé la Cour de justice de l'Union européenne dans son arrêt du 21 décembre 2016, une telle conservation, dès lors qu'elle ne révèle pas le contenu d'une communication, n'est pas de nature à porter atteinte au " contenu essentiel " des droits consacrés par les articles 7 et 8 de la Charte. En outre, la Cour a depuis lors rappelé, dans son avis 1/15 du 26 juillet 2017, que ces droits " n'apparaissent pas comme étant des prérogatives absolues " et qu'un objectif d'intérêt général de l'Union est susceptible de justifier des ingérences, même graves, dans ces droits fondamentaux, après avoir relevé que " la protection de la sécurité publique contribue également à la protection des droits et des libertés d'autrui " et que " l'article 6 de la Charte énonce le droit de toute personne non seulement à la liberté, mais également à la sûreté ".

25. Dans ces conditions, la question de déterminer si l'obligation de conservation généralisée et indifférenciée, imposée aux fournisseurs sur le fondement des dispositions permissives de l'article 15, paragraphe 1, de la directive du 12 juillet 2002, ne doit pas être regardée, notamment eu égard aux garanties et contrôles, évoqués aux points 7 à 13, dont sont assortis les accès administratifs aux données de connexion et l'utilisation de celles-ci, comme une ingérence justifiée par le droit à la sûreté garanti à l'article 6 de la Charte des droits fondamentaux de l'Union européenne et les exigences de la sécurité nationale, dont la responsabilité incombe aux seuls Etats-membres en vertu de l'article 4 du traité sur l'Union européenne, soulève une première difficulté d'interprétation du droit de l'Union européenne.

Quant aux autres obligations susceptibles d'être imposées aux fournisseurs d'un service de communications électroniques :

26. Les dispositions de l'article L. 851-2 du code de la sécurité intérieure autorisent, pour les seuls besoins de la prévention du terrorisme, le recueil des informations ou documents prévus à l'article L. 851-1, auprès des mêmes personnes. Ce recueil, qui ne concerne qu'un ou plusieurs individus préalablement identifiés comme étant susceptibles d'être en lien avec une menace terroriste, s'effectue en temps réel. Il en va de même des dispositions de l'article L. 851-4 du même code, qui autorisent la transmission en temps réel par les opérateurs des seules données techniques relatives à la localisation des équipements terminaux. Il suit de là que ces techniques ne font pas peser sur les fournisseurs concernés une exigence de conservation supplémentaire par rapport à ce qui est nécessaire à la facturation de leurs services, à la commercialisation de ceux-ci et à la fourniture de services à valeur ajoutée. Par ailleurs, ainsi qu'il a été rappelé au point 15, les dispositions de l'article L. 851-3 du code de la sécurité intérieure n'impliquent pas davantage une conservation généralisée et indifférenciée.

27. Or, d'une part, il est constant que les accès en temps réel aux données de connexion permettent de suivre, avec une forte réactivité, les comportements d'individus susceptibles de représenter une menace immédiate pour l'ordre public. D'autre part, la technique prévue à l'article L. 851-3 du code de la sécurité intérieure permet de détecter, sur le fondement de critères précisément définis à cette fin, les individus dont les comportements, notamment compte tenu de leurs modes de communication, sont susceptibles de révéler une menace terroriste. Dans un contexte marqué par des menaces graves et persistantes pour la sécurité nationale, tenant en particulier au risque terroriste, ces techniques présentent ainsi une utilité opérationnelle sans équivalent.

28. D'autre part, ainsi que l'a relevé la Cour de justice de l'Union européenne dans son arrêt du 21 décembre 2016, une telle conservation, dès lors qu'elle ne révèle pas le contenu d'une communication, n'est pas de nature à porter atteinte au " contenu essentiel " des droits consacrés par les articles 7 et 8 de la Charte. En outre, la Cour a depuis lors rappelé, dans son avis 1/15 du

26 juillet 2017, que ces droits " n'apparaissent pas comme étant des prérogatives absolues " et qu'un objectif d'intérêt général de l'Union est susceptible de justifier des ingérences, même graves, dans ces droits fondamentaux, après avoir relevé que " la protection de la sécurité publique contribue également à la protection des droits et des libertés d'autrui " et que " l'article 6 de la Charte énonce le droit de toute personne non seulement à la liberté, mais également à la sûreté ".

