COMMISSION
DES AFFAIRES
EUROPÉENNES

Conséquences de l'arrêt de la Cour de justice *Quadrature du net* sur la lutte contre le terrorisme et la criminalité

Communication de
Mme Aude Bono-Vandorme (LaREM)
et Mme Marietta Karamanli (SOC)
Mercredi 26 mai 2021

Mesdames les Présidentes,
Mesdames et Messieurs,

Nous sommes ravies de retrouver nos collègues de la commission de la défense pour aborder ce sujet européen, qui intéresse bien au-delà des habituels commentateurs de la vie institutionnelle bruxelloise et a fait l'objet d'une couverture médiatique assez importante pour un sujet d'articulation de normes.

Le 6 octobre 2020, la Cour de justice de l'Union européenne a rendu deux décisions complétant sa jurisprudence sur la protection des données à caractère personnel.

Celle qui nous intéresse au premier chef répond à une série de **questions préjudicielles du Conseil d'État** français, saisi par des associations de défense des libertés sur internet, notamment *La Quadrature du Net*. La saisine porte sur le régime de conservation, par les opérateurs de télécom, fournisseurs d'accès à internet et intermédiaires techniques du web, des données de connexion des utilisateurs. Il est actuellement prévu par la loi française que ces **métadonnées** sont conservées pendant un an.

Notre ambition a été de comprendre les conséquences de la jurisprudence récente de la Cour de justice, qui porte sur une matière complexe et entourée de beaucoup de secret, afin de vous en restituer les principaux enjeux. Ce faisant, nous avons constaté une ligne de partage très nette entre partisans des libertés numériques et préoccupations des services opérationnels de plusieurs États, en particulier en France.

Le Conseil d'État, qui a rendu le 21 avril 2021 une décision de 39 pages – une longueur inhabituelle – a choisi une position nuancée mais qui prend des distances claires avec certaines analyses des juges de Luxembourg. Nous avons souhaité expliquer les sous-jacents, les raisons et les conséquences de ces différents arrêts. Ici, la matière juridique est au carrefour d'enjeux politiques et opérationnels d'une actualité très vive.

Nous ne prétendrons pas ici à l'exhaustivité, mais à attirer l'attention sur les points qui nous semblent importants pour la bonne compréhension de ce qui s'est joué au Palais Royal le mois dernier.

I. L'ARRÊT DE LA COUR DE JUSTICE, BIEN QUE S'INSCRIVANT DANS UNE SUITE JURISPRUDENTIELLE LOGIQUE, ENTRAÎNE DES CONSÉQUENCES IMPORTANTES ET PARTICULIÈRES POUR LA FRANCE

Cet arrêt a été très largement commenté et parfois vivement critiqué. Il s'inscrit néanmoins dans une suite jurisprudentielle qui a déjà plusieurs années.

A. La protection des données personnelles par la Cour de justice

Si la conservation générale et indifférenciée des données de connexion était auparavant bien rendue possible par un instrument de droit européen, à savoir une directive de 2006(1), la Cour de justice a annulé cet instrument dans un arrêt retentissant de 2014, *Digital Rights Ireland*(2). Elle considère, dans cette décision de Grande Chambre, que le dispositif européen n'est pas assorti de garanties suffisantes pour la garantie de la vie privée des personnes.

Dans un autre arrêt non moins commenté de 2016, *Tele2*, *Sverige*(3), qui est la suite logique du précédent, la Cour juge qu'une législation nationale prévoyant une conservation générale et indifférenciée des données à des fins d'enquête et de répression des infractions pénales est également contraire au droit de l'Union. À ce moment, la Cour ne se prononce pas encore sur la question de l'utilisation de ces données à des fins de renseignement.

Ainsi, l'arrêt du 6 octobre 2020 intervient dans un contexte où il devient clair que la Cour de justice construit une jurisprudence volontariste dans le domaine de la protection des données et de la vie privée des citoyens, en témoignent les décisions rendues dans d'autres affaires très connues : *Google Spain, Schrems* ou encore sur le *Passenger Name Record* (PNR).

