THEORIE GENERALE DU DROIT PRIVE
M2 Droit privé général
M2 Personnes, famille
Université Paris I Panthéon Sorbonne
Pr. D. Mainguy

UNIVERSITÉ PARIS 1
PANTHÉON SORBONNE

LA JURISPRUDENCE ET LE DROIT PRIVE

DOC. V : LA JURISPRUDENCE COMBATTUE PAR ELLE-MEME

Code de la sécurité intérieure (extraits) p. 3
CJUE E 6 oct. 2020, *Quadtradure du Net* p. 9
Déc. Cons. constit. QPC 15 oct. 2021, *Air France* p. 52
CE 21 avr. 2021 *French Data Network* p. 56
CJUE 15 juill. 2021 p. 123
CE 17 déc. 2021 p. 136
Cass. Crim. 12 juill. 2022 p. 144

Code de la sécurité intérieure

Art. L. 111-1. La sécurité est un droit fondamental et l'une des conditions de l'exercice des libertés individuelles et collectives.
L'Etat a le devoir d'assurer la sécurité en veillant, sur l'ensemble du territoire de la République, à la défense des institutions et des intérêts nationaux, au respect des lois, au maintien de la paix et de l'ordre publics, à la protection des personnes et des biens.
Il associe à la politique de sécurité, dans le cadre de dispositifs locaux dont la structure est définie par voie réglementaire, les collectivités territoriales et les établissements publics de coopération intercommunale ainsi que les représentants des professions, des services et des associations confrontés aux manifestations de la délinquance ou œuvrant dans les domaines de la prévention, de la médiation, de la lutte contre l'exclusion ou de l'aide aux victimes.

LIVRE 8 DU RENSEIGNEMENT

Art. 801-1 (ord. 12 déc. 2018). Le respect de la vie privée, dans toutes ses composantes, notamment le secret des correspondances, la protection des données à caractère personnel et l'inviolabilité du domicile, est garanti par la loi. L'autorité publique ne peut y porter atteinte que dans les seuls cas de nécessité d'intérêt public prévus par la loi, dans les limites fixées par celle-ci et dans le respect du principe de proportionnalité.
L'autorisation et la mise en œuvre sur le territoire national des techniques de recueil de renseignement mentionnées aux chapitres Ier à III du titre V du présent livre ne peuvent être décidées que si :
1° Elles procèdent d'une autorité ayant légalement compétence pour le faire ;
2° Elles résultent d'une procédure conforme au titre II du même livre ;
3° Elles respectent les missions confiées aux services mentionnés à l'article L. 811-2 ou aux services désignés par le décret en Conseil d'Etat prévu à l'article L. 811-4 ;
4° Elles sont justifiées par les menaces, les risques et les enjeux liés aux intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3 ;
5° Les atteintes qu'elles portent au respect de la vie privée sont proportionnées aux motifs invoqués.
La Commission nationale de contrôle des techniques de renseignement s'assure, dans les conditions prévues au présent livre, du respect de ces principes. Le Conseil d'Etat statue sur les recours formés contre les décisions relatives à l'autorisation et à la mise en œuvre de ces techniques et ceux portant sur la conservation des renseignements collectés.

Art. 811-2. Les services spécialisés de renseignement sont désignés par décret en Conseil d'Etat. Ils ont pour missions, en France et à l'étranger, la recherche, la collecte, l'exploitation et la mise à disposition du Gouvernement des renseignements relatifs aux enjeux géopolitiques et stratégiques ainsi qu'aux menaces et aux risques susceptibles d'affecter la vie de la Nation. Ils contribuent à la connaissance et à l'anticipation de ces enjeux ainsi qu'à la prévention et à l'entrave de ces risques et de ces menaces.
Ils agissent dans le respect de la loi, sous l'autorité du Gouvernement et conformément aux orientations déterminées par le Conseil national du renseignement.
La mise en œuvre sur le territoire national du chapitre II du titre II et des chapitres Ier à III du titre V du présent livre est effectuée sans préjudice du second alinéa de l'article 40 du code de procédure pénale.

Art. 811-3. Pour le seul exercice de leurs missions respectives, les services spécialisés de renseignement peuvent recourir aux techniques mentionnées au titre V du présent livre pour le recueil des renseignements relatifs à la défense et à la promotion des intérêts fondamentaux de la Nation suivants :
1° L'indépendance nationale, l'intégrité du territoire et la défense nationale ;
2° Les intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère ;
3° Les intérêts économiques, industriels et scientifiques majeurs de la France ;
4° La prévention du terrorisme ;
5° La prévention :
a) Des atteintes à la forme républicaine des institutions ;
b) Des actions tendant au maintien ou à la reconstitution de groupements dissous en application de l'article L. 212-1 ;
c) Des violences collectives de nature à porter gravement atteinte à la paix publique ;
6° La prévention de la criminalité et de la délinquance organisées ;
7° La prévention de la prolifération des armes de destruction massive.

Code des Postes et Télécommunication

Article L34-1 (L ; 31 juill. 2021)

I. – Le présent article s'applique au traitement des données à caractère personnel dans le cadre de la fourniture au public de services de communications électroniques ; il s'applique notamment aux réseaux qui prennent en charge les dispositifs de collecte de données et d'identification.

II. – Les opérateurs de communications électroniques, et notamment les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, effacent ou rendent anonymes, sous réserve des II bis à VI, les données relatives aux communications électroniques.

Les personnes qui fournissent au public des services de communications électroniques établissent, dans le respect des dispositions de l'alinéa précédent, des procédures internes permettant de répondre aux demandes des autorités compétentes .

Les 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, y compris à titre gratuit, sont soumises au respect des dispositions applicables aux opérateurs de communications électroniques en vertu du présent article.

II bis.-Les opérateurs de communications électroniques sont tenus de conserver :

1° Pour les besoins des procédures pénales, de la prévention des menaces contre la sécurité publique et de la sauvegarde de la sécurité nationale, les informations relatives à l'identité civile de l'utilisateur, jusqu'à l'expiration d'un délai de cinq ans à compter de la fin de validité de son contrat ;

2° Pour les mêmes finalités que celles énoncées au 1° du présent II bis, les autres informations fournies par l'utilisateur lors de la souscription d'un contrat ou de la création d'un compte ainsi que les informations relatives au paiement, jusqu'à l'expiration d'un délai d'un an à compter de la fin de validité de son contrat ou de la clôture de son compte ;

3° Pour les besoins de la lutte contre la criminalité et la délinquance grave, de la prévention des menaces graves contre la sécurité publique et de la sauvegarde de la sécurité nationale, les données techniques permettant d'identifier la source de la connexion ou celles relatives aux équipements terminaux utilisés, jusqu'à l'expiration d'un délai d'un an à compter de la connexion ou de l'utilisation des équipements terminaux.

III.-Pour des motifs tenant à la sauvegarde de la sécurité nationale, lorsqu'est constatée une menace grave, actuelle ou prévisible, contre cette dernière, le Premier ministre peut enjoindre par décret aux opérateurs de communications électroniques de conserver, pour une durée d'un an, certaines catégories de données de trafic, en complément de celles mentionnées au 3° du II bis, et de données de localisation précisées par décret en Conseil d'Etat.

L'injonction du Premier ministre, dont la durée d'application ne peut excéder un an, peut être renouvelée si les conditions prévues pour son édiction continuent d'être réunies. Son expiration est sans incidence sur la durée de conservation des données mentionnées au premier alinéa du présent III.

III bis.-Les données conservées par les opérateurs en application du présent article peuvent faire l'objet d'une injonction de conservation rapide par les autorités disposant, en application de la loi, d'un accès aux données relatives aux communications électroniques à des fins de prévention et de répression de la criminalité, de la délinquance grave et des autres manquements graves aux règles dont elles ont la charge d'assurer le respect, afin d'accéder à ces données.

IV. – Pour les besoins de la facturation et du paiement des prestations de communications électroniques, les opérateurs peuvent, jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement, utiliser, conserver et, le cas échéant, transmettre à des tiers concernés directement par la facturation ou le recouvrement les catégories de données techniques qui sont déterminées, dans les limites fixées par le VI, selon l'activité des opérateurs et la nature de la communication, par décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés.

Les opérateurs peuvent en outre réaliser un traitement des données relatives au trafic en vue de commercialiser leurs propres services de communications électroniques ou de fournir des services à valeur ajoutée, si les abonnés y consentent expressément et pour une durée déterminée. Cette durée ne peut, en aucun cas, être supérieure à la période nécessaire pour la fourniture ou la commercialisation de ces services. Ils peuvent également conserver certaines données en vue d'assurer la sécurité de leurs réseaux.

V. – Sans préjudice des dispositions du III et du IV, les données permettant de localiser l'équipement terminal de l'utilisateur ne peuvent ni être utilisées pendant la communication à des fins autres que son acheminement, ni être conservées et traitées après l'achèvement de la communication que moyennant le consentement de l'abonné, dûment informé des catégories de données en cause, de la durée du traitement, de ses fins et du fait que ces données seront ou non transmises à des fournisseurs de services tiers. L'abonné peut retirer à tout moment et gratuitement, hormis les coûts liés à la transmission du retrait, son consentement. L'utilisateur peut suspendre le consentement

donné, par un moyen simple et gratuit, hormis les coûts liés à la transmission de cette suspension. Tout appel destiné à un service d'urgence vaut consentement de l'utilisateur jusqu'à l'aboutissement de l'opération de secours qu'il déclenche et seulement pour en permettre la réalisation.

VI. – Les données conservées et traitées dans les conditions définies aux II bis à V 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.

Elles 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.

Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés et de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse, détermine, selon l'activité des opérateurs et la nature des communications, les informations et catégories de données conservées en application des II bis et III ainsi que les modalités de compensation des surcoûts identifiables et spécifiques des prestations assurées à ce titre, à la demande de l'Etat, par les opérateurs.

La conservation et le traitement de ces données s'effectuent dans le respect des dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Les opérateurs prennent toutes mesures pour empêcher une utilisation de ces données à des fins autres que celles prévues au présent article.

Code de la sécurité intérieure

TITRE V : DES TECHNIQUES DE RECUEIL DE RENSEIGNEMENT SOUMISES A AUTORISATION (Articles L851-1 à L855-1 C)

Chapitre Ier : Des accès administratifs aux données de connexion (Articles L851-1 à L851-7)

Article L851-1 (L. 34 juill. 2015).

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.

Par dérogation à l'article L. 821-2, les demandes écrites et motivées portant sur les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, ou au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée sont directement transmises à la Commission nationale de contrôle des techniques de renseignement par les agents individuellement désignés et habilités des services de renseignement mentionnés aux articles L. 811-2 et L. 811-4. La commission rend son avis dans les conditions prévues à l'article L. 821-3.

Un service du Premier ministre est chargé de recueillir les informations ou documents auprès des opérateurs et des personnes mentionnés au premier alinéa du présent article. La Commission nationale de contrôle des techniques de renseignement dispose d'un accès permanent, complet, direct et immédiat aux informations ou documents collectés.

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 techniques de renseignement.

Article L851-2 (L. 30 juill. 2021)

I.-Dans les conditions prévues au chapitre Ier du titre II du présent livre et pour les seuls besoins de la prévention du terrorisme, peut être individuellement autorisé le recueil en temps réel, sur les réseaux des opérateurs et des personnes mentionnés à l'article L. 851-1, des informations ou documents mentionnés au même article L. 851-1 relatifs à une personne préalablement identifiée susceptible d'être en lien avec une menace, ainsi que des adresses complètes de ressources sur internet utilisées par cette personne. Lorsqu'il existe des raisons sérieuses de penser qu'une ou plusieurs personnes appartenant à l'entourage de la personne concernée par l'autorisation sont susceptibles de fournir des informations au titre de la finalité qui motive l'autorisation, celle-ci peut être également accordée individuellement pour chacune de ces personnes.

I bis.-Le nombre maximal des autorisations délivrées en application du présent article en vigueur simultanément est arrêté par le Premier ministre, après avis de la Commission nationale de contrôle des techniques de renseignement. La décision fixant ce contingent et sa répartition entre les ministres mentionnés au premier alinéa de l'article L. 821-2 ainsi que le nombre d'autorisations d'interception délivrées sont portés à la connaissance de la commission.
II.-(abrogé)

Art. 851-3 (L. 31 juill. 2021)
I.-Dans les conditions prévues au chapitre Ier du titre II du présent livre et pour les seuls besoins de la prévention du terrorisme, à la demande des services spécialisés de renseignement mentionnés à l'article L. 811-2, peuvent être autorisés, sur les données transitant par les réseaux des opérateurs et des personnes mentionnées à l'article L. 851-1, des traitements automatisés destinés, en fonction de paramètres précisés dans l'autorisation, à détecter des connexions susceptibles de révéler une menace terroriste.
Ces traitements automatisés utilisent exclusivement les informations ou documents mentionnés à l'article L. 851-1 ainsi que les adresses complètes de ressources utilisées sur internet, sans recueillir d'autres données que celles qui répondent à leurs paramètres de conception et sans permettre l'identification des personnes auxquelles les informations, documents ou adresses se rapportent.
Dans le respect du principe de proportionnalité, l'autorisation du Premier ministre précise le champ technique de la mise en œuvre de ces traitements.
II.-La Commission nationale de contrôle des techniques de renseignement émet un avis sur la demande d'autorisation relative aux traitements automatisés et les paramètres de détection retenus. Elle dispose d'un accès permanent, complet et direct à ces traitements ainsi qu'aux informations et données recueillies. Elle est informée de toute modification apportée aux traitements et paramètres et peut émettre des recommandations.
La première autorisation de mise en œuvre des traitements automatisés prévue au I du présent article est délivrée pour une durée de deux mois. L'autorisation est renouvelable dans les conditions de durée prévues au chapitre Ier du titre II du présent livre. La demande de renouvellement comporte un relevé du nombre d'identifiants signalés par le traitement automatisé et une analyse de la pertinence de ces signalements.
III.-Les conditions prévues à l'article L. 871-6 sont applicables aux opérations matérielles effectuées par les opérateurs et les personnes mentionnés à l'article L. 851-1.
IV.-Lorsque les traitements mentionnés au I du présent article détectent des données susceptibles de caractériser l'existence d'une menace à caractère terroriste, le Premier ministre ou l'une des personnes déléguées par lui peut autoriser, après avis de la Commission nationale de contrôle des techniques de renseignement donné dans les conditions prévues au chapitre Ier du titre II du présent livre, l'identification de la ou des personnes concernées et le recueil des données y afférentes. Ces données sont exploitées dans un délai de soixante jours à compter de ce recueil et sont détruites à l'expiration de ce délai.
Les données non détectées par les traitements comme susceptibles de révéler une menace à caractère terroriste sont détruites immédiatement.
V.-Le caractère d'urgence mentionné à la dernière phrase du deuxième alinéa de l'article L. 821-1 ne peut être invoqué pour les autorisations délivrées sur le fondement des I et II du présent article.
VI.-Un service du Premier ministre est seul habilité à exécuter les traitements et opérations mis en œuvre sur le fondement des I et IV, sous le contrôle de la Commission nationale de contrôle des techniques de renseignement.

Art. 851-4 (L. 24 juill. 2015)
Dans les conditions prévues au chapitre Ier du titre II du présent livre, les données techniques relatives à la localisation des équipements terminaux utilisés mentionnées à l'article L. 851-1 peuvent être recueillis sur sollicitation du réseau et transmis en temps réel par les opérateurs à un service du Premier ministre

Art. 851-6 (L. 24 juill. 2015)
I.-Dans les conditions prévues au chapitre Ier du titre II du présent livre, peuvent être directement recueillies, au moyen d'un appareil ou d'un dispositif technique mentionné au 1° de l'article 226-3 du code pénal, les données techniques de connexion permettant l'identification d'un équipement terminal ou du numéro d'abonnement de son utilisateur ainsi que les données relatives à la localisation des équipements terminaux utilisés.
Par dérogation à l'article L. 821-4 du présent code, l'autorisation est délivrée pour une durée de deux mois, renouvelable dans les mêmes conditions de durée.
II.-Les appareils ou dispositifs techniques mentionnés au I font l'objet d'une inscription dans un registre spécial tenu à la disposition de la Commission nationale de contrôle des techniques de renseignement et ne peuvent être mis en œuvre que par des agents individuellement désignés et habilités.
III.-Un service du Premier ministre centralise les informations ou documents recueillis, qui sont :

1° Conservés dans les conditions prévues à l'article L. 822-2, s'ils se rapportent à l'autorisation de mise en œuvre ;
2° Détruits dès qu'il apparaît qu'ils ne sont pas en rapport avec l'autorisation de mise en œuvre, dans un délai maximal de quatre-vingt-dix jours.
IV.-Le nombre maximal d'appareils ou de dispositifs techniques mentionnés au II du présent article pouvant être utilisés simultanément est arrêté par le Premier ministre, après avis de la Commission nationale de contrôle des techniques de renseignement. La décision fixant ce contingent et sa répartition entre les ministres mentionnés au premier alinéa de l'article L. 821-2 est portée à la connaissance de la commission.

Chapitre II : Des interceptions de sécurité (Articles L852-1 à L852-3)
Article L852-1 (L. 21 juill. 2016)
I.-Dans les conditions prévues au chapitre Ier du titre II du présent livre, peuvent être autorisées les interceptions de correspondances émises par la voie des communications électroniques et susceptibles de révéler des renseignements relatifs aux finalités mentionnées à l'article L. 811-3. Lorsqu'il existe des raisons sérieuses de croire qu'une ou plusieurs personnes appartenant à l'entourage d'une personne concernée par l'autorisation sont susceptibles de fournir des informations au titre de la finalité qui motive l'autorisation, celle-ci peut être également accordée pour ces personnes.
II.-Pour les seules finalités mentionnées aux 1° et 4° et a du 5° de l'article L. 811-3 du présent code, peut être autorisée, pour une durée de quarante-huit heures renouvelable, l'utilisation d'un appareil ou d'un dispositif technique mentionné au 1° de l'article 226-3 du code pénal afin d'intercepter des correspondances émises ou reçues par un équipement terminal. Les correspondances interceptées par cet appareil ou ce dispositif technique sont détruites dès qu'il apparaît qu'elles sont sans lien avec l'autorisation délivrée, dans la limite du délai prévu au 1° du I de l'article L. 822-2 du présent code.
III.-L'autorisation vaut autorisation de recueil des informations ou documents mentionnés à l'article L. 851-1 associés à l'exécution de l'interception et à son exploitation.
IV.-Un service du Premier ministre organise la centralisation de l'exécution des interceptions mentionnées au I. Après avis de la Commission nationale de contrôle des techniques de renseignement, le Premier ministre définit les modalités de la centralisation des correspondances interceptées en application du II.
V.-Les opérations de transcription et d'extraction des communications interceptées, auxquelles la Commission nationale de contrôle des techniques de renseignement dispose d'un accès permanent, complet, direct et immédiat, sont effectuées au sein d'un service du Premier ministre.
VI.-Le nombre maximal des autorisations d'interception en vigueur simultanément est arrêté par le Premier ministre, après avis de la Commission nationale de contrôle des techniques de renseignement. La décision fixant ce contingent et sa répartition entre les ministres mentionnés au premier alinéa de l'article L. 821-2 ainsi que le nombre d'autorisations d'interception délivrées sont portés à la connaissance de la commission.

Chapitre III : De la sonorisation de certains lieux et véhicules et de la captation d'images et de données informatiques (Articles L853-1 à L853-3)

Article L853-1 (L. 31 juill. 2021)
I.-Dans les conditions prévues au chapitre Ier du titre II du présent livre, peut être autorisée, lorsque les renseignements ne peuvent être recueillis par un autre moyen légalement autorisé, l'utilisation de dispositifs techniques permettant la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou confidentiel, ou d'images dans un lieu privé.
II.-Par dérogation à l'article L. 821-4, l'autorisation est délivrée pour une durée maximale de deux mois, renouvelable dans les mêmes conditions de durée.
III.-Les dispositifs techniques mentionnés au I du présent article ne peuvent être utilisés que par des agents appartenant à l'un des services mentionnés aux articles L. 811-2 et L. 811-4 dont la liste est fixée par décret en Conseil d'Etat.
IV.-Le service autorisé à recourir à la technique mentionnée au I du présent article rend compte à la Commission nationale de contrôle des techniques de renseignement de sa mise en œuvre. La commission peut à tout moment adresser une recommandation tendant à ce que cette opération soit interrompue et que les renseignements collectés soient détruits.
IV bis.-Le caractère d'urgence mentionné à la dernière phrase du deuxième alinéa de l'article L. 821-1 ne peut être invoqué que si l'autorisation prévue au présent article a été délivrée au titre du 1°, du 4° ou du a du 5° de l'article L. 811-3.
V.-Si la mise en œuvre de cette technique nécessite l'introduction dans un véhicule ou dans un lieu privé, cette mesure s'effectue selon les modalités définies à l'article L. 853-3.

Art. 853-2 (L. 31 juill. 2021)

I.-Dans les conditions prévues au chapitre Ier du titre II du présent livre, peut être autorisée, lorsque les renseignements ne peuvent être recueillis par un autre moyen légalement autorisé, l'utilisation de dispositifs techniques permettant d'accéder à des données informatiques stockées dans un système informatique, de les enregistrer, de les conserver et de les transmettre, et permettant d'accéder à ces mêmes données informatiques, de les enregistrer, de les conserver et de les transmettre, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données, telles qu'il les y introduit par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques.
II. - Par dérogation à l'article L. 821-4, l'autorisation de mise en œuvre de la technique mentionnée au I du présent article est délivrée pour une durée maximale de deux mois. L'autorisation est renouvelable dans les mêmes conditions de durée.
III. - Les dispositifs techniques mentionnés au I du présent article ne peuvent être utilisés que par des agents appartenant à l'un des services mentionnés aux articles L. 811-2 et L. 811-4 dont la liste est fixée par décret en Conseil d'Etat.
IV. - Le service autorisé à recourir à la technique mentionnée au I rend compte à la Commission nationale de contrôle des techniques de renseignement de sa mise en œuvre. La commission peut à tout moment adresser une recommandation tendant à ce que cette opération soit interrompue et que les renseignements collectés soient détruits.
IV bis.-Le caractère d'urgence mentionné à la dernière phrase du deuxième alinéa de l'article L. 821-1 ne peut être invoqué que si l'autorisation prévue au présent article a été délivrée au titre du 1°, du 4° ou du a du 5° de l'article L. 811-3.
V. - Si la mise en œuvre de cette technique nécessite l'introduction dans un véhicule ou dans un lieu privé, cette mesure s'effectue selon les modalités définies à l'article L. 853-3.

Chapitre IV : Des mesures de surveillance des communications électroniques internationales (Articles L854-1 à L854-9)

Article L854-1 (L. 13 juill. 2018)
Dans les conditions prévues au présent chapitre, peut être autorisée, aux seules fins de défense et de promotion des intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3, la surveillance des communications qui sont émises ou reçues à l'étranger.
Cette surveillance, qu'elle porte sur des correspondances ou sur des données de connexion, est exclusivement régie par le présent chapitre.
Les mesures prises à ce titre ne peuvent avoir pour objet d'assurer la surveillance individuelle des communications de personnes utilisant des numéros d'abonnement ou des identifiants techniques rattachables au territoire national, à l'exception du cas où ces personnes communiquent depuis l'étranger et, soit faisaient l'objet d'une autorisation d'interception de sécurité, délivrée en application de l'article L. 852-1, à la date à laquelle elles ont quitté le territoire national, soit sont identifiées comme présentant une menace au regard des intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3.
Les autorisations prévues aux articles L. 851-1, L. 851-2 et au I de l'article L. 852-1 peuvent valoir, lorsque la décision d'autorisation le prévoit, autorisation d'exploitation des communications, ou des seules données de connexion, interceptées dans le cadre de la mise en œuvre de mesures de surveillance des communications internationales, dans la limite de la portée de ces autorisations et dans le respect des garanties qui les entourent.
Sous réserve des dispositions particulières des troisième et quatrième alinéas du présent article ainsi que du V de l'article L. 854-2, lorsqu'il apparaît que des communications électroniques interceptées sont échangées entre des personnes ou des équipements utilisant des numéros d'abonnement ou des identifiants techniques rattachables au territoire national, y compris lorsque ces communications transitent par des équipements non rattachables à ce territoire, celles-ci sont instantanément détruites.

CJUE ARRÊT DE LA COUR (grande chambre)
6 octobre 2020
[Texte rectifié par ordonnance du 16 novembre 2020]
Table des matières

Le cadre juridique
Le droit de l'Union
La directive 95/46
La directive 97/66
La directive 2000/31
La directive 2002/21
La directive 2002/58
Le règlement 2016/679
Le droit français
Le code de la sécurité intérieure
Le CPCE
La loi n o 2004-575, du 21 juin 2004, pour la confiance dans l'économie numérique
Le décret n o 2011-219
Le droit belge
Les litiges au principal et les questions préjudicielles
L'affaire C 511/18
L'affaire C 512/18
L'affaire C 520/18
Sur la procédure devant la Cour
Sur les questions préjudicielles
Sur les premières questions dans les affaires C 511/18 et C512/18 ainsi que sur les première et deuxième questions dans l'affaire C520/18
Observations liminaires
Sur le champ d'application de la directive 2002/58
Sur l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58
– Sur les mesures législatives prévoyant la conservation préventive des données relatives au trafic et des données de localisation aux fins de la sauvegarde de la sécurité nationale
– Sur les mesures législatives prévoyant la conservation préventive des données relatives au trafic et des données de localisation aux fins de la lutte contre la criminalité et de la sauvegarde de la sécurité publique
– Sur les mesures législatives prévoyant la conservation préventive des adresses IP et des données relatives à l'identité civile aux fins de la lutte contre la criminalité et de la sauvegarde de la sécurité publique
– Sur les mesures législatives prévoyant la conservation rapide des données relatives au trafic et des données de localisation aux fins de la lutte contre la criminalité grave
Sur les deuxième et troisième questions dans l'affaire C 511/18
Sur l'analyse automatisée des données relatives au trafic et des données de localisation
Sur le recueil en temps réel des données relatives au trafic et des données de localisation
Sur l'information des personnes dont les données ont été recueillies ou analysées
Sur la seconde question dans l'affaire C 512/18
Sur la troisième question dans l'affaire C 520/18
Sur les dépens

« Renvoi préjudiciel – Traitement des données à caractère personnel dans le secteur des communications électroniques – Fournisseurs de services de communications électroniques – Fournisseurs de services d'hébergement et fournisseurs d'accès à Internet – Conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation – Analyse automatisée des données – Accès en temps réel aux données – Sauvegarde de la sécurité nationale et lutte contre le terrorisme – Lutte contre la criminalité – Directive 2002/58/CE – Champ d'application – Article 1er, paragraphe 3, et article 3 – Confidentialité des communications électroniques – Protection – Article 5 et article 15, paragraphe 1 – Directive 2000/31/CE – Champ d'application – Charte des droits fondamentaux de l'Union européenne – Articles 4, 6 à 8 et 11 et article 52, paragraphe 1 – Article 4, paragraphe 2, TUE »
Dans les affaires jointes C-511/18, C-512/18 et C-520/18,
ayant pour objet des demandes de décision préjudicielle au titre de l'article 267 TFUE, introduites par le Conseil d'État (France), par décisions du 26 juillet 2018, parvenues à la Cour le 3 août 2018 (C-511/18 et C-512/18), et par la Cour constitutionnelle (Belgique), par décision du 19 juillet 2018, parvenue à la Cour le 2 août 2018 (C-520/18), dans les procédures
La Quadrature du Net (C-511/18 et C-512/18),

French Data Network (C-511/18 et C-512/18),
Fédération des fournisseurs d'accès à Internet associatifs (C-511/18 et C-512/18),
Igwan.net (C-511/18),
contre
Premier ministre (C-511/18 et C-512/18),
Garde des Sceaux, ministre de la Justice (C-511/18 et C-512/18),
Ministre de l'Intérieur (C-511/18),
Ministre des Armées (C-511/18), en présence de :
Privacy International (C-512/18),
Center for Democracy and Technology (C-512/18),
et
Ordre des barreaux francophones et germanophone,
Académie Fiscale ASBL,
UA,
Liga voor Mensenrechten ASBL,
Ligue des Droits de l'Homme ASBL,
VZ,
WY,
XX
contre
Conseil des ministres,
en présence de :
Child Focus (C-520/18),
LA COUR (grande chambre),
composée de M. K. Lenaerts, président, M^me^ R. Silva de Lapuerta, vice-présidente, MM. J.-C. Bonichot, A. Arabadjiev, M^me^ A. Prechal, MM. M. Safjan, P. G. Xuereb et M^me^ L. S. Rossi, présidents de chambre, MM. J. Malenovský, L. Bay Larsen, T. von Danwitz (rapporteur), M^mes^ C. Toader, K. Jürimäe, MM. C. Lycourgos et N. Piçarra, juges,
avocat général : M. M. Campos Sánchez-Bordona,
greffier : M^me^ C. Strömholm, administratrice,
vu la procédure écrite et à la suite de l'audience des 9 et 10 septembre 2019,
considérant les observations présentées :
– pour la Quadrature du Net, la Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net et le Center for Democracy and Technology, par M^e^ A. Fitzjean Ò Cobhthaigh, avocat,
– pour French Data Network, par M^e^ Y. Padova, avocat,
– pour Privacy International, M^e^ H. Roy, avocat,
– pour l'Ordre des barreaux francophones et germanophone, par M^es^ E. Kiehl, P. Limbrée, E. Lemmens, A. Cassart et J.-F. Henrotte, avocats,
– pour l'Académie Fiscale ASBL et UA, par M. J.-P. Riquet,
– pour la Liga voor Mensenrechten ASBL, par M^e^ J. Vander Velpen, avocat,
– pour la Ligue des Droits de l'Homme ASBL, par M^es^ R. Jespers et J. Fermon, avocats,
– pour VZ, WY et XX, par M^e^ D. Pattyn, avocat,
– pour Child Focus, par M^es^ N. Buisseret, K. De Meester et J. Van Cauter, avocats,
– pour le gouvernement français, initialement par MM. D. Dubois, F. Alabrune et D. Colas ainsi que par M^mes^ E. de Moustier et A.-L. Desjonquères, puis par MM. D. Dubois et F. Alabrune ainsi que par M^mes^ E. de Moustier et A.-L. Desjonquères, en qualité d'agents,
– pour le gouvernement belge, par MM. J.-C. Halleux et P. Cottin ainsi que par M^me^ C. Pochet, en qualité d'agents, assistés de M^es^ J. Vanpraet, Y. Peeters, S. Depré et E. de Lophem, avocats,
– pour le gouvernement tchèque, par MM. M. Smolek, J. Vláčil et O. Serdula, en qualité d'agents,
– pour le gouvernement danois, initialement par M. J. Nymann-Lindegren ainsi que par M^mes^ M. Wolff et P. Ngo, puis par M. J. Nymann-Lindegren et M^me^ M. Wolff, en qualité d'agents,
– pour le gouvernement allemand, initialement par MM. J. Möller, M. Hellmann, E. Lankenau, R. Kanitz et T. Henze, puis par MM. J. Möller, M. Hellmann, E. Lankenau et R. Kanitz, en qualité d'agents,
– pour le gouvernement estonien, par M^mes^ N. Grünberg et A. Kalbus, en qualité d'agents,
– pour le gouvernement irlandais, par M. A. Joyce ainsi que par M^mes^ M. Browne et G. Hodge, en qualité d'agents, assistés de M. D. Fennelly, BL,
– pour le gouvernement espagnol, initialement par MM. L. Aguilera Ruiz et A. Rubio González, puis par M. L. Aguilera Ruiz, en qualité d'agent,
– pour le gouvernement chypriote, par M^me^ E. Neofytou, en qualité d'agent,
– pour le gouvernement letton, par M^me^ V. Soņeca, en qualité d'agent,

– pour le gouvernement hongrois, initialement par M. M. Z. Fehér et Mme Z. Wagner, puis par M. M. Z. Fehér, en qualité d'agent,
– pour le gouvernement néerlandais, par Mmes M. K. Bulterman et M. A. M. de Ree, en qualité d'agents,
– pour le gouvernement polonais, par M. B. Majczyna ainsi que par Mmes J. Sawicka et M. Pawlicka, en qualité d'agents,
– pour le gouvernement suédois, initialement par Mmes H. Shev, H. Eklinder, C. Meyer-Seitz, et A. Falk, puis par Mmes H. Shev, H. Eklinder, C. Meyer-Seitz et J. Lundberg, en qualité d'agents,
– pour le gouvernement du Royaume-Uni, par M. S. Brandon, en qualité d'agent, assisté de M. G. Facenna, QC, et de M. C. Knight, barrister,
– tiret supprimé par ordonnance du 16 novembre 2020,
– pour la Commission européenne, initialement par MM. H. Kranenborg et M. Wasmeier ainsi que par Mme P. Costa de Oliveira, puis par MM. H. Kranenborg et M. Wasmeier, en qualité d'agents,
– pour le Contrôleur européen de la protection des données, par M T. Zerdick et Mme A. Buchta, en qualité d'agents,
ayant entendu l'avocat général en ses conclusions à l'audience du 15 janvier 2020,
rend le présent

Arrêt

1 Les demandes de décision préjudicielle portent sur l'interprétation, d'une part, de l'article 15, paragraphe 1, de 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 (directive vie privée et communications électroniques) (JO 2002, L 201, p. 37), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009 (JO 2009, L 337, p. 11) (ci-après la directive 2002/58), et, d'autre part, des articles 12 à 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 (« directive sur le commerce électronique ») (JO 2000, L 178, p. 1), lus à la lumière des articles 4, 6 à 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne (ci-après la « Charte ») et de l'article 4, paragraphe 2, TUE.