29. Dans ces conditions, soulève une deuxième difficulté sérieuse d'interprétation du droit de l'Union européenne la question de déterminer si la directive du 12 juillet 2002 lue à la lumière de la Charte des droits fondamentaux de l'Union européenne doit être interprétée en ce sens qu'elle autorise des mesures législatives relevant d'activités concernant la sécurité publique, la défense et la sûreté de l'Etat telles que les mesures de recueil en temps réel des données relatives au trafic et à la localisation d'individus déterminés, qui, tout en affectant les droits et obligations des fournisseurs d'un service de communications électroniques, ne leur imposent pas pour autant une obligation spécifique de conservation de leurs données.

Quant à l'accès des autorités nationales compétentes aux données conservées :

30. Dans son arrêt du 21 décembre 2016, la Cour de justice de l'Union européenne a également dit pour droit que l'article 15, paragraphe 1, de la directive du 12 juillet 2002 " doit être interprété en ce sens qu'il s'oppose à une réglementation nationale régissant la protection et la sécurité des données relatives au trafic et des données de localisation, en particulier l'accès des autorités nationales compétentes aux données conservées, sans limiter, dans le cadre de la lutte contre la criminalité, cet accès aux seules fins de lutte contre la criminalité grave, sans soumettre ledit accès à un contrôle préalable par une juridiction ou une autorité administrative indépendante, et sans exiger que les données en cause soient conservées sur le territoire de l'Union. ". La Cour a, à cette occasion, estimé " qu'il importe que les autorités nationales compétentes auxquelles l'accès aux données conservées a été accordé, en informent les personnes concernées, dans le cadre des procédures nationales applicables, dès le moment où cette communication n'est pas susceptible de compromettre les enquêtes menées par ces autorités. En effet, cette information est, de fait, nécessaire pour permettre à celles-ci d'exercer, notamment, le droit de recours, explicitement prévu à l'article 15, paragraphe 2, de la directive 2002/58, lu en combinaison avec l'article 22 de la directive 95/46, en cas de violation de leurs droits ".

31. Soulève une troisième difficulté sérieuse d'interprétation du droit de l'Union la question de déterminer si la directive du 12 juillet 2002, lue à la lumière de la Charte des droits fondamentaux de l'Union européenne, doit être interprétée en ce sens qu'elle subordonne dans tous les cas la régularité des procédures de recueil des données de connexion à une exigence d'information des personnes concernées lorsqu'une telle information n'est plus susceptible de compromettre les enquêtes menées par les autorités compétentes ou si de telles procédures peuvent être regardées comme régulières compte tenu de l'ensemble des autres garanties procédurales existantes, dès lors que ces dernières assurent l'effectivité du droit au recours.

32. Les trois questions énoncées aux points 25 à 31 sont déterminantes pour la solution des litiges que doit trancher le Conseil d'Etat sur les quatre décrets attaqués en tant qu'ils ont été pris pour la mise en œuvre des articles L. 851-1 à L. 851-4 du code de la sécurité intérieure. Elles présentent, ainsi qu'il a été dit, plusieurs difficultés sérieuses d'interprétation du droit de l'Union européenne. Il y a lieu, par suite, d'en saisir la Cour de justice de l'Union européenne en application de l'article 267 du traité sur le fonctionnement de l'Union européenne et, jusqu'à ce que celle-ci se soit prononcée, de surseoir à statuer, dans cette mesure et sans qu'il soit besoin de statuer sur les fins de non-recevoir opposées en défense, sur les requêtes des associations requérantes et de rejeter le surplus de leurs conclusions.