Dans cet arrêt *Quadrature du Net*, la Cour confirme que le droit de l'Union s'oppose à des mesures législatives prévoyant, à titre préventif, la **conservation généralisée et indifférenciée** des données relatives au trafic et des données de localisation. Sur ce point, elle réitère simplement sa jurisprudence antérieure.

(1) Directive 2006/24/CE du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE.
(2) Cour de justice [GC], Digital Rights Ireland, 8 avril 2014, C-293/12.
(3) Cour de justice [GC], Tele2 Sverige, 21 décembre 2016, C-203/15.

Elle précise également le contour des **exceptions** dans lesquelles la conservation massive des données est autorisée :

D'abord, une conservation généralisée et indifférenciée des données est possible pour une durée limitée au strict nécessaire **en cas de menace grave pour la sécurité nationale**[(4)] .

Une **conservation ciblée** des données peut être délimitée en fonction de catégories de personnes ciblées ou au moyen d'un critère géographique.

Le **recueil en temps réel des données** de connexion, particulièrement attentatoire à la privée, doit selon la Cour de justice être limité aux personnes dont on soupçonne qu'elles sont impliquées dans des activités de terrorisme, et soumis à un contrôle préalable.

Ces exceptions sont décrites comme **très insuffisantes** pour permettre aux services de renseignement et aux enquêteurs de maintenir leurs capacités actuelles de lutte contre le terrorisme et la criminalité. Elles conduiraient de facto à limiter les outils à leur disposition.

Si la France, à l'instar de quatorze autres États membres, est intervenue à l'audience devant la Cour de justice sur cette affaire, c'est parce qu'elle est concernée au premier chef par cette question juridique.

La décision *Quadrature du Net* est rendue sur question préjudicielle **renvoyée par le Conseil d'État français**. En effet, le droit français prévoit que cette obligation de conservation des métadonnées pesant sur les fournisseurs de services porte sur une durée d'un an.

Les garanties qui visent concrètement à protéger les citoyens d'une utilisation abusive que feraient les pouvoirs publics de leurs données résident essentiellement dans les **conditions d'accès** aux données, entourées de garanties légales. La Cour de justice, quant à elle, considère que c'est insuffisant, dans la mesure où **la conservation des données serait par elle-même attentatoire à la vie privée** des personnes.

(4) Ainsi que, dans ces mêmes conditions, le recours à l'analyse automatisée des données de l'ensemble des utilisateurs de moyens de communications électroniques,

B. Les conséquences sur les services opérationnels

Nous avons pu constater que cette décision n'a pas laissé les **services opérationnels** indifférents. L'arrêt de la Cour de justice a des conséquences nettes sur deux volets que nous traiterons du plus évident au plus nuancé : le renseignement d'abord, et le pénal ensuite.

En ce qui concerne les missions de défense et de promotion des intérêts fondamentaux de la Nation confiées aux services de renseignement : cette remise en cause de la conservation des donnés pendant un an risque de pénaliser leur activité. C'est une idée qui nous a été clairement exposée, entre autres, lors de la table ronde tenue par nos deux commissions le 17 mars 2021.

Pouvoir retrouver les données de connexion peut servir deux objectifs essentiels : identifier une personne pour la rattacher à des faits connus, ou rechercher les agissements passés d'une personne qu'on a déjà identifiée. Il y a deux arguments principaux qui portent respectivement sur la méthode et sur la taille des enjeux.

D'abord, dans le cadre spécifique du travail des services de renseignement, pouvoir rechercher ces données dans le passé est d'autant plus important que le passage à l'acte peut être très rapide, ne permettant pas d'identifier suffisamment en amont les personnes à surveiller.

Par ailleurs, l'importance des enjeux liés à la sécurité nationale dont les services de renseignement ont à connaître justifie des ingérences dans les droits fondamentaux, au rang desquels le droit à la vie privée et à la protection des données personnelles, si ces atteintes sont nécessaires et proportionnées.