2 La demande dans l'affaire C-511/18 a été présentée dans le cadre de litiges opposant la Quadrature du Net, French Data Network, la Fédération des fournisseurs d'accès à Internet associatifs et Igwan.net au Premier ministre (France), au Garde des Sceaux, ministre de la Justice (France), au ministre de l'Intérieur (France) et au ministre des Armées (France) au sujet de la légalité du décret no 2015-1185, du 28 septembre 2015, portant désignation des services spécialisés de renseignement (JORF du 29 septembre 2015, texte 1 sur 97, ci-après le « décret no 2015-1185 »), du décret no 2015-1211, 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'État (JORF du 2 octobre 2015, texte 7 sur 108, ci-après le « décret no 2015-1211 »), du décret no 2015-1639, 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 (JORF du 12 décembre 2015, texte 28 sur 127, ci-après le « décret no 2015-1639 »), ainsi que du décret no 2016-67, du 29 janvier 2016, relatif aux techniques de recueil de renseignement (JORF du 31 janvier 2016, texte 2 sur 113, ci-après le « décret no 2016-67 »).

3 La demande dans l'affaire C-512/18 a été présentée dans le cadre de litiges opposant French Data Network, la Quadrature du Net et la Fédération des fournisseurs d'accès à Internet associatifs, au Premier ministre (France) et au Garde des Sceaux, ministre de la justice (France), au sujet de la légalité de l'article R. 10-13 du code des postes et des communications électroniques (ci-après le « CPCE ») et du décret no 2011-219, du 25 février 2011, relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne (JORF du 1er mars 2011, texte 32 sur 170, ci-après le « décret no 2011-219 »).

4 La demande dans l'affaire C-520/18 a été présentée dans le cadre de litiges opposant l'Ordre des barreaux francophones et germanophone, l'Académie Fiscale ASBL, UA, la Liga voor Mensenrechten ASBL, la Ligue des Droits de l'Homme ASBL, VZ, WY et XX au Conseil des ministres (Belgique) au sujet de la légalité de la loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques (*Moniteur belge* du 18 juillet 2016, p. 44717, ci-après la « loi du 29 mai 2016 »).

Le cadre juridique

Le droit de l'Union

La directive 95/46

5 La directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO 1995, L 281, p. 31), a été abrogée, avec effet au 25 mai 2018, par le règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, 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, et abrogeant la directive 95/46 (JO 2016, L 119, p. 1). L'article 3, paragraphe 2, de la directive 95/46 disposait :

« La présente directive ne s'applique pas au traitement de données à caractère personnel :

– mis en œuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire, telles que celles prévues aux titres V et VI du traité sur l'Union européenne, et, en tout état de cause, aux traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État (y compris le bien-être économique de l'État lorsque ces traitements sont liés à des questions de sûreté de l'État) et les activités de l'État relatives à des domaines du droit pénal,

– effectué par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques. »

6 L'article 22 de la directive 95/46, figurant au chapitre III de celle-ci, intitulé « Recours juridictionnels, responsabilité et sanctions », était libellé comme suit :

« Sans préjudice du recours administratif qui peut être organisé, notamment devant l'autorité de contrôle visée à l'article 28, antérieurement à la saisine de l'autorité judiciaire, les États membres prévoient que toute personne dispose d'un recours juridictionnel en cas de violation des droits qui lui sont garantis par les dispositions nationales applicables au traitement en question. »

La directive 97/66

7 Aux termes de l'article 5 de la directive 97/66/CE du Parlement européen et du Conseil, du 15 décembre 1997, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications (JO 1997, L 24, p. 1), intitulé « Confidentialité des communications » :

« 1. Les États membres garantissent, au moyen de réglementations nationales, la confidentialité des communications effectuées au moyen d'un réseau public de télécommunications ou de services de télécommunications accessible au public. En particulier, ils interdisent à toute autre personne que les utilisateurs, sans le consentement des utilisateurs concernés, d'écouter, d'intercepter, de stocker les communications ou de les soumettre à quelque autre moyen d'interception ou de surveillance, sauf lorsque ces activités sont légalement autorisées, conformément à l'article 14, paragraphe 1.

2. Le paragraphe 1 n'affecte pas l'enregistrement légalement autorisé de communications, dans le cadre des usages professionnels licites, afin de fournir la preuve d'une transaction commerciale ou de toute autre communication commerciale. »

La directive 2000/31

8 Les considérants 14 et 15 de la directive 2000/31 prévoient :

« (14) La protection des personnes physiques à l'égard du traitement des données à caractère personnel est uniquement régie par la directive [95/46] et par la directive [97/66], qui sont pleinement applicables aux services de la société de l'information. Ces directives établissent d'ores et déjà un cadre juridique communautaire dans le domaine des données à caractère personnel et, par conséquent, il n'est pas nécessaire de traiter cette question dans la présente directive afin d'assurer le bon fonctionnement du marché intérieur, et notamment la libre circulation des données à caractère personnel entre les États membres. La mise en œuvre et l'application de la présente directive devraient être conformes aux principes relatifs à la protection des données à caractère personnel, notamment pour ce qui est des communications commerciales non sollicitées et de la responsabilité des intermédiaires. La présente directive ne peut pas empêcher l'utilisation anonyme de réseaux ouverts tels qu'Internet.

(15) Le secret des communications est garanti par l'article 5 de la directive [97/66]. Conformément à cette directive, les États membres doivent interdire tout type d'interception illicite ou la surveillance de telles communications par d'autres que les expéditeurs et les récepteurs, sauf lorsque ces activités sont légalement autorisées. »

9 L'article 1er de la directive 2000/31 est libellé comme suit :

« 1. La présente directive a pour objectif de contribuer au bon fonctionnement du marché intérieur en assurant la libre circulation des services de la société de l'information entre les États membres.

2. La présente directive rapproche, dans la mesure nécessaire à la réalisation de l'objectif visé au paragraphe 1, certaines dispositions nationales applicables aux services de la société de l'information et qui concernent le marché intérieur, l'établissement des prestataires, les communications commerciales, les contrats par voie électronique, la responsabilité des intermédiaires, les codes de conduite, le règlement extrajudiciaire des litiges, les recours juridictionnels et la coopération entre États membres.

3. La présente directive complète le droit communautaire applicable aux services de la société de l'information sans préjudice du niveau de protection, notamment en matière de santé publique et des intérêts

des consommateurs, établi par les instruments communautaires et la législation nationale les mettant en œuvre dans la mesure où cela ne restreint pas la libre prestation de services de la société de l'information.
[...]
5. La présente directive n'est pas applicable :
[...]
b) aux questions relatives aux services de la société de l'information couvertes par les directives [95/46] et [97/66] ;
[...] »
10 L'article 2 de la directive 2000/31 est libellé comme suit :
« Aux fins de la présente directive, on entend par :
a) "services de la société de l'information" : les services au sens de l'article 1er, paragraphe 2, de la directive 98/34/CE [du Parlement européen et du Conseil, du 22 juin 1998, prévoyant une procédure d'information dans le domaine des normes et réglementations techniques (JO 1998, L 204, p. 37)], telle que modifiée par la directive 98/48/CE [du Parlement européen et du Conseil, du 20 juillet 1998 (JO 1998, L 217, p. 18)] ;
[...] »
11 L'article 15 de la directive 2000/31 prévoit :
« 1. Les États membres ne doivent pas imposer aux prestataires, pour la fourniture des services visée aux articles 12, 13 et 14, 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.
2. Les États membres peuvent instaurer, pour les prestataires de services de la société de l'information, l'obligation d'informer promptement les autorités publiques compétentes d'activités illicites alléguées qu'exerceraient les destinataires de leurs services ou d'informations illicites alléguées que ces derniers fourniraient ou de communiquer aux autorités compétentes, à leur demande, les informations permettant d'identifier les destinataires de leurs services avec lesquels ils ont conclu un accord d'hébergement. »

La directive 2002/21

12 Aux termes du considérant 10 de la directive 2002/21/CE du Parlement européen et du Conseil, du 7 mars 2002, relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques (directive « cadre ») (JO 2002, L 108, p. 33) :
« La définition du "service de la société de l'information", qui figure à l'article 1er de la directive [98/34], telle que modifiée par la directive [98/48], se rapporte à une large gamme d'activités économiques se déroulant en ligne ; la plupart de ces activités ne sont pas couvertes par le champ d'application de la présente directive, car elles ne consistent pas entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques ; les services de téléphonie vocale et de transmission de courrier électronique sont couverts par la présente directive. La même entreprise, par exemple un prestataire de services Internet, peut proposer à la fois un service de communications électroniques, tel que l'accès à Internet, et des services non couverts par la présente directive, tels que la fourniture de contenus sur la toile. »
13 L'article 2 de la directive 2002/21 prévoit :
« Aux fins de la présente directive, on entend par :
[...]
c) "service de communications électroniques" : le service fourni normalement contre rémunération qui consiste entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques, y compris les services de télécommunications et les services de transmission sur les réseaux utilisés pour la radiodiffusion, mais qui exclut les services consistant à fournir des contenus à l'aide de réseaux et de services de communications électroniques ou à exercer une responsabilité éditoriale sur ces contenus ; il ne comprend pas les services de la société de l'information tels que définis à l'article 1er de la directive [98/34], qui ne consistent pas entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques ;
[...] »

La directive 2002/58

14 Les considérants 2, 6, 7, 11, 22, 26 et 30 de la directive 2002/58 énoncent :
« (2) La présente directive vise à respecter les droits fondamentaux et observe les principes reconnus notamment par la [Charte]. En particulier, elle vise à garantir le plein respect des droits exposés aux articles 7 et 8 de cette charte.
[...]
(6) L'Internet bouleverse les structures commerciales traditionnelles en offrant une infrastructure mondiale commune pour la fourniture de toute une série de services de communications électroniques. Les services de communications électroniques accessibles au public sur l'Internet ouvrent de nouvelles possibilités aux utilisateurs, mais présentent aussi de nouveaux dangers pour leurs données à caractère personnel et leur vie privée.

(7) Dans le cas des réseaux publics de communications, il convient d'adopter des dispositions législatives, réglementaires et techniques spécifiques afin de protéger les droits et les libertés fondamentaux des personnes physiques et les intérêts légitimes des personnes morales, notamment eu égard à la capacité accrue de stockage et de traitement automatisés de données relatives aux abonnés et aux utilisateurs.

[...]

(11) À l'instar de la directive [95/46], la présente directive ne traite pas des questions de protection des droits et libertés fondamentaux liées à des activités qui ne sont pas régies par le droit [de l'Union]. Elle ne modifie donc pas l'équilibre existant entre le droit des personnes à une vie privée et la possibilité dont disposent les États membres de prendre des mesures telles que celles visées à l'article 15, paragraphe 1, de la présente directive, nécessaires pour la protection de la sécurité publique, de la défense, de 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) et de l'application du droit pénal. Par conséquent, la présente directive ne porte pas atteinte à la faculté des États membres de procéder aux interceptions légales des communications électroniques ou d'arrêter d'autres mesures si cela s'avère nécessaire pour atteindre l'un quelconque des buts précités, dans le respect de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, [signée à Rome le 4 novembre 1050,] telle qu'interprétée par la Cour européenne des droits de l'homme dans ses arrêts. Lesdites mesures doivent être appropriées, rigoureusement proportionnées au but poursuivi et nécessaires dans une société démocratique. Elles devraient également être subordonnées à des garanties appropriées, dans le respect de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.

[...]

(22) L'interdiction du stockage des communications et des données relatives au trafic y afférentes par des personnes autres que les utilisateurs ou sans le consentement de ceux-ci ne vise pas à interdire tout stockage automatique, intermédiaire et transitoire de ces informations si ce stockage a lieu dans le seul but d'effectuer la transmission dans le réseau de communications électroniques, pour autant que les informations ne soient pas stockées pour une durée plus longue que le temps nécessaire à la transmission et à la gestion du trafic et qu'au cours de la période de stockage la confidentialité des informations reste garantie. [...]

[...]

(26) Les données relatives aux abonnés qui sont traitées dans des réseaux de communications électroniques pour établir des connexions et transmettre des informations contiennent des informations sur la vie privée des personnes physiques et touchent au droit au secret de leur correspondance ainsi qu'aux intérêts légitimes des personnes morales. Ces données ne peuvent être stockées que dans la mesure où cela est nécessaire à la fourniture du service, aux fins de la facturation et des paiements pour interconnexion, et ce, pour une durée limitée. Tout autre traitement de ces données [...] ne peut être autorisé que si l'abonné a donné son accord sur la base d'informations précises et complètes fournies par le fournisseur du service de communications électroniques accessible au public sur la nature des autres traitements qu'il envisage d'effectuer, ainsi que sur le droit de l'abonné de ne pas donner son consentement à ces traitements ou de retirer son consentement. Il convient également d'effacer ou de rendre anonymes les données relatives au trafic utilisées pour la commercialisation de services de communications [...]

[...]

(30) Les systèmes mis au point pour la fourniture de réseaux et de services de communications électroniques devraient être conçus de manière à limiter au strict minimum la quantité de données personnelles nécessaires. [...] »

15 L'article 1er de la directive 2002/58, intitulé « Champ d'application et objectif », dispose :

« 1. La présente directive prévoit l'harmonisation des dispositions nationales nécessaires pour assurer un niveau équivalent de protection des droits et libertés fondamentaux, et en particulier du droit à la vie privée et à la confidentialité, en ce qui concerne le traitement des données à caractère personnel dans le secteur des communications électroniques, ainsi que la libre circulation de ces données et des équipements et services de communications électroniques dans [l'Union européenne].

2. Les dispositions de la présente directive précisent et complètent la directive [95/46] aux fins énoncées au paragraphe 1. En outre, elles prévoient la protection des intérêts légitimes des abonnés qui sont des personnes morales.

3. La présente directive ne s'applique pas aux activités qui ne relèvent pas du [TFUE], telles que celles visées dans les titres V et VI du traité sur l'Union 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. »

16 Selon l'article 2 de la directive 2002/58, intitulé « Définitions » :

« Sauf disposition contraire, les définitions figurant dans la directive [95/46] et dans la directive [2002/21] s'appliquent aux fins de la présente directive.

Les définitions suivantes sont aussi applicables :

a) “utilisateur” : toute personne physique utilisant un service de communications électroniques accessible au public à des fins privées ou professionnelles sans être nécessairement abonnée à ce service ;
b) “données relatives au trafic” : toutes les données traitées en vue de l’acheminement d’une communication par un réseau de communications électroniques ou de sa facturation ;
c) “données de localisation” : toutes les données traitées dans un réseau de communications électroniques ou par un service de communications électroniques indiquant la position géographique de l’équipement terminal d’un utilisateur d’un service de communications électroniques accessible au public ;
d) “communication” : toute information échangée ou acheminée entre un nombre fini de parties au moyen d’un service de communications électroniques accessible au public. Cela ne comprend pas les informations qui sont acheminées dans le cadre d’un service de radiodiffusion au public par l’intermédiaire d’un réseau de communications électroniques, sauf dans la mesure où un lien peut être établi entre l’information et l’abonné ou utilisateur identifiable qui la reçoit ;
[...] »

17 L’article 3 de la directive 2002/58, intitulé « Services concernés », prévoit :

« La présente directive s’applique au traitement des données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux de communications publics dans la Communauté, y compris les réseaux de communications publics qui prennent en charge les dispositifs de collecte de données et d’identification. »

18 Aux termes de l’article 5 de la directive 2002/58, intitulé « Confidentialité des communications » :

« 1. Les États membres garantissent, par la législation nationale, la confidentialité des communications effectuées au moyen d’un réseau public de communications et de services de communications électroniques accessibles au public, ainsi que la confidentialité des données relatives au trafic y afférentes. En particulier, ils interdisent à toute autre personne que les utilisateurs d’écouter, d’intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d’interception ou de surveillance, sans le consentement des utilisateurs concernés sauf lorsque cette personne y est légalement autorisée, conformément à l’article 15, paragraphe 1. Le présent paragraphe n’empêche pas le stockage technique nécessaire à l’acheminement d’une communication, sans préjudice du principe de confidentialité.
[...]
3. Les États membres garantissent que le stockage d’informations, ou l’obtention de l’accès à des informations déjà stockées, dans l’équipement terminal d’un abonné ou d’un utilisateur n’est permis qu’à condition que l’abonné ou l’utilisateur ait donné son accord, après avoir reçu, dans le respect de la directive [95/46], une information claire et complète, entre autres sur les finalités du traitement. Cette disposition ne fait pas obstacle à un stockage ou à un accès techniques visant exclusivement à effectuer la transmission d’une communication par la voie d’un réseau de communications électroniques, ou strictement nécessaires au fournisseur pour la fourniture d’un service de la société de l’information expressément demandé par l’abonné ou l’utilisateur. »

19 L’article 6 de la directive 2002/58, intitulé « Données relatives au trafic », dispose :

« 1. Les données relatives au trafic concernant les abonnés et les utilisateurs traitées et stockées par le fournisseur d’un réseau public de communications ou d’un service de communications électroniques accessibles au public doivent être effacées ou rendues anonymes lorsqu’elles ne sont plus nécessaires à la transmission d’une communication sans préjudice des paragraphes 2, 3 et 5, du présent article ainsi que de l’article 15, paragraphe 1.
2. Les données relatives au trafic qui sont nécessaires pour établir les factures des abonnés et les paiements pour interconnexion peuvent être traitées. Un tel traitement n’est autorisé que jusqu’à la fin de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement.
3. Afin de commercialiser des services de communications électroniques ou de fournir des services à valeur ajoutée, le fournisseur d’un service de communications électroniques accessible au public peut traiter les données visées au paragraphe 1 dans la mesure et pour la durée nécessaires à la fourniture ou à la commercialisation de ces services, pour autant que l’abonné ou l’utilisateur que concernent ces données ait donné son consentement préalable. Les utilisateurs ou abonnés ont la possibilité de retirer à tout moment leur consentement pour le traitement des données relatives au trafic.
[...]
5. Le traitement des données relatives au trafic effectué conformément aux dispositions des paragraphes 1, 2, 3 et 4 doit être restreint aux personnes agissant sous l’autorité des fournisseurs de réseaux publics de communications et de services de communications électroniques accessibles au public qui sont chargées d’assurer la facturation ou la gestion du trafic, de répondre aux demandes de la clientèle, de détecter les fraudes et de commercialiser les services de communications électroniques ou de fournir un service à valeur ajoutée ; ce traitement doit se limiter à ce qui est nécessaire à de telles activités. »

20 L’article 9 de cette directive, intitulé « Données de localisation autres que les données relatives au trafic », prévoit, à son paragraphe 1 :

« Lorsque des données de localisation, autres que des données relatives au trafic, concernant des utilisateurs ou abonnés de réseaux publics de communications ou de services de communications électroniques accessibles au public ou des abonnés à ces réseaux ou services, peuvent être traitées, elles ne le seront qu'après avoir été rendues anonymes ou moyennant le consentement des utilisateurs ou des abonnés, dans la mesure et pour la durée nécessaires à la fourniture d'un service à valeur ajoutée. Le fournisseur du service doit informer les utilisateurs ou les abonnés, avant d'obtenir leur consentement, du type de données de localisation autres que les données relatives au trafic qui sera traité, des objectifs et de la durée de ce traitement, et du fait que les données seront ou non transmises à un tiers en vue de la fourniture du service à valeur ajoutée. [...] »

21 L'article 15 de ladite directive, intitulé « Application de certaines dispositions de la directive [95/46] », énonce :

« 1. 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]. 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 [de l'Union], y compris ceux visés à l'article 6, paragraphes 1 et 2, du traité sur l'Union européenne.

[...]

2. Les dispositions du chapitre III de la directive [95/46] relatif aux recours juridictionnels, à la responsabilité et aux sanctions sont applicables aux dispositions nationales adoptées en application de la présente directive ainsi qu'aux droits individuels résultant de la présente directive.

[...] »

Le règlement 2016/679

22 Le considérant 10 du règlement 2016/679 énonce :

« Afin d'assurer un niveau cohérent et élevé de protection des personnes physiques et de lever les obstacles aux flux de données à caractère personnel au sein de l'Union, le niveau de protection des droits et des libertés des personnes physiques à l'égard du traitement de ces données devrait être équivalent dans tous les États membres. Il convient dès lors d'assurer une application cohérente et homogène des règles de protection des libertés et droits fondamentaux des personnes physiques à l'égard du traitement des données à caractère personnel dans l'ensemble de l'Union. [...] »

23 L'article 2 de ce règlement dispose :

« 1. Le présent règlement s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier.

2. Le présent règlement ne s'applique pas au traitement de données à caractère personnel effectué :

a) dans le cadre d'une activité qui ne relève pas du champ d'application du droit de l'Union ;

b) par les États membres dans le cadre d'activités qui relèvent du champ d'application du chapitre 2 du titre V du traité sur l'Union européenne ;

[...]

d) par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre des menaces pour la sécurité publique et la prévention de telles menaces.

[...]

4. Le présent règlement s'applique sans préjudice de la directive [2000/31], et notamment de ses articles 12 à 15 relatifs à la responsabilité des prestataires de services intermédiaires. »

24 L'article 4 dudit règlement prévoit :

« Aux fins du présent règlement, on entend par :

1) "données à caractère personnel", toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée "personne concernée") ; est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ;

2) "traitement", toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la

collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ;
[...] »

25 L'article 5 du règlement 2016/679 dispose :

« 1. Les données à caractère personnel doivent être :

a) traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence) ;

b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités ; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales (limitation des finalités) ;

c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ;

d) exactes et, si nécessaire, tenues à jour ; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude) ;

e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation) ;

f) traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité) ;

[...] »

26 L'article 6 de ce règlement est libellé comme suit :

« 1. Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie :

[...]

c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;

[...]

3. Le fondement du traitement visé au paragraphe 1, [sous] c) et e), est défini par :

a) le droit de l'Union ; ou

b) le droit de l'État membre auquel le responsable du traitement est soumis.

Les finalités du traitement sont définies dans cette base juridique [...] Cette base juridique peut contenir des dispositions spécifiques pour adapter l'application des règles du présent règlement, entre autres : les conditions générales régissant la licéité du traitement par le responsable du traitement ; les types de données qui font l'objet du traitement ; les personnes concernées ; les entités auxquelles les données à caractère personnel peuvent être communiquées et les finalités pour lesquelles elles peuvent l'être ; la limitation des finalités ; les durées de conservation ; et les opérations et procédures de traitement, y compris les mesures visant à garantir un traitement licite et loyal, telles que celles prévues dans d'autres situations particulières de traitement comme le prévoit le chapitre IX. Le droit de l'Union ou le droit des États membres répond à un objectif d'intérêt public et est proportionné à l'objectif légitime poursuivi.

[...] »

27 L'article 23 dudit règlement prévoit :

« 1. Le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement ou le sous-traitant est soumis peuvent, par la voie de mesures législatives, limiter la portée des obligations et des droits prévus aux articles 12 à 22 et à l'article 34, ainsi qu'à l'article 5 dans la mesure où les dispositions du droit en question correspondent aux droits et obligations prévus aux articles 12 à 22, lorsqu'une telle limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir :

a) la sécurité nationale ;

b) la défense nationale ;

c) la sécurité publique ;

d) la prévention et la détection d'infractions pénales, ainsi que les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces ;
e) d'autres objectifs importants d'intérêt public général de l'Union ou d'un État membre, notamment un intérêt économique ou financier important de l'Union ou d'un État membre, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale ;
f) la protection de l'indépendance de la justice et des procédures judiciaires ;
g) la prévention et la détection de manquements à la déontologie des professions réglementées, ainsi que les enquêtes et les poursuites en la matière ;
h) une mission de contrôle, d'inspection ou de réglementation liée, même occasionnellement, à l'exercice de l'autorité publique, dans les cas visés aux points a) à e) et g) ;
i) la protection de la personne concernée ou des droits et libertés d'autrui ;
j) l'exécution des demandes de droit civil.
2. En particulier, toute mesure législative visée au paragraphe 1 contient des dispositions spécifiques relatives, au moins, le cas échéant :
a) aux finalités du traitement ou des catégories de traitement ;
b) aux catégories de données à caractère personnel ;
c) à l'étendue des limitations introduites ;
d) aux garanties destinées à prévenir les abus ou l'accès ou le transfert illicites ;
e) à la détermination du responsable du traitement ou des catégories de responsables du traitement ;
f) aux durées de conservation et aux garanties applicables, en tenant compte de la nature, de la portée et des finalités du traitement ou des catégories de traitement ;
g) aux risques pour les droits et libertés des personnes concernées ; et
h) au droit des personnes concernées d'être informées de la limitation, à moins que cela risque de nuire à la finalité de la limitation. »

28 Selon l'article 79, paragraphe 1, dudit règlement :

« Sans préjudice de tout recours administratif ou extrajudiciaire qui lui est ouvert, y compris le droit d'introduire une réclamation auprès d'une autorité de contrôle au titre de l'article 77, chaque personne concernée a droit à un recours juridictionnel effectif si elle considère que les droits que lui confère le présent règlement ont été violés du fait d'un traitement de ses données à caractère personnel effectué en violation du présent règlement. »

29 Aux termes de l'article 94 du règlement 2016/679 :

« 1. La directive [95/46] est abrogée avec effet au 25 mai 2018.
2. Les références faites à la directive abrogée s'entendent comme faites au présent règlement. Les références faites au groupe de protection des personnes à l'égard du traitement des données à caractère personnel institué par l'article 29 de la directive [95/46] s'entendent comme faites au comité européen de la protection des données institué par le présent règlement. »

30 L'article 95 de ce règlement dispose :

« Le présent règlement n'impose pas d'obligations supplémentaires aux personnes physiques ou morales quant au traitement dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux publics de communications dans l'Union en ce qui concerne les aspects pour lesquels elles sont soumises à des obligations spécifiques ayant le même objectif énoncées dans la directive [2002/58]. »

Le droit français

Le code de la sécurité intérieure

31 Le livre VIII de la partie législative du code de la sécurité intérieure (ci-après le « CSI »), prévoit, à ses articles L. 801-1 à L. 898-1, des règles relatives au renseignement.

32 L. 811-3 du CSI dispose :

« Pour le seul exercice de leurs missions respectives, les services spécialisés de renseignement peuvent recourir aux techniques mentionnées au titre V du présent livre pour le recueil des renseignements relatifs à la défense et à la promotion des intérêts fondamentaux de la Nation suivants :
1° L'indépendance nationale, l'intégrité du territoire et la défense nationale ;
2° Les intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère ;
3° Les intérêts économiques, industriels et scientifiques majeurs de la France ;
4° La prévention du terrorisme ;
5° La prévention :
a) Des atteintes à la forme républicaine des institutions ;

b) Des actions tendant au maintien ou à la reconstitution de groupements dissous en application de l'article L. 212-1 ;
c) Des violences collectives de nature à porter gravement atteinte à la paix publique ;
6° La prévention de la criminalité et de la délinquance organisées ;
7° La prévention de la prolifération des armes de destruction massive. »

33 L'article L. 811-4 du CSI énonce :

« Un décret en Conseil d'État, pris après avis de la Commission nationale de contrôle des techniques de renseignement, désigne les services, autres que les services spécialisés de renseignement, relevant des ministres de la défense, de l'intérieur et de la justice ainsi que des ministres chargés de l'économie, du budget ou des douanes, qui peuvent être autorisés à recourir aux techniques mentionnées au titre V du présent livre dans les conditions prévues au même livre. Il précise, pour chaque service, les finalités mentionnées à l'article L. 811-3 et les techniques qui peuvent donner lieu à autorisation. »

34 L'article L. 821-1, premier alinéa, du CSI précise ce qui suit :

« La mise en œuvre sur le territoire national des techniques de recueil de renseignement mentionnées aux chapitres Ier à IV du titre V du présent livre est soumise à autorisation préalable du Premier ministre, délivrée après avis de la Commission nationale de contrôle des techniques de renseignement. »

35 L'article L. 821-2 du CSI prévoit :

« L'autorisation mentionnée à l'article L. 821-1 est délivrée sur demande écrite et motivée du ministre de la défense, du ministre de l'intérieur, du ministre de la justice ou des ministres chargés de l'économie, du budget ou des douanes. Chaque ministre ne peut déléguer cette attribution individuellement qu'à des collaborateurs directs habilités au secret de la défense nationale.

La demande précise :

1° La ou les techniques à mettre en œuvre ;
2° Le service pour lequel elle est présentée ;
3° La ou les finalités poursuivies ;
4° Le ou les motifs des mesures ;
5° La durée de validité de l'autorisation ;
6° La ou les personnes, le ou les lieux ou véhicules concernés.

Pour l'application du 6°, les personnes dont l'identité n'est pas connue peuvent être désignées par leurs identifiants ou leur qualité et les lieux ou véhicules peuvent être désignés par référence aux personnes faisant l'objet de la demande.

[…] »

36 Aux termes de l'article L. 821-3, premier alinéa, du CSI :

« La demande est communiquée au président ou, à défaut, à l'un des membres de la Commission nationale de contrôle des techniques de renseignement parmi ceux mentionnés aux 2° et 3° de l'article L. 831-1, qui rend un avis au Premier ministre dans un délai de vingt-quatre heures. Si la demande est examinée par la formation restreinte ou par la formation plénière de la commission, le Premier ministre en est informé sans délai et l'avis est rendu dans un délai de soixante-douze heures. »

37 L'article L. 821-4 du CSI dispose :

« L'autorisation de mise en œuvre des techniques mentionnées aux chapitres Ier à IV du titre V du présent livre est délivrée par le Premier ministre pour une durée maximale de quatre mois. […] L'autorisation comporte les motivations et mentions prévues aux 1° à 6° de l'article L. 821-2. Toute autorisation est renouvelable dans les mêmes conditions que celles prévues au présent chapitre.

Lorsque l'autorisation est délivrée après un avis défavorable de la Commission nationale de contrôle des techniques de renseignement, elle indique les motifs pour lesquels cet avis n'a pas été suivi.

[...] »

38 L'article L. 833-4 du CSI figurant dans le chapitre III de ce titre dispose :

« De sa propre initiative ou lorsqu'elle est saisie d'une réclamation de toute personne souhaitant vérifier qu'aucune technique de renseignement n'est irrégulièrement mise en œuvre à son égard, la commission procède au contrôle de la ou des techniques invoquées en vue de vérifier qu'elles ont été ou sont mises en œuvre dans le respect du présent livre. Elle notifie à l'auteur de la réclamation qu'il a été procédé aux vérifications nécessaires, sans confirmer ni infirmer leur mise en œuvre. »

39 L'article L. 841-1, premier et deuxième alinéas, du CSI est libellé comme suit :

« Sous réserve des dispositions particulières prévues à l'article L. 854-9 du présent code, le Conseil d'État est compétent pour connaître, dans les conditions prévues au chapitre III bis du titre VII du livre VII du code de justice administrative, des requêtes concernant la mise en œuvre des techniques de renseignement mentionnées au titre V du présent livre.

Il peut être saisi par :

1° Toute personne souhaitant vérifier qu'aucune technique de renseignement n'est irrégulièrement mise en œuvre à son égard et justifiant de la mise en œuvre préalable de la procédure prévue à l'article L. 833-4 ;

2° La Commission nationale de contrôle des techniques de renseignement, dans les conditions prévues à l'article L. 833-8. »

40 Le titre V du livre VIII de la partie législative du CSI, relatif aux « techniques de recueil de renseignement soumises à autorisation », comporte, notamment, un chapitre Ier, intitulé « Des accès administratifs aux données de connexion », qui contient les articles L. 851-1 à L. 851-7 du CSI.

41 L'article L. 851-1 du CSI dispose :

« 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 [CPCE] ainsi que des personnes mentionnées aux 1 et 2 du I de l'article 6 de la loi no 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique [(JORF du 22 juin 2004, p. 11168)], 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 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.

Par dérogation à l'article L. 821-2, les demandes écrites et motivées portant sur les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, ou au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée sont directement transmises à la Commission nationale de contrôle des techniques de renseignement par les agents individuellement désignés et habilités des services de renseignement mentionnés aux articles L. 811-2 et L. 811-4. La commission rend son avis dans les conditions prévues à l'article L. 821-3.

Un service du Premier ministre est chargé de recueillir les informations ou documents auprès des opérateurs et des personnes mentionnés au premier alinéa du présent article. La Commission nationale de contrôle des techniques de renseignement dispose d'un accès permanent, complet, direct et immédiat aux informations ou documents collectés.

Les modalités d'application du présent article sont fixées par décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés et de la Commission nationale de contrôle des techniques de renseignement. »

42 L'article L. 851-2 du CSI énonce :

« I. – Dans les conditions prévues au chapitre Ier du titre II du présent livre et pour les seuls besoins de la prévention du terrorisme, peut être individuellement autorisé le recueil en temps réel, sur les réseaux des opérateurs et des personnes mentionnés à l'article L. 851–1, des informations ou documents mentionnés au même article L. 851-1 relatifs à une personne préalablement identifiée susceptible d'être en lien avec une menace. Lorsqu'il existe des raisons sérieuses de penser qu'une ou plusieurs personnes appartenant à l'entourage de la personne concernée par l'autorisation sont susceptibles de fournir des informations au titre de la finalité qui motive l'autorisation, celle-ci peut être également accordée individuellement pour chacune de ces personnes.

I bis. Le nombre maximal des autorisations délivrées en application du présent article en vigueur simultanément est arrêté par le Premier ministre, après avis de la Commission nationale de contrôle des techniques de renseignement. La décision fixant ce contingent et sa répartition entre les ministres mentionnés au premier alinéa de l'article L. 821-2 ainsi que le nombre d'autorisations d'interception délivrées sont portés à la connaissance de la commission.

[...] »

43 L'article L. 851-3 du CSI prévoit :

« I. – Dans les conditions prévues au chapitre Ier du titre II du présent livre et pour les seuls besoins de la prévention du terrorisme, il peut être imposé aux opérateurs et aux personnes mentionnés à l'article L. 851-1 la mise en œuvre sur leurs réseaux de traitements automatisés destinés, en fonction de paramètres précisés dans l'autorisation, à détecter des connexions susceptibles de révéler une menace terroriste.