[…]

Conseil d'Etat, 7 décembre 2017, *Avis sur un projet de loi d'adaptation au droit de l'Union européenne de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés,* n° 393836 (extraits). **Document n° 7**

[…]

1. Saisi le 17 novembre 2017 d'un projet de loi d'adaptation au droit de l'Union européenne de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, le Conseil d'Etat observe en premier lieu que la richesse et l'ampleur du règlement (UE) 2016/679 et de la directive (UE) 2016/680 du Parlement européen et du Conseil en date du 27 avril 2016 ne permettent pas de décrire leur contenu dans le présent avis sans risquer d'en méconnaître des aspects importants. Le Conseil d'Etat souhaite cependant attirer l'attention sur deux aspects majeurs des changements qu'apportent ce règlement et cette directive dans le mode d'intervention des pouvoirs publics pour protéger les libertés fondamentales lors du traitement des données personnelles, changements dont la bonne appréhension est essentielle à la compréhension des appréciations qu'il porte sur l'équilibre du projet de loi examiné.

Auparavant, une directive de 1995 visait à harmoniser des pratiques nationales écloses dans chaque Etat, la France en premier, au fur et à mesure des évolutions. Celles-ci ont conduit à la création dans chaque Etat membre d'une ou plusieurs autorités de contrôle, aux pouvoirs inégaux d'un pays à l'autre, coordonnées par un groupe les réunissant, dénué de pouvoirs propres. Le régime de supervision des traitements reposait sur des prohibitions absolues, tempérées par un système de formalités préalables allant de la déclaration du traitement, jusqu'à son autorisation sous de strictes contraintes de procédure et de fond, proportionnées au degré d'atteinte portée par le traitement aux libertés.

Le nouveau régime opère un renversement complet des logiques antérieures.

Le champ des données à traiter ne comporte plus que de rares prohibitions absolues et invite à raisonner en termes de risques d'atteinte aux libertés et droits fondamentaux. La charge de cette analyse n'est plus définie a priori par le législateur, imposant des contrôles progressivement durcis, mais incombe aux responsables du traitement. Ces derniers devront mener une analyse critique réalisée par un délégué à la protection des données, interne à l'organisation mais indépendant qui, chargé de faire respecter le règlement, la directive et les textes pris pour leur application, est désormais le pivot de leur respect. Dans le cas où un traitement a des effets potentiels graves, l'autorité de contrôle est saisie. Son rôle est désormais d'abord de déterminer de bonnes pratiques, en liaison avec les responsables, et de définir des référentiels, pour encadrer la création des traitements les plus communs et les harmoniser. Pour assurer le bon fonctionnement du système, l'autorité de contrôle est dotée de pouvoirs d'investigation et de sanctions renforcés.

[…]

3. Ces évolutions significatives invitent à la plus grande vigilance d'abord dans la charge qui est désormais transférée sur les responsables de traitement : le coût économique de celle-ci, comme la responsabilité accrue qui leur est donnée, avec les risques qu'elle comporte, demandent que la loi soit la plus précise et la plus claire pour assurer un environnement robuste à leur prise de décision. Il faut assurer en même temps le maintien d'un standard élevé de protection, non seulement par l'usage, le cas échéant, des facultés reconnues aux Etats par leur droit interne de renforcer les contrôles (par exemple par des autorisations a priori), mais aussi par l'adoption des règles qui, pour relever du droit souple, doivent être claires et rigoureuses : les évolutions permises par le contrôle juridictionnel en la matière contribueront à l'atteinte de cet objectif.

La cohérence de la mise en œuvre du droit de l'Union sur l'ensemble de son territoire est également essentielle à son plein effet. Elle ne sera atteinte que par une claire répartition des compétences entre autorités, selon les critères fixés par le règlement et rappelés ci-dessus. Elle dépend aussi de la fidélité

des droits nationaux aux règles posées par le règlement et la directive qui, en dépit des nombreuses marges de manœuvre laissées aux Etas-membres, doivent construire un standard européen homogène et ambitieux, capable d'influencer de bonnes pratiques au niveau mondial. Le Conseil d'Etat y veille particulièrement à l'occasion de son examen.

[…]

36. Le Gouvernement entend user, au profit des traitements mis en œuvre par l'Etat, de la faculté que lui reconnaît l'article 23 du règlement (UE) 2016/679 de déroger à la plupart des droits garantis au profit des destinataires d'un traitement pour des motifs d'intérêt général largement définis, à condition d'entourer cette dérogation des garanties nécessaires la préservation des droits et libertés fondamentales.