De fait, en permettant une conservation des données générale et indifférenciée, quoique temporaire, dans les cas de menace grave et avérée pour la sécurité nationale, la Cour de justice a fait un pas vers l'assouplissement de sa position en direction des pays, comme la France, qui sont soumis à un haut niveau de menace terroriste.

En ce qui concerne la recherche, la constatation et la poursuite des infractions, notamment pénales, qui est le second volet de cet arrêt, il faut rappeler que les données de connexion sont aussi mobilisées dans le cadre **judiciaire**.

Dans le contexte des enquêtes de police, il est fait une utilisation quasi systématique des données de connexion. Là encore, ces données peuvent servir à identifier l'auteur d'une infraction, ou de prouver la participation d'une personne identifiée à la commission d'une infraction.

Les données de connexion sont utilisées pour pallier les faiblesses des méthodes d'enquête traditionnelles, comme la filature, ou de la recherche de preuves scientifiques, comme les traces d'ADN. Les données de connexion sont une ressource précieuse qui, combinée à d'autres éléments, peut permettre de constituer le faisceau d'indices permettant de donner une valeur probante aux enquêtes.

Cette pratique des services français amène naturellement à s'interroger sur celles des autres États membres, également soumis à la décision de la Cour de justice, afin d'apporter des **éléments de comparaison**. Il faut en effet rappeler que l'interprétation donnée dans les arrêts en cause, bien que répondant à des questions préjudicielles française et belge, s'impose dans toute l'Union européenne.

À cet égard, les situations sont contrastées. Les quatorze États étant intervenus à l'audience ont plaidé dans le même sens que la France, en arguant de la nécessité opérationnelle des données de connexion.

Cependant, ils n'ont pas tous les mêmes pratiques. Le droit allemand impose par exemple, depuis 2015, une rétention de 4 et 10 semaines respectivement pour les données de localisation et de connexion, soit une durée bien inférieure à la France. Ce sont ces points de comparaison qui nous amènent à questionner l'équilibre général du dispositif législatif.

Par ailleurs, certains États membres ont d'ores et déjà français adapté leur législation nationale à la suite de l'arrêt *Tele 2* pour mettre fin à la conservation généralisée et indifférenciée des données. C'est le cas de la Suède, de la Roumanie ou encore de l'Autriche. Il est par définition malaisé de mesurer la part des enquêtes qui ne sont pas résolues du fait d'un outil manquant. Néanmoins, la fin de l'obligation légale de conservation des données rend les services de l'État qui en ont l'usage dépendants de la transmission des informations par les entreprises privées. De fait, l'affaiblissement de leur capacité d'action est incontestable.

II. LE CONSEIL D'ETAT CHOISIT UNE POSITION EN DEMI-TEINTE QUI GARANTIT LA CONTINUITÉ DES PRATIQUES FRANÇAISES EN MATIÈRE DE CONSERVATION DES DONNÉES DE CONNEXION

Dans ce contexte à fort enjeu, qui lui a été largement exposé dans le cadre des audiences d'instruction orales, le Conseil d'État a rendu un arrêt d'assemblée le 16 avril 2021 qui garantit, pour l'heure et pour l'essentiel, la continuité des pratiques françaises.

A. Un arrêt audacieux qui ménage des réserves au regard de l'interprétation de la Cour de justice

Cet arrêt ménage en effet des réserves au regard de l'interprétation de la Cour de justice, par un arbitrage délicat entre souveraineté constitutionnelle et respect de la primauté du droit de l'Union. Le Conseil d'État se pense et s'analyse en effet comme un acteur du dialogue des juges et des réseaux européens.