Ces traitements automatisés utilisent exclusivement les informations ou documents mentionnés à l'article L. 851-1, sans recueillir d'autres données que celles qui répondent à leurs paramètres de conception et sans permettre l'identification des personnes auxquelles les informations ou documents se rapportent.

Dans le respect du principe de proportionnalité, l'autorisation du Premier ministre précise le champ technique de la mise en œuvre de ces traitements.

II. – La Commission nationale de contrôle des techniques de renseignement émet un avis sur la demande d'autorisation relative aux traitements automatisés et les paramètres de détection retenus. Elle dispose d'un accès permanent, complet et direct à ces traitements ainsi qu'aux informations et données recueillies. Elle est informée de toute modification apportée aux traitements et paramètres et peut émettre des recommandations.

La première autorisation de mise en œuvre des traitements automatisés prévue au I du présent article est délivrée pour une durée de deux mois. L'autorisation est renouvelable dans les conditions de durée prévues

au chapitre Ier du titre II du présent livre. La demande de renouvellement comporte un relevé du nombre d'identifiants signalés par le traitement automatisé et une analyse de la pertinence de ces signalements.

III. – Les conditions prévues à l'article L. 871-6 sont applicables aux opérations matérielles effectuées pour cette mise en œuvre par les opérateurs et les personnes mentionnés à l'article L. 851-1.

IV. – Lorsque les traitements mentionnés au I du présent article détectent des données susceptibles de caractériser l'existence d'une menace à caractère terroriste, le Premier ministre ou l'une des personnes déléguées par lui peut autoriser, après avis de la Commission nationale de contrôle des techniques de renseignement donné dans les conditions prévues au chapitre Ier du titre II du présent livre, l'identification de la ou des personnes concernées et le recueil des données y afférentes. Ces données sont exploitées dans un délai de soixante jours à compter de ce recueil et sont détruites à l'expiration de ce délai, sauf en cas d'éléments sérieux confirmant l'existence d'une menace terroriste attachée à une ou plusieurs des personnes concernées.

[…] »

44 L'article L. 851-4 du CSI est libellé comme suit :

« Dans les conditions prévues au chapitre Ier du titre II du présent livre, les données techniques relatives à la localisation des équipements terminaux utilisés mentionnées à l'article L. 851-1 peuvent être recueillies sur sollicitation du réseau et transmises en temps réel par les opérateurs à un service du Premier ministre. »

45 L'article R. 851-5 du CSI, qui figure dans la partie réglementaire de ce code, prévoit :

« I. – Les informations ou documents mentionnés à l'article L. 851-1 sont, à l'exclusion du contenu des correspondances échangées ou des informations consultées :

1° Ceux énumérés aux articles R. 10-13 et R. 10-14 du [CPCE] et à l'article 1er du décret [no 2011-219] ;

2° Les données techniques autres que celles mentionnées au 1° :

a) Permettant de localiser les équipements terminaux ;

b) Relatives à l'accès des équipements terminaux aux réseaux ou aux services de communication au public en ligne ;

c) Relatives à l'acheminement des communications électroniques par les réseaux ;

d) Relatives à l'identification et à l'authentification d'un utilisateur, d'une connexion, d'un réseau ou d'un service de communication au public en ligne ;

e) Relatives aux caractéristiques des équipements terminaux et aux données de configuration de leurs logiciels.

II. – Seuls les informations et documents mentionnés au 1° du I peuvent être recueillis en application de l'article L. 851-1. Ce recueil a lieu en temps différé.

Les informations énumérées au 2° du I ne peuvent être recueillies qu'en application des articles L. 851-2 et L. 851-3 dans les conditions et limites prévues par ces articles et sous réserve de l'application de l'article R. 851-9. »

Le CPCE

46 L'article L. 34-1 du CPCE dispose :

« I. – Le présent article s'applique au traitement des données à caractère personnel dans le cadre de la fourniture au public de services de communications électroniques ; il s'applique notamment aux réseaux qui prennent en charge les dispositifs de collecte de données et d'identification.

II. – Les opérateurs de communications électroniques, et notamment les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, effacent ou rendent anonyme toute donnée relative au trafic, sous réserve des dispositions des III, IV, V et VI.

Les personnes qui fournissent au public des services de communications électroniques établissent, dans le respect des dispositions de l'alinéa précédent, des procédures internes permettant de répondre aux demandes des autorités compétentes.

Les 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, y compris à titre gratuit, sont soumises au respect des dispositions applicables aux opérateurs de communications électroniques en vertu du présent article.

III. – Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales ou d'un manquement à l'obligation définie à l'article L. 336-3 du code de la propriété intellectuelle ou pour les besoins de la prévention des atteintes aux systèmes de traitement automatisé de données prévues et réprimées par les articles 323-1 à 323-3-1 du code pénal et dans le seul but de permettre, en tant que de besoin, la mise à disposition de l'autorité judiciaire ou de la haute autorité mentionnée à l'article L. 331-12 du code de la propriété intellectuelle ou de l'autorité nationale de sécurité des systèmes d'information mentionnée à l'article L. 2321-1 du code de la défense, il peut être différé pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques. Un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés, détermine, dans les limites fixées par le VI, ces catégories de données et la durée de leur conservation, selon l'activité des opérateurs et la nature des communications ainsi que les modalités de compensation, le cas échéant, des

surcoûts identifiables et spécifiques des prestations assurées à ce titre, à la demande de l'État, par les opérateurs.
[...]
VI. – Les données conservées et traitées dans les conditions définies aux III, IV et V 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.
Elles 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.
La conservation et le traitement de ces données s'effectuent dans le respect des dispositions de la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
Les opérateurs prennent toutes mesures pour empêcher une utilisation de ces données à des fins autres que celles prévues au présent article. »
47 L'article R. 10-13 du CPCE est libellé comme suit :
« I. – En application du III de l'article L. 34-1 les opérateurs de communications électroniques conservent pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales :
a) Les informations permettant d'identifier l'utilisateur ;
b) Les données relatives aux équipements terminaux de communication utilisés ;
c) Les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ;
d) Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ;
e) Les données permettant d'identifier le ou les destinataires de la communication.
II. – Pour les activités de téléphonie l'opérateur conserve les données mentionnées au II et, en outre, celles permettant d'identifier l'origine et la localisation de la communication.
III. – La durée de conservation des données mentionnées au présent article est d'un an à compter du jour de l'enregistrement.
IV. – Les surcoûts identifiables et spécifiques supportés par les opérateurs requis par les autorités judiciaires pour la fourniture des données relevant des catégories mentionnées au présent article sont compensés selon les modalités prévues à l'article R. 213-1 du code de procédure pénale. »
48 L'article R. 10-14 du CPCE prévoit :
« I. – En application du IV de l'article L. 34-1 les opérateurs de communications électroniques sont autorisés à conserver pour les besoins de leurs opérations de facturation et de paiement les données à caractère technique permettant d'identifier l'utilisateur ainsi que celles mentionnées aux b, c et d du I de l'article R. 10-13.
II. – Pour les activités de téléphonie, les opérateurs peuvent conserver, outre les données mentionnées au I, les données à caractère technique relatives à la localisation de la communication, à l'identification du ou des destinataires de la communication et les données permettant d'établir la facturation.
III. – Les données mentionnées aux I et II du présent article ne peuvent être conservées que si elles sont nécessaires à la facturation et au paiement des services rendus. Leur conservation devra se limiter au temps strictement nécessaire à cette finalité sans excéder un an.
IV. – Pour la sécurité des réseaux et des installations, les opérateurs peuvent conserver pour une durée n'excédant pas trois mois :
a) Les données permettant d'identifier l'origine de la communication ;
b) Les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ;
c) Les données à caractère technique permettant d'identifier le ou les destinataires de la communication ;
d) Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs. »

La loi nº 2004-575, du 21 juin 2004, pour la confiance dans l'économie numérique

49 L'article 6 de la loi nº 2004-575, du 21 juin 2004, pour la confiance dans l'économie numérique (JORF du 22 juin 2004, p. 11168, ci-après la « LCEN ») prévoit :
« I. – 1. Les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne informent leurs abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner et leur proposent au moins un de ces moyens.
[...]
2. Les personnes physiques ou morales 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 ne peuvent pas voir leur responsabilité civile engagée du fait des activités ou des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de leur caractère illicite ou de faits et circonstances faisant apparaître ce caractère ou si, dès le moment où elles en ont eu cette connaissance, elles ont agi promptement pour retirer ces données ou en rendre l'accès impossible.
[...]

II. – Les personnes mentionnées aux 1 et 2 du I détiennent et conservent les données 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.
Elles fournissent aux personnes qui éditent un service de communication au public en ligne des moyens techniques permettant à celles-ci de satisfaire aux conditions d'identification prévues au III.
L'autorité judiciaire peut requérir communication auprès des prestataires mentionnés aux 1 et 2 du I des données mentionnées au premier alinéa.
Les dispositions des articles 226-17, 226-21 et 226-22 du code pénal sont applicables au traitement de ces données.
Un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés, définit les données mentionnées au premier alinéa et détermine la durée et les modalités de leur conservation.
[...] »

Le décret nº 2011-219

50 Le chapitre Ier du décret nº 2011-219, pris sur le fondement de l'article 6, II, dernier alinéa, de la LCEN, contient les articles 1 à 4 de ce décret.

51 L'article 1er du décret nº 2011-219 dispose :

« Les données mentionnées au II de l'article 6 de la [LCEN], que les personnes sont tenues de conserver en vertu de cette disposition, sont les suivantes :

1° Pour les personnes mentionnées au 1 du I du même article et pour chaque connexion de leurs abonnés :

a) L'identifiant de la connexion ;

b) L'identifiant attribué par ces personnes à l'abonné ;

c) L'identifiant du terminal utilisé pour la connexion lorsqu'elles y ont accès ;

d) Les dates et heure de début et de fin de la connexion ;

e) Les caractéristiques de la ligne de l'abonné ;

2° Pour les personnes mentionnées au 2 du I du même article et pour chaque opération de création :

a) L'identifiant de la connexion à l'origine de la communication ;

b) L'identifiant attribué par le système d'information au contenu, objet de l'opération ;

c) Les types de protocoles utilisés pour la connexion au service et pour le transfert des contenus ;

d) La nature de l'opération ;

e) Les date et heure de l'opération ;

f) L'identifiant utilisé par l'auteur de l'opération lorsque celui-ci l'a fourni ;

3° Pour les personnes mentionnées aux 1 et 2 du I du même article, les informations fournies lors de la souscription d'un contrat par un utilisateur ou lors de la création d'un compte :

a) Au moment de la création du compte, l'identifiant de cette connexion ;

b) Les nom et prénom ou la raison sociale ;

c) Les adresses postales associées ;

d) Les pseudonymes utilisés ;

e) Les adresses de courrier électronique ou de compte associées ;

f) Les numéros de téléphone ;

g) Le mot de passe ainsi que les données permettant de le vérifier ou de le modifier, dans leur dernière version mise à jour ;

4° Pour les personnes mentionnées aux 1 et 2 du I du même article, lorsque la souscription du contrat ou du compte est payante, les informations suivantes relatives au paiement, pour chaque opération de paiement :

a) Le type de paiement utilisé ;

b) La référence du paiement ;

c) Le montant ;

d) La date et l'heure de la transaction.

Les données mentionnées aux 3° et 4° ne doivent être conservées que dans la mesure où les personnes les collectent habituellement. »

52 L'article 2 de ce décret est libellé comme suit :

« La contribution à une création de contenu comprend les opérations portant sur :

a) Des créations initiales de contenus ;

b) Des modifications des contenus et de données liées aux contenus ;

c) Des suppressions de contenus. »

53 L'article 3 dudit décret prévoit :

« La durée de conservation des données mentionnées à l'article 1er est d'un an :

a) S'agissant des données mentionnées aux 1° et 2°, à compter du jour de la création des contenus, pour chaque opération contribuant à la création d'un contenu telle que définie à l'article 2 ;

b) S'agissant des données mentionnées au 3°, à compter du jour de la résiliation du contrat ou de la fermeture du compte ;

c) S'agissant des données mentionnées au 4°, à compter de la date d'émission de la facture ou de l'opération de paiement, pour chaque facture ou opération de paiement. »

Le droit belge

54 La loi du 29 mai 2016 a modifié, notamment, la loi du 13 juin 2005 relative aux communications électroniques (*Moniteur belge* du 20 juin 2005, p. 28070, ci-après la « loi du 13 juin 2005 »), le code d'instruction criminelle et la loi du 30 novembre 1998 organique des services de renseignement et de sécurité (*Moniteur belge* du 18 décembre 1998, p. 40312, ci-après la « loi du 30 novembre 1998 »).

55 L'article 126 de la loi du 13 juin 2005, dans sa version issue de la loi du 29 mai 2016, dispose :

« § 1er. Sans préjudice de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, les fournisseurs au public de services de téléphonie, en ce compris par internet, d'accès à l'Internet, de courrier électronique par Internet, les opérateurs fournissant des réseaux publics de communications électroniques ainsi que les opérateurs fournissant un de ces services, conservent les données visées au paragraphe 3, qui sont générées ou traitées par eux dans le cadre de la fourniture des services de communications concernés.

Le présent article ne porte pas sur le contenu des communications.

L'obligation de conserver les données visées au paragraphe 3 s'applique également aux appels infructueux, pour autant que ces données soient, dans le cadre de la fourniture des services de communications concernés :

1° en ce qui concerne les données de la téléphonie, générées ou traitées par les opérateurs de services de communications électroniques accessibles au public ou d'un réseau public de communications électroniques, ou

2° en ce qui concerne les données de l'internet, journalisées par ces fournisseurs.

§ 2. Seules les autorités suivantes peuvent obtenir, sur simple demande, des fournisseurs et opérateurs visés au paragraphe 1er, alinéa 1er, des données conservées en vertu du présent article, pour les finalités et selon les conditions énumérées ci-dessous :

1° les autorités judiciaires, en vue de la recherche, de l'instruction et de la poursuite d'infractions, pour l'exécution des mesures visées aux articles 46bis et 88bis du Code d'instruction criminelle et dans les conditions fixées par ces articles ;

2° les services de renseignement et de sécurité, afin d'accomplir des missions de renseignement en ayant recours aux méthodes de recueil de données visées aux articles 16/2, 18/7 et 18/8 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et dans les conditions fixées par cette loi ;

3° tout officier de police judiciaire de l'[Institut belge des services postaux et des télécommunications], en vue de la recherche, de l'instruction et de la poursuite d'infractions aux articles 114, 124 et au présent article ;

4° les services d'urgence offrant de l'aide sur place, lorsque, à la suite d'un appel d'urgence, ils n'obtiennent pas du fournisseur ou de l'opérateur concerné les données d'identification de l'appelant à l'aide de la base de données visée à l'article 107, § 2, alinéa 3, ou obtiennent des données incomplètes ou incorrectes. Seules les données d'identification de l'appelant peuvent être demandées et au plus tard dans les 24 heures de l'appel ;

5° l'officier de police judiciaire de la Cellule des personnes disparues de la Police Fédérale, dans le cadre de sa mission d'assistance à personne en danger, de recherche de personnes dont la disparition est inquiétante et lorsqu'il existe des présomptions ou indices sérieux que l'intégrité physique de la personne disparue se trouve en danger imminent. Seules les données visées au paragraphe 3, alinéas 1 et 2, relatives à la personne disparue et conservées au cours des 48 heures précédant la demande d'obtention des données peuvent être demandées à l'opérateur ou au fournisseur concerné par l'intermédiaire d'un service de police désigné par le Roi ;

6° le Service de médiation pour les télécommunications, en vue de l'identification de la personne ayant effectué une utilisation malveillante d'un réseau ou d'un service de communications électroniques, conformément aux conditions visées à l'article 43bis, § 3, 7°, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques. Seules les données d'identification peuvent être demandées.

Les fournisseurs et opérateurs visés au paragraphe 1er, alinéa 1er, font en sorte que les données visées au paragraphe 3, soient accessibles de manière illimitée à partir de la Belgique et que ces données et toute autre information nécessaire concernant ces données puissent être transmises sans délai et aux seules autorités visées au présent paragraphe.

Sans préjudice d'autres dispositions légales, les fournisseurs et opérateurs visés au paragraphe 1er, alinéa 1er, ne peuvent utiliser les données conservées en vertu du paragraphe 3 pour d'autres finalités.

§ 3. Les données visant à identifier l'utilisateur ou l'abonné et les moyens de communication, à l'exclusion des données spécifiquement prévues aux alinéas 2 et 3, sont conservées pendant douze mois à compter de la date à partir de laquelle une communication est possible pour la dernière fois à l'aide du service utilisé.

Les données relatives à l'accès et la connexion de l'équipement terminal au réseau et au service et à la localisation de cet équipement, y compris le point de terminaison du réseau, sont conservées pendant douze mois à partir de la date de la communication.

Les données de communication, à l'exclusion du contenu, en ce compris leur origine et leur destination, sont conservées pendant douze mois à partir de la date de la communication.
Le Roi fixe, par arrêté délibéré en Conseil des ministres, sur proposition du ministre de la Justice et du ministre [compétent pour les matières relatives aux communications électroniques], et après avis de la Commission de la protection de la vie privée et de l'Institut, les données à conserver par type de catégories visées aux alinéas 1 à 3 ainsi que les exigences auxquelles ces données doivent répondre.
[...] »

Les litiges au principal et les questions préjudicielles

L'affaire C-511/18

56 Par des requêtes introduites les 30 novembre 2015 et 16 mars 2016, jointes dans la procédure au principal, la Quadrature du Net, French Data Network et la Fédération des fournisseurs d'accès à Internet associatifs ainsi que Igwan.net ont saisi le Conseil d'État (France) de recours tendant à l'annulation des décrets n^{os} 2015-1185, 2015-1211, 2015-1639 et 2016-67, au motif, notamment, qu'ils méconnaîtraient la Constitution française, la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (ci-après la « CEDH ») ainsi que les directives 2000/31 et 2002/58, lues à la lumière des articles 7, 8 et 47 de la Charte.

57 S'agissant, en particulier, des moyens tirés de la méconnaissance de la directive 2000/31, la juridiction de renvoi relève que les dispositions de l'article L. 851-3 du CSI imposent aux opérateurs de communications électroniques et aux prestataires techniques « la mise en œuvre sur leurs réseaux de traitements automatisés destinés, en fonction de paramètres précisés dans l'autorisation, à détecter des connexions susceptibles de révéler une menace terroriste ». Cette technique viserait à recueillir uniquement pendant une durée limitée, parmi l'ensemble des données de connexion traitées par ces opérateurs et ces prestataires, celles de ces données qui pourraient présenter un lien avec une telle infraction grave. Dans ces conditions, lesdites dispositions, qui n'imposeraient pas une obligation générale de surveillance active, ne méconnaîtraient pas l'article 15 de la directive 2000/31.

58 En ce qui concerne les moyens tirés de la méconnaissance de la directive 2002/58, la juridiction de renvoi considère qu'il résulte notamment des dispositions de cette directive ainsi que de l'arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a. (C-203/15 et C-698/15, ci-après l'« arrêt Tele2 », EU:C:2016:970), que les dispositions nationales imposant des obligations aux fournisseurs de services de communications électroniques, telles que la conservation généralisée et indifférenciée des données de trafic et des données de localisation de leurs utilisateurs et de leurs abonnés, aux fins mentionnées à l'article 15, paragraphe 1, de ladite directive, parmi lesquelles figurent la sauvegarde de la sécurité nationale, de la défense et de la sécurité publique, relèvent du champ d'application de la même directive dans la mesure où ces réglementations régissent l'activité desdits fournisseurs. Il en irait de même des réglementations régissant l'accès des autorités nationales aux données ainsi que leur utilisation.

59 La juridiction de renvoi en déduit que relèvent du champ d'application de la directive 2002/58 tant l'obligation de conservation résultant de l'article L. 851-1 du CSI que les accès administratifs auxdites données, y compris ceux en temps réel, prévus aux articles L. 851-1, L. 851-2 et L. 851-4 dudit code. Il en va de même, selon cette juridiction, des dispositions de l'article L. 851-3 de ce même code qui, si elles ne font pas peser sur les opérateurs concernés une obligation générale 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.

60 En revanche, cette juridiction considère que ne relèvent pas du champ d'application de la directive 2002/58 les dispositions du CSI visées par les demandes d'annulation qui portent sur des techniques de recueil de renseignement directement mises en œuvre par l'État, sans régir les activités des fournisseurs de services de communications électroniques en leur imposant des obligations spécifiques. Ces dispositions ne sauraient donc être regardées comme mettant en œuvre le droit de l'Union, de telle sorte que les moyens tirés de la méconnaissance par celles-ci de la directive 2002/58 ne pourraient être utilement invoqués.

61 Ainsi, en vue de trancher les litiges portant sur la légalité des décrets n^{os} 2015-1185, 2015-1211, 2015-1639 et 2016-67 au regard de la directive 2002/58 en tant qu'ils ont été pris pour la mise en œuvre des articles L. 851-1 à L. 851-4 du CSI, se poseraient trois questions d'interprétation du droit de l'Union.

62 S'agissant de l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58, la juridiction de renvoi s'interroge, en premier lieu, sur le point de savoir si une obligation de conservation généralisée et indifférenciée imposée aux fournisseurs de services de communications électroniques sur le fondement des articles L. 851-1 et R. 851-5 du CSI ne doit pas être regardée, notamment eu égard aux garanties et aux contrôles 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 et les exigences de la sécurité nationale, dont la responsabilité incombe aux seuls États membres en vertu de l'article 4 TUE.

63 En ce qui concerne, en deuxième lieu, les autres obligations susceptibles d'être imposées aux fournisseurs de services de communications électroniques, la juridiction de renvoi relève que les dispositions de l'article L. 851-2 du CSI autorisent, pour les seuls besoins de la prévention du terrorisme, le recueil des

informations ou des documents prévus à l'article L. 851-1 de ce code, auprès des mêmes personnes. Ce recueil, qui ne concernerait qu'un ou plusieurs individus préalablement identifiés comme étant susceptibles d'être en lien avec une menace terroriste, s'effectuerait en temps réel. Il en irait de même des dispositions de l'article L. 851-4 dudit code autorisant la transmission en temps réel par les opérateurs des seules données techniques relatives à la localisation des équipements terminaux. Ces techniques régiraient pour des finalités et selon des modalités différentes des accès administratifs en temps réel aux données conservées au titre du CPCE et de la LCEN, sans pour autant faire peser sur les fournisseurs concernés une exigence de conservation supplémentaire par rapport à ce qui serait nécessaire à la facturation et à la fourniture de leurs services. De même, les dispositions de l'article L. 851-3 du CSI, qui prévoient une obligation pour les fournisseurs de services de mettre en œuvre sur leurs réseaux une analyse automatisée des connexions, n'impliqueraient pas davantage une conservation généralisée et indifférenciée.

64 Or, d'une part, la juridiction de renvoi considère que tant la conservation généralisée et indifférenciée que les accès en temps réel aux données de connexion présentent, dans un contexte marqué par des menaces graves et persistantes pour la sécurité nationale, tenant en particulier au risque terroriste, une utilité opérationnelle sans équivalent. En effet, la conservation généralisée et indifférenciée permettrait aux services de renseignement d'accéder aux données relatives aux communications avant que soient identifiées les raisons de considérer que la personne concernée présente une menace pour la sécurité publique, la défense ou la sûreté de l'État. En outre, les accès en temps réel aux données de connexion permettraient de suivre, avec une forte réactivité, les comportements d'individus susceptibles de représenter une menace immédiate pour l'ordre public.

65 D'autre part, la technique prévue à l'article L. 851-3 du CSI permettrait de détecter, sur le fondement de critères précisément définis à cette fin, les individus dont les comportements sont susceptibles, compte tenu de leurs modes de communication, de révéler une menace terroriste.

66 En troisième lieu, s'agissant de l'accès des autorités compétentes aux données conservées, la juridiction de renvoi se demande si la directive 2002/58, lue à la lumière de la Charte, 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 prévues par le droit national lorsque que celles-ci assurent l'effectivité du droit au recours.

67 S'agissant de ces autres garanties procédurales, la juridiction de renvoi précise notamment que toute personne souhaitant vérifier qu'aucune technique de renseignement n'est irrégulièrement mise en œuvre à son égard peut saisir une formation spécialisée du Conseil d'État à laquelle il appartient de vérifier, au vu des éléments qui lui sont communiqués hors procédure contradictoire si le requérant a fait l'objet d'une technique et si celle-ci a été mise en œuvre en conformité avec le livre VIII du CSI. Les pouvoirs dont cette formation serait investie pour instruire les requêtes garantiraient l'effectivité du contrôle juridictionnel qu'elle exerce. Ainsi, elle serait compétente 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. En outre, il appartiendrait à la Commission nationale de contrôle des techniques de renseignement de vérifier que les techniques de recueil de renseignement sont mises en œuvre, sur le territoire national, conformément aux exigences découlant du CSI. Ainsi, la circonstance que les dispositions législatives en cause au principal ne prévoient pas la notification aux personnes concernées des mesures de surveillance dont elles ont fait l'objet ne constituerait pas, par elle-même, une atteinte excessive au droit au respect de la vie privée.

68 C'est dans ces conditions que le Conseil d'État a décidé de surseoir à statuer et de poser à la Cour les questions préjudicielles suivantes :

« 1) 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 [2002/58], ne doit-elle pas être regardée, dans un contexte marqué par des menaces graves et persistantes pour la sécurité nationale, et en particulier par le risque terroriste, comme une ingérence justifiée par le droit à la sûreté garanti à l'article 6 de la [Charte] et les exigences de la sécurité nationale, dont la responsabilité incombe aux seuls États membres en vertu de l'article 4 [TUE] ?

2) La directive [2002/58] lue à la lumière de la [Charte] doit-elle être interprétée en ce sens qu'elle autorise des mesures législatives, 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 ?

3) La directive [2002/58], lue à la lumière de la [Charte], doit-elle 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 de telles procédures peuvent-elles 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 ? »

L'affaire C-512/18

69 Par une requête introduite le 1er septembre 2015, French Data Network, la Quadrature du Net et la Fédération des fournisseurs d'accès à Internet associatifs ont saisi le Conseil d'État d'un recours en annulation de la décision implicite de rejet née du silence gardé par le Premier ministre sur leur demande d'abrogation de l'article R. 10-13 du CPCE ainsi que du décret no 2011-219, au motif, notamment, que ces textes méconnaîtraient l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 de la Charte. Privacy International ainsi que le Center for Democracy and Technology ont été admises à intervenir dans la procédure au principal.

70 S'agissant de l'article R. 10-13 du CPCE et de l'obligation de conservation généralisée et indifférenciée des données relatives aux communications qui y est prévue, la juridiction de renvoi, qui exprime des considérations similaires à celles émises dans le cadre de l'affaire C-511/18, fait observer qu'une telle conservation permet à l'autorité judiciaire d'accéder aux données relatives aux communications qu'un individu a effectuées avant d'être suspecté d'avoir commis une infraction pénale, de telle sorte que cette conservation présente une utilité sans équivalent pour la recherche, la constatation et la poursuite des infractions pénales.

71 En ce qui concerne le décret no 2011-219, la juridiction de renvoi estime que l'article 6, II, de la LCEN, qui impose une obligation de détention et de conservation des seules données relatives à la création de contenu, entre non pas dans le champ d'application de la directive 2002/58, dans la mesure où celui-ci est limité, conformément à son article 3, paragraphe 1, à la fourniture de services de communications électroniques accessibles au public sur les réseaux publics de communications dans l'Union, mais dans le champ d'application de la directive 2000/31.

72 Cette juridiction estime toutefois qu'il ressort de l'article 15, paragraphes 1 et 2, de la directive 2000/31 que celle-ci n'instaure pas une interdiction de principe de conserver des données relatives à la création de contenu, à laquelle il pourrait seulement être dérogé par exception. Ainsi, se poserait la question de savoir si les articles 12, 14 et 15 de ladite directive, lus à la lumière des articles 6 à 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, doivent être interprétés en ce sens qu'ils permettent à un État membre d'instaurer une réglementation nationale, telle que l'article 6, II, de la LCEN, qui impose aux personnes concernées de conserver les données 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, afin que l'autorité judiciaire puisse, le cas échéant, en requérir communication en vue de faire respecter les règles relatives à la responsabilité civile ou pénale.

73 C'est dans ces conditions que le Conseil d'État a décidé de surseoir à statuer et de poser à la Cour les questions préjudicielles suivantes :

« 1) 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 [2002/58], ne doit-elle pas être regardée, notamment eu égard aux garanties et contrôles dont sont assortis ensuite le recueil et l'utilisation de ces données de connexion, comme une ingérence justifiée par le droit à la sûreté garanti à l'article 6 de la [Charte] et les exigences de la sécurité nationale, dont la responsabilité incombe aux seuls États membres en vertu de l'article 4 [TUE] ?

2) Les dispositions de la directive [2000/31], lues à la lumière des articles 6, 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la [Charte], doivent-elles être interprétées en ce sens qu'elles permettent à un État d'instaurer une réglementation nationale imposant aux personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne et aux personnes physiques ou morales 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, de conserver les données 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, afin que l'autorité judiciaire puisse, le cas échéant, en requérir communication en vue de faire respecter les règles relatives à la responsabilité civile ou pénale ? »

L'affaire C-520/18

74 Par des requêtes introduites les 10 janvier, 16 janvier, 17 janvier et 18 janvier 2017, jointes dans le cadre de la procédure au principal, l'Ordre des barreaux francophones et germanophone, l'Académie Fiscale ASBL et UA, la Liga voor Mensenrechten ASBL et la Ligue des Droits de l'Homme ASBL ainsi que VZ, WY et XX ont saisi la Cour constitutionnelle (Belgique) de recours visant l'annulation de la loi du 29 mai 2016, au motif que celle-ci violerait les articles 10 et 11 de la Constitution belge, lue en combinaison avec les articles 5, 6 à 11, 14, 15, 17 et 18 de la CEDH, les articles 7, 8, 11 et 47 ainsi que l'article 52, paragraphe 1, de la Charte, l'article 17 du pacte international relatif aux droits civils et politiques, adopté par l'Assemblée générale des Nations unies le 16 décembre 1966 et entré en vigueur le 23 mars 1976, les principes généraux de sécurité

juridique, de proportionnalité et d'autodétermination en matière d'information ainsi que l'article 5, paragraphe 4, du TUE.

75 À l'appui de leurs recours, les requérants au principal font valoir en substance que l'illégalité de la loi du 29 mai 2016 tient notamment au fait que celle-ci dépasse les limites du strict nécessaire et ne prévoit pas de garanties de protection suffisantes. En particulier, ni ses dispositions relatives à la conservation des données ni celles régissant l'accès des autorités aux données conservées ne répondraient aux exigences découlant de l'arrêt du 8 avril 2014, Digital Rights Ireland e.a. (C-293/12 et C-594/12, ci-après l'« arrêt Digital Rights », EU:C:2014:238), et de l'arrêt du 21 décembre 2016, Tele2 (C-203/15 et C-698/15, EU:C:2016:970). En effet, ces dispositions comporteraient le risque que soient établis des profils de personnalité, avec les possibles abus en découlant de la part des autorités compétentes, et ne prévoiraient pas non plus un niveau approprié de sécurisation et de protection des données conservées. Enfin, cette loi couvrirait des personnes soumises au secret professionnel ainsi que des personnes ayant une obligation de confidentialité, et concernerait des données de communication sensibles, à caractère personnel, sans comporter de garanties spéciales aux fins de protéger ces dernières données.

76 La juridiction de renvoi relève que les données que doivent conserver les fournisseurs de services de téléphonie, en ce compris par Internet, d'accès à Internet et de courrier électronique par Internet ainsi que les opérateurs fournissant des réseaux publics de communications électroniques, en vertu de la loi du 29 mai 2016, sont identiques à celles énumérées par la directive 2006/24/CE du Parlement européen et du Conseil, 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 (JO 2006, L 105, p. 54), sans que soit prévue une distinction quant aux personnes concernées ou en fonction de l'objectif poursuivi. À ce dernier égard, cette juridiction précise que l'objectif poursuivi par le législateur au moyen de cette loi est non seulement de lutter contre le terrorisme et la pédopornographie, mais également de pouvoir utiliser les données conservées dans une grande variété de situations dans le cadre de l'enquête pénale. En outre, la juridiction de renvoi constate qu'il ressort de l'exposé des motifs de ladite loi que le législateur national a considéré qu'il était impossible, à la lumière de l'objectif poursuivi, de mettre en place une obligation de conservation ciblée et différenciée, et qu'il a choisi d'assortir l'obligation de conservation générale et indifférenciée de garanties strictes, tant sur le plan des données conservées que sur le plan de l'accès à celles-ci, afin de limiter à un minimum l'ingérence dans le droit au respect de la vie privée.

77 La juridiction de renvoi ajoute que l'article 126, paragraphe 2, 1° et 2°, de la loi du 13 juin 2005, dans sa version issue de la loi du 29 mai 2016, prévoit les conditions dans lesquelles, respectivement, les autorités judiciaires et les services de renseignement et de sécurité peuvent obtenir l'accès aux données conservées, de telle sorte que l'examen de la légalité de cette loi au regard des exigences du droit de l'Union devrait être suspendu jusqu'à ce que la Cour rende ses décisions dans deux procédures préjudicielles, pendantes devant elles, relatives à un tel accès.

78 Enfin, la juridiction de renvoi relève que la loi du 29 mai 2016 vise à permettre une instruction pénale efficace et des sanctions effectives en cas d'abus sexuels à l'égard de mineurs ainsi qu'à rendre possible l'identification de l'auteur d'un tel délit, même lorsqu'il est fait usage de moyens de communications électroniques. Lors de la procédure devant elle, l'attention aurait été attirée à cet égard sur les obligations positives découlant des articles 3 et 8 de la CEDH. Ces obligations pourraient également découler des dispositions correspondantes de la Charte, susceptibles d'avoir des répercussions sur l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58.