Mais la simple reproduction, au demeurant incomplète, du dispositif de l'article 23 du règlement de l'Union apparaît au Conseil d'Etat comme étant à la fois inutile et incertaine. Elle risque surtout d'entacher d'incompétence négative l'intervention du législateur en renvoyant trop généralement à des dispositions réglementaires pour définir les droits reconnus aux personnes concernées.

Le Conseil d'Etat écarte pour ces motifs les dispositions envisagées, mais il admet en revanche un premier cas de mise en œuvre de la faculté de l'article 23 : pour les seuls traitements répondant à une obligation légale, et aux seules fins de protection de la sécurité nationale, de la défense nationale ou de la sécurité publique, le seul droit à être informé des violations d'un traitement de données personnelles, régi par l'article 34 du règlement, peut être restreint par l'acte créant ce traitement. L'effet concret de ces dispositions est de permettre aux responsables du traitement de ne pas prévenir la personne dont les données ont fait l'objet d'une violation par un tiers dans des conditions mettant en cause, à raison de données ou à raison de l'emploi de la personne (par exemple s'il s'agit d'un agent des forces de sécurité ou d'un militaire), la sécurité ou la défense, afin de mieux assurer la lutte contre les auteurs de ces violations. L'intervention du législateur pour aménager une garantie à l'exercice des libertés publiques est justifiée. Elle est suffisamment précise pour permettre un contrôle de l'adéquation de la restriction aux finalités poursuivies.

[…]

47. S'agissant des traitements relevant à la fois du champ de la directive et de celui du règlement, ce double régime paraît complexe à mettre en œuvre pour les droits des personnes concernées. Le Conseil d'Etat relève en effet qu'existent deux droits prévus par le règlement et absents de la directive : le droit à l'oubli (article 17 du règlement) et le droit à la portabilité des données (article 20 du règlement). Dans les deux cas, le règlement prévoit que ces droits ne sont pas applicables, lorsque le traitement est nécessaire « *à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement* ». Ces droits devraient donc être inapplicables aux traitements de données dont les finalités sont mixtes. Les autres droits des personnes concernées (information, accès, opposition…) sont plus ouverts dans le règlement que dans la directive. Le Conseil d'Etat estime que, dès lors que les données sur lesquelles la personne concernée demande à exercer ses droits ne pourront pas être exclusivement rattachées soit aux finalités prévues par la directive, soit aux autres finalités du traitement de données, il convient que l'acte ayant autorisé le traitement de données à finalités mixtes s'appuie sur l'article 23 du règlement, qui permet une diminution de la portée des droits de la personne concernée sous plusieurs conditions, dont la sécurité publique et la préservation des procédures pénales, afin de déterminer un régime des droits des personnes concernées cohérent pour l'ensemble des données traitées pour les diverses finalités. Pour être conforme aux exigences du second paragraphe de l'article 23 du règlement, les dispositions apportant de telles limitations doivent être précises et ne sauraient prendre la forme d'habilitations générales.

[…]

Protection des données personnelles - La réforme de la protection des données en voie de finalisation - Focus par Laurence IDOT

Document: Europe n° 5, Mai 2016, alerte 32

Europe n° 5, Mai 2016, alerte 32

La réforme de la protection des données en voie de finalisation

Focus par Laurence IDOT professeur à l'université Panthéon Assas (Paris 2) Collège européen de Paris

Les obstacles ont été levés ! Dans la foulée de l'accord informel intervenu à la fin de l'année dernière, après le Conseil qui a donné son accord final sur le paquet le 8 avril, le Parlement européen a adopté définitivement la réforme de la protection des données, le 14 avril 2016. Les propositions de la Commission remontaient à janvier 2012. Partant du constat que la directive 95/46/CE avait été conçue à une époque où Internet en était encore à ses débuts, la Commission proposait de réformer fondamentalement ce cadre juridique (V. *communication, « Protection de la vie privée dans un monde en réseau. Un cadre européen relatif à la protection des données, adapté aux défis du 21ème siècle », COM (2012) 9 final, 25 janv. 2012*). Le paquet présenté comportait deux textes : une proposition de règlement (...) relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données (*COM (2012) 11 final*) et une proposition de directive (...) relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel 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, et à la libre circulation de ces données (*COM (2012)10 final*). Le contenu a été âprement débattu puisque ce paquet est celui de tous les records : le nombre total d'amendements s'élève à 3999, soit le plus grand nombre d'amendements déposés pour un seul dossier législatif (V. les faits et chiffres dans le dossier, Q & R, du Parlement). Il faut cependant relever que le règlement de plus de 200 pages est un texte particulièrement touffu.