Tout d'abord, le Conseil d'État, suivant en cela le rapporteur public, refuse d'accueillir l'argument du Gouvernement qui avançait l'incompétence de la Cour de justice lorsque la conservation des données est mise au service de la sécurité nationale. Cet argument, fondé sur le périmètre de l'article 4 du Traité sur l'Union européenne (TUE), devait conduire à un périlleux **contrôle de l'*ultra vires* auquel la juridiction française refuse de se livrer.**

Cependant, l'invocation, par le Gouvernement, de l'identité constitutionnelle de la France, a été partiellement suivie par le Conseil d'État, bien que le rapporteur public ait appuyé la nécessaire prudence dans le maniement de ce concept. Empruntant la voie de crête qu'il s'était déjà ménagée en 2007 dans son arrêt Arcelor(5), le juge national s'autorise à vérifier que le respect du **droit européen, tel qu'interprété par la CJUE, ne compromet pas les exigences constitutionnelles françaises** de sauvegarde des intérêts fondamentaux de la Nation, de prévention des atteintes à l'ordre public et de recherche des auteurs d'infractions pénales – trois louables objectifs servis par la conservation des données de connexion.

C'est parce qu'il considère que ces principes ne bénéficient pas, en droit de l'Union, d'une protection équivalente à celle garantie par la Constitution, qu'il s'éloigne de la lettre de la décision rendue par la Cour de justice. Il étudie aussi le caractère opérationnel ou non, réaliste ou non, des exceptions prévues par la Cour de justice. Étudiant l'hypothèse de conservation ciblée des données considérée comme conforme au droit européen par la Cour de justice, il conclut à son impraticabilité – il est impossible de prévoir la commission des crimes, à moins de sombrer dans la définition hasardeuse et potentiellement très discriminatoire de personnes et de zones géographiques à surveiller.

Le Conseil d'État, s'il a entendu les arguments du Gouvernement dans sa position de défendeur, **fait droit à certaines demandes des requérants**. D'abord, sa décision a pour effet de contraindre le Gouvernement à réévaluer régulièrement la menace qui pèse sur le territoire si cette menace est mobilisée pour justifier la conservation généralisée et indifférenciée des données. Néanmoins, aucun lien n'est établi entre cette situation de menace et, par exemple, un état d'urgence soumis au contrôle du Parlement.

(5) Conseil d'État Ass., 8 février 2007, *Société Arcelor Atlantique et Lorraine et autres*.

Il demande également de subordonner l'exploitation de ces données par les services de renseignement à l'autorisation d'une autorité indépendante. Le cadre juridique actuel, qui résulte de la loi relative au renseignement de 2015, impose des garanties matérielles et procédurales qui encadrent étroitement l'accès des services aux données de connexion, comme contrepartie à une conservation très large. Cependant, le Conseil d'État considère que le contrôle exercé actuellement par la Commission nationale de contrôle des techniques de renseignement (CNCTR), qui rend des avis simples sur les demandes d'accès, n'est pas suffisant, même s'il est en pratique suivi par le Premier ministre. Pour l'avenir, il devra être rendu contraignant.

Dans son arrêt, le Conseil d'État accorde un **délai de six mois** au Premier ministre pour adapter le cadre règlementaire à ses diverses exigences, ce qui permettra en tout état de cause d'éviter une transition trop brusque entre un avant et un après, qui était très redoutée.

Le Gouvernement a tiré les conséquences de cet arrêt par une lettre rectificative datée du 12 mai au projet de loi relatif à la prévention d'actes de terrorisme et au renseignement, présenté en conseil des ministres le 28 avril 2021.

Bien que la décision impose, sur certains aspects, une adaptation du droit français, elle maintient le statu quo sur l'essentiel et place, en cela, la France dans une position singulière.

Rappelons que les arrêts du 6 octobre 2020 portant sur des questions préjudicielles françaises et belges, il semble indispensable de s'arrêter sur la solution retenue par la **Cour constitutionnelle belge** dans son arrêt du 22 avril 2021[(6)], rendu en miroir une semaine après celui du Conseil d'État. Pourtant, les juges belges tirent des conséquences différentes du même arrêt de la Cour de justice.