79 C'est dans ces conditions que la Cour constitutionnelle a décidé de surseoir à statuer et de poser à la Cour les questions préjudicielles suivantes :

« 1) L'article 15, paragraphe 1, de la directive [2002/58], lu en combinaison avec le droit à la sécurité, garanti par l'article 6 de la [Charte], et le droit au respect des données personnelles, tel que garanti par les articles 7, 8 et 52, [paragraphe] l, de la [Charte], doit-il être interprété en ce sens qu'il s'oppose à une réglementation nationale telle que celle en cause, qui prévoit une obligation générale pour les opérateurs et fournisseurs de services de communications électroniques de conserver les données de trafic et de localisation au sens de la directive [2002/58], générées ou traitées par eux dans le cadre de la fourniture de ces services, réglementation nationale qui n'a pas seulement pour objectif la recherche, la détection et la poursuite de faits de criminalité grave, mais également la garantie de la sécurité nationale, de la défense du territoire et de la sécurité publique, la recherche, la détection et la poursuite d'autres faits que ceux de criminalité grave ou la prévention d'un usage interdit des systèmes de communications électroniques, ou la réalisation d'un autre objectif identifié par l'article 23, paragraphe l, du règlement [2016/679] et qui est en outre sujette à des garanties précisées dans cette réglementation sur le plan de la conservation des données et de l'accès à celles-ci ?

2) L'article 15, paragraphe l, de la directive [2002/58], combiné avec les articles 4, 7, 8, 11 et 52, paragraphe l, de la [Charte], doit-il être interprété en ce sens qu'il s'oppose à une réglementation nationale telle celle en cause, qui prévoit une obligation générale pour les opérateurs et fournisseurs de services de

communications électroniques de conserver les données de trafic et de localisation au sens de la directive [2002/58], générées ou traitées par eux dans le cadre de la fourniture de ces services, si cette réglementation a notamment pour objet de réaliser les obligations positives incombant à l'autorité en vertu des articles 4 et [7] de la Charte, consistant à prévoir un cadre légal qui permette une enquête pénale effective et une répression effective de l'abus sexuel des mineurs et qui permette effectivement d'identifier l'auteur du délit, même lorsqu'il est fait usage de moyens de communications électroniques ?

3) Si, sur la base des réponses données à la première ou à la deuxième question préjudicielle, la Cour constitutionnelle devait arriver à la conclusion que la loi litigieuse méconnaît une ou plusieurs des obligations découlant des dispositions mentionnées dans ces questions, pourrait-elle maintenir provisoirement les effets de la loi du [29 mai 2016] afin d'éviter une insécurité juridique et de permettre que les données collectées et conservées précédemment puissent encore être utilisées pour les objectifs visés par la loi ? »

Sur la procédure devant la Cour

80 Par décision du président de la Cour du 25 septembre 2018, les affaires C-511/18 et C-512/18 ont été jointes aux fins des procédures écrite et orale ainsi que de l'arrêt. L'affaire C-520/18 a été jointe à ces affaires par décision du président de la Cour du 9 juillet 2020 aux fins de l'arrêt.

Sur les questions préjudicielles

Sur les premières questions dans les affaires C-511/18 et C-512/18 ainsi que sur les première et deuxième questions dans l'affaire C-520/18

81 Par les premières questions dans les affaires C-511/18 et C-512/18 ainsi que par les première et deuxième questions dans l'affaire C-520/18, qu'il convient d'examiner conjointement, les juridictions de renvoi cherchent, en substance, à savoir si l'article 15, paragraphe 1, de la directive 2002/58 doit être interprété en ce sens qu'il s'oppose à une réglementation nationale imposant aux fournisseurs de services de communications électroniques, à des fins prévues à cet article 15, paragraphe 1, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation.

Observations liminaires

82 Il ressort des dossiers dont dispose la Cour que les réglementations en cause au principal couvrent l'ensemble des moyens de communications électroniques et englobent l'ensemble des utilisateurs de ces moyens, sans qu'une différenciation ou une exception ne soit faite à cet égard. En outre, les données que ces réglementations imposent aux fournisseurs de services de communications électroniques de conserver sont, en particulier, celles qui sont nécessaires pour retrouver la source d'une communication et la destination de celle-ci, déterminer la date, l'heure, la durée et le type de la communication, identifier le matériel de communication utilisé ainsi que localiser les équipements terminaux et les communications, données au nombre desquelles figurent, notamment, le nom et l'adresse de l'utilisateur, les numéros de téléphone de l'appelant et de l'appelé ainsi que l'adresse IP pour les services Internet. En revanche, lesdites données ne couvrent pas le contenu des communications concernées.

83 Ainsi, les données qui doivent, en vertu des réglementations nationales en cause au principal, être conservées pendant un an permettent, notamment, de savoir quelle est la personne avec laquelle l'utilisateur d'un moyen de communication électronique a communiqué et par quel moyen cette communication a eu lieu, de déterminer la date, l'heure et la durée des communications et des connexions à Internet ainsi que l'endroit à partir duquel celles-ci ont eu lieu, et de connaître la localisation des équipements terminaux sans qu'une communication ne soit nécessairement acheminée. En outre, elles offrent la possibilité de déterminer la fréquence des communications de l'utilisateur avec certaines personnes pendant une période donnée. Enfin, s'agissant de la réglementation nationale en cause dans les affaires C-511/18 et C-512/18, il semble que celle-ci, en ce qu'elle couvre également les données relatives à l'acheminement des communications électroniques par les réseaux, permettent également d'identifier la nature des informations consultées en ligne.

84 Quant aux finalités poursuivies, il y a lieu de relever que les réglementations en cause dans les affaires C-511/18 et C-512/18 visent, entre autres finalités, la recherche, la constatation et la poursuite des infractions pénales en général, l'indépendance nationale, l'intégrité du territoire et la défense nationale, les intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux de la France, les intérêts économiques, industriels et scientifiques majeurs de la France, ainsi que la prévention du terrorisme, des atteintes à la forme républicaine des institutions et des violences collectives de nature à porter gravement atteinte à la paix publique. Pour ce qui est de la réglementation en cause dans l'affaire C-520/18, celle-ci a pour objectifs, entre autres, la recherche, la détection et la poursuite d'infractions pénales ainsi que la sauvegarde de la sécurité nationale, de la défense du territoire et de la sécurité publique.

85 Les juridictions de renvoi s'interrogent, en particulier, sur les incidences éventuelles quant à l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58, du droit à la sécurité consacré à l'article 6 de la Charte. De même, elles se demandent si l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte que comporte la conservation des données prévue par les réglementations en cause au principal peut, au regard de l'existence de règles restreignant l'accès des autorités nationales aux données conservées, être regardée comme étant justifiée. En outre, selon le Conseil d'État, cette question se posant dans un contexte marqué par des menaces graves et persistantes pour la sécurité nationale, elle doit

également être appréciée au regard de l'article 4, paragraphe 2, TUE. La Cour constitutionnelle, quant à elle, souligne que la réglementation nationale en cause dans l'affaire C-520/18 met également en œuvre des obligations positives découlant des articles 4 et 7 de la Charte, consistant à prévoir un cadre légal permettant la répression effective de l'abus sexuel des mineurs.

86 Si tant le Conseil d'État que la Cour constitutionnelle partent de la prémisse selon laquelle les réglementations nationales en cause au principal, qui régissent la conservation des données relatives au trafic et des données de localisation ainsi que l'accès à ces données par les autorités nationales à des fins prévues à l'article 15, paragraphe 1, de la directive 2002/58, telles que la sauvegarde de la sécurité nationale, relèvent du champ d'application de cette directive, certaines parties au principal et certains des États membres ayant soumis des observations écrites à la Cour expriment un avis divergent à cet égard, en particulier concernant l'interprétation de l'article 1er, paragraphe 3, de ladite directive. Il convient donc d'examiner, tout d'abord, si lesdites réglementations relèvent du champ d'application de cette même directive.

Sur le champ d'application de la directive 2002/58

87 La Quadrature du Net, la Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net, Privacy International et le Center for Democracy and Technology avancent en substance, en se prévalant à cet égard de la jurisprudence de la Cour portant sur le champ d'application de la directive 2002/58, que tant la conservation des données que l'accès aux données conservées relèvent de ce champ d'application, que cet accès ait lieu en temps différé ou en temps réel. En effet, l'objectif de sauvegarde de la sécurité nationale étant expressément mentionné à l'article 15, paragraphe 1, de cette directive, la poursuite de cet objectif n'entraînerait pas l'inapplicabilité de ladite directive. L'article 4, paragraphe 2, TUE, visé par les juridictions de renvoi, n'affecterait pas cette appréciation.

88 S'agissant des mesures de renseignement que les autorités françaises compétentes mettent directement en œuvre sans régir l'activité des fournisseurs de services de communications électroniques en leur imposant des obligations spécifiques, le Center for Democracy and Technology fait observer que ces mesures relèvent nécessairement du champ d'application de la directive 2002/58 et de celui de la Charte, dès lors qu'elles constituent des dérogations au principe de confidentialité garanti à l'article 5 de cette directive. Lesdites mesures devraient donc respecter les exigences découlant de l'article 15, paragraphe 1, de celle-ci.

89 En revanche, les gouvernements français, tchèque et estonien, l'Irlande, les gouvernements chypriote, hongrois, polonais, suédois et du Royaume-Uni font, en substance, valoir que la directive 2002/58 ne s'applique pas à des réglementations nationales telles que celles en cause au principal, dans la mesure où celles-ci ont pour finalité la sauvegarde de la sécurité nationale. Les activités des services de renseignement, en ce qu'elles tiennent au maintien de l'ordre public ainsi qu'à la sauvegarde de la sécurité intérieure et de l'intégrité territoriale, relèveraient des fonctions essentielles des États membres et, par suite, seraient de la seule compétence de ces derniers, comme en témoignerait notamment l'article 4, paragraphe 2, troisième phrase, TUE.

90 Ces gouvernements ainsi que l'Irlande se réfèrent de surcroît à l'article 1er, paragraphe 3, de la directive 2002/58, qui exclurait du champ d'application de celle-ci, à l'instar de ce que prévoyait déjà l'article 3, paragraphe 2, premier tiret, de la directive 95/46, les activités concernant la sécurité publique, la défense et la sûreté de l'État. Ils prennent appui à cet égard sur l'interprétation de cette dernière disposition figurant dans l'arrêt du 30 mai 2006, Parlement/Conseil et Commission (C-317/04 et C-318/04, EU:C:2006:346).

91 À cet égard, il y a lieu d'indiquer que, aux termes de son article 1er, paragraphe 1, la directive 2002/58 prévoit, notamment, l'harmonisation des dispositions nationales nécessaires pour assurer un niveau équivalent de protection des droits et des libertés fondamentaux, et en particulier du droit à la vie privée et à la confidentialité, en ce qui concerne le traitement des données à caractère personnel dans le secteur des communications électroniques.

92 L'article 1er, paragraphe 3, de cette directive exclut du champ d'application de celle-ci les « activités de l'État » dans les domaines qui y sont visés, parmi lesquelles figurent les activités de l'État dans le domaine pénal ainsi que celles concernant la sécurité publique, la défense et 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. Les activités ainsi mentionnées à titre d'exemples sont, dans tous les cas, des activités propres aux États ou aux autorités étatiques, étrangères aux domaines d'activité des particuliers (arrêt du 2 octobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, point 32 et jurisprudence citée).

93 En outre, l'article 3 de la directive 2002/58 énonce que cette directive s'applique au traitement des données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux de communications publics dans l'Union, y compris les réseaux de communications publics qui prennent en charge les dispositifs de collecte de données et d'identification (ci-après les « services de communications électroniques »). Partant, ladite directive doit être regardée comme régissant les activités des fournisseurs de tels services (arrêt du 2 octobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, point 33 et jurisprudence citée).

94 Dans ce cadre, l'article 15, paragraphe 1, de la directive 2002/58 autorise les États membres à adopter, dans le respect des conditions qu'il prévoit, 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 [cette] directive » (arrêt du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, point 71).

95 Or, l'article 15, paragraphe 1, de la directive 2002/58 présuppose nécessairement que les mesures législatives nationales qui y sont visées relèvent du champ d'application de celle-ci, puisque cette dernière n'autorise expressément les États membres à les adopter que dans le respect des conditions qu'elle prévoit. En outre, de telles mesures régissent, aux fins mentionnées à cette disposition, l'activité des fournisseurs de services de communications électroniques (arrêt du 2 octobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, point 34 et jurisprudence citée).

96 C'est notamment au regard de ces considérations que la Cour a jugé que l'article 15, paragraphe 1, de la directive 2002/58, lu en combinaison avec l'article 3 de celle-ci, doit être interprété en ce sens que relèvent du champ d'application de cette directive non seulement une mesure législative qui impose aux fournisseurs de services de communications électroniques de conserver les données relatives au trafic et les données de localisation, mais également une mesure législative leur imposant d'accorder aux autorités nationales compétentes l'accès à ces données. En effet, de telles mesures législatives impliquent obligatoirement un traitement, par lesdits fournisseurs, desdites données et ne sauraient, en ce qu'elles régissent les activités de ces mêmes fournisseurs, être assimilées à des activités propres aux États, visées à l'article 1er, paragraphe 3, de ladite directive (voir, en ce sens, arrêt du 2 octobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, points 35 et 37 ainsi que jurisprudence citée).

97 En outre, eu égard aux considérations figurant au point 95 du présent arrêt et à l'économie générale de la directive 2002/58, une interprétation de cette directive selon laquelle les mesures législatives visées à son article 15, paragraphe 1, seraient exclues du champ d'application de ladite directive du fait que les finalités auxquelles de telles mesures doivent répondre recoupent substantiellement les finalités poursuivies par les activités visées à l'article 1er, paragraphe 3, de la même directive, priverait cet article 15, paragraphe 1, de tout effet utile (voir, en ce sens, arrêt du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, points 72 et 73).

98 La notion d'« activités » figurant à l'article 1er, paragraphe 3, de la directive 2002/58 ne saurait donc, comme l'a relevé en substance M. l'avocat général au point 75 de ses conclusions dans les affaires jointes La Quadrature du Net e.a. (C-511/18 et C-512/18, EU:C:2020:6), être interprétée comme couvrant les mesures législatives visées à l'article 15, paragraphe 1, de cette directive.

99 Les dispositions de l'article 4, paragraphe 2, TUE, auxquelles se sont référés les gouvernements mentionnés au point 89 du présent arrêt, ne sauraient infirmer cette conclusion. En effet, conformément à la jurisprudence constante de la Cour, bien qu'il appartienne aux États membres de définir leurs intérêts essentiels de sécurité et d'arrêter les mesures propres à assurer leur sécurité intérieure et extérieure, le seul fait qu'une mesure nationale a été prise aux fins de la protection de la sécurité nationale ne saurait entraîner l'inapplicabilité du droit de l'Union et dispenser les États membres du respect nécessaire de ce droit [voir, en ce sens, arrêts du 4 juin 2013, ZZ, C-300/11, EU:C:2013:363, point 38 ; du 20 mars 2018, Commission/Autriche (Imprimerie d'État), C-187/16, EU:C:2018:194, points 75 et 76, ainsi que du 2 avril 2020, Commission/Pologne, Hongrie et République tchèque (Mécanisme temporaire de relocalisation de demandeurs de protection internationale), C-715/17, C-718/17 et C-719/17, EU:C:2020:257, points 143 et 170].

100 Il est vrai que, dans l'arrêt du 30 mai 2006, Parlement/Conseil et Commission (C-317/04 et C-318/04, EU:C:2006:346, points 56 à 59), la Cour a jugé que le transfert des données à caractère personnel par des compagnies aériennes à des autorités publiques d'un État tiers à des fins de prévention ainsi que de lutte contre le terrorisme et d'autres crimes graves ne relevait pas, en vertu de l'article 3, paragraphe 2, premier tiret, de la directive 95/46, du champ d'application de cette directive, puisque ce transfert s'insérait dans un cadre institué par les pouvoirs publics visant la sécurité publique.

101 Toutefois, eu égard aux considérations figurant aux points 93, 95 et 96 du présent arrêt, cette jurisprudence n'est pas transposable à l'interprétation de l'article 1er, paragraphe 3, de la directive 2002/58. En effet, comme l'a relevé, en substance, M. l'avocat général aux points 70 à 72 de ses conclusions dans les affaires jointes La Quadrature du Net e.a. (C-511/18 et C-512/18, EU:C:2020:6), l'article 3, paragraphe 2, premier tiret, de la directive 95/46, auquel se rapporte ladite jurisprudence, excluait du champ d'application de cette dernière directive, de manière générale, les « traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État », sans opérer de distinction en fonction de l'auteur du traitement de données concerné. En revanche, dans le cadre de l'interprétation de l'article 1er, paragraphe 3, de la directive 2002/58, une telle distinction s'avère nécessaire. En effet, ainsi qu'il ressort des points 94 à 97 du présent arrêt, l'ensemble des traitements de données à caractère personnel effectués par les fournisseurs de services de communications électroniques relève du champ d'application de ladite directive, en ce compris les traitements qui découlent d'obligations qui leur sont imposées par les pouvoirs publics, alors que ces derniers traitements pouvaient, le cas échéant, relever de l'exception prévue à l'article 3, paragraphe 2, premier tiret, de la directive 95/46, compte tenu de la formulation plus large de cette disposition, visant l'ensemble des traitements, quel qu'en soit l'auteur, ayant pour objet la sécurité publique, la défense ou la sûreté de l'État.

102 Par ailleurs, il y a lieu de relever que la directive 95/46 en cause dans l'affaire ayant conduit à l'arrêt du 30 mai 2006, Parlement/Conseil et Commission (C-317/04 et C-318/04, EU:C:2006:346), a été, en vertu de l'article 94, paragraphe 1, du règlement 2016/679, abrogée et remplacée par celui-ci, avec effet au 25 mai 2018. Or, si ledit règlement précise, à son article 2, paragraphe 2, sous d), qu'il ne s'applique pas aux traitements effectués « par les autorités compétentes » à des fins, notamment, de prévention et de détection des infractions pénales, y compris la protection contre des menaces pour la sécurité publique et la prévention de telles menaces, il ressort de l'article 23, paragraphe 1, sous d) et h), du même règlement que les traitements de données à caractère personnel effectués à ces mêmes fins par des particuliers relèvent du champ d'application de celui-ci. Il s'ensuit que l'interprétation de l'article 1er, paragraphe 3, de l'article 3 et de l'article 15, paragraphe 1, de la directive 2002/58 qui précède est cohérente avec la délimitation du champ d'application du règlement 2016/679 que cette directive complète et précise.

103 En revanche, lorsque les États membres mettent directement en œuvre des mesures dérogeant à la confidentialité des communications électroniques, sans imposer des obligations de traitement aux fournisseurs de services de telles communications, la protection des données des personnes concernées relève non pas de la directive 2002/58, mais du seul droit national, sous réserve de l'application de la directive (UE) 2016/680 du Parlement européen et du Conseil, du 27 avril 2016, 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, et abrogeant la décision-cadre 2008/977/JAI du Conseil (JO 2016, L 119, p. 89), de telle sorte que les mesures en cause doivent respecter notamment le droit national de rang constitutionnel et les exigences de la CEDH.

104 Il résulte des considérations qui précèdent qu'une réglementation nationale imposant aux fournisseurs de services de communications électroniques de conserver des données relatives au trafic et des données de localisation aux fins de la protection de la sécurité nationale et de la lutte contre la criminalité, telle que celles en cause au principal, relève du champ d'application de la directive 2002/58.

Sur l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58

105 Il convient de rappeler, à titre liminaire, qu'il est de jurisprudence constante que, afin d'interpréter une disposition du droit de l'Union, il convient non seulement de se référer aux termes de celle-ci, mais également de tenir compte de son contexte et des objectifs poursuivis par la réglementation dont elle fait partie ainsi que de prendre en considération, notamment, la genèse de cette réglementation (voir, en ce sens, arrêt du 17 avril 2018, Egenberger, C-414/16, EU:C:2018:257, point 44).

106 La directive 2002/58 a pour finalité, ainsi qu'il ressort notamment de ses considérants 6 et 7, de protéger les utilisateurs des services de communications électroniques contre les dangers pour leurs données à caractère personnel et leur vie privée résultant des nouvelles technologies et, notamment, de la capacité accrue de stockage et de traitement automatisés de données. En particulier, ladite directive vise, ainsi que l'énonce son considérant 2, à garantir le plein respect des droits énoncés aux articles 7 et 8 de la Charte. À cet égard, il ressort de l'exposé des motifs de la proposition de directive du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques [COM (2000) 385 final], à l'origine de la directive 2002/58, que le législateur de l'Union a entendu « faire en sorte qu'un niveau élevé de protection des données à caractère personnel et de la vie privée continue à être garanti pour tous les services de communications électroniques, quelle que soit la technologie utilisée ».

107 À cet effet, l'article 5, paragraphe 1, de la directive 2002/58 consacre le principe de confidentialité tant des communications électroniques que des données relatives au trafic y afférentes et implique, notamment, l'interdiction faite, en principe, à toute personne autre que les utilisateurs de stocker, sans le consentement de ceux-ci, ces communications et ces données.

108 S'agissant, en particulier, du traitement et du stockage des données relatives au trafic par les fournisseurs de services de communications électroniques, il ressort de l'article 6 ainsi que des considérants 22 et 26 de la directive 2002/58 qu'un tel traitement n'est autorisé que dans la mesure et pour la durée nécessaires à la commercialisation des services, à la facturation de ceux-ci et à la fourniture de services à valeur ajoutée. Une fois cette durée expirée, les données ayant été traitées et stockées doivent être effacées ou rendues anonymes. Quant aux données de localisation autres que les données relatives au trafic, l'article 9, paragraphe 1, de ladite directive prévoit que ces données ne peuvent être traitées que sous certaines conditions et après avoir été rendues anonymes ou moyennant le consentement des utilisateurs ou des abonnés (arrêt du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, point 86 et jurisprudence citée).

109 Ainsi, en adoptant cette directive, le législateur de l'Union a concrétisé les droits consacrés aux articles 7 et 8 de la Charte, de telle sorte que les utilisateurs des moyens de communications électroniques sont en droit de s'attendre, en principe, à ce que leurs communications et les données y afférentes restent, en l'absence de leur consentement, anonymes et ne puissent pas faire l'objet d'un enregistrement.

110 Toutefois, l'article 15, paragraphe 1, de la directive 2002/58 permet aux États membres d'introduire des exceptions à l'obligation de principe, énoncée à l'article 5, paragraphe 1, de cette directive, de garantir la confidentialité des données à caractère personnel ainsi qu'aux obligations correspondantes, mentionnées notamment aux articles 6 et 9 de ladite directive, lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale, 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. 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 l'un de ces motifs.

111 Cela étant, la faculté de déroger aux droits et aux obligations prévus aux articles 5, 6 et 9 de la directive 2002/58 ne saurait justifier que la dérogation à l'obligation de principe de garantir la confidentialité des communications électroniques et des données y afférentes et, en particulier, à l'interdiction de stocker ces données, explicitement prévue à l'article 5 de cette directive, devienne la règle (voir, en ce sens, arrêt du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, points 89 et 104).

112 Quant aux objectifs susceptibles de justifier une limitation des droits et des obligations prévus, notamment, aux articles 5, 6 et 9 de la directive 2002/58, la Cour a déjà jugé que l'énumération des objectifs figurant à l'article 15, paragraphe 1, première phrase, de cette directive revêt un caractère exhaustif, de telle sorte qu'une mesure législative adoptée au titre de cette disposition doit répondre effectivement et strictement à l'un de ces objectifs (voir, en ce sens, arrêt du 2 octobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, point 52 et jurisprudence citée).

113 En outre, il ressort de l'article 15, paragraphe 1, troisième phrase, de la directive 2002/58 que les États membres ne sont autorisés à prendre des mesures législatives visant à limiter la portée des droits et des obligations visés aux articles 5, 6 et 9 de cette directive que dans le respect des principes généraux du droit de l'Union, parmi lesquels figure le principe de proportionnalité, et des droits fondamentaux garantis par la Charte. À cet égard, la Cour a déjà jugé que l'obligation imposée par un État membre aux fournisseurs de services de communications électroniques, par une réglementation nationale, de conserver les données relatives au trafic aux fins de les rendre, le cas échéant, accessibles aux autorités nationales compétentes soulève des questions relatives au respect non seulement des articles 7 et 8 de la Charte, relatifs, respectivement à la protection de la vie privée ainsi qu'à la protection des données à caractère personnel, mais également de l'article 11 de la Charte, relatif à la liberté d'expression (voir, en ce sens, arrêts du 8 avril 2014, Digital Rights, C-293/12 et C-594/12, EU:C:2014:238, points 25 et 70, ainsi que du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, points 91 et 92 ainsi que jurisprudence citée).

114 Ainsi, l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58 doit tenir compte de l'importance tant du droit au respect de la vie privée, garanti à l'article 7 de la Charte, que du droit à la protection des données à caractère personnel, garanti à l'article 8 de celle-ci, telle qu'elle ressort de la jurisprudence de la Cour, ainsi que du droit à la liberté d'expression, ce droit fondamental, garanti à l'article 11 de la Charte, constituant l'un des fondements essentiels d'une société démocratique et pluraliste et faisant partie des valeurs sur lesquelles est, conformément à l'article 2 TUE, fondée l'Union (voir, en ce sens, arrêts du 6 mars 2001, Connolly/Commission, C-274/99 P, EU:C:2001:127, point 39, ainsi que du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, point 93 et jurisprudence citée).

115 Il y a lieu de préciser, à cet égard, que la conservation des données relatives au trafic et des données de localisation constitue, par elle-même, d'une part, une dérogation à l'interdiction, prévue à l'article 5, paragraphe 1, de la directive 2002/58, faite à toute autre personne que les utilisateurs de stocker ces données et, d'autre part, une ingérence dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel, consacrés aux articles 7 et 8 de la Charte, sans qu'il importe de savoir si les informations relatives à la vie privée concernées présentent ou non un caractère sensible ou si les intéressés ont ou non subi d'éventuels inconvénients en raison de cette ingérence [voir, en ce sens, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, points 124 et 126 ainsi que jurisprudence citée ; voir, par analogie, en ce qui concerne l'article 8 de la CEDH, Cour EDH, 30 janvier 2020, Breyer c. Allemagne, CE:ECHR:2020:0130JUD005000112, § 81].

116 Il est également sans pertinence que les données conservées soient ou non utilisées par la suite (voir, par analogie, en ce qui concerne l'article 8 de la CEDH, Cour EDH, 16 février 2000, Amann c. Suisse, CE:ECHR:2000:0216JUD002779895, § 69, ainsi que 13 février 2020, Trjakovski et Chipovski c. Macédonie du Nord, CE:ECHR:2020:0213JUD005320513, § 51), l'accès à de telles données constituant, quelle que soit l'utilisation qui en est faite ultérieurement, une ingérence distincte dans les droits fondamentaux visés au point précédent [voir, en ce sens, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, points 124 et 126].

117 Cette conclusion apparaît d'autant plus justifiée que les données relatives au trafic et les données de localisation sont susceptibles de révéler des informations sur un nombre important d'aspects de la vie privée des personnes concernées, y compris des informations sensibles, telles que l'orientation sexuelle, les opinions politiques, les convictions religieuses, philosophiques, sociétales ou autres ainsi que l'état de santé, alors que

de telles données jouissent, par ailleurs, d'une protection particulière en droit de l'Union. Prises dans leur ensemble, lesdites données peuvent 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 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 (voir, en ce sens, arrêts du 8 avril 2014, Digital Rights, C-293/12 et C-594/12, EU:C:2014:238, point 27, ainsi que du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, point 99).

118 Dès lors, d'une part, la conservation des données relatives au trafic et des données de localisation à des fins policières est susceptible, à elle seule, de porter atteinte au droit au respect des communications, consacré à l'article 7 de la Charte, et d'entraîner des effets dissuasifs sur l'exercice par les utilisateurs des moyens de communications électroniques de leur liberté d'expression, garantie à l'article 11 de celle-ci (voir, en ce sens, arrêts du 8 avril 2014, Digital Rights, C-293/12 et C-594/12, EU:C:2014:238, point 28, ainsi que du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, point 101). Or, de tels effets dissuasifs peuvent affecter en particulier les personnes dont les communications sont soumises, selon les règles nationales, au secret professionnel ainsi que les lanceurs d'alerte dont les activités sont protégées par la directive (UE) 2019/1937 du Parlement européen et du Conseil, du 23 octobre 2019, sur la protection des personnes qui signalent des violations du droit de l'Union (JO 2019, L 305, p. 17). En outre, ces effets sont d'autant plus graves que le nombre et la variété des données conservées sont élevés.

119 D'autre part, compte tenu de la quantité importante de données relatives au trafic et de données de localisation susceptibles d'être conservées de manière continue par une mesure de conservation généralisée et indifférenciée ainsi que du caractère sensible des informations que ces données peuvent fournir, la seule conservation desdites données par les fournisseurs de services de communications électroniques comporte des risques d'abus et d'accès illicite.

120 Cela étant, en ce qu'il permet aux États membres d'introduire les dérogations visées au point 110 du présent arrêt, l'article 15, paragraphe 1, de la directive 2002/58 reflète la circonstance que les droits consacrés aux articles 7, 8 et 11 de la Charte n'apparaissent pas comme étant des prérogatives absolues, mais doivent être pris en considération par rapport à leur fonction dans la société (voir, en ce sens, arrêt du 16 juillet 2020, Facebook Ireland et Schrems, C-311/18, EU:C:2020:559, point 172 ainsi que jurisprudence citée).

121 En effet, ainsi qu'il ressort de l'article 52, paragraphe 1, de la Charte, celle-ci admet des limitations à l'exercice de ces droits, pour autant que ces limitations soient prévues par la loi, qu'elles respectent le contenu essentiel desdits droits et que, dans le respect du principe de proportionnalité, elles soient nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et des libertés d'autrui.

122 Ainsi, l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58 à la lumière de la Charte requiert de tenir compte également de l'importance des droits consacrés aux articles 3, 4, 6 et 7 de la Charte et de celle que revêtent les objectifs de protection de la sécurité nationale et de lutte contre la criminalité grave en contribuant à la protection des droits et des libertés d'autrui.

123 À cet égard, l'article 6 de la Charte, auquel se réfèrent le Conseil d'État et la Cour constitutionnelle, consacre le droit de toute personne non seulement à la liberté mais également à la sûreté et garantit des droits correspondant à ceux qui le sont à l'article 5 de la CEDH (voir, en ce sens, arrêts du 15 février 2016, N., C-601/15 PPU, EU:C:2016:84, point 47 ; du 28 juillet 2016, JZ, C-294/16 PPU, EU:C:2016:610, point 48, ainsi que du 19 septembre 2019, Rayonna prokuratura Lom, C-467/18, EU:C:2019:765, point 42 et jurisprudence citée).

124 En outre, il y a lieu de rappeler que l'article 52, paragraphe 3, de la Charte vise à assurer la cohérence nécessaire entre les droits contenus dans cette dernière et les droits correspondants garantis par la CEDH, sans porter atteinte à l'autonomie du droit de l'Union et de la Cour de justice de l'Union européenne. Il convient donc de tenir compte des droits correspondants de la CEDH en vue de l'interprétation de la Charte, en tant que seuil de protection minimale [voir, en ce sens, arrêts du 12 février 2019, TC, C-492/18 PPU, EU:C:2019:108, point 57, ainsi que du 21 mai 2019, Commission/Hongrie (Usufruits sur terres agricoles), C-235/17, EU:C:2019:432, point 72 et jurisprudence citée].

125 S'agissant de l'article 5 de la CEDH, qui consacre le « droit à la liberté » et le « droit à la sûreté », celui-ci vise, selon la jurisprudence de la Cour européenne des droits de l'homme, à protéger l'individu contre toute privation de liberté arbitraire ou injustifiée (voir, en ce sens, Cour EDH, 18 mars 2008, Ladent c. Pologne, CE:ECHR:2008:0318JUD001103603, §§ 45 et 46 ; 29 mars 2010, Medvedyev et autres c. France, CE:ECHR:2010:0329JUD000339403, §§ 76 et 77, ainsi que 13 décembre 2012, El-Masri v. « The former Yugoslav Republic of Macedonia », CE:ECHR:2012:1213JUD003963009, § 239). Toutefois, dans la mesure où cette disposition vise une privation de liberté commise par une autorité publique, l'article 6 de la Charte ne saurait être interprété comme imposant aux pouvoirs publics une obligation d'adopter des mesures spécifiques en vue de réprimer certaines infractions pénales.

126 En revanche, en ce qui concerne, en particulier, la lutte effective contre les infractions pénales dont sont victimes, notamment, les mineurs et les autres personnes vulnérables, évoquée par la Cour constitutionnelle, il convient de souligner que des obligations positives à la charge des pouvoirs publics peuvent résulter de l'article 7 de la Charte, en vue de l'adoption de mesures juridiques visant à protéger la vie privée et familiale [voir, en ce sens, arrêt du 18 juin 2020, Commission/Hongrie (Transparence associative), C-78/18, EU:C:2020:476, point 123 et jurisprudence citée de la Cour européenne des droits de l'homme]. De telles obligations sont également susceptibles de découler dudit article 7 en ce qui concerne la protection du domicile et des communications, ainsi que des articles 3 et 4 s'agissant de la protection de l'intégrité physique et psychique des personnes ainsi que de l'interdiction de la torture et des traitements inhumains et dégradants.

127 Or, face à ces différentes obligations positives, il convient de procéder à une conciliation nécessaire des différents intérêts et droits en cause.