L'objectif est bien sûr d'actualiser et d'approfondir les principes de la directive 95/46/CE, dont le fondement reste le principe de la reconnaissance d'un droit à la protection des données personnelles. Les innovations sont doubles. Sur le plan substantiel, en-dehors d'un renforcement de l'information, y compris en cas de piratage des données, l'objectif est de conférer aux personnes une plus grande maîtrise de l'utilisation qui sera faite de leurs données à caractère personnel et d'en faciliter l'accès. Les nouvelles règles les plus emblématiques concernent le droit à l'oubli numérique, le droit à la portabilité des données, la limitation du recours au profilage. Le règlement a également pour conséquence de renforcer les obligations sur les entreprises qui traitent des données personnelles, qui auront, à l'exception des PME, l'obligation de désigner un responsable de la protection. Mais sur le fond, l'on passe d'un régime de notification préalable à un système que l'on pourrait qualifier d'autoévaluation. Des sanctions élevées sont prévues, puisqu'elles pourront aller jusqu'à 4 % du chiffre d'affaires mondial des entreprises. Le changement est tout aussi important sur le plan institutionnel. L'adoption d'un règlement permet de substituer une seule législation aux 28 droits nationaux actuellement applicables. L'unité de législation n'étant pas suffisante, un système de guichet unique a été mis en place. L'objectif est que les entreprises soient soumises à une autorité de contrôle unique, celle du lieu de leur siège, ce qui n'empêche pas l'action conjointe de plusieurs autorités avec une autorité chef de file lorsque le responsable du traitement est établi dans plusieurs États membres. Le maintien de la cohérence de l'ensemble est assuré par le comité européen de la protection des données. Au final, l'on retrouve des évolutions comparables à celles que l'on a connu en droit antitrust avec le règlement (CE) n° 1/2003.

Le deuxième élément du paquet, la directive, vise à remplacer la décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale (*JOUE n° L 350, 30 déc. 2008*), dont le champ est limité puisqu'elle s'applique uniquement aux traitements transfrontières de données, et non aux traitements effectués par les autorités policières et judiciaires au niveau strictement national. Tout en élargissant le champ d'application, le nouveau texte garantit la protection des données à caractère personnel des personnes impliquées dans une procédure pénale, que ce soit en qualité de témoin, de victime ou de suspect, mais facilite également l'échange d'informations entre les autorités policières et judiciaires nationales, pour améliorer la coopération dans la lutte contre le terrorisme et les autres formes graves de criminalité en Europe.

Ces différents textes, qui requièrent une étude approfondie, seront bientôt publiés au JOUE. Un délai de deux ans est prévu tant pour la transposition de la directive, que pour l'application du règlement. Mais plus que l'application dans le temps, l'une des questions cruciales illustrée en dernier lieu par l'arrêt *Schrems* (*CJUE, gde ch., 6 oct. 2015, aff. C-362/14 : Europe, 2015, comm. 468*), qui a été suivi d'une communication de la Commission (*COM (2015) 566 final, 6 nov. 2015*) sur les conséquences à en tirer dans l'attente de la mise en place du nouveau cadre juridique, est celle de la portée territoriale du dispositif. Dans cette optique, l'on ne manquera pas de relever que, le même jour, soit le 14 avril 2016, le Parlement européen a adopté en première lecture la proposition de directive « relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière », dite PNR, dont l'origine est plus ancienne puisqu'elle remonte à 2011 (*COM (2011) 32 final, 2 févr. 2011*) et qui était présentée parfois comme un « serpent de mer ». L'objectif de parvenir à adopter le texte définitif avant la fin de l'année 2015 n'a pas été atteint (V. *Europe, 2015, alerte 6*), mais ce sera peut-être pour 2016. Qu'on les envisage à des fins économiques, ou à des fins de prévention de la criminalité, les données sont partout...