En particulier, la juridiction constitutionnelle constate que l'arrêt de la CJUE impose un changement de perspective par rapport au choix du législateur belge – ou du législateur français. **L'obligation de conservation des données de communications électroniques doit être l'exception, et non la règle**. Elle annule les dispositions législatives imposant la conservation généralisée et indifférenciée en Belgique.

Ces différences de position entre deux pays aux traditions juridiques pourtant extrêmement proches et aux enjeux sécuritaires pour le moins convergents doit nécessairement interroger. Dans un espace de droit intégré comme se veut l'Union européenne, il est surprenant que coexistent des divergences quant à la lecture des décisions des juges de Luxembourg, cour suprême de cet ordre juridique inédit.

(6) Cour constitutionnelle belge, 22 avril 2021, n° 57/2021.

B. Une décision qui place la France dans une position singulière

Au-delà des raffinements juridiques, qui intéressent surtout les juristes, cette décision du juge administratif suprême, qui répond à une demande explicite du Gouvernement, prête le flanc à des **critiques de nature plus politique**.

La France se singularise par rapport à d'autres États membres ayant choisi une position proactive de mise en conformité avec la jurisprudence de la CJUE. Si l'on regarde du côté des autorités allemandes, elles sont actuellement en attente de la décision sur l'affaire *SpaceNet*, pendante devant la Cour de justice, sur renvoi du *Bundesverwaltungsgericht*, (cour suprême de l'ordre administratif, qui siège à Leipzig). Tant que cette décision n'est pas rendue, l'Allemagne a suspendu sa législation relative à la conservation des données.

Si le spectre de la condamnation en manquement d'État du fait d'une décision de justice semble raisonnablement éloigné, le message demeure celui d'une **divergence**, à l'heure où l'exemplarité est un atout pour faire appliquer les principes de l'État de droit partout en Europe.

Pour conclure, rappelons que cette question qui semble seulement technique est en réalité très politique. L'équilibre entre sécurité et libertés est au cœur des débats qui agitent les sociétés démocratiques au XXI^{e} siècle, confrontées à la criminalité ordinaire, mais aussi à des formes de violence nouvelles doublées de modes opératoires innovants. Les outils numériques sont, pour la sécurité de nos concitoyens, à la fois le poison et le remède : ils permettent aux malfaiteurs d'échapper à la surveillance, comme aux enquêteurs de résoudre bien des enquêtes qui seraient restées muettes il y a quelques décennies. L'enjeu est celui d'un juste compromis animé par le pragmatisme, le sens de la mesure et l'attention portée aux dérives illibérales.

Le projet de loi relatif à la prévention d'actes de terrorisme et au renseignement, qui sera examiné à l'Assemblée nationale dans les semaines à venir, apporte de nouveaux éléments à ce débat. Ce travail sur les données de connexion nous aura permis de mesurer que, face à ces sujets complexes, le temps de la réflexion et de l'assimilation est nécessaire. Ce temps peut manquer lorsque le Parlement est contraint par la procédure d'urgence.

* *

*

ANNEXE
COMPTE RENDU DES DEBATS EN COMMISSION

Mme la Présidente Sabine Thillaye. Je vous remercie pour votre travail très intéressant, qui montre une fois de plus combien l'Union européenne intervient dans divers domaines liés les uns aux autres. Il rappelle également l'interdépendance entre les juridictions européennes et les juridictions nationales qui, on l'oublie souvent, appliquent aussi le droit européen. Enfin, il montre à quel point la Cour de justice de l'Union veille à l'harmonisation de l'application de ce droit, en tentant compte des identités constitutionnelles des États membres.