128 En effet, la Cour européenne des droits de l'homme a jugé que les obligations positives découlant des articles 3 et 8 de la CEDH, dont les garanties correspondantes figurent aux articles 4 et 7 de la Charte, impliquent, notamment, l'adoption de dispositions matérielles et procédurales ainsi que de mesures d'ordre pratique permettant une lutte efficace à l'encontre des infractions contre les personnes à travers une enquête et des poursuites effectives, cette obligation étant d'autant plus importante lorsque le bien-être physique et moral d'un enfant est menacé. Cela étant, les mesures qu'il appartient aux autorités compétentes de prendre doivent pleinement respecter les voies légales et les autres garanties qui sont de nature à limiter l'étendue des pouvoirs d'investigations pénales ainsi que les autres libertés et droits. En particulier, selon cette juridiction, il convient d'instaurer un cadre légal permettant de concilier les différentes intérêts et droits à protéger (Cour EDH, 28 octobre 1998, Osman c. Royaume-Uni, CE:ECHR:1998:1028JUD002345294, §§ 115 et 116 ; 4 mars 2004, M.C. c. Bulgarie, CE:ECHR:2003:1204JUD003927298, § 151 ; 24 juin 2004, Von Hannover c. Allemagne, CE:ECHR:2004:0624JUD005932000, §§ 57 et 58, ainsi que 2 décembre 2008, K.U. c. Finlande, CE:ECHR:2008:1202JUD 000287202, §§ 46, 48 et 49).

129 En ce qui concerne le respect du principe de proportionnalité, l'article 15, paragraphe 1, première phrase, de la directive 2002/58 dispose que les États membres peuvent adopter une mesure dérogeant au principe de confidentialité des communications et des données relatives au trafic y afférentes lorsqu'une telle mesure est « nécessaire, appropriée et proportionnée, au sein d'une société démocratique », au regard des objectifs que cette disposition énonce. Le considérant 11 de cette directive précise qu'une mesure de cette nature doit être « rigoureusement » proportionnée au but poursuivi.

130 À cet égard, il convient de rappeler que la protection du droit fondamental au respect de la vie privée exige, conformément à la jurisprudence constante de la Cour, que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci s'opèrent dans les limites du strict nécessaire. En outre, un objectif d'intérêt général ne saurait être poursuivi sans tenir compte du fait qu'il doit être concilié avec les droits fondamentaux concernés par la mesure, ce en effectuant une pondération équilibrée entre, d'une part, l'objectif d'intérêt général et, d'autre part, les droits en cause [voir, en ce sens, arrêts du 16 décembre 2008, Satakunnan Markkinapörssi et Satamedia, C-73/07, EU:C:2008:727, point 56 ; du 9 novembre 2010, Volker und Markus Schecke et Eifert, C-92/09 et C-93/09, EU:C:2010:662, point 76, 77 et 86, ainsi que du 8 avril 2014, Digital Rights, C-293/12 et C-594/12, EU:C:2014:238, point 52 ; avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 140].

131 Plus particulièrement, il découle de la jurisprudence de la Cour que la possibilité pour les États membres de justifier une limitation aux droits et aux obligations prévus, notamment, aux articles 5, 6 et 9 de la directive 2002/58 doit être appréciée en mesurant la gravité de l'ingérence que comporte une telle limitation et en vérifiant que l'importance de l'objectif d'intérêt général poursuivi par cette limitation est en relation avec cette gravité (voir, en ce sens, arrêt du 2 octobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, point 55 et jurisprudence citée).

132 Pour satisfaire à l'exigence de proportionnalité, une réglementation doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant des exigences minimales, de telle sorte que les personnes dont les données à caractère personnel sont concernées disposent de garanties suffisantes permettant de protéger efficacement ces données contre les risques d'abus. Cette réglementation doit être légalement contraignante en droit interne et, en particulier, indiquer en quelles circonstances et sous quelles conditions une mesure prévoyant le traitement de telles données peut être prise, garantissant ainsi que l'ingérence soit limitée au strict nécessaire. La nécessité de disposer de telles garanties est d'autant plus importante lorsque les données à caractère personnel sont soumises à un traitement automatisé, notamment lorsqu'il existe un risque important d'accès illicite à ces données. Ces considérations valent en particulier lorsqu'est en jeu la protection de cette catégorie particulière de données à caractère personnel que sont les données sensibles [voir, en ce sens, arrêts du 8 avril 2014, Digital Rights, C-293/12 et C-594/12, EU:C:2014:238, points 54 et 55, ainsi que du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, point 117 ; avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 141].

133 Ainsi, une réglementation prévoyant une conservation des données à caractère personnel doit toujours répondre à des critères objectifs, établissant un rapport entre les données à conserver et l'objectif poursuivi [voir, en ce sens, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, points 191 et jurisprudence citée, ainsi que arrêt du 3 octobre 2019, A e.a., C-70/18, EU:C:2019:823, point 63].

– *Sur les mesures législatives prévoyant la conservation préventive des données relatives au trafic et des données de localisation aux fins de la sauvegarde de la sécurité nationale*

134 Il y a lieu de faire observer que l'objectif de sauvegarde de la sécurité nationale, évoqué par les juridictions de renvoi et les gouvernements ayant présenté des observations, n'a pas encore été spécifiquement examiné par la Cour dans ses arrêts interprétant la directive 2002/58.

135 À cet égard, il convient de relever, d'emblée, que l'article 4, paragraphe 2, TUE énonce que la sécurité nationale reste de la seule responsabilité de chaque État membre. Cette responsabilité correspond à l'intérêt primordial de protéger les fonctions essentielles de l'État et les intérêts fondamentaux de la société et inclut la prévention et la répression d'activités de nature à déstabiliser gravement les structures constitutionnelles, politiques, économiques ou sociales fondamentales d'un pays, et en particulier à menacer directement la société, la population ou l'État en tant que tel, telles que notamment des activités de terrorisme.

136 Or, l'importance de l'objectif de sauvegarde de la sécurité nationale, lu à l'aune de l'article 4, paragraphe 2, TUE, dépasse celle des autres objectifs visés à l'article 15, paragraphe 1, de la directive 2002/58, notamment des objectifs de lutte contre la criminalité en général, même grave, ainsi que de sauvegarde de la sécurité publique. En effet, des menaces telles que celles visées au point précédent se distinguent, par leur nature et leur particulière gravité, du risque général de survenance de tensions ou de troubles, même graves, à la sécurité publique. Sous réserve du respect des autres exigences prévues à l'article 52, paragraphe 1, de la Charte, l'objectif de sauvegarde de la sécurité nationale est dès lors susceptible de justifier des mesures comportant des ingérences dans les droits fondamentaux plus graves que celles que pourraient justifier ces autres objectifs.

137 Ainsi, dans des situations telles que celles décrites aux points 135 et 136 du présent arrêt, 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, en principe, à une mesure législative qui autorise les autorités compétentes à enjoindre aux fournisseurs de services de communications électroniques de procéder à la conservation des données relatives au trafic et des données de localisation de l'ensemble des utilisateurs des moyens de communications électroniques pendant une période limitée, dès lors qu'il existe des circonstances suffisamment concrètes permettant de considérer que l'État membre concerné fait face à une menace grave telle que celle visée aux points 135 et 136 du présent arrêt pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible. Même si une telle mesure vise, de manière indifférenciée, tous les utilisateurs de moyens de communications électroniques sans que ceux-ci paraissent, de prime abord, présenter de rapport, au sens de la jurisprudence visée au point 133 du présent arrêt, avec une menace pour la sécurité nationale de cet État membre, il y a lieu néanmoins de considérer que l'existence d'une telle menace est de nature, par elle-même, à établir ce rapport.

138 L'injonction prévoyant la conservation préventive des données de l'ensemble des utilisateurs des moyens de communications électroniques doit, néanmoins, être temporellement limitée au strict nécessaire. S'il ne peut être exclu que l'injonction faite aux fournisseurs de services de communications électroniques de procéder à la conservation des données puisse, en raison de la persistance d'une telle menace, être renouvelée, la durée de chaque injonction ne saurait dépasser un laps de temps prévisible. De surcroît, une telle conservation des données doit être sujette à des limitations et encadrée par des garanties strictes permettant de protéger efficacement les données à caractère personnel des personnes concernées contre les risques d'abus. Ainsi, cette conservation ne saurait présenter un caractère systématique.

139 Eu égard à la gravité de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte résultant d'une telle mesure de conservation généralisée et indifférenciée des données, il importe d'assurer que le recours à celle-ci soit effectivement limité aux situations dans lesquelles il existe une menace grave pour la sécurité nationale, telles que celles visées aux points 135 et 136 du présent arrêt. À cet effet, il est essentiel qu'une décision faisant injonction aux fournisseurs de services de communications électroniques de procéder à une telle conservation des données puisse faire l'objet d'un contrôle effectif soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, visant à vérifier l'existence d'une de ces situations ainsi que le respect des conditions et des garanties devant être prévues.

– *Sur les mesures législatives prévoyant la conservation préventive des données relatives au trafic et des données de localisation aux fins de la lutte contre la criminalité et de la sauvegarde de la sécurité publique*

140 Pour ce qui est de l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales, conformément au principe de proportionnalité, seules la lutte contre la criminalité grave et la prévention des menaces graves contre la sécurité publique sont de nature à justifier des ingérences graves dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, telles que celles qu'implique la conservation des données relatives au trafic et des données de localisation. Dès lors, seules des ingérences

dans lesdits droits fondamentaux ne présentant pas un caractère grave peuvent être justifiées par l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales en général [voir, en ce sens, arrêts du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, point 102, ainsi que du 2 octobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, points 56 et 57; avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 149].

141 Une réglementation nationale prévoyant la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, en vue de lutter contre la criminalité grave, excède 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 (voir, en ce sens, arrêt du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, point 107).

142 En effet, compte tenu du caractère sensible des informations que peuvent fournir les données relatives au trafic et les données de localisation, la confidentialité de ces dernières est essentielle pour le droit au respect de la vie privée. Ainsi, et compte tenu, d'une part, des effets dissuasifs sur l'exercice des droits fondamentaux consacrés aux articles 7 et 11 de la Charte, visés au point 118 du présent arrêt, que la conservation de ces données est susceptible d'entraîner et, d'autre part, de la gravité de l'ingérence que comporte une telle conservation, il importe, dans une société démocratique, que celle-ci soit, comme le prévoit le système mis en place par la directive 2002/58, l'exception et non la règle et que ces données ne puissent faire l'objet d'une conservation systématique et continue. Cette conclusion s'impose même à l'égard des objectifs de lutte contre la criminalité grave et de prévention des menaces graves contre la sécurité publique ainsi que de l'importance qu'il convient de leur reconnaître.

143 En outre, la Cour a souligné qu'une réglementation prévoyant la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation couvre les communications électroniques de la quasi-totalité de la population sans qu'aucune différenciation, limitation ni exception soient opérées en fonction de l'objectif poursuivi. Une telle réglementation, contrairement à l'exigence rappelée au point 133 du présent arrêt, 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 cet objectif de lutte contre des actes de criminalité grave et, en particulier, sans que soit prévue une relation entre les données dont la conservation est prévue et une menace pour la sécurité publique (voir, en ce sens, arrêts du 8 avril 2014, Digital Rights, C-293/12 et C-594/12, EU:C:2014:238, points 57 et 58, ainsi que du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, point 105).

144 En particulier, comme l'a déjà jugé la Cour, une telle réglementation 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 grave (voir, en ce sens, arrêts du 8 avril 2014, Digital Rights, C-293/12 et C-594/12, EU:C:2014:238, point 59, et du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, point 106).

145 Or, même les obligations positives des États membres susceptibles de découler, selon le cas, des articles 3, 4 et 7 de la Charte et portant, ainsi qu'il a été relevé aux points 126 et 128 du présent arrêt, sur la mise en place de règles permettant une lutte effective contre les infractions pénales ne sauraient avoir pour effet de justifier des ingérences aussi graves que celles que comporte une réglementation prévoyant une conservation des données relatives au trafic et des données de localisation dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte de la quasi-totalité de la population sans que les données des personnes concernées soient susceptibles de révéler un lien, au moins indirect, avec l'objectif poursuivi.

146 En revanche, conformément à ce qui a été relevé aux points 142 à 144 du présent arrêt, et eu égard à la conciliation nécessaire des droits et des intérêts en cause, les objectifs de lutte contre la criminalité grave, de prévention d'atteintes graves à la sécurité publique et, a fortiori, de sauvegarde de la sécurité nationale sont susceptibles de justifier, compte tenu de leur importance, au regard des obligations positives rappelées au point précédent et auxquelles s'est référée notamment la Cour constitutionnelle, l'ingérence particulièrement grave que comporte une conservation ciblée des données relatives au trafic et des données de localisation.

147 Ainsi, comme l'a déjà jugé la Cour, 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, une conservation ciblée des données relatives au trafic et des données de localisation aux fins de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, tout comme aux fins de la sauvegarde de la sécurité nationale, à condition qu'une telle conservation 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 (voir, en ce sens, arrêt du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, point 108).

148 S'agissant de la délimitation dont doit faire l'objet une telle mesure de conservation des données, celle-ci peut, notamment, être fixée en fonction des catégories de personnes concernées, dès lors que l'article 15, paragraphe 1, de la directive 2002/58 ne s'oppose pas à une réglementation fondée sur des éléments objectifs, permettant de viser les personnes dont les données relatives au trafic et les données de localisation 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 ou encore un risque pour la sécurité nationale (voir, en ce sens, arrêt du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, point 111).

149 À cet égard, il convient de préciser que les personnes ainsi visées peuvent notamment être celles ayant été préalablement identifiées, dans le cadre des procédures nationales applicables et sur la base d'éléments objectifs, comme présentant une menace pour la sécurité publique ou la sécurité nationale de l'État membre concerné.

150 La délimitation d'une mesure prévoyant la conservation des données relatives au trafic et des données de localisation peut également être fondée sur un critère géographique lorsque les autorités nationales compétentes considèrent, sur la base d'éléments objectifs et non discriminatoires, qu'il existe, dans une ou plusieurs zones géographiques, une situation caractérisée par un risque élevé de préparation ou de commission d'actes de criminalité grave (voir, en ce sens, arrêt du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, point 111). Ces zones peuvent être, notamment, des lieux caractérisés par un nombre élevé d'actes de criminalité grave, des lieux particulièrement exposés à la commission d'actes de criminalité grave, tels que des lieux ou infrastructures fréquentés régulièrement par un nombre très élevé de personnes, ou encore des lieux stratégiques, tels que des aéroports, des gares ou des zones de péages.

151 Afin d'assurer que l'ingérence que comportent les mesures de conservation ciblée décrites aux points 147 à 150 du présent arrêt soit conforme au principe de proportionnalité, leur durée ne saurait dépasser celle qui est strictement nécessaire au regard de l'objectif poursuivi ainsi que des circonstances les justifiant, sans préjudice d'un renouvellement éventuel en raison de la persistance de la nécessité de procéder à une telle conservation.

– *Sur les mesures législatives prévoyant la conservation préventive des adresses IP et des données relatives à l'identité civile aux fins de la lutte contre la criminalité et de la sauvegarde de la sécurité publique*

152 Il y a lieu de relever que les adresses IP, quoique faisant partie des données relatives au trafic, sont générées sans être rattachées à une communication déterminée et servent principalement à identifier, par l'intermédiaire des fournisseurs de services de communications électroniques, la personne physique propriétaire d'un équipement terminal à partir duquel une communication au moyen de l'Internet est effectuée. Ainsi, en matière de courrier électronique ainsi que de téléphonie par Internet, pour autant que seules les adresses IP de la source de la communication sont conservées et non celles du destinataire de celle-ci, ces adresses ne révèlent, en tant que telles, aucune information sur les tierces personnes ayant été en contact avec la personne à l'origine de la communication. Cette catégorie de données présente donc un degré de sensibilité moindre que les autres données relatives au trafic.

153 Toutefois, les adresses IP pouvant être utilisées pour effectuer notamment le traçage exhaustif du parcours de navigation d'un internaute et, par suite, de son activité en ligne, ces données permettent d'établir le profil détaillé de ce dernier. Ainsi, la conservation et l'analyse desdites adresses IP que nécessite un tel traçage constituent des ingérences graves dans les droits fondamentaux de l'internaute consacrés aux articles 7 et 8 de la Charte, pouvant avoir des effets dissuasifs tels que ceux visés au point 118 du présent arrêt.

154 Or, aux fins de la conciliation nécessaire des droits et des intérêts en cause exigée par la jurisprudence citée au point 130 du présent arrêt, il y a lieu de tenir compte du fait que, dans le cas d'une infraction commise en ligne, l'adresse IP peut constituer le seul moyen d'investigation permettant l'identification de la personne à laquelle cette adresse était attribuée au moment de la commission de cette infraction. À cela s'ajoute le fait que la conservation des adresses IP par les fournisseurs de services de communications électroniques au-delà de la durée d'attribution de ces données n'apparaît, en principe, pas nécessaire aux fins de la facturation des services en cause, de telle sorte que la détection des infractions commises en ligne peut, de ce fait, comme l'ont indiqué plusieurs gouvernements dans leurs observations soumises à la Cour, s'avérer impossible sans avoir recours à une mesure législative au titre de l'article 15, paragraphe 1, de la directive 2002/58. Tel peut notamment être le cas, ainsi que l'ont fait valoir ces gouvernements, des infractions particulièrement graves en matière de pédopornographie, telles que l'acquisition, la diffusion, la transmission ou la mise à disposition en ligne de pédopornographie, au sens de l'article 2, sous c), de la directive 2011/93/UE du Parlement européen et du Conseil, du 13 décembre 2011, relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI du Conseil (JO 2011, L 335, p. 1).

155 Dans ces conditions, s'il est vrai qu'une mesure législative prévoyant la conservation des adresses IP de l'ensemble des personnes physiques propriétaires d'un équipement terminal à partir duquel un accès à Internet peut être effectué viserait des personnes qui ne présentent, de prime abord, pas de lien, au sens de la jurisprudence citée au point 133 du présent arrêt, avec les objectifs poursuivis et que les internautes disposent, conformément à ce qui a été constaté au point 109 du présent arrêt, du droit de s'attendre, en vertu des articles 7 et 8 de la Charte, à ce que leur identité ne soit, en principe, pas dévoilée, une mesure législative prévoyant la conservation généralisée et indifférenciée des seules adresses IP attribuées à la source d'une connexion n'apparaît pas, en principe, contraire à l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des article 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, pourvu que cette possibilité soit soumise au strict respect des conditions matérielles et procédurales devant régir l'utilisation de ces données.

156 Eu égard au caractère grave de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte que comporte cette conservation, seule la lutte contre la criminalité grave et la prévention des menaces graves contre la sécurité publique sont de nature, à l'instar de la sauvegarde de la sécurité nationale, à justifier cette ingérence. En outre, la durée de conservation ne saurait excéder celle qui est strictement nécessaire au regard de l'objectif poursuivi. Enfin, une mesure de cette nature doit prévoir des conditions et des garanties strictes quant à l'exploitation de ces données, notamment par un traçage, à l'égard des communications et des activités effectuées en ligne par les personnes concernées.

157 En ce qui concerne, enfin, les données relatives à l'identité civile des utilisateurs des moyens de communications électroniques, ces données ne permettent pas, à elles seules, de connaître la date, l'heure, la durée et les destinataires des communications effectuées, non plus que les endroits où ces communications ont eu lieu ou la fréquence de celles-ci avec certaines personnes pendant une période donnée, de telle sorte qu'elles ne fournissent, mises à part les coordonnées de ceux-ci, telles que leurs adresses, aucune information sur les communications données et, par voie de conséquence, sur leur vie privée. Ainsi, l'ingérence que comporte une conservation de ces données ne saurait, en principe, être qualifiée de grave (voir, en ce sens, arrêt du 2 octobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, points 59 et 60).

158 Il en découle que, conformément à ce qui a été exposé au point 140 du présent arrêt, les mesures législatives visant le traitement de ces données en tant que telles, notamment leur conservation et l'accès à celles-ci à la seule fin de l'identification de l'utilisateur concerné, et sans que lesdites données puissent être associées à des informations relatives aux communications effectuées, sont susceptibles d'être justifiées par l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales en général, auquel se réfère l'article 15, paragraphe 1, première phrase, de la directive 2002/58 (voir, en ce sens, arrêt du 2 octobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, point 62).

159 Dans ces conditions, eu égard à la conciliation nécessaire des droits et des intérêts en cause et pour les raisons figurant aux points 131 et 158 du présent arrêt, il y a lieu de considérer que, même en l'absence de lien entre l'ensemble des utilisateurs des moyens de communications électroniques et les objectifs poursuivis, 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 une mesure législative imposant, sans délai particulier, aux fournisseurs de services de communications électroniques la conservation des données relatives à l'identité civile de l'ensemble des utilisateurs des moyens de communications électroniques aux fins de la prévention, de la recherche, de la détection et de la poursuite d'infractions pénales ainsi que de la sauvegarde de la sécurité publique, sans qu'il soit nécessaire que les infraction pénales ou que les menaces contre ou les atteintes à la sécurité publique soient graves.

– *Sur les mesures législatives prévoyant la conservation rapide des données relatives au trafic et des données de localisation aux fins de la lutte contre la criminalité grave*

160 En ce qui concerne les données relatives au trafic et les données de localisation traitées et stockées par les fournisseurs de services de communications électroniques sur la base des articles 5, 6 et 9 de la directive 2002/58, ou sur celle de mesures législatives prises en vertu de l'article 15, paragraphe 1, de celle-ci, telles que décrites aux points 134 à 159 du présent arrêt, il y a lieu de relever que ces données doivent, en principe, être, selon le cas, effacées ou rendues anonymes au terme des délais légaux dans lesquels doivent intervenir, conformément aux dispositions nationales transposant cette directive, leur traitement et leur stockage.

161 Toutefois, pendant ce traitement et ce stockage, peuvent se présenter des situations dans lesquelles survient la nécessité de conserver lesdites données au-delà de ces délais aux fins de l'élucidation d'infractions pénales graves ou d'atteintes à la sécurité nationale, et ce tant dans la situation où ces infractions ou ces atteintes ont déjà pu être constatées que dans celle où leur existence peut, au terme d'un examen objectif de l'ensemble des circonstances pertinentes, être raisonnablement soupçonnée.

162 À cet égard, il y a lieu de relever que la convention sur la cybercriminalité du Conseil de l'Europe du 23 novembre 2001 (série des traités européens – n° 185), laquelle a été signée par les 27 États membres et ratifiée par 25 d'entre eux, et dont l'objectif est de faciliter la lutte contre les infractions pénales commises au moyen des réseaux informatiques, prévoit, à son article 14, que les parties contractantes adoptent aux fins d'enquêtes ou de procédures pénales spécifiques certaines mesures quant aux données relatives au trafic déjà

stockées, telles que la conservation rapide de ces données. En particulier, l'article 16, paragraphe 1, de cette convention stipule que les parties contractantes adoptent les mesures législatives qui se révèlent nécessaires pour permettre à leurs autorités compétentes d'ordonner ou d'imposer d'une autre manière la conservation rapide des données relatives au trafic stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que ces données sont susceptibles de perte ou de modification.

163 Dans une situation telle que celle visée au point 161 du présent arrêt, il est loisible aux États membres, eu égard à la conciliation nécessaire des droits et des intérêts en cause visée au point 130 du présent arrêt, de prévoir, dans une législation adoptée en vertu de l'article 15, paragraphe 1, de la directive 2002/58, la possibilité, au moyen d'une décision de l'autorité compétente soumise à un contrôle juridictionnel effectif, d'enjoindre aux fournisseurs de services de communications électroniques de procéder, pour une durée déterminée, à la conservation rapide des données relatives au trafic et des données de localisation dont ils disposent.

164 Dans la mesure où la finalité d'une telle conservation rapide ne correspond plus à celles pour lesquelles les données ont été collectées et conservées initialement et où tout traitement de données doit, en vertu de l'article 8, paragraphe 2, de la Charte, répondre à des fins déterminées, les États membres doivent préciser, dans leur législation, la finalité pour laquelle la conservation rapide des données peut avoir lieu. Eu égard au caractère grave de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte qu'est susceptible de comporter une telle conservation, seule la lutte contre la criminalité grave et, a fortiori, la sauvegarde de la sécurité nationale sont de nature à justifier cette ingérence. En outre, afin d'assurer que l'ingérence que comporte une mesure de ce type soit limitée au strict nécessaire, il convient, d'une part, que l'obligation de conservation porte sur les seules données de trafic et données de localisation susceptibles de contribuer à l'élucidation de l'infraction pénale grave ou de l'atteinte à la sécurité nationale concernée. D'autre part, la durée de conservation des données doit être limitée au strict nécessaire, celle-ci pouvant néanmoins être prolongée lorsque les circonstances et l'objectif poursuivi par ladite mesure le justifient.

165 À cet égard, il importe de préciser qu'une telle conservation rapide ne doit pas être limitée aux données des personnes concrètement soupçonnées d'avoir commis une infraction pénale ou une atteinte à la sécurité nationale. Tout en respectant le cadre dressé par 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, et compte tenu des considérations figurant au point 133 du présent arrêt, une telle mesure peut, selon le choix du législateur et tout en respectant les limites du strict nécessaire, être étendue aux données relatives au trafic et aux données de localisation afférentes à des personnes autres que celles qui sont soupçonnées d'avoir projeté ou commis une infraction pénale grave ou une atteinte à la sécurité nationale, pour autant que ces données peuvent, sur la base d'éléments objectifs et non discriminatoires, contribuer à l'élucidation d'une telle infraction ou d'une telle atteinte à la sécurité nationale, telles que les données de la victime de celle-ci, de son entourage social ou professionnel, ou encore de zones géographiques déterminées, telles que les lieux de la commission et de la préparation de l'infraction ou de l'atteinte à la sécurité nationale en cause. En outre, l'accès des autorités compétentes aux données ainsi conservées doit s'effectuer dans le respect des conditions résultant de la jurisprudence ayant interprété la directive 2002/58 (voir, en ce sens, arrêt du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, points 118 à 121 et jurisprudence citée).

166 Il convient encore d'ajouter que, ainsi qu'il ressort en particulier des points 115 et 133 du présent arrêt, l'accès à des données de trafic et à des données de localisation conservées par des fournisseurs en application d'une mesure prise au titre de l'article 15, paragraphe 1, de la directive 2002/58 ne peut en principe être justifié que par l'objectif d'intérêt général pour lequel cette conservation a été imposée à ces fournisseurs. Il s'ensuit, en particulier, qu'un accès à de telles données à des fins de poursuite et de sanction d'une infraction pénale ordinaire ne saurait en aucun cas être accordé lorsque leur conservation a été justifiée par l'objectif de lutte contre la criminalité grave ou, a fortiori, de sauvegarde de la sécurité nationale. En revanche, conformément au principe de proportionnalité tel qu'il a été précisé au point 131 du présent arrêt, un accès à des données conservées en vue de la lutte contre la criminalité grave peut, pour autant que soient respectées les conditions matérielles et procédurales entourant un tel accès visées au point précédent, être justifié par l'objectif de sauvegarde de la sécurité nationale.

167 À cet égard, il est loisible aux États membres de prévoir dans leur législation qu'un accès à des données relatives au trafic et à des données de localisation peut, dans le respect de ces mêmes conditions matérielles et procédurales, avoir lieu à des fins de lutte contre la criminalité grave ou de sauvegarde de la sécurité nationale lorsque lesdites données sont conservées par un fournisseur d'une manière conforme aux articles 5, 6 et 9 ou encore à l'article 15, paragraphe 1, de la directive 2002/58.

168 Eu égard à l'ensemble des considérations qui précèdent, il y a lieu de répondre aux premières questions dans les affaires C-511/18 et C-512/18 ainsi qu'aux première et deuxième questions dans l'affaire C-520/18 que 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, doit être interprété en ce sens qu'il s'oppose à des mesures législatives prévoyant, aux fins prévues à cet article 15, paragraphe 1, à titre préventif, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation. En revanche, ledit article 15,

paragraphe 1, 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 des mesures législatives

– permettant, aux fins de la sauvegarde de la sécurité nationale, le recours à une injonction faite aux fournisseurs de services de communications électroniques de procéder à une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, dans des situations où l'État membre concerné fait face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, la décision prévoyant cette injonction pouvant faire l'objet d'un contrôle effectif soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, visant à vérifier l'existence d'une de ces situations ainsi que le respect des conditions et des garanties devant être prévues, et ladite injonction ne pouvant être émise que pour une période temporellement limitée au strict nécessaire, mais renouvelable en cas de persistance de cette menace ;

– prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation ciblée des données relatives au trafic et des données de localisation qui soit délimitée, sur la base d'éléments objectifs et non discriminatoires, en fonction de catégories de personnes concernées ou au moyen d'un critère géographique, pour une période temporellement limitée au strict nécessaire, mais renouvelable ;

– prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion, pour une période temporellement limitée au strict nécessaire ;

– prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité et de la sauvegarde de la sécurité publique, une conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques, et

– permettant, aux fins de la lutte contre la criminalité grave et, a fortiori, de la sauvegarde de la sécurité nationale, le recours à une injonction faite aux fournisseurs de services de communications électroniques, au moyen d'une décision de l'autorité compétente soumise à un contrôle juridictionnel effectif, de procéder, pour une durée déterminée, à la conservation rapide des données relatives au trafic et des données de localisation dont disposent ces fournisseurs de services,

dès lors que ces mesures assurent, par des règles claires et précises, que la conservation des données en cause est subordonnée au respect des conditions matérielles et procédurales y afférentes et que les personnes concernées disposent de garanties effectives contre les risques d'abus.

Sur les deuxième et troisième questions dans l'affaire C-511/18

169 Par les deuxième et troisième questions dans l'affaire C-511/18, la juridiction de renvoi demande, en substance, si 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, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale imposant aux fournisseurs de services de communications électroniques la mise en œuvre sur leurs réseaux de mesures permettant, d'une part, l'analyse automatisée ainsi que le recueil en temps réel des données relatives au trafic et des données de localisation et, d'autre part, le recueil en temps réel des données techniques relatives à la localisation des équipements terminaux utilisés, sans que soit prévue l'information des personnes concernées par ces traitements et ces recueils.

170 La juridiction de renvoi précise que les techniques de recueil de renseignement prévues aux articles L. 851-2 à L. 851-4 du CSI n'impliquent pas, pour les fournisseurs de services de communications électroniques, une exigence spécifique de conservation des données relatives au trafic et des données de localisation. S'agissant, en particulier, de l'analyse automatisée visée à l'article L. 851-3 du CSI, cette juridiction relève que ce traitement a pour objet de détecter, en fonction de critères définis à cette fin, des connexions susceptibles de révéler une menace terroriste. Quant au recueil en temps réel visé à l'article L. 851-2 du CSI, ladite juridiction constate qu'il ne concerne qu'une ou plusieurs personnes préalablement identifiées comme étant susceptibles d'être en lien avec une menace terroriste. Selon la même juridiction, ces deux techniques ne peuvent être mises en œuvre qu'en vue de la prévention du terrorisme et portent sur les données visées aux articles L. 851-1 et R. 851-5 du CSI.

171 À titre liminaire, il convient de préciser que la circonstance que, selon l'article L. 851-3 du CSI, l'analyse automatisée qu'il prévoit ne permet pas, en tant que telle, l'identification des utilisateurs dont les données sont soumises à cette analyse ne fait pas obstacle à la qualification de telles données en tant que « données à caractère personnel ». En effet, dès lors que la procédure prévue au point IV de cette même disposition permet, à un stade ultérieur, l'identification de la ou des personnes concernées par des données dont l'analyse automatisée a révélé qu'elles étaient susceptibles de caractériser l'existence d'une menace terroriste, toutes les personnes dont les données font l'objet de l'analyse automatisée demeurent identifiables à partir de ces données. Or, selon la définition des données à caractère personnel contenue à l'article 4, point 1, du règlement 2016/679, constituent de telles données les informations se rapportant, notamment, à une personne identifiable.

Sur l'analyse automatisée des données relatives au trafic et des données de localisation

172 Il ressort de l'article L. 851-3 du CSI que l'analyse automatisée qu'il prévoit correspond, en substance, à un filtrage de la totalité des données relatives au trafic et des données de localisation conservées par les fournisseurs de services de communications électroniques, effectué par ces derniers à la demande des autorités nationales compétentes et en application des paramètres que celles-ci ont déterminés. Il s'ensuit que les données des utilisateurs des moyens de communications électroniques sont toutes vérifiées si elles correspondent à ces paramètres. Dès lors, une telle analyse automatisée doit être considérée comme impliquant, pour les fournisseurs de services de communications électroniques concernés, de pratiquer, pour le compte de l'autorité compétente, un traitement généralisé et indifférencié, prenant la forme d'une utilisation à l'aide d'un procédé automatisé, au sens de l'article 4, point 2, du règlement 2016/679, couvrant l'ensemble des données relatives au trafic et des données de localisation de tous les utilisateurs de moyens de communications électroniques. Ce traitement est indépendant du recueil subséquent des données afférentes aux personnes identifiées à la suite de l'analyse automatisée, recueil qui est autorisé sur le fondement de l'article L. 851-3, IV, du CSI.

173 Or, une réglementation nationale qui autorise une telle analyse automatisée des données relatives au trafic et des données de localisation déroge à l'obligation de principe, posée à l'article 5 de la directive 2002/58, de garantir la confidentialité des communications électroniques et des données y afférentes. Une telle réglementation est également constitutive d'une ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, quelle que soit l'utilisation ultérieure qui est faite de ces données. Enfin, ladite réglementation est, conformément à la jurisprudence citée au point 118 du présent arrêt, susceptible d'entraîner des effets dissuasifs sur l'exercice de la liberté d'expression consacrée à l'article 11 de la Charte.

174 En outre, l'ingérence résultant d'une analyse automatisée des données relatives au trafic et des données de localisation, telle que celle en cause au principal, s'avère particulièrement grave dès lors qu'elle couvre de manière généralisée et indifférenciée les données des personnes faisant usage des moyens de communications électroniques. Ce constat s'impose d'autant plus lorsque, ainsi qu'il ressort de la réglementation nationale en cause au principal, les données faisant l'objet de l'analyse automatisée sont susceptibles de révéler la nature des informations consultées en ligne. Au surplus, une telle analyse automatisée s'applique de manière globale à l'ensemble des personnes faisant usage des moyens de communications électroniques et, par suite, également à celles pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement pourrait avoir un lien, même indirect ou lointain, avec des activités de terrorisme.

175 S'agissant de la justification d'une telle ingérence, il convient de préciser que l'exigence, posée à l'article 52, paragraphe 1, de la Charte, selon laquelle toute limitation de l'exercice des droits fondamentaux doit être prévue par la loi implique que la base légale qui permet celle-ci doit définir elle-même la portée de la limitation de l'exercice du droit concerné (voir, en ce sens, arrêt du 16 juillet 2020, Facebook Ireland et Schrems, C-311/18, EU:C:2020:559, point 175 ainsi que jurisprudence citée).

176 En outre, pour satisfaire à l'exigence de proportionnalité rappelée aux points 130 et 131 du présent arrêt, selon laquelle les dérogations à la protection des données à caractère personnel et les limitations de celle-ci doivent s'opérer dans les limites du strict nécessaire, une réglementation nationale régissant l'accès des autorités compétentes à des données relatives au trafic et à des données de localisation conservées doit respecter les exigences résultant de la jurisprudence citée au point 132 du présent arrêt. En particulier, une telle réglementation ne saurait se limiter à exiger que l'accès des autorités aux données réponde à la finalité poursuivie par cette réglementation, mais elle doit également prévoir les conditions matérielles et procédurales régissant cette utilisation [voir, par analogie, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 192 et jurisprudence citée].

177 À cet égard, il y a lieu de rappeler que l'ingérence particulièrement grave que comporte une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, visée par les considérations figurant aux points 134 à 139 du présent arrêt, ainsi que l'ingérence particulièrement grave que constitue leur analyse automatisée ne peuvent satisfaire à l'exigence de proportionnalité que dans des situations dans lesquelles un État membre se trouve face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, et à la condition que la durée de cette conservation soit limitée au strict nécessaire.

178 Dans des situations telles que celles visées au point précédent, la mise en œuvre d'une analyse automatisée des données relatives au trafic et des données de localisation de l'ensemble des utilisateurs de moyens de communications électroniques, pendant une période strictement limitée, peut être considérée comme étant justifiée au regard des exigences découlant de 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.

179 Cela étant, afin de garantir que le recours à une telle mesure se limite effectivement à ce qui est strictement nécessaire à la protection de la sécurité nationale, et plus particulièrement à la prévention du terrorisme, il est essentiel, conformément à ce qui a été constaté au point 139 du présent arrêt, que la décision autorisant l'analyse automatisée puisse faire l'objet d'un contrôle effectif soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, visant à vérifier

l'existence d'une situation justifiant ladite mesure ainsi que le respect des conditions et des garanties devant être prévues.

180 À cet égard, il convient de préciser que les modèles et les critères préétablis sur lesquels se fonde ce type de traitement de données doivent être, d'une part, spécifiques et fiables, permettant d'aboutir à des résultats identifiant des individus à l'égard desquels pourrait peser un soupçon raisonnable de participation à des infractions terroristes et, d'autre part, non discriminatoires [voir, en ce sens, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 172].

181 En outre, il importe de rappeler que toute analyse automatisée effectuée en fonction de modèles et de critères fondés sur le postulat selon lequel l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, l'état de santé ou la vie sexuelle d'une personne pourraient, par eux-mêmes et indépendamment du comportement individuel de cette personne, être pertinents au regard de la prévention du terrorisme méconnaîtrait les droits garantis aux articles 7 et 8 de la Charte, lus en combinaison avec l'article 21 de celle-ci. Ainsi, les modèles et les critères préétablis aux fins d'une analyse automatisée visant à prévenir des activités de terrorisme présentant une menace grave pour la sécurité nationale ne sauraient être fondés sur ces seules données sensibles [voir, en ce sens, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 165].

182 Par ailleurs, les analyses automatisées des données relatives au trafic et des données de localisation comportant nécessairement un certain taux d'erreur, tout résultat positif obtenu à la suite d'un traitement automatisé doit être soumis à un réexamen individuel par des moyens non automatisés avant l'adoption d'une mesure individuelle produisant des effets préjudiciables à l'égard des personnes concernées, tel le recueil subséquent des données relatives au trafic et des données de localisation en temps réel, une telle mesure ne pouvant en effet être fondée de manière décisive sur le seul résultat d'un traitement automatisé. De même, aux fins de garantir, en pratique, que les modèles et les critères préétablis, l'usage qui en est fait ainsi que les bases de données utilisées ne présentent pas un caractère discriminatoire et soient limités au strict nécessaire au regard de l'objectif de prévenir des activités de terrorisme présentant une menace grave pour la sécurité nationale, la fiabilité et l'actualité de ces modèles et de ces critères préétablis ainsi que des bases de données utilisées doivent faire l'objet d'un réexamen régulier [voir, en ce sens, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, points 173 et 174]

Sur le recueil en temps réel des données relatives au trafic et des données de localisation

183 S'agissant du recueil en temps réel des données relatives au trafic et des données de localisation visé à l'article L. 851-2 du CSI, il y a lieu de relever que celui-ci peut être individuellement autorisé en ce qui concerne « une personne préalablement identifiée susceptible d'être en lien avec une menace [terroriste] ». De même, selon cette disposition, « lorsqu'il existe des raisons sérieuses de penser qu'une ou plusieurs personnes appartenant à l'entourage de la personne concernée par l'autorisation sont susceptibles de fournir des informations au titre de la finalité qui motive l'autorisation, celle-ci peut être également accordée individuellement pour chacune de ces personnes ».

184 Les données faisant l'objet d'une mesure de cette nature permettent aux autorités nationales compétentes de surveiller, pendant la durée de l'autorisation, de manière continue et en temps réel, les interlocuteurs avec lesquels les personnes concernées communiquent, les moyens qu'elles utilisent, la durée des communications qu'elles passent, ainsi que leurs lieux de séjours et leurs déplacements. De même, elles semblent susceptibles de révéler la nature des informations consultées en ligne. Prises dans leur ensemble, ces données permettent, ainsi qu'il ressort du 117 point du présent arrêt, de tirer des conclusions très précises concernant la vie privée des personnes concernées et fournissent les moyens d'établir le profil de celles-ci, une telle information étant tout aussi sensible, au regard du droit au respect de la vie privée, que le contenu même des communications.

185 Quant au recueil de données en temps réel visé à l'article L. 851-4 du CSI, cette disposition autorise le recueil des données techniques relatives à la localisation des équipements terminaux et la transmission en temps réel à un service du Premier ministre. Il apparaît que de telles données permettent au service compétent, à tout moment pendant la durée de l'autorisation, de localiser, de manière continue et en temps réel, des équipements terminaux utilisés, tels des téléphones mobiles.

186 Or, une réglementation nationale autorisant de tels recueils en temps réel déroge, à l'instar de celle qui autorise l'analyse automatisée des données, à l'obligation de principe, posée à l'article 5 de la directive 2002/58, de garantir la confidentialité des communications électroniques et des données y afférentes. Elle est dès lors également constitutive d'une ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte et est susceptible d'entraîner des effets dissuasifs sur l'exercice de la liberté d'expression garantie à l'article 11 de la Charte.

187 Il y a lieu de souligner que l'ingérence que comporte le recueil en temps réel des données permettant de localiser un équipement terminal apparaît particulièrement grave, dès lors que ces données fournissent aux autorités nationales compétentes le moyen d'un suivi précis et permanent des déplacements des utilisateurs des téléphones mobiles. Dans la mesure où ces données doivent ainsi être considérées comme étant particulièrement sensibles, l'accès en temps réel des autorités compétentes à de telles données doit être

distingué d'un accès en temps différé à celles-ci, le premier étant davantage intrusif en ce qu'il permet une surveillance quasiment parfaite de ces utilisateurs (voir, par analogie, en ce qui concerne l'article 8 de la CEDH, Cour EDH, 8 février 2018, Ben Faiza c. France, CE:ECHR:2018:0208JUD003144612, § 74). L'intensité de cette ingérence est en outre aggravée lorsque le recueil en temps réel s'étend également aux données relatives au trafic des personnes concernées.

188 Si l'objectif de prévention du terrorisme que poursuit la réglementation nationale en cause au principal est susceptible, eu égard à son importance, de justifier l'ingérence que comporte le recueil en temps réel des données relatives au trafic et des données de localisation, une telle mesure ne saurait être mise en œuvre, compte tenu de son caractère particulièrement intrusif, qu'à l'égard des personnes pour lesquelles il existe une raison valable de soupçonner qu'elles sont impliquées d'une manière ou d'une autre dans des activités de terrorisme. Quant aux données des personnes ne relevant pas de cette catégorie, elles peuvent seulement faire l'objet d'un accès en temps différé, celui-ci ne pouvant avoir lieu, conformément à la jurisprudence de la Cour, que dans des situations particulières, telles que celles dans lesquelles sont en cause des activités de terrorisme, et lorsqu'il existe des éléments objectifs permettant de considérer que ces données pourraient, dans un cas concret, apporter une contribution effective à la lutte contre le terrorisme (voir, en ce sens, arrêt du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, point 119 et jurisprudence citée).

189 En outre, une décision autorisant le recueil en temps réel des données relatives au trafic et des données de localisation doit être fondée sur des critères objectifs prévus dans la législation nationale. En particulier, cette législation doit définir, conformément à la jurisprudence citée au point 176 du présent arrêt, les circonstances et les conditions dans lesquelles un tel recueil peut être autorisé et prévoir que, ainsi qu'il a été précisé au point précédent, seules peuvent être concernées les personnes présentant un lien avec l'objectif de prévention du terrorisme. En outre, une décision autorisant le recueil en temps réel des données relatives au trafic et des données de localisation doit être fondée sur des critères objectifs et non discriminatoires prévus dans la législation nationale. Aux fins de garantir, en pratique, le respect de ces conditions, il est essentiel que la mise en œuvre de la mesure autorisant le recueil en temps réel soit soumise à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, cette juridiction ou cette entité devant notamment s'assurer qu'un tel recueil en temps réel n'est autorisé que dans la limite de ce qui est strictement nécessaire (voir, en ce sens, arrêt du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, point 120). En cas d'urgence dûment justifiée, le contrôle doit intervenir dans de brefs délais.

Sur l'information des personnes dont les données ont été recueillies ou analysées

190 Il importe que les autorités nationales compétentes procédant au recueil en temps réel des données relatives au trafic et des données de localisation en informent les personnes concernées, dans le cadre des procédures nationales applicables, pour autant que et dès le moment où cette communication n'est pas susceptible de compromettre les missions qui incombent à ces autorités. En effet, cette information est, de fait, nécessaire pour permettre à ces personnes d'exercer leurs droits, découlant des articles 7 et 8 de la Charte, de demander l'accès à leurs données à caractère personnel faisant l'objet de ces mesures et, le cas échéant, la rectification ou la suppression de celles-ci, ainsi que d'introduire, conformément à l'article 47, premier alinéa, de la Charte, un recours effectif devant un tribunal, un tel droit étant d'ailleurs explicitement garanti à l'article 15, paragraphe 2, de la directive 2002/58, lu en combinaison avec l'article 79, paragraphe 1, du règlement 2016/679 [voir, en ce sens, arrêt du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, point 121 et jurisprudence citée, ainsi que avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, points 219 et 220].

191 S'agissant de l'information requise dans le contexte d'une analyse automatisée des données relatives au trafic et des données de localisation, l'autorité nationale compétente est tenue de publier des renseignements de nature générale relatifs à cette analyse, sans devoir procéder à une information individuelle des personnes concernées. En revanche, dans l'hypothèse où les données répondent aux paramètres précisés dans la mesure autorisant l'analyse automatisée et où cette autorité procède à l'identification de la personne concernée aux fins d'analyser plus en profondeur les données la concernant, l'information individuelle de cette personne s'avère nécessaire. Une telle information ne doit toutefois intervenir que pour autant que et qu'à partir du moment où elle n'est pas susceptible de compromettre les missions incombant à ladite autorité [voir, par analogie, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, points 222 à 224].

192 Eu égard à l'ensemble des considérations qui précèdent, il y a lieu de répondre aux deuxième et troisième questions dans l'affaire C-511/18 que 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, doit être interprété en ce sens qu'il ne s'oppose pas à une réglementation nationale imposant aux fournisseurs de services de communications électroniques de recourir, d'une part, à l'analyse automatisée ainsi qu'au recueil en temps réel, notamment, des données relatives au trafic et des données de localisation et, d'autre part, au recueil en temps réel des données techniques relatives à la localisation des équipements terminaux utilisés, lorsque

– le recours à l'analyse automatisée est limité à des situations dans lesquelles un État membre se trouve confronté à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, le recours

à cette analyse pouvant faire l'objet d'un contrôle effectif, soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, visant à vérifier l'existence d'une situation justifiant ladite mesure ainsi que le respect des conditions et des garanties devant être prévues, et que

– le recours à un recueil en temps réel des données relatives au trafic et des données de localisation est limité aux personnes à l'égard desquelles il existe une raison valable de soupçonner qu'elles sont impliquées d'une manière ou d'une autre dans des activités de terrorisme et est soumis à un contrôle préalable, effectué, soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, afin de s'assurer qu'un tel recueil en temps réel n'est autorisé que dans la limite de ce qui est strictement nécessaire. En cas d'urgence dûment justifiée, le contrôle doit intervenir dans de brefs délais.

Sur la seconde question dans l'affaire C-512/18

193 Par la seconde question dans l'affaire C-512/18, la juridiction de renvoi cherche, en substance, à savoir si les dispositions de la directive 2000/31, lues à la lumière des articles 6 à 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, doivent être interprétées en ce sens qu'elles s'opposent à une réglementation nationale imposant aux fournisseurs d'accès à des services de communication au public en ligne et aux fournisseurs de services d'hébergement la conservation généralisée et indifférenciée, notamment, des données à caractère personnel afférentes à ces services.

194 Tout en considérant que de tels services relèvent du champ d'application de la directive 2000/31, et non de celui de la directive 2002/58, la juridiction de renvoi est d'avis que l'article 15, paragraphes 1 et 2, de la directive 2000/31, lu en combinaison avec les articles 12 et 14 de celle-ci, n'instaure pas, par lui-même, une interdiction de principe de conserver des données relatives à la création de contenu à laquelle il pourrait seulement être dérogé de manière exceptionnelle. Cette juridiction se demande néanmoins si cette appréciation doit être retenue, compte tenu du respect nécessaire des droits fondamentaux consacrés aux articles 6 à 8 et 11 de la Charte.

195 En outre, la juridiction de renvoi précise que sa question vise l'obligation de conservation prévue à l'article 6 de la LCEN, lu en combinaison avec le décret n° 2011-219. Les données que doivent conserver les fournisseurs de services concernés à ce titre incluent, notamment, les données relatives à l'identité civile des personnes ayant fait usage de ces services, tels que leurs nom, prénom, leurs adresses postales associées, leurs adresses de courrier électronique ou de compte associées, leurs mots de passe et, lorsque la souscription du contrat ou du compte est payante, le type de paiement utilisé, la référence du paiement, le montant ainsi que la date et l'heure de la transaction.

196 De même, les données visées par l'obligation de conservation couvrent les identifiants des abonnés, des connexions et des équipements terminaux utilisés, les identifiants attribués aux contenus, les dates et heures de début et de fin des connexions et des opérations ainsi que les types de protocoles utilisés pour la connexion au service et pour le transfert des contenus. L'accès à ces données, dont la durée de conservation s'élève à un an, peut être sollicité dans le cadre des procédures pénales et civiles, en vue de faire respecter les règles relatives à la responsabilité civile ou pénale, ainsi que dans le cadre de mesures de recueil de renseignement auxquelles l'article L. 851-1 du CSI s'applique.

197 À cet égard, il y a lieu de relever que, conformément à son article 1er, paragraphe 2, la directive 2000/31 rapproche certaines dispositions nationales applicables aux services de la société de l'information visés à son article 2, sous a).

198 De tels services englobent, certes, ceux qui sont fournis à distance au moyen d'équipements électroniques de traitement et de stockage de données, à la demande individuelle d'un destinataire de services et, normalement, contre rémunération, tels que des services d'accès à Internet ou à un réseau de communication ainsi que des services d'hébergement (voir, en ce sens, arrêts du 24 novembre 2011, Scarlet Extended, C-70/10, EU:C:2011:771, point 40 ; du 16 février 2012, SABAM, C-360/10, EU:C:2012:85, point 34 ; du 15 septembre 2016, Mc Fadden, C-484/14, EU:C:2016:689, point 55, ainsi que du 7 août 2018, SNB-REACT, C-521/17, EU:C:2018:639, point 42 et jurisprudence citée).

199 Toutefois, l'article 1er, paragraphe 5, de la directive 2000/31 dispose que celle-ci n'est pas applicable aux questions relatives aux services de la société de l'information qui sont couvertes par les directives 95/46 et 97/66. À cet égard, il ressort des considérants 14 et 15 de la directive 2000/31 que la protection de la confidentialité des communications ainsi que des personnes physiques à l'égard du traitement des données à caractère personnel dans le cadre des services de la société de l'information est uniquement régie par les directives 95/46 et 97/66, cette dernière interdisant, à son article 5, aux fins de la protection de la confidentialité des communications, toute forme d'interception ou de surveillance des communications.

200 Ainsi, des questions liées à la protection de la confidentialité des communications et des données à caractère personnel doivent être appréciées à l'aune de la directive 2002/58 et du règlement 2016/679, ceux-ci ayant remplacé respectivement la directive 97/66 et la directive 95/46, étant précisé que la protection que vise à assurer la directive 2000/31 ne peut en tout état de cause pas porter atteinte aux exigences résultant de la directive 2002/58 et du règlement 2016/679 (voir, en ce sens, arrêt du 29 janvier 2008, Promusicae, C-275/06, EU:C:2008:54, point 57).

201 L'obligation imposée par la réglementation nationale visée au point 195 du présent arrêt aux fournisseurs d'accès à des services de communication au public en ligne et aux fournisseurs de services d'hébergement de conserver des données à caractère personnel afférentes à ces services doit donc, comme l'a relevé en substance M. l'avocat général au point 141 de ses conclusions dans les affaires jointes La Quadrature du Net e.a. (C-511/18 et C-512/18, EU:C:2020:6), être appréciée à l'aune de la directive 2002/58 ou du règlement 2016/679.

202 Ainsi, selon que la fourniture des services couverts par cette réglementation nationale relève ou non de la directive 2002/58, elle sera régie soit par cette dernière directive, en particulier par l'article 15, paragraphe 1, de celle-ci, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, soit par le règlement 2016/679, en particulier par l'article 23, paragraphe 1, dudit règlement, lu à la lumière des mêmes dispositions de la Charte.

203 En l'occurrence, il ne saurait être exclu, comme l'a relevé la Commission européenne dans ses observations écrites, que certains des services auxquels s'applique la réglementation nationale visée au point 195 du présent arrêt constituent des services de communications électroniques, au sens de la directive 2002/58, ce qu'il appartient à la juridiction de renvoi de vérifier.

204 À cet égard, il convient de relever que la directive 2002/58 couvre les services de communications électroniques qui remplissent les conditions énoncées à l'article 2, sous c), de la directive 2002/21, auquel renvoie l'article 2 de la directive 2002/58 et qui définit le service de communications électroniques comme étant « le service fourni normalement contre rémunération qui consiste entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques, y compris les services de télécommunications et les services de transmission sur les réseaux utilisés pour la radiodiffusion ». S'agissant des services de la société de l'information, tels que visés aux points 197 et 198 du présent arrêt et couverts par la directive 2000/31, ceux-ci constituent des services de communications électroniques dès lors qu'ils consistent entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques (voir, en ce sens, arrêt du 5 juin 2019, Skype Communications, C-142/18, EU:C:2019:460, points 47 et 48).

205 Ainsi, les services d'accès à Internet, lesquels paraissent être couverts par la réglementation nationale visée au point 195 du présent arrêt, constituent, comme le confirme le considérant 10 de la directive 2002/21, des services de communications électroniques, au sens de cette directive (voir, en ce sens, arrêt du 5 juin 2019, Skype Communications, C-142/18, EU:C:2019:460, point 37). Tel est également le cas des services de messageries sur Internet, dont il ne semble pas exclu qu'ils relèvent également de cette réglementation nationale, dès lors que, sur le plan technique, ils impliquent entièrement ou principalement la transmission de signaux sur des réseaux de communications électroniques (voir, en ce sens, arrêt du 13 juin 2019, Google, C-193/18, EU:C:2019:498, points 35 et 38).

206 S'agissant des exigences découlant de 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, il convient de renvoyer à l'ensemble des constatations et des appréciations faites dans le cadre de la réponse apportée aux premières questions dans les affaires C-511/18 et C-512/18 ainsi qu'aux première et deuxième questions dans l'affaire C-520/18.

207 Quant aux exigences découlant du règlement 2016/679, il convient de rappeler que celui-ci vise, notamment, ainsi qu'il ressort de son considérant 10, à assurer un niveau élevé de protection des personnes physiques au sein de l'Union et, à cette fin, à assurer une application cohérente et homogène des règles de protection des libertés et des droits fondamentaux de ces personnes à l'égard du traitement des données à caractère personnel dans l'ensemble de l'Union (voir, en ce sens, arrêt du 16 juillet 2020, Facebook Ireland et Schrems, C-311/18, EU:C:2020:559, point 101).

208 À cette fin, tout traitement de données à caractère personnel doit, sous réserve des dérogations admises à l'article 23 du règlement 2016/679, respecter les principes régissant les traitements des données à caractère personnel ainsi que les droits de la personne concernée énoncés respectivement dans les chapitres II et III de ce règlement. En particulier, tout traitement de données à caractère personnel doit, d'une part, être conforme aux principes énoncés à l'article 5 dudit règlement et, d'autre part, satisfaire aux conditions de licéité énumérées à l'article 6 de ce même règlement (voir, par analogie, en ce qui concerne la directive 95/46, arrêt du 30 mai 2013, Worten, C-342/12, EU:C:2013:355, point 33 et jurisprudence citée).

209 Pour ce qui est, plus particulièrement, de l'article 23, paragraphe 1, du règlement 2016/679, il y a lieu de relever que celui-ci, à l'instar de ce qui est prévu à l'article 15, paragraphe 1, de la directive 2002/58, permet aux États membres de limiter, au regard des finalités qu'il prévoit et au moyen de mesures législatives, la portée des obligations et des droits qui y sont visés « lorsqu'une telle limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir » la finalité poursuivie. Toute mesure législative prise sur ce fondement doit, en particulier, respecter les exigences spécifiques posées à l'article 23, paragraphe 2, de ce règlement.

210 Ainsi, l'article 23, paragraphes 1 et 2, du règlement 2016/679 ne saurait être interprété comme pouvant conférer aux États membres le pouvoir de porter atteinte au respect de la vie privée, en méconnaissance de l'article 7 de la Charte, tout comme aux autres garanties prévues par celle-ci (voir, par analogie, en ce qui

concerne la directive 95/46, arrêt du 20 mai 2003, Österreichischer Rundfunk e.a., C-465/00, C-138/01 et C-139/01, EU:C:2003:294, point 91). En particulier, à l'instar de ce qui vaut pour l'article 15, paragraphe 1, de la directive 2002/58, le pouvoir que confère l'article 23, paragraphe 1, du règlement 2016/679 aux États membres ne saurait être exercé que dans le respect de l'exigence de proportionnalité, selon laquelle les dérogations à la protection des données à caractère personnel et les limitations de celles-ci doivent s'opérer dans les limites du strict nécessaire (voir, par analogie, s'agissant de la directive 95/46, arrêt du 7 novembre 2013, IPI, C-473/12, EU:C:2013:715, point 39 et jurisprudence citée).

211 Il s'ensuit que les constatations et les appréciations faites dans le cadre de la réponse apportée aux premières questions dans les affaires C-511/18 et C-512/18 ainsi qu'aux première et deuxième questions dans l'affaire C-520/18 s'appliquent mutatis mutandis à l'article 23 du règlement 2016/679.

212 Au regard des considérations qui précèdent, il convient de répondre à la seconde question dans l'affaire C-512/18 que la directive 2000/31 doit être interprétée en ce sens qu'elle n'est pas applicable en matière de protection de la confidentialité des communications et des personnes physiques à l'égard du traitement des données à caractère personnel dans le cadre des services de la société de l'information, cette protection étant, selon le cas, régie par la directive 2002/58 ou par le règlement 2016/679. L'article 23, paragraphe 1, du règlement 2016/679, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale imposant aux fournisseurs d'accès à des services de communication au public en ligne et aux fournisseurs de services d'hébergement la conservation généralisée et indifférenciée, notamment, des données à caractère personnel afférentes à ces services.

Sur la troisième question dans l'affaire C-520/18

213 Par la troisième question dans l'affaire C-520/18, la juridiction de renvoi cherche, en substance, à savoir si une juridiction nationale peut faire application d'une disposition de son droit national qui l'habilite à limiter dans le temps les effets d'une déclaration d'illégalité lui incombant, en vertu de ce droit, à l'égard d'une législation nationale imposant aux fournisseurs de services de communications électroniques, en vue, entre autres, de la poursuite des objectifs de sauvegarde de la sécurité nationale et de lutte contre la criminalité, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, résultant de son caractère incompatible avec 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.

214 Le principe de primauté du droit de l'Union consacre la prééminence du droit de l'Union sur le droit des États membres. Ce principe impose dès lors à toutes les instances des États membres de donner leur plein effet aux différentes normes de l'Union, le droit des États membres ne pouvant affecter l'effet reconnu à ces différentes normes sur le territoire desdits États [arrêts du 15 juillet 1964, Costa, 6/64, EU:C:1964:66, p. 1159 et 1160, ainsi que du 19 novembre 2019, A. K. e.a. (Indépendance de la chambre disciplinaire de la Cour suprême), C-585/18, C-624/18 et C-625/18, EU:C:2019:982, points 157 et 158 et jurisprudence citée].

215 En vertu du principe de primauté, à défaut de pouvoir procéder à une interprétation de la réglementation nationale conforme aux exigences du droit de l'Union, le juge national chargé d'appliquer, dans le cadre de sa compétence, les dispositions du droit de l'Union a l'obligation d'assurer le plein effet de celles-ci en laissant au besoin inappliquée, de sa propre autorité, toute disposition contraire de la législation nationale, même postérieure, sans qu'il ait à demander ou à attendre l'élimination préalable de celle-ci par voie législative ou par tout autre procédé constitutionnel [arrêts du 22 juin 2010, Melki et Abdeli, C-188/10 et C-189/10, EU:C:2010:363, point 43 et jurisprudence citée ; du 24 juin 2019, Popławski, C-573/17, EU:C:2019:530, point 58, ainsi que du 19 novembre 2019, A. K. e.a. (Indépendance de la chambre disciplinaire de la Cour suprême), C-585/18, C-624/18 et C-625/18, EU:C:2019:982, point 160].

216 Seule la Cour peut, à titre exceptionnel et pour des considérations impérieuses de sécurité juridique, accorder une suspension provisoire de l'effet d'éviction exercé par une règle du droit de l'Union à l'égard du droit national contraire à celle-ci. Une telle limitation dans le temps des effets de l'interprétation de ce droit donnée par la Cour ne peut être accordée que dans l'arrêt même qui statue sur l'interprétation sollicitée [voir, en ce sens, arrêts du 23 octobre 2012, Nelson e.a., C-581/10 et C-629/10, EU:C:2012:657, points 89 et 91 ; du 23 avril 2020, Herst, C-401/18, EU:C:2020:295, points 56 et 57, ainsi que du 25 juin 2020, A e.a. (Éoliennes à Aalter et à Nevele), C-24/19, EU:C:2020:503, point 84 et jurisprudence citée].

217 Il serait porté atteinte à la primauté et à l'application uniforme du droit de l'Union si des juridictions nationales avaient le pouvoir de donner aux dispositions nationales la primauté par rapport au droit de l'Union auquel ces dispositions contreviennent, serait-ce même à titre provisoire (voir, en ce sens, arrêt du 29 juillet 2019, Inter-Environnement Wallonie et Bond Beter Leefmilieu Vlaanderen, C-411/17, EU:C:2019:622, point 177 ainsi que jurisprudence citée).

218 Toutefois, la Cour a jugé, dans une affaire où était en cause la légalité de mesures adoptées en méconnaissance de l'obligation édictée par le droit de l'Union d'effectuer une évaluation préalable des incidences d'un projet sur l'environnement et sur un site protégé, qu'une juridiction nationale peut, si le droit interne le permet, exceptionnellement maintenir les effets de telles mesures lorsque ce maintien est justifié par des considérations impérieuses liées à la nécessité d'écarter une menace réelle et grave de rupture de

l'approvisionnement en électricité de l'État membre concerné, à laquelle il ne pourrait être fait face par d'autres moyens et alternatives, notamment dans le cadre du marché intérieur, ledit maintien ne pouvant couvrir que le laps de temps strictement nécessaire pour remédier à cette illégalité (voir, en ce sens, arrêt du 29 juillet 2019, Inter-Environnement Wallonie et Bond Beter Leefmilieu Vlaanderen, C-411/17, EU:C:2019:622, points 175, 176, 179 et 181).

219 Or, contrairement à l'omission d'une obligation procédurale telle que l'évaluation préalable des incidences d'un projet dans le domaine spécifique de la protection de l'environnement, une méconnaissance de 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 saurait faire l'objet d'une régularisation par voie d'une procédure comparable à celle mentionnée au point précédent. En effet, le maintien des effets d'une législation nationale, telle que celle en cause au principal, signifierait que cette législation continue à imposer aux fournisseurs de services de communications électroniques des obligations qui sont contraires au droit de l'Union et qui comportent des ingérences graves dans les droits fondamentaux des personnes dont les données ont été conservées.

220 Partant, la juridiction de renvoi ne saurait faire application d'une disposition de son droit national qui l'habilite à limiter dans le temps les effets d'une déclaration d'illégalité lui incombant, en vertu de ce droit, de la législation nationale en cause au principal.

221 Cela étant, dans leurs observations soumises à la Cour, VZ, WY et XX font valoir que la troisième question soulève, implicitement mais nécessairement, le point de savoir si le droit de l'Union s'oppose à une exploitation, dans le cadre d'une procédure pénale, des informations et des éléments de preuve qui ont été obtenus par une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation incompatible avec ce droit.

222 À cet égard et afin de donner une réponse utile à la juridiction de renvoi, il y a lieu de rappeler que, en l'état actuel du droit de l'Union, il appartient, en principe, au seul droit national de déterminer les règles relatives à l'admissibilité et à l'appréciation, dans le cadre d'une procédure pénale ouverte à l'encontre de personnes soupçonnées d'actes de criminalité grave, d'informations et d'éléments de preuve qui ont été obtenus par une telle conservation de données contraire au droit de l'Union.

223 En effet, il est de jurisprudence constante que, en l'absence de règles de l'Union en la matière, il appartient à l'ordre juridique interne de chaque État membre, en vertu du principe d'autonomie procédurale, de régler les modalités procédurales des recours en justice destinés à assurer la sauvegarde des droits que les justiciables tirent du droit de l'Union, à condition toutefois qu'elles ne soient pas moins favorables que celles régissant des situations similaires soumises au droit interne (principe d'équivalence) et qu'elles ne rendent pas impossible en pratique ou excessivement difficile l'exercice des droits conférés par le droit de l'Union (principe d'effectivité) (voir, en ce sens, arrêts du 6 octobre 2015, Târşia, C-69/14, EU:C:2015:662, points 26 et 27 ; du 24 octobre 2018, XC e.a., C-234/17, EU:C:2018:853, points 21 et 22 ainsi que jurisprudence citée, et du 19 décembre 2019, Deutsche Umwelthilfe, C-752/18, EU:C:2019:1114, point 33).

224 En ce qui concerne le principe d'équivalence, il appartient au juge national saisi d'une procédure pénale fondée sur des informations ou des éléments de preuve obtenus en méconnaissance des exigences résultant de la directive 2002/58 de vérifier si le droit national régissant cette procédure prévoit des règles moins favorables en ce qui concerne l'admissibilité et l'exploitation de telles informations et de tels éléments de preuve que celles régissant les informations et les éléments de preuve obtenus en violation du droit interne.

225 Quant au principe d'effectivité, il convient de relever que les règles nationales relatives à l'admissibilité et à l'exploitation des informations et des éléments de preuve ont pour objectif, en vertu des choix opérés par le droit national, d'éviter que des informations et des éléments de preuve qui ont été obtenus de manière illégale portent indûment préjudice à une personne soupçonnée d'avoir commis des infractions pénales. Or, cet objectif peut, selon le droit national, être atteint non seulement par une interdiction d'exploiter de telles informations et de tels éléments de preuve, mais également par des règles et des pratiques nationales régissant l'appréciation et la pondération des informations et des éléments de preuve, voire par une prise en considération de leur caractère illégal dans le cadre de la détermination de la peine.

226 Cela étant, il ressort de la jurisprudence de la Cour que la nécessité d'exclure des informations et des éléments de preuve obtenus en méconnaissance des prescriptions du droit de l'Union doit être appréciée au regard, notamment, du risque que l'admissibilité de tels informations et éléments de preuve comporte pour le respect du principe du contradictoire et, partant, du droit à un procès équitable (voir, en ce sens, arrêt du 10 avril 2003, Steffensen, C-276/01, EU:C:2003:228, points 76 et 77). Or, une juridiction qui considère qu'une partie n'est pas en mesure de commenter efficacement un moyen de preuve qui ressortit à un domaine échappant à la connaissance des juges et qui est susceptible d'influencer de manière prépondérante l'appréciation des faits doit constater une violation du droit à un procès équitable et exclure ce moyen de preuve afin d'éviter une telle violation (voir, en ce sens, arrêt du 10 avril 2003, Steffensen, C-276/01, EU:C:2003:228, points 78 et 79).