M. Christophe Lejeune. Le 21 avril 2021, le Conseil d'État a rendu un arrêt relatif à la conservation des données électroniques dans le cadre de la lutte contre les menaces affectant la sécurité nationale. Il a été saisi par plusieurs associations, dont Quadrature du Net, sur la conformité de la législation française au droit européen, ce qui lui a également permis de vérifier que l'application du droit européen ne compromettait pas les exigences constitutionnelles françaises. L'arrêt de la Cour de justice, s'il a rappelé que la conservation généralisée et indifférenciée des données était une atteinte au droit à la vie privée, a néanmoins admis une nouvelle exception, en cas de menace grave, actuelle ou prévisible pour la sécurité nationale. Ainsi, le Conseil d'État a jugé qu'une telle conservation était possible compte tenu de la menace terroriste pesant sur la France depuis 2015, pour autant que l'existence de cette menace soit prouvée chaque année. Par ailleurs, il a jugé illégale une telle conservation pour des besoins autres que ceux de la sécurité nationale. Enfin, l'avis de la commission nationale de contrôle des techniques de renseignement, dont l'avis était consultatif, devient obligatoire.

Nous savons tous que, pour les services de renseignement, ces données sont essentielles afin de lutter contre le terrorisme. Pouvez-vous nous dire comment ils ont accueilli cet arrêt ?

Mme Marguerite Deprez-Audebert. Avec l'arrêt rendu par le Conseil d'État le 21 avril 2021, on mesure l'importance politique et juridique de concilier le respect de la vie privée avec la lutte contre la criminalité et le terrorisme. Le Conseil d'État s'est appuyé sur la clause de sauvegarde qui stipule que dans le cas d'une directive ou d'un règlement européen ayant pour effet de priver de garantie effective une exigence de nature constitutionnelle sans protection équivalente en droit européen, le juge administratif doit l'écarter dans la stricte mesure qu'exige le respect de la Constitution. Le Conseil d'État semble avoir ainsi répondu aux attentes du gouvernement qui s'était appuyé sur plusieurs dispositions constitutionnelles, dont la sauvegarde des intérêts fondamentaux de la nation.

Néanmoins, il ordonne au gouvernement de réévaluer chaque année la menace qui pèse sur le territoire pour justifier la conservation généralisée des données et subordonne leur utilisation au contrôle d'une autorité indépendante. Dès lors, cet arrêt méconnaît-il la primauté du droit européen ou, au contraire, évite-t-il de s'interroger sur le respect de la répartition des compétences entre l'Union et ses membres ?

Mme Liliana Tanguy. La communication de la Commission européenne de décembre dernier sur le programme de lutte anti-terroriste pour l'Union européenne souligne la nécessité d'une coopération policière et en matière d'échange d'informations. Nous ne pourrons pas lutter efficacement contre le terrorisme sans coopération au sein de l'Union européenne. C'est cette conviction qui m'avait conduite à recommander la création d'un parquet européen anti-terroriste dans mon rapport de novembre dernier portant observations sur le projet de loi relatif au Parquet européen et à la justice pénale spécialisée. Les informations de connexion permettant l'identification de l'utilisateur occupent une place centrale dans une grande partie des enquêtes menées en matière de terrorisme. En France, en 2020, la justice a effectué près de 2,5 millions de requêtes auprès des opérateurs afin d'obtenir les données de connexion de personnes faisant l'objet de procédures judiciaires.

La Commission propose de collaborer avec les États membres afin de déterminer les solutions juridiques, opérationnelles et techniques pour assurer un accès licite à ces informations, tout en préservant l'efficacité du cryptage des données relatives à la vie privée. Comment l'Union européenne pourrait-elle concilier son programme de lutte contre le terrorisme et favoriser l'échange d'informations tout en respectant sa jurisprudence protégeant la vie privée en ligne des Européens ?

Mme Aude Bono-Vandorme, rapporteure. L'arrêt du Conseil d'État a été accueilli avec un grand soulagement par la communauté du renseignement, après la forte inquiétude que nous avions perçue lors de nos auditions sur les conséquences de la décision de la CJUE. Celle-ci pouvait faire craindre un bouleversement total des pratiques du renseignement français, susceptible de porter atteinte à ses capacités opérationnelles dans un contexte de menace terroriste élevée.