227 Partant, le principe d'effectivité impose au juge pénal national d'écarter des informations et des éléments de preuve qui ont été obtenus au moyen d'une conservation généralisée et indifférenciée des

données relatives au trafic et des données de localisation incompatible avec le droit de l'Union, dans le cadre d'une procédure pénale ouverte à l'encontre de personnes soupçonnées d'actes de criminalité, si ces personnes ne sont pas en mesure de commenter efficacement ces informations et ces éléments de preuve, provenant d'un domaine échappant à la connaissance des juges et qui sont susceptibles d'influencer de manière prépondérante l'appréciation des faits.

228 Eu égard aux considérations qui précèdent, il y a lieu de répondre à la troisième question dans l'affaire C-520/18 qu'une juridiction nationale ne peut faire application d'une disposition de son droit national qui l'habilite à limiter dans le temps les effets d'une déclaration d'illégalité lui incombant, en vertu de ce droit, à l'égard d'une législation nationale imposant aux fournisseurs de services de communications électroniques, en vue, notamment, de la sauvegarde de la sécurité nationale et de la lutte contre la criminalité, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation incompatible avec 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. Cet article 15, paragraphe 1, interprété à la lumière du principe d'effectivité, impose au juge pénal national d'écarter des informations et des éléments de preuve qui ont été obtenus par une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation incompatible avec le droit de l'Union, dans le cadre d'une procédure pénale ouverte à l'encontre de personnes soupçonnées d'actes de criminalité, si ces personnes ne sont pas en mesure de commenter efficacement ces informations et ces éléments de preuve, provenant d'un domaine échappant à la connaissance des juges et qui sont susceptibles d'influencer de manière prépondérante l'appréciation des faits.

Sur les dépens

229 La procédure revêtant, à l'égard des parties au principal, le caractère d'un incident soulevé devant les juridictions de renvoi, il appartient à celles-ci de statuer sur les dépens. Les frais exposés pour soumettre des observations à la Cour, autres que ceux desdites parties, ne peuvent faire l'objet d'un remboursement.

Par ces motifs, la Cour (grande chambre) dit pour droit :

1) **L'article 15, paragraphe 1, de 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 (directive vie privée et communications électroniques), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009, 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 des mesures législatives prévoyant, aux fins prévues à cet article 15, paragraphe 1, à titre préventif, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation. En revanche, l'article 15, paragraphe 1, de la directive 2002/58, telle que modifiée par la directive 2009/136, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux, ne s'oppose pas à des mesures législatives**

– **permettant, aux fins de la sauvegarde de la sécurité nationale, le recours à une injonction faite aux fournisseurs de services de communications électroniques de procéder à une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, dans des situations où l'État membre concerné fait face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, la décision prévoyant cette injonction pouvant faire l'objet d'un contrôle effectif, soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, visant à vérifier l'existence d'une de ces situations ainsi que le respect des conditions et des garanties devant être prévues, et ladite injonction ne pouvant être émise que pour une période temporellement limitée au strict nécessaire, mais renouvelable en cas de persistance de cette menace ;**

– **prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation ciblée des données relatives au trafic et des données de localisation qui soit délimitée, sur la base d'éléments objectifs et non discriminatoires, en fonction de catégories de personnes concernées ou au moyen d'un critère géographique, pour une période temporellement limitée au strict nécessaire, mais renouvelable ;**

– **prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion, pour une période temporellement limitée au strict nécessaire ;**

– prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité et de la sauvegarde de la sécurité publique, une conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques, et

– permettant, aux fins de la lutte contre la criminalité grave et, a fortiori, de la sauvegarde de la sécurité nationale, le recours à une injonction faite aux fournisseurs de services de communications électroniques, par le biais d'une décision de l'autorité compétente soumise à un contrôle juridictionnel effectif, de procéder, pour une durée déterminée, à la conservation rapide des données relatives au trafic et des données de localisation dont disposent ces fournisseurs de services,

dès lors que ces mesures assurent, par des règles claires et précises, que la conservation des données en cause est subordonnée au respect des conditions matérielles et procédurales y afférentes et que les personnes concernées disposent de garanties effectives contre les risques d'abus.

2) **L'article 15, paragraphe 1, de la directive 2002/58, telle que modifiée par la directive 2009/136, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux, doit être interprété en ce sens qu'il ne s'oppose pas à une réglementation nationale imposant aux fournisseurs de services de communications électroniques de recourir, d'une part, à l'analyse automatisée ainsi qu'au recueil en temps réel, notamment, des données relatives au trafic et des données de localisation et, d'autre part, au recueil en temps réel des données techniques relatives à la localisation des équipements terminaux utilisés, lorsque**

– le recours à l'analyse automatisée est limité à des situations dans lesquelles un État membre se trouve confronté à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, le recours à cette analyse pouvant faire l'objet d'un contrôle effectif, soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, visant à vérifier l'existence d'une situation justifiant ladite mesure ainsi que le respect des conditions et des garanties devant être prévues, et que

– le recours à un recueil en temps réel des données relatives au trafic et des données de localisation est limité aux personnes à l'égard desquelles il existe une raison valable de soupçonner qu'elles sont impliquées d'une manière ou d'une autre dans des activités de terrorisme et est soumis à un contrôle préalable, effectué, soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, afin de s'assurer qu'un tel recueil en temps réel n'est autorisé que dans la limite de ce qui est strictement nécessaire. En cas d'urgence dûment justifiée, le contrôle doit intervenir dans de brefs délais.

3) **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 (« directive sur le commerce électronique »), doit être interprétée en ce sens qu'elle n'est pas applicable en matière de protection de la confidentialité des communications et des personnes physiques à l'égard du traitement des données à caractère personnel dans le cadre des services de la société de l'information, cette protection étant, selon le cas, régie par la directive 2002/58, telle que modifiée par la directive 2009/136, ou par le règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, 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, et abrogeant la directive 95/46. L'article 23, paragraphe 1, du règlement 2016/679, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale imposant aux fournisseurs d'accès à des services de communication au public en ligne et aux fournisseurs de services d'hébergement la conservation généralisée et indifférenciée, notamment, des données à caractère personnel afférentes à ces services.**

4) **Une juridiction nationale ne peut faire application d'une disposition de son droit national qui l'habilite à limiter dans le temps les effets d'une déclaration d'illégalité lui incombant, en vertu de ce droit, à l'égard d'une législation nationale imposant aux fournisseurs de services de communications électroniques, en vue, notamment, de la sauvegarde de la sécurité nationale et de la lutte contre la criminalité, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation incompatible avec l'article 15, paragraphe 1, de la directive 2002/58, telle que modifiée par la directive 2009/136, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux. Cet article 15, paragraphe 1, interprété à la lumière du principe d'effectivité, impose au juge pénal national d'écarter des informations et des éléments de preuve qui ont été obtenus par une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation incompatible avec le droit de l'Union, dans le cadre d'une procédure pénale ouverte à l'encontre de personnes soupçonnées d'actes de criminalité, si ces personnes ne sont pas en mesure de commenter efficacement ces informations et ces éléments de preuve, provenant d'un domaine échappant à la**

connaissance des juges et qui sont susceptibles d'influencer de manière prépondérante l'appréciation des faits.

Décision n° 2021-940 QPC du 15 octobre 2021
(Société Air France)

LE CONSEIL CONSTITUTIONNEL A ÉTÉ SAISI le 15 juillet 2021
par le Conseil d'État (décision n° 450480 du 9 juillet 2021), dans les conditions prévues à l'article 61-1 de la Constitution, d'une question prioritaire de constitutionnalité. Cette question a été posée pour la société Air France par la SCP Rocheteau et Uzan-Sarano, avocat au Conseil d'État et à la Cour de cassation. Elle a été enregistrée au secrétariat général du Conseil constitutionnel sous le n° 2021-940 QPC. Elle est relative à la conformité aux droits et libertés que la Constitution garantit de l'article L. 213-4 et du 1° de l'article L. 625-7 du code de l'entrée et du séjour des étrangers et du droit d'asile.

Au vu des textes suivants :

- la Constitution ;
- l'ordonnance n° 58-1067 du 7 novembre 1958 portant loi organique sur le Conseil constitutionnel ;
- la convention d'application de l'accord de Schengen du 14 juin 1985, signée le 19 juin 1990, notamment son article 26 ;
- la directive 2001/51/CE du Conseil du 28 juin 2001 visant à compléter les dispositions de l'article 26 de la convention d'application de l'accord de Schengen du 14 juin 1985 ;
- le code de l'entrée et du séjour des étrangers et du droit d'asile ;
- le code des transports ;
- l'ordonnance n° 2004-1248 du 24 novembre 2004 relative à la partie législative du code de l'entrée et du séjour des étrangers et du droit d'asile, ratifiée par l'article 120 de la loi n° 2006-911 du 24 juillet 2006 relative à l'immigration et à l'intégration ;
- la loi n° 2016-274 du 7 mars 2016 relative au droit des étrangers en France ;
- le règlement du 4 février 2010 sur la procédure suivie devant le Conseil constitutionnel pour les questions prioritaires de constitutionnalité ;

Au vu des pièces suivantes :

- les observations présentées par le Premier ministre, enregistrées le 4 août 2021 ;
- les observations en intervention présentées pour l'association nationale d'assistance aux frontières pour les étrangers par la SCP Zribi et Texier, avocat au Conseil d'État et à la Cour de cassation, enregistrées le même jour ;
- les secondes observations présentées pour la société requérante par la SCP Rocheteau et Uzan-Sarano, enregistrées le 16 août 2021 ;
- les autres pièces produites et jointes au dossier ;

Après avoir entendu Me Cédric Uzan-Sarano, avocat au Conseil d'État et à la Cour de cassation, pour la société requérante, Me Isabelle Zribi, avocate au Conseil d'État et à la Cour de cassation, pour l'association intervenante, et M. Antoine Pavageau, désigné par le Premier ministre, à l'audience publique du 5 octobre 2021 ;
Au vu des pièces suivantes :

- la note en délibéré présentée pour la société requérante par la SCP Rocheteau et Uzan-Sarano, enregistrée le 8 octobre 2021 ;
- la note en délibéré présentée par le Premier ministre, enregistrée le 11 octobre 2021 ;
- la note en délibéré présentée pour l'association intervenante par la SCP Zribi et Texier, enregistrée le 13 octobre 2021 ;

Et après avoir entendu le rapporteur ;

LE CONSEIL CONSTITUTIONNEL S'EST FONDÉ SUR CE QUI SUIT :

1. La question prioritaire de constitutionnalité doit être considérée comme portant sur les dispositions applicables au litige à l'occasion duquel elle a été posée. Dès lors, le Conseil constitutionnel est saisi de l'article L. 213-4 du code de l'entrée et du séjour des étrangers et du droit d'asile dans sa rédaction résultant de l'ordonnance du 24 novembre

2004 mentionnée ci-dessus et du 1° de l'article L. 625-7 du même code dans sa rédaction résultant de la loi du 7 mars 2016 mentionnée ci-dessus.

2. L'article L. 213-4 du code de l'entrée et du séjour des étrangers et du droit d'asile, dans cette rédaction, prévoit :

« Lorsque l'entrée en France est refusée à un étranger non ressortissant d'un État membre de l'Union européenne, l'entreprise de transport aérien ou maritime qui l'a acheminé est tenue de ramener sans délai, à la requête des autorités chargées du contrôle des personnes à la frontière, cet étranger au point où il a commencé à utiliser le moyen de transport de cette entreprise, ou, en cas d'impossibilité, dans l'État qui a délivré le document de voyage avec lequel il a voyagé ou en tout autre lieu où il peut être admis ».

3. Le 1° de l'article L. 625-7 du même code, dans cette rédaction, prévoit qu'est punie d'une amende d'un montant maximal de 30 000 euros :

« L'entreprise de transport aérien ou maritime qui ne respecte pas les obligations fixées aux articles L. 213-4 à L. 213-6 ».

4. La société requérante reproche à ces dispositions d'obliger les entreprises de transport aérien à réacheminer les personnes étrangères auxquelles l'accès au territoire national a été refusé, le cas échéant en exerçant des contraintes sur celles dont le comportement présente un risque pour la sécurité à bord de l'aéronef. Ces dispositions auraient ainsi pour effet de déléguer à une personne privée des compétences de police administrative générale inhérentes à l'exercice de la force publique, en violation de l'article 12 de la Déclaration des droits de l'homme et du citoyen de 1789. La société requérante reproche également à ces dispositions d'obliger ces entreprises à détenir contre leur gré, au cours de ce réacheminement, les personnes qui refuseraient de se soumettre à cette mesure, en méconnaissance de l'article 66 de la Constitution. En outre, ces dispositions permettraient d'engager la responsabilité des entreprises de transport quand bien même l'inexécution de cette obligation ne serait imputable qu'au comportement du passager. Elles méconnaîtraient ainsi l'article 9 de la Déclaration de 1789.

5. La société requérante soutient, par ailleurs, que ces dispositions, en imposant aux entreprises de transport de prendre en charge l'ensemble des coûts liés à l'obligation de réacheminement, les soumettraient à des sujétions excessives. Ce faisant, elles méconnaitraient l'article 13 de la Déclaration de 1789.

6. Enfin, ces dispositions, en ne prévoyant aucune exception à cette obligation de réacheminement, seraient entachées d'incompétence négative.

7. Ces griefs sont ainsi dirigés contre l'obligation de réacheminement mise à la charge des transporteurs aériens. Par conséquent, la question prioritaire de constitutionnalité porte sur les mots *« est tenue de ramener »* figurant à l'article L. 213-4 du code de l'entrée et du séjour des étrangers et du droit d'asile.

8. L'association nationale d'assistance aux frontières pour les étrangers est fondée à intervenir dans la procédure de la présente question prioritaire de constitutionnalité dans la seule mesure où son intervention porte sur ces mêmes mots. Elle soutient, pour les mêmes raisons que la société requérante, que ces dispositions méconnaîtraient l'article 12 de la Déclaration de 1789.

– <u>Sur le contrôle exercé par le Conseil constitutionnel</u> :

9. Aux termes de l'article 88-1 de la Constitution : *« La République participe à l'Union européenne constituée d'États qui ont choisi librement d'exercer en commun certaines de leurs compétences en vertu du traité sur l'Union européenne et du traité sur le fonctionnement de l'Union européenne, tels qu'ils résultent du traité signé à Lisbonne le 13 décembre 2007 »*. La transposition d'une directive ou l'adaptation du droit interne à un règlement ne sauraient aller à l'encontre d'une règle ou d'un principe inhérent à l'identité constitutionnelle de la France, sauf à ce que le constituant y ait consenti. En l'absence de mise en cause d'une telle règle ou d'un tel principe, le Conseil constitutionnel n'est pas compétent pour contrôler la conformité à la Constitution de dispositions législatives qui se bornent à tirer les conséquences nécessaires de dispositions inconditionnelles et précises d'une directive ou des dispositions d'un règlement de l'Union européenne. Dans cette hypothèse, il n'appartient qu'au juge de l'Union européenne, saisi le cas échéant à titre préjudiciel, de contrôler le respect par cette directive ou ce règlement des droits fondamentaux garantis par

l'article 6 du traité sur l'Union européenne.

10. En application de l'article 26 de la convention d'application de l'accord de Schengen signée le 19 juin 1990, les États signataires se sont engagés à instaurer l'obligation pour les entreprises de transport de *« reprendre en charge sans délai »* les personnes étrangères dont l'entrée sur le territoire de ces États a été refusée et de les ramener vers un État tiers.
Cette obligation a été reprise et précisée par la directive du 28 juin 2001 mentionnée ci-dessus.

11. Les dispositions contestées de l'article L. 213-4 du code de l'entrée et du séjour des étrangers et du droit d'asile visent à assurer la transposition de cette directive en prévoyant que l'entreprise de transport aérien ou maritime est tenue de ramener une personne étrangère non ressortissante d'un État membre de l'Union européenne en cas de refus d'entrée sur le territoire national.

12. Ces dispositions se bornent ainsi à tirer les conséquences nécessaires de dispositions inconditionnelles et précises de la directive du 28 juin 2001.

13. **Par conséquent, le Conseil constitutionnel n'est compétent pour contrôler la conformité des dispositions contestées aux droits et libertés que la Constitution garantit que dans la mesure où elles mettent en cause une règle ou un principe qui, ne trouvant pas de protection équivalente dans le droit de l'Union européenne, est inhérent à l'identité constitutionnelle de la France.**

– Sur le fond :

14. **En premier lieu, le droit à la sûreté, le principe de responsabilité personnelle et l'égalité devant les charges publiques, qui sont protégés par le droit de l'Union européenne, ne constituent pas des règles ou principes inhérents à l'identité constitutionnelle de la France. Il n'appartient donc pas au Conseil constitutionnel de se prononcer sur ces griefs.**

15. En second lieu, selon l'article 12 de la Déclaration de 1789 : *« La garantie des droits de l'Homme et du Citoyen nécessite une force publique : cette force est donc instituée pour l'avantage de tous, et non pour l'utilité particulière de ceux auxquels elle est confiée »*. Il en résulte l'interdiction de déléguer à des personnes privées des compétences de police administrative générale inhérentes à l'exercice de la *« force publique »* nécessaire à la garantie des droits. Cette exigence constitue un principe inhérent à l'identité constitutionnelle de la France.

16. La décision de mettre en œuvre le réacheminement d'une personne non admise sur le territoire français relève de la compétence exclusive des autorités chargées du contrôle des personnes à la frontière. En application des dispositions contestées, les entreprises de transport aérien ne sont tenues, à la requête de ces autorités, que de prendre en charge ces personnes et d'assurer leur transport.

17. Ainsi, les dispositions contestées n'ont ni pour objet ni pour effet de mettre à la charge de ces entreprises une obligation de surveiller la personne devant être réacheminée ou d'exercer sur elle une contrainte, de telles mesures relevant des seules compétences des autorités de police. Elles ne privent pas non plus le commandant de bord de sa faculté de débarquer une personne présentant un danger pour la sécurité, la santé, la salubrité ou le bon ordre de l'aéronef, en application de l'article L. 6522-3 du code des transports.

18. Le grief tiré de la méconnaissance des exigences résultant de l'article 12 de la Déclaration de 1789 doit donc être écarté. Il en va de même du grief tiré de la méconnaissance par le législateur de l'étendue de sa compétence dans des conditions affectant ces mêmes exigences.

19. Par conséquent, les dispositions contestées doivent être déclarées conformes à la Constitution.

LE CONSEIL CONSTITUTIONNEL DÉCIDE :

Article 1er. – Les mots *« est tenue de ramener »* figurant à l'article L. 213-4 du code de l'entrée et du séjour des

étrangers et du droit d'asile, dans sa rédaction résultant de l'ordonnance n° 2004-1248 du 24 novembre 2004 relative à la partie législative du code de l'entrée et du séjour des étrangers et du droit d'asile, sont conformes à la Constitution.

Article 2. – Cette décision sera publiée au *Journal officiel* de la République française et notifiée dans les conditions prévues à l'article 23-11 de l'ordonnance du 7 novembre 1958 susvisée.

Jugé par le Conseil constitutionnel dans sa séance du 14 octobre 2021, où siégeaient : M. Laurent FABIUS, Président, Mme Claire BAZY MALAURIE, M. Alain JUPPÉ, Mmes Dominique LOTTIN, Corinne LUQUIENS, Nicole MAESTRACCI, MM. Jacques MÉZARD, François PILLET et Michel PINAULT.

Rendu public le 15 octobre 2021.

RFDA

RFDA 2021 p.421

Données personnelles : droit de l'Union européenne et Constitution

Conclusions sur Conseil d'État, assemblée, 21 avril 2021, *French Data Network et autres*, n° 393099 et autres (1), Lebon ; AJDA 2021. 828 ; *ibid.* 1194, chron. C. Malverti et C. Beaufils ; D. 2021. 797, et les obs. ; AJ pénal 2021. 309, chron. A. Archambault ; Légipresse 2021. 253 et les obs.

Alexandre Lallet, Maître des requêtes au Conseil d'Etat, rapporteur public

I. - *13 novembre 2015 :* les « attentats du Bataclan » font 130 morts et plus de 350 blessés. Une image de vidéo-surveillance montre l'un des terroristes du Stade de France passer un appel téléphonique peu avant d'actionner sa ceinture d'explosifs. Le recensement de l'ensemble des appels passés dans le même secteur, croisé avec le contenu d'un téléphone retrouvé dans une poubelle du XI^e^ arrondissement, révèle un contact commun en Belgique et permet son identification avant l'arrestation des vingt personnes directement impliquées, dans les semaines et mois suivants.

12 janvier 2018 : le corps du caporal Arthur Noyer est retrouvé près de Chambéry. Nordahl Lelandais, déjà mis en examen pour l'enlèvement de la petite Maëlys, avoue l'avoir tué, après que les enquêteurs ont découvert que son portable avait « borné » au même endroit que celui du militaire au moment de sa disparition, en avril 2017.

Derrière ces deux affaires médiatiques et l'émotion qu'elles peuvent susciter, qui est souvent mauvaise conseillère de justice, il y a surtout l'impressionnante réalité des chiffres. Les données de connexion, parfois appelées « métadonnées » pour les distinguer de celles qui portent sur le contenu des échanges, ce sont aujourd'hui plus de 2 millions de réquisitions judiciaires par an transitant par la plateforme nationale des interceptions judiciaires (2), auxquelles les opérateurs de téléphonie mobile et les fournisseurs d'accès à internet répondent le plus souvent en quelques minutes, pour les besoins de plus de quatre enquêtes judiciaires sur cinq et, parmi elles, de 100 % des investigations en matière de criminalité et délinquance en bande organisée. Ce sont aussi plus de 50 000 demandes des services de renseignement autorisées chaque année par le Premier ministre après avis de la Commission nationale de contrôle des techniques de renseignement (CNCTR) et donnant lieu à la réquisition de centaines de milliers de données *via* le Groupement interministériel de contrôle (GIC), à des fins de lutte contre le terrorisme, de contre-espionnage, de détection des narco-trafics ou de surveillance des groupuscules extrémistes violents. C'est la technique d'investigation n° 1, enseignée dans les écoles d'officiers de police et de gendarmerie presque comme on forme les auditeurs au Conseil d'État au maniement des bases de jurisprudence. Elle ne sert pas seulement à lutter contre la cybercriminalité, c'est-à-dire les infractions commises sur ou au moyen d'internet. Elle permet d'exploiter les traces numériques que laissent une part croissante des activités humaines, plus encore à l'heure de l'internet des objets, pour prévenir et réprimer des agissements commis exclusivement dans le monde physique.

On peut, schématiquement, distinguer trois catégories de données de connexion :

- *les données d'identité* permettent de savoir qui se cache derrière un numéro de téléphone, un numéro de carte

SIM (IMSI), un identifiant de téléphone (IMEI), un numéro d'abonné, une adresse *IP* ou encore une adresse mail ;

- *les données relatives au trafic* révèlent les contacts que vous avez eus par téléphone ou *SMS*, à quel moment et pour quelle durée - ce sont les factures détaillées, les fameuses « fadettes », mais aussi quels appareils et quelles cartes *SIM* ont été utilisés. S'agissant d'internet, ces données de trafic portent notamment sur l'adresse *IP*, la liste des sites internet consultés à partir de cette adresse ou encore l'historique de l'envoi et de la réception de mails - à l'exclusion du contenu, toujours ;

- enfin, *les données de localisation* permettent de connaître les zones d'émission et de réception d'une communication passée avec un téléphone mobile identifié, d'obtenir la liste des appels ayant transité par la même antenne relais - aussi appelée « cellule » ou « borne », d'où le terme usuel de « bornage » -, et même de localiser un portable en veille.

L'extraordinaire potentiel informatif de ces données, qu'elles concernent des « honnêtes gens » ou des criminels, des « quidam » ou des « *people* », en fait aussi, naturellement, l'exceptionnelle sensibilité. Les données de connexion ne sont ni plus ni moins que le reflet numérique de votre vie quotidienne, le portable en poche et l'ordinateur en bandoulière. De la couche numérique exsudent des aspects parfois anodins, parfois intimes de votre vie privée, de vos déplacements au supermarché du coin à votre fréquentation récurrente d'une église ou d'une mosquée, d'un club libertin ou d'un bar *gay*, de votre participation assidue à un forum de *geeks* ou d'alcooliques qu'on hésitera ici à qualifier d'anonymes, d'échanges parfaitement banals avec vos amis au colloque singulier avec votre médecin ou une personnalité politique, fût-elle cachée derrière un nom d'emprunt.

Ce sujet n'en était pas un lorsque le législateur a entrepris, il y a trente ans, d'encadrer les écoutes téléphoniques, c'est-à-dire l'accès au contenu des correspondances - à l'époque, il s'agissait du bon vieux téléphone fixe. Personne n'a songé, alors, à obliger France Télécom à conserver les données de connexion pour les besoins des enquêtes pénales.

Il n'a fallu que quelques années pour que tout change. La généralisation des téléphones mobiles et d'internet ont bouleversé les usages et les techniques d'investigation. Le droit s'y est adapté.

Une directive de 1997 (3) prévoyait l'obligation pour les opérateurs de communications électroniques, principalement les opérateurs de téléphonie mobile et les fournisseurs d'accès à internet, d'effacer ou d'anonymiser les données de connexion, tout en permettant aux États membres de prendre les mesures nécessaires aux fins d'assurer leur sécurité. Il semble que ce soit autant ce texte, et la condamnation de la France en raison du retard à le transposer (4), que les attentats du 11 septembre 2001, qui ont décidé le gouvernement à déposer quelques semaines plus tard un amendement en nouvelle lecture au projet de loi relatif à la sécurité quotidienne (5), afin d'introduire dans le code des postes et des communications électroniques - le CPCE - un article L. 32-3-1, devenu L. 34-1 (6), qui constitue toujours le socle de la conservation des données de connexion par les opérateurs.

Cet article pose, dans son II, le principe de l'effacement ou de l'anonymisation des données une fois la communication acheminée. Mais ce principe est immédiatement assorti d'exceptions :

- d'une part, le IV permet la conservation par les opérateurs des données techniques nécessaires à la *facturation et au paiement des prestations*, pendant un an (7) ou jusqu'à la fin des poursuites engagées le cas échéant. Ils peuvent aussi conserver certaines données en vue d'assurer la sécurité de leurs réseaux, pour une durée maximale de trois mois. La liste de ces données se trouve à l'article R. 10-14 du CPCE ;

- d'autre part, le III de cet article L. 34-1 prévoit qu'il « peut être différé » aux opérations d'effacement ou d'anonymisation des données de connexion pour une durée maximale d'un an *pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales*, sans distinction. Cette formulation ne doit pas tromper. Il ressort sans la moindre ambiguïté des travaux préparatoires de la loi de 2001 (8) que le législateur

n'a pas simplement souhaité ouvrir une faculté au pouvoir réglementaire ou aux opérateurs. Il a entendu créer une *authentique obligation de conservation,* assortie d'un délit en cas de non-conservation des données techniques dans les cas prévus « par la loi »(9). Du reste, tant le principe que les principales caractéristiques d'une telle obligation relèvent évidemment du domaine de la loi, au titre des obligations civiles et commerciales, du point de vue des opérateurs, et des garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques, du point de vue des utilisateurs. Le Conseil constitutionnel a eu l'occasion de s'assurer que le législateur n'était pas resté en deçà de sa compétence à cet égard(10). L'article R. 10-13 du même code, qui est l'une des dispositions en cause, énumère les catégories de données relevant de ce régime, fixe leur durée de conservation à un an à compter de leur enregistrement et définit les modalités de la compensation financière versée aux opérateurs.

Ce dispositif s'est ajouté à celui, issu d'une loi de 2000(11), et figurant désormais au II de l'article 6 de la loi n° 2004-575 du 21 juin 2004 *pour la confiance dans l'économie numérique* - la *LCEN* -, qui fait obligation aux *fournisseurs d'accès à internet* et aux *hébergeurs* de conserver les données nécessaires à l'identification des personnes créant, modifiant ou supprimant des contenus en ligne. Ce même texte ouvre un droit d'accès à l'autorité judiciaire, quelle que soit l'infraction recherchée ou poursuivie. Le décret n° 2011-219 du 25 février 2011, également en litige, détaille ces données dans son article 1er et fixe la durée de conservation à un an dans son article 3.

Au fil du temps, un nombre croissant d'autorités administratives ont été autorisées à s'abreuver dans ces vastes lacs de données, des services fiscaux(12) à l'Autorité de la concurrence(13), en passant par les douaniers(14), l'Autorité des marchés financiers (AMF)(15), la HADOPI (Haute autorité pour la diffusion des oeuvres et la protection des droits sur internet)(16), l'Agence nationale de la sécurité des systèmes d'informations (ANSSI)(17) ou l'Inspection du travail(18).

Les *services de renseignement* n'ont pas été en reste, à partir de 2006, pour les seuls besoins de la prévention du terrorisme(19), puis plus largement, à partir de la loi de programmation militaire de 2013 et de la loi dite « renseignement » de 2015(20), pour la défense et la promotion des différents intérêts fondamentaux de la nation dont ils ont la charge, du contre-espionnage à la lutte contre la criminalité organisée. Ces services peuvent, selon le cas, recourir à quatre techniques de renseignement mobilisant les opérateurs :

- *l'accès en temps différé aux données de connexion conservées par ces opérateurs,* qui permet de connaître le passé : il est organisé à l'article L. 851-1 du code de la sécurité intérieure (CSI) ;

- *l'accès en temps réel aux données de connexion conservées ou traitées* (21) *par les opérateurs*, prévue à l'article L. 851-2 du même code : il s'agit cette fois de suivre le présent. Cette technique est limitée à la prévention du terrorisme ;

- *la géolocalisation en temps réel*, qui est, en quelque sorte, un sous-ensemble de la technique précédente mais qui peut être utilisée pour l'ensemble des missions des services de renseignement. Elle est régie par l'article L. 851-4 ;

- enfin, la mise en oeuvre par les opérateurs de *traitements algorithmiques paramétrés par les services* permettant une analyse automatisée du flux des données de connexions susceptibles de révéler une menace terroriste : elle est encadrée par l'article L. 851-3. Elle est une porte ouverte sur le futur.

Ces techniques ne peuvent en principe être mises en oeuvre que sur autorisation du Premier ministre, après avis de la CNCTR, autorité administrative indépendante composée de magistrats, de parlementaires et d'une personnalité qualifiée. Si un avis défavorable n'est pas suivi, la Commission peut demander à la formation spécialisée du Conseil d'État d'ordonner l'interruption de la technique et la destruction des données collectées.

***

II. - Ce qui est en jeu aujourd'hui, devant vous, c'est l'économie générale du dispositif que nous venons de décrire à grands traits.

Les requêtes n^os^ 424717 et 424718, qui émanent d'un opérateur de téléphonie mobile et d'un fournisseur d'accès à internet bien connus, tendent à l'annulation du refus du Premier ministre d'abroger l'article R. 10-13 du CPCE. La requête n° 393099, introduite par des associations de défense des libertés sur internet, articule la même contestation et y ajoute le contentieux du refus d'abroger le décret du 25 février 2011. Ces actions portent donc sur *l'obligation de conservation généralisée des données*. Vous examinerez ces trois demandes à la lumière des circonstances de droit et de fait à la date de votre décision, conformément à votre jurisprudence *Association des Américains accidentels*.

Les trois autres requêtes vous demandent l'annulation pour excès de pouvoir de trois décrets d'application de la loi « renseignement » de 2015. Il vous faudra, cette fois, vous placer à la date de ces décrets pour en apprécier la légalité. Ces requêtes invoquent essentiellement la contrariété au droit de l'Union, des dispositions législatives organisant *la conservation et l'accès par les services de renseignement*. C'est ce qui a conduit vos 10^e^ et 9^e^ chambres réunies à renvoyer à la Cour de justice une question, ou plutôt un questionnaire préjudiciel, en 2018, sur lequel nous allons revenir dans un instant.

Avant cela, il nous faut circonscrire le débat et, en particulier, examiner l'opérance des moyens d'inconventionnalité dirigés contre les dispositions législatives en cause. Nous ne pensons pas, à cet égard, que la décision de renvoi de 2018 puisse être regardée comme ayant définitivement tranché la question. Il est vrai qu'une décision de renvoi empêche tout débat ultérieur sur la *recevabilité des conclusions*, dans la mesure où une question préjudicielle ne peut être posée que si elle est déterminante pour la solution du litige (22). Mais cette solution n'a pas vocation à être transposée à l'opérance des moyens dont le sort est réservé jusqu'à la décision définitive. Ce d'autant que l'arrêt préjudiciel peut tout à fait modifier les termes de ce débat. La solution inverse vous contraindrait, le cas échéant, à faire droit à un moyen radicalement inopérant, faute d'avoir relevé cette inopérance au stade du renvoi. Ce serait donner beaucoup de portée à une décision qui n'est qu'un avant dire droit dans cette mesure (23).

Le problème d'opérance, en l'espèce, vient de ce que, selon la jurisprudence bien établie de vos chambres réunies, la contrariété d'une disposition législative aux engagements européens et internationaux de la France ne peut utilement être invoquée à l'appui de conclusions dirigées contre un acte réglementaire *que si ce dernier a été pris pour son application ou qu'elle constitue sa base légale* (24). Nous vous proposons de consacrer dans cette formation solennelle cette *transposition du raisonnement d'opérance de l'exception d'illégalité* (25) *à l'exception d'inconventionnalité de la loi*. Nous ne voyons pas de raison d'adopter la logique plus généreuse de l'annulation par voie de conséquence car la loi inconventionnelle n'est ni annulée ni abrogée. Elle est simplement laissée inappliquée par le juge (26).