Le Conseil d'État a maintenu en grande partie la possibilité de recourir aux données de connexion, aussi longtemps qu'il existe une menace pour la sécurité nationale. En contrepartie, le gouvernement est tenu de réévaluer cette menace tous les ans. Cela témoigne de la soumission croissante des services de renseignement au droit depuis 2015.

Mme Marietta Karamanli, rapporteure. Je confirme qu'une partie des membres des services auditionnés était très inquiète des conséquences de la décision de la CJUE, qui remettait en cause leurs pratiques et leurs habitudes.

La semaine dernière, le président de la Cour de justice a rappelé que la Cour n'était pas là pour embêter les services, mais pour rappeler le droit de l'Union, qui est supérieur au droit national.

Les différents États saisissent la Cour pour confronter les pratiques des différents États membres et vérifier qu'ils respectent bien le droit de l'Union. La France a plaidé sa cause auprès de la Cour de justice, qui a introduit une exception en matière de terrorisme. Il ne s'agit pas de conserver les données constamment, mais sur une période qui soit liée à une exception, le terrorisme.

Le Conseil d'État a pris en compte les différentes inquiétudes et demandé que la menace qui pèse sur le territoire soit réévaluée régulièrement pour vérifier si la conservation généralisée et indifférenciée des données reste justifiée.

Il est important de rappeler la primauté du droit de l'Union européenne. Ce n'est pas la Cour qui est venue imposer le droit de l'Union, ce sont les États qui ont choisi de se soumettre à un droit de l'Union supérieur au droit national.

Le combat pour construire le parquet européen a commencé il y a vingt ans. C'est seulement par le texte voté en début d'année que nous avons harmonisé notre droit avec le règlement européen. Nous avons toujours dit que les compétences dont il est doté aujourd'hui n'étaient pas suffisantes ; il ne faut pas se limiter aux intérêts financiers de l'Union européenne, mais prendre en compte aussi d'autres intérêts qui concernent tous les pays, comme la criminalité, le terrorisme et la traite des êtres humains.

L'échange d'informations est essentiel pour lutter contre la criminalité ; la coopération entre États est indispensable. On ne peut pas se contenter de partager les informations entre services d'un même État sans regarder comment nous pouvons coopérer avec d'autres États membres qui appliquent le même droit de l'Union européenne et sont confrontés aux mêmes problématiques.

Mme Aude Bono-Vandorme, rapporteure. Le recours à des applications de messagerie cryptées se développe de plus en plus et les communications sont de plus en plus difficiles à intercepter. C'est tout l'intérêt des métadonnées, qui renseignent sur qui parle à qui, quand et comment, et non sur le contenu du message.

Pour favoriser la coopération entre les services de renseignement, je rappelle le rôle central d'Europol, en particulier du centre européen de la lutte contre le terrorisme. Il fait office de plateforme d'échange des informations entre des services qui sont souvent réticents à ce partage.

Mme Marietta Karamanli, rapporteure. Je rappelle que nous avions obtenu un contrôle des parlements nationaux sur Europol, ce qui est important pour construire la confiance des citoyens.

J’insiste sur un élément important de l’arrêt du Conseil d’État, qui est l’obligation de recourir à une autorité indépendante pour autoriser l’exploitation des données par les services de renseignement.

Mme la Présidente Sabine Thillaye. Le principe de la primauté du droit de l’Union reste fragile, parce qu’il ne figure pas dans les traités. Il figurait dans le traité établissant une constitution pour l’Europe, mais n’a pas été repris dans le traité de Lisbonne. Il repose par conséquent toujours sur l’arrêt Costa contre ENEL de la Cour de justice de 1964. Pour la cohésion de l’Union européenne, nous devons veiller à ce qu’il soit respecté.

Mme Patricia Mirallès, vice-présidente de la commission de la Défense nationale et des forces armées. Je félicite les rapporteures pour la qualité de leur travail. Nos deux commissions se retrouveront probablement prochainement pour travailler sur d’autres sujets communs.