À cette aune, vous pourrez d'emblée rejeter la requête n° 394922. Le décret n° 2015-1185 du 28 septembre 2015 attaqué sous ce numéro a deux objets :

- il fixe d'abord la liste des *services spécialisés de renseignement*, dit du « premier cercle », comme la Direction générale de la sécurité intérieure (DGSI) et la Direction générale de la sécurité extérieure (DGSE), autorisés en principe à recourir à l'ensemble des techniques de renseignement pour l'ensemble des finalités énumérés à l'article L. 811-3 du CSI (27). Ce faisant, il se borne à mettre en oeuvre l'article L. 811-2 de ce code qui définit les missions générales de ces entités et renvoie à un décret en Conseil d'État le soin d'énumérer ces services. Cet article ne traite en rien des conditions de conservation et d'accès aux données de connexion. Faire rejaillir l'éventuelle inconventionnalité de ces conditions sur ces dispositions serait aussi incongru qu'annuler les décrets créant les centres hospitaliers régionaux au motif qu'un des actes thérapeutiques qu'ils sont autorisés à réaliser serait proscrit par le droit de l'Union. Cela ne soustrait évidemment en rien les services spécialisés à l'obligation

de respecter les règles applicables à chacune des techniques ;

- les autres dispositions de ce décret trouvent leur base légale dans les articles L. 853-1 à L. 853-3 du même code qui régissent *d'autres techniques de renseignement* que celles en cause.

Le décret n° 2015-1639 du 11 décembre 2015, attaqué sous le n° 397844, est quant à lui pris pour l'application de l'article L. 811-4 du même code, qui renvoie à un décret en Conseil d'État le soin de désigner les autres services de renseignement, dits du « second cercle », qui peuvent être autorisés à recourir aux techniques de renseignement, en distinguant, pour chaque service, celles qu'il peut utiliser et pour quelles finalités. La liste générale de ces services, qui figure à l'article R. 811-2 issu de l'article 2 du décret, est hors de cause pour la même raison que précédemment. Il en va de même des articles R. 851-3 et R. 851-4 résultant de l'article 3 du décret, ainsi que de ses articles 4 et 5, qui sont relatifs à des techniques de renseignement différentes. En revanche, les articles R. 851-1 et R. 851-2, issus de l'article 3 du décret, ainsi que les articles 6 à 9 en tant qu'ils rendent applicables ces dispositions outre-mer traitent de l'accès en temps différé et de la géolocalisation en temps réel. Il ne fait pas de doute que ces dispositions sont aussi prises pour l'application, respectivement, des articles L. 851-1 et L. 851-4 : par conséquent, la critique d'inconventionnalité qui les vise est assurément opérante en tant qu'elle porte sur les conditions d'accès aux données.

On peut, en revanche, hésiter à admettre l'opérance du débat d'inconventionnalité portant sur l'obligation de *conservation* des données pour les besoins des services de renseignement. On cherchera en vain dans le code de la sécurité intérieure une disposition législative contraignant explicitement les opérateurs à conserver les données de connexion pour les besoins de la mise en oeuvre des techniques de renseignement, et pour l'application de laquelle le décret serait pris. Seul l'accès est formellement organisé. Il en va de même des dispositions réglementaires en litige (28).

Nous vous invitons toutefois à dépasser les apparences et à prêter au législateur des intentions logiques, comme il se doit : il est évident qu'il n'a pas entendu subordonner la conservation en vue de l'accès administratif, à la licéité de la conservation à des fins judiciaires, et encore moins au bon vouloir des opérateurs. Si les législations sectorielles ne traitent pas de la question, c'est simplement par souci de ne pas doublonner l'article L. 34-1 du CPCE et l'article 6 de la *LCEN*, qui imposent déjà la constitution du même entrepôt de données pour les besoins des enquêtes pénales. C'est la raison pour laquelle, à chaque fois qu'elle a ouvert un nouvel accès administratif à ces données, la loi s'est bornée à le greffer sur ces dispositions, par commodité légistique. Mais nous sommes convaincu qu'il résulte de l'économie générale du code de la sécurité intérieure et des renvois qu'il opère, en particulier au CPCE, que les opérateurs sont tout autant tenus de conserver les données à des fins judiciaires qu'à des fins administratives et, en particulier, pour les besoins du renseignement. Par conséquent, nous pensons que les requérants peuvent utilement soutenir en l'espèce que l'obligation de conservation pour les besoins des services de renseignement est contraire au droit de l'Union (29).

S'agissant enfin du décret n° 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement, l'inconventionnalité éventuelle des obligations de conservation et des conditions d'accès est susceptible d'affecter le 3° de l'article R. 823-1 introduit dans le CSI par l'article 1er, qui porte sur le recueil et la conservation des données par le groupement interministériel de contrôle dans le cadre de l'accès en temps différé par les services, et l'article R. 851-5 en tant qu'il délimite le périmètre des données de connexion accessibles par référence aux articles R. 10-13 et R. 10-14 du CPCE et à l'article 1er du décret du 25 février 2011. Il en va de même, pour les conditions d'accès, de la définition des données communicables dans le cadre de l'accès en temps réel et de la mise en oeuvre des traitements algorithmiques (30), de même que des dispositions qui précisent les modalités opérationnelles de mise en oeuvre de l'ensemble de ces techniques de renseignement. En revanche, les autres mesures sont prises pour l'application d'autres dispositions législatives, qu'il s'agisse de la règle générale, applicable à l'ensemble des techniques de renseignement, selon laquelle seuls des agents individuellement désignés et habilités par le ministre ou le directeur dont ils relèvent peuvent mettre en oeuvre l'ensemble des techniques de renseignement (31), des compensations financières dues aux opérateurs (32), des modalités de saisine du Conseil d'État par la CNCTR (33) ou de la cryptologie (34).

Il faut enfin signaler que les requérants sont revenus à la charge après la réponse de la Cour de justice sur les *mesures de surveillance internationale* prévues par les articles L. 854-1 et suivants du CSI. Mais cette fois, vous devrez opposer l'autorité de la chose jugée par la décision de renvoi, qui a écarté ces moyens et rejeté les conclusions correspondantes (35).

En résumé, le litige dont vous êtes saisis porte : *1° sur l'obligation de conservation des données de connexion pour les besoins des enquêtes pénales et du renseignement, 2° sur l'accès des services de renseignement aux données, en temps différé et en temps réel, et 3° sur la technique de l'algorithme*. Ne sont pas directement en cause, en revanche, les modalités d'accès de l'autorité judiciaire - c'est-à-dire le droit des réquisitions judiciaires - qui résultent du code de procédure pénale (36), et qui ne sont en rien régies par les dispositions réglementaires litigieuses. De même, les droits d'accès particuliers dont bénéficient les diverses autorités administratives que nous avons mentionnées ne sont pas en litige. Évidemment, toutes sont directement intéressées, en pratique, par le sort que vous réserverez au vivier de données dans lequel elles peuvent aujourd'hui puiser.

***

III. - Parmi les nombreuses particularités que présente ce litige, l'une tient à ce que, entre l'introduction de la première requête en 2015 et l'audience de ce jour, le rapport de forces juridique entre les parties s'est tout simplement inversé.

À l'origine, l'État pouvait, assez sereinement, défendre l'idée que la conservation des données par les opérateurs pour les besoins des autorités administratives et judiciaires soulève peu de difficulté en soi, et que le recueil des données par les services de renseignement est entouré de garde-fous suffisamment solides, comme le Conseil constitutionnel l'a jugé.

Au niveau européen, les règles de la directive de 1997, qui n'a suscité que des contentieux de manquements (37), ont été très largement reprises par la directive dite « *e-privacy* » du 12 juillet 2002 (38). Celle-ci a connu une enfance assez calme et les forces de sécurité s'en sont peu préoccupées. On peut le comprendre : le paragraphe 3 de son article 1er exclut de son champ d'application l'ensemble des activités concernant la sécurité publique, la sûreté de l'État et les activités de l'État dans des domaines relevant du droit pénal. Par ailleurs, le paragraphe 1 de son article 15, éclairé par son considérant 11, permet aux États membres d'adopter ou de maintenir des mesures législatives dérogeant au principe de confidentialité et d'effacement immédiat des données après usage par les opérateurs pour sauvegarder la sécurité nationale, la défense et la sécurité publique, ou pour la prévention, la recherche, la détection et la poursuite d'infractions pénales, y compris en prévoyant une conservation des données pendant une durée limitée, sous réserve de respecter les exigences de nécessité, d'adéquation et de proportionnalité. Le dispositif français, par ailleurs largement répandu dans son principe au sein de l'Union européenne, semblait pouvoir prendre place confortablement dans ce cadre général.

La jurisprudence de la Cour européenne des droits de l'homme confortait cette analyse : elle juge certes que la seule conservation de données à caractère personnel constitue une ingérence dans le droit au respect de la vie privée, mais jusqu'à présent au moins, elle s'est surtout attachée, dans le cadre de son contrôle concret, à la manière dont elles sont ensuite utilisées par les autorités, aux résultats qui en sont tirés (39) et à l'encadrement du recueil et de la réutilisation. C'est la raison pour laquelle vos chambres réunies ont pris sur elles d'écarter les moyens d'inconventionnalité correspondants dans leur décision de renvoi.

La seule ombre au tableau gouvernemental résultait d'un arrêt *Digital Rights Ireland* du 8 avril 2014 (40). La grande chambre de la Cour de justice de l'Union européenne y a invalidé une directive de 2006 qui avait cru pouvoir imposer aux États membres d'obliger les opérateurs à conserver les données de connexion entre six mois et deux ans en vue de leur exploitation à des fins de recherche, de détection et de poursuites d'infractions graves. Mais aux yeux de nombreux commentateurs (41) et de vos 10e et 9e chambre réunies, dans leur décision inédite du 12 février 2016, *Association French Data Network et autres* (42), la Cour avait surtout

reproché au législateur européen l'extrême légèreté de l'encadrement de l'accès aux données ainsi conservées.

La suite de l'histoire a désavoué cette lecture. Elle a été écrite par cinq arrêts de la grande chambre de la Cour de justice qui nous emmènent aux quatre coins de l'Europe : *Télé2 Sverige AB* de 2016 ; *Ministerio fiscal* de 2018 (43) ; *La Quadrature du Net et autres* du 6 octobre 2020 (44), rendu dans le présent litige à la suite du renvoi préjudiciel de vos chambres réunies visant à faire réexaminer l'arrêt *Télé2*, et joint à un renvoi de la Cour constitutionnelle de Belgique ; *Privacy international* (45), du même jour, au Royaume-Uni ; et, enfin, *H.K. c/ Prokuratuur*, en Estonie, rendu le 2 mars dernier (46). Nous analyserons ces décisions en bloc, en dépit de l'intérêt que présenterait un exposé chronologique. Et nous nous concentrerons à ce stade sur les développements relatifs à *l'obligation de conservation et aux règles générales d'accès* - nous reviendrons à la fin de nos conclusions sur les points spécifiques à certaines techniques de renseignement mises en cause. Précisons simplement que l'histoire continue de s'écrire à Luxembourg puisque d'autres questions préjudicielles sont pendantes, l'une à l'initiative de la Cour administrative fédérale allemande, sur des questions analogues, et, l'autre, de la Cour de cassation, sur le sujet spécifique de l'accès aux données de connexion de l'AMF pour la recherche des manquements d'initiés.

***

IV. - La Cour apporte d'abord une réponse nette à la question, un temps controversée, de l'inclusion des opérations litigieuses dans le champ d'application de la directive *e-privacy*.

De façon logique, elle considère que son article 15, en ce qu'il encadre les mesures dérogatoires que les États membres peuvent prendre à des fins de sécurités nationale et publique, traduit nécessairement l'intention des auteurs du texte d'attraire dans son champ les dispositifs de conservation et d'accès pour ces motifs, sauf à le priver de toute portée utile. Plus largement, la directive s'applique dès l'instant qu'une obligation pèse sur les opérateurs au titre du traitement des données relatives aux communications qu'ils acheminent. Ces opérateurs sont avant tout des entreprises devant obéir à des règles unifiées au sein du marché intérieur des services de communications électroniques, dans le respect de la vie privée des citoyens européens ; ce n'est que de façon incidente qu'ils jouent le rôle de collaborateurs du service public de la sécurité (47). Ce sont bien eux les responsables des traitements. C'est évident pour ce qui concerne la conservation ; c'est aussi le cas pour ce qu'il est convenu d'appeler « l'accès », qui est en réalité un terme impropre au regard de la terminologie du droit des données à caractère personnel (48) : l'État ne dispose pas, en effet, d'un accès direct aux entrepôts de données des opérateurs, dans lesquels il pourrait piocher à sa guise ; ce sont ces derniers qui lui communiquent les données qu'il demande, au cas par cas.

La Cour s'interroge peu sur ce qui reste de l'effet utile de l'article 1er de la directive, en tant qu'il exclut purement et simplement ces activités régaliennes de son champ (49). On peut penser que cette exclusion couvrirait les activités d'opérateurs d'État dédiés à ces missions. Il est en tous les cas certain - nous y reviendrons brièvement dans la dernière partie de nos conclusions - que la directive ne régit pas les traitements subséquents par les autorités publiques qui ont recueilli les données.

La Cour précise en outre que cette directive de 2002 s'applique aux *fournisseurs d'accès à internet et aux opérateurs de téléphonie mobile*, mais non aux *hébergeurs*, c'est-à-dire aux prestataires qui assurent le stockage sur leurs serveurs des données nécessaires au fonctionnement des sites internet (50). Ces derniers relèvent en revanche du règlement général sur la protection des données (RGPD). Et elle considère, de façon très expédiente, que l'article 23 de ce règlement consacre, en substance, les mêmes règles que l'article 15 de la directive *e-privacy*, contrairement à ce que suggère une lecture du dispositif de l'arrêt du 6 octobre dernier déconnecté de son point 211, comme le soutiennent les requérants.

Ces règles, la Cour les tire avec une précision prodigieuse des quelques phrases pertinentes que renferment ces deux actes de droit dérivé, interprétées à la lumière des articles 7, 8 et 11 de la Charte des droits fondamentaux de l'Union européenne, qui protègent respectivement le droit au respect de la vie privée et familiale, le droit à la

protection des données à caractère personnel et la liberté d'expression(51). La philosophie qui l'anime dans cet exercice est fondamentalement différente de celle qui fonde la législation française comme la jurisprudence du Conseil constitutionnel, toute entière tournée vers l'encadrement de l'accès.

La Cour part de l'idée incontestable que les données de connexion d'une personne peuvent permettre de tirer des conclusions très précises concernant sa vie privée, y compris sur des aspects très sensibles, sans même qu'il soit besoin d'accéder au contenu des échanges ou des informations consultées. Et elle estime qu'une ingérence dans ses droits fondamentaux naît non seulement lorsque ces données sont effectivement recueillies et exploitées par l'État, mais aussi dès l'obligation faite aux opérateurs de les conserver. Cette ingérence est d'autant plus grave, sinon anormale, que la *conservation est généralisée et indifférenciée*, au sens où elle porte sur l'ensemble des utilisateurs des services et l'ensemble des communications sur le territoire national. C'est l'image évocatrice, utilisée par les requérants, du « registre national des déplacements des Français et de leurs correspondances » - encore qu'il serait plus juste de parler de registres au pluriel, ne serait-ce que parce que chaque opérateur en tient un. La Cour caractérise laconiquement l'ingérence liée à la conservation en se référant aux « risques d'abus et d'accès illicite »(52).

Vous observez à ce stade qu'elle ne s'embarrasse pas d'une analyse des garanties pourtant sérieuses dont cette conservation doit être entourée, notamment pour prévenir le vol, l'altération des données ou les accès non autorisés. L'article 4 de la directive *e-privacy* comme l'article 32 du RGPD font obligation aux opérateurs de mettre en place des mesures organisationnelles et techniques adaptées à la sensibilité des données. La fédération française des télécoms vous indique à cet égard que les mesures prises par ses adhérents correspondent aux standards les plus élevés. Pour reprendre l'exemple donné par la société Free lors de la séance orale d'instruction organisée par votre 10e chambre, la liste des identifiants des relais téléphoniques, d'une part, et leur emplacement géographique, d'autre part, sont stockés dans des bases distinctes qui ne sont rapprochées que lors et pour les besoins de la réquisition(53). Autrement dit, les « registres » dont il est question sont loin d'être en lecture directe. Les mesures de sécurisation peuvent être auditées par l'ANSSI, et leur insuffisance peut justifier le prononcé par la Commission nationale de l'informatique et des libertés (CNIL) d'une amende pouvant atteindre 2 % du chiffre d'affaires mondial du responsable de traitement, à laquelle s'ajoute, en France, la sanction pénale prévue à l'article 226-17 du code pénal, soit cinq ans d'emprisonnement et 300 000 € d'amende.

Pas plus que ses avocats généraux(54), la Cour n'estime utile d'illustrer son propos générique sur les risques d'accès illicite par des incidents constatés par le passé, notamment en France, depuis vingt ans. Alors que la cybercriminalité prospère, l'éventualité ne peut évidemment être écartée. On songe par exemple à l'utilisation de données de trafic et de localisation volées à des fins de chantage et d'usurpation d'identité. Mais la fédération française des télécoms vous a indiqué ne pas en avoir eu connaissance et la CNIL ne s'est jamais fait l'écho de la notification par un opérateur d'une violation de la sécurité de ces données. Peut-être aiguisent-elles moins les appétits que les numéros de carte bancaire.

Peu importe enfin à la Cour, pour apprécier la gravité de l'ingérence que constitue la conservation et alors même qu'elle identifie à ce titre le risque d'accès abusif ou illicite, les restrictions et garanties entourant cet accès, en aval, qu'il s'agisse de la durée de stockage des données par les autorités les ayant requises, de la nature de ces données, des garde-fous procéduraux et techniques, notamment la traçabilité des accès et les contrôles *a posteriori*, et des sanctions en cas d'accès frauduleux, déloyal ou illicite - en France, le tarif maximal est là encore de cinq ans d'emprisonnement et 300 000 € d'amende(55).

Son raisonnement repose au fond sur une double logique qu'elle n'a pas besoin d'expliciter pour être comprise, qui fonde la démarche des requérants et qu'il faut savoir entendre à défaut d'y adhérer :

- *une logique de précaution, d'abord* : elle consiste à ne pas s'en remettre à la responsabilité des acteurs et à la sanction lorsque le manquement est commis et que le dommage survient, *mais à réduire en amont les risques à un minimum considéré comme socialement acceptable*, « quoi qu'il en coûte », en quelque sorte(56) ;

- *et, de façon plus spécifique, une logique de méfiance à l'égard des autorités publiques*, qu'il faut se garder de soumettre à la tentation, à défaut de les délivrer d'un mal qui sommeille en chacune d'elles : c'est le spectre de la surveillance de masse et de l'intrusion permanente dans la « vie des autres », dont l'histoire a livré des manifestations durablement traumatisantes dans une partie au moins de l'Europe, et que la bonne science-fiction s'est employée à transposer dans un avenir qui pourrait être le nôtre. Pour certains, il est déjà notre présent. Il est bien entendu permis de penser, alternativement, que les forces de sécurité de ce pays consacrent les moyens qu'on leur donne à protéger les Français plutôt qu'à les espionner.

La Cour n'ignore pas pour autant, naturellement, que des *limitations* peuvent être apportées à l'exercice des droits fondamentaux en vertu de l'article 52 de la Charte, pourvu qu'elles soient prévues par la loi, qu'elles respectent le contenu essentiel de ces droits, qu'elles soient nécessaires et adéquates au regard des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et des libertés d'autrui, et qu'elles respectent le principe de proportionnalité.

À cet égard, elle écarte sans surprise l'idée que le *droit à la sûreté* garanti par l'article 6 de la Charte puisse, comme l'avait suggéré votre décision de renvoi, justifier une ingérence dans les droits en cause : loin d'être le droit à être protégé *par* l'État, il est celui d'être protégé *contre* l'État et, plus précisément, contre toute privation de liberté arbitraire ou injustifiée. C'est aussi le sens que lui confère la Déclaration de 1789, dans la même logique que l'*habeas corpus*. En revanche, la Cour admet l'importance des *objectifs de protection de la sécurité nationale et de lutte contre la criminalité grave*, qui contribuent à la protection des droits et libertés d'autrui (57). Elle précise toutefois que les mesures de restriction prises sur le fondement de l'article 15 de la directive *e-privacy* étant dérogatoires aux principes de confidentialité et d'effacement ou d'anonymisation rapides des données posés par le même texte, elles doivent s'interpréter strictement et ne sauraient devenir la règle (58).

Ce cadre de raisonnement général la conduit à rédiger un chapitre alternatif des codes de procédure pénale et de sécurité intérieure des États membres. Il se conçoit comme un *tableau de concordance entre, d'une part, le niveau de gravité de l'ingérence que constitue l'obligation de conservation*, selon le triptyque « non grave », « grave », « particulièrement grave », et, d'autre part, *la gravité de la menace qui justifie cette ingérence*, selon le triptyque « lutte contre la criminalité et prévention des menaces contre la sécurité publique en général », « lutte contre la criminalité grave et prévention des menaces *graves* pour la sécurité publique » et enfin, « sauvegarde de la sécurité nationale ».

La Cour applique ce mode d'emploi à trois catégories de données distinctes.

Les données relatives à *l'identité civile des utilisateurs*, c'est-à-dire le nom, le prénom et l'adresse (59), ne présentent qu'une très faible sensibilité. L'obligation de conservation généralisée et indifférenciée constitue à ses yeux une ingérence non grave. Elle peut donc être ordonnée, sans limitation de durée, pour les trois objectifs.

Il en va différemment de *l'adresse IP* - c'est-à-dire du numéro unique attribué de façon permanente ou provisoire par le serveur du réseau à l'appareil qui accède à internet. Elle permet de suivre le parcours de navigation de l'utilisateur de l'équipement, non pas, comme la Cour semble le suggérer avec prudence au point 83 de son arrêt du 6 octobre, au niveau de granularité de la page de site internet consultée ou d'un contenu précis, comme une vidéo, mais au niveau du nom de domaine - c'est-à-dire qu'on peut seulement savoir quels sites internet ont été consultés. En soi, cette donnée peut naturellement fournir, dans certains cas, en particulier pour les sites thématiques, des informations sensibles ou précieuses, selon le point de vue (60). L'ingérence dans les droits fondamentaux est ici qualifiée de « grave ». La Cour tient compte toutefois de ce que l'adresse *IP* peut être le seul moyen d'investigation pour identifier l'auteur d'une infraction en ligne. Elle cite en particulier le cas de la pédopornographie. Elle en conclut que la conservation généralisée et indifférenciée des adresses *IP* attribuées à la source d'une connexion n'est pas interdite en soi ; mais elle doit être réservée aux deux motifs les plus sérieux : lutte contre la criminalité grave et sauvegarde de la sécurité nationale. Elle doit par ailleurs être limitée à une durée strictement nécessaire.

Pour *toutes les autres données de connexion*, en particulier celles qui portent sur les communications téléphoniques - les fadettes - et les données de localisation, *le principe est celui de l'interdiction de la conservation obligatoire à des fins de sécurité*. Mais la Cour le module en fonction du motif poursuivi.

Ce principe ne souffre aucune exception lorsqu'il s'agit de *lutter contre les infractions pénales ordinaires*. Pour ce motif, seules les données d'identification peuvent donc donner lieu à une obligation de conservation.

Pour la *lutte contre la criminalité grave et la prévention des menaces graves pour la sécurité publique*, la conservation généralisée et indifférenciée de ces autres données de connexion est regardée comme excédant les limites du strict nécessaire et non justifiée dans une société démocratique. En dépit de l'insistance de votre décision de renvoi, qui pointait l'impossibilité d'identifier *a priori* les personnes susceptibles de commettre une infraction, donc la nécessité d'une conservation indifférenciée, la cour n'admet pas la constitution à cette fin d'un lac de données de précaution, incluant les données de personnes dont rien ne laisse suspecter qu'elles auraient commis ou pourraient commettre une infraction grave. Elle envisage seulement, par exception, l'aménagement de bassins de rétention selon deux modalités alternatives :

- la première, qu'on trouvait déjà dans l'arrêt *Télé2*, est la *conservation ciblée*, selon deux critères :

> un *critère personnel*, d'abord : il consiste à circonscrire l'obligation de conservation à certaines personnes ou catégories de personnes dont les données présentent un lien, au moins indirect, avec des actes de criminalité grave ou pourraient contribuer d'une manière ou d'une autre à la lutte contre celle-ci ou à la prévention d'un risque grave de sécurité publique ;

> un *critère géographique*, ensuite : il permet de cibler la conservation sur certaines zones caractérisées par un risque élevé de préparation d'actes de criminalité grave ou particulièrement exposées à la commission de tels actes, comme des lieux très fréquentés ou stratégiques. La Cour donne l'exemple des aéroports, des gares et des barrières de péage.

Dans tous les cas, elle exige que le ciblage repose sur des éléments objectifs et non discriminatoires et que la conservation soit limitée à la durée strictement nécessaire, mais renouvelable en cas de persistance de la menace. Il s'agit donc de bassins de rétention à évaporation rapide.

- la seconde soupape, qui est une innovation de l'arrêt du 6 octobre dernier, est la *conservation dite « rapide »*. La Cour a puisé cette notion dans l'article 16 de la Convention de Budapest sur la cybercriminalité du 23 novembre 2001 (61), ratifiée ou approuvée par la quasi-totalité des États membres, dont la France (62). Elle ne désigne pas, contrairement à ce que sa terminologie pourrait laisser penser, une conservation brève, mais un *gel immédiat de données* - d'où son appellation courante : « *quick freeze* » (63).

Là encore, la Cour pose ses conditions à la création et à l'usage de ce pouvoir :

> d'une part, la législation doit préciser la ou les *finalités* pour la - ou lesquelles - une conservation rapide peut être ordonnée. Cette finalité ne peut être, on l'a dit, la lutte contre des agissements « non graves ». Vous noterez au passage que la Convention de Budapest ne fixe quant à elle aucun seuil de gravité pour l'accès aux données de connexion, à la différence de l'interception du contenu des échanges (64) ;

> d'autre part, une mesure de conservation rapide ne peut porter que sur les données de trafic et de localisation *susceptibles de contribuer à la prévention ou à la répression d'une infraction déterminée*. Toutefois, elle peut ne pas être limitée aux données des personnes soupçonnées de vouloir commettre ou d'avoir commis une infraction pénale. La Cour admet ainsi qu'elle englobe les données d'autres personnes, pourvu qu'elles puissent, sur la base d'éléments objectifs et non discriminatoires, contribuer à l'élucidation de l'infraction ou la prévention de la menace. Il peut s'agir de données de victimes, de l'entourage social ou professionnel des protagonistes, ou

encore de zones géographiques déterminées, notamment les lieux de la commission et de la préparation de l'infraction.

À la différence de l'arrêt *Télé2*, la décision du 6 octobre dernier identifie un dernier étage de la fusée sécuritaire, qui montre que le dialogue des juges est loin d'être un dialogue de sourds : c'est la *sauvegarde de la sécurité nationale*. Aiguillonnée par vos chambres réunies, la Cour y voit une finalité d'une nature différente, notamment parce que l'article 4 du Traité sur l'Union européenne (TUE) en confie la responsabilité aux seuls États membres. Elle en donne une définition sur laquelle nous reviendrons, pour les besoins de l'interprétation de l'article 15 de la directive qui y fait expressément référence. La gravité de cette menace est telle qu'on peut, cette fois, admettre, exceptionnellement, l'absence de lien entre le vivier des personnes dont les données sont conservées et celui des personnes constituant ou susceptibles de constituer une telle menace. La Cour juge en conséquence que la directive de 2002 et le RGPD permettent aux États membres d'adresser aux opérateurs une injonction de procéder à la conservation généralisée et indifférenciée de l'ensemble des données de connexion à cette fin (65). Mais elle assortit cette faculté de trois conditions :

- d'une part, il doit exister une menace grave pour la sécurité nationale, qui peut être réelle ou actuelle, ou simplement prévisible ;

- d'autre part, la durée de cette injonction doit être limitée au strict nécessaire. Si son renouvellement « ne peut être exclu » en cas de persistance de la menace grave, elle ne saurait présenter un « caractère systématique » (66) ;

- enfin, une telle injonction doit être soumise au contrôle d'un juge ou d'une autorité administrative indépendante dotée d'un pouvoir contraignant, qui vérifiera l'existence et la gravité de la menace, ainsi que le respect de conditions et garanties contre les abus.

La Cour complète ce mode d'emploi de la conservation par un *encadrement draconien de l'accès*. Elle pose essentiellement cinq règles que nous énumérons rapidement :

- *premièrement, une règle de régularité de la conservation* : l'accès ne peut être octroyé que pour autant que les données ont été conservées conformément aux exigences de la directive ou du RGPD (67) ;

- *deuxièmement, une règle de concordance des finalités* : l'accès n'est possible que pour la finalité ayant justifié la conservation, ou une finalité « plus grave », selon la logique « qui peut le plus peut le moins » (68). Vous observerez que cette règle, en apparence logique, n'a absolument rien d'évident. En effet, les inconvénients et risques résultant de la conservation d'une même donnée, c'est-à-dire de son existence même dans une base, sont indépendantes des finalités pour lesquelles elle est ensuite recueillie : ils sont subis de toute façon. L'accès est un traitement distinct : la gravité de l'ingérence qui en résulte ne dépend pas du motif pour lequel la donnée a été conservée à l'origine, mais de la sensibilité propre de cette donnée. Il nous semble que l'arrêt souffre sur ce point d'un problème de cohérence. Il pourrait être surmonté en fondant cette règle de concordance sur la volonté de proscrire tout *effet d'aubaine* dans l'accès. Mais cette logique devrait aussi conduire à interdire à l'État d'accéder aux données spontanément conservées par les opérateurs pour leurs propres besoins, ce que la Cour admet pourtant ;

- *la troisième règle* est que l'accès aux données de trafic et de localisation, permettant de tirer des conclusions précises sur la vie privée, constitue par principe une *ingérence grave*, quelle que soit la nature exacte des données recueillies, leur quantité et la profondeur temporelle du recueil. Il est donc par principe interdit d'accéder à ces données relatives au trafic et aux données de localisation pour la recherche et la poursuite d'infractions pénales « non graves » (69) ;

- *quatrièmement, une règle de contrôle préalable* : l'accès doit être soumis au *contrôle préalable* d'une juridiction ou d'une autorité administrative indépendante dotée d'un pouvoir contraignant (70). Cette autorité de

contrôle doit impérativement être un tiers par rapport à l'autorité qui recueille. Tel n'est pas le cas, selon l'arrêt *H.K.,* du procureur de la République estonien à l'égard des officiers de police judiciaire, dans un dispositif qui ressemble furieusement à son homologue français. En cas d'urgence dûment justifiée, le contrôle peut cependant intervenir *a posteriori*, mais à bref délai (71) ;

- *cinquièmement, une règle d'information* : les autorités ayant eu accès aux données doivent en informer les personnes concernées, pour autant que et dès le moment où cette communication n'est plus susceptible de compromettre les missions qui leur incombent, afin de les mettre à même d'exercer leur droit au recours (72).

***

V. - Il n'est pas nécessaire à ce stade d'entrer dans le jeu des sept différences pour comprendre que le droit national que nous avons décrit ne se coule pas avec aisance dans ce moule européen.

« Conséquences désastreuses » et « absolument dramatiques », pour reprendre des mots écrits ou prononcés dans la présente procédure ; « *hold-up* jurisprudentiel », selon le récent rapport d'information parlementaire d'évaluation de la loi « renseignement », commentant l'arrêt *Téléd2* (73). Il est peu dire que la Cour a suscité la sidération et la consternation parmi les autorités et professionnels concernés, en France comme à l'étranger. Peut-être serait-il plus juste, d'ailleurs, de parler d'un effet d'hallucination, à laquelle les intéressés n'ont pas voulu croire : car, paradoxalement, aucune conséquence concrète n'en a été tirée en France depuis 2016, ni par le législateur, qui a continué à étendre les droits d'accès comme si de rien n'était, ni par l'autorité judiciaire, ni par la CNCTR.

C'est qu'aux yeux du gouvernement, cette jurisprudence compromet purement et simplement l'exercice de leurs missions tant par les services de renseignement que par les services d'enquête judiciaire. Pour la première fois depuis la signature du traité de Rome, à notre connaissance, il vous demande en conséquence de ne pas appliquer un arrêt de la Cour de justice de l'Union européenne.

1° À titre principal, il vous invite à une percée conceptuelle par laquelle vous vous reconnaîtriez la possibilité d'écarter le droit de l'Union tel qu'interprété par la Cour de justice lorsqu'il *excède manifestement la compétence dévolue par les traités à l'Union*.

Ce contrôle, connu sous le vocable latin d'*ultra vires*, ne serait pas une innovation française, loin de là. Il existe de longue date dans la jurisprudence de la Cour constitutionnelle fédérale allemande et dans celle de la Cour suprême danoise (74). La première à l'avoir effectivement utilisé est la Cour constitutionnelle tchèque dans son arrêt *Holubec* de 2012 (75). Elle a été suivie dans ses travaux pratiques par les Danois en 2016 (76) et par le *Bundesverfassungsgericht* dans son retentissant arrêt du 5 mai 2020. Ce dernier écarte au titre de l'*ultra vires* la décision de la Banque centrale européenne (BCE) portant sur le programme *PSPP* (*Public sector asset purchase programme*) d'achat de titres du secteur public sur les marchés secondaires, et l'arrêt de la Cour de justice qui avait cru pouvoir constater la validité de cette décision sur renvoi préjudiciel. Pour la Cour de Karlsruhe, tant la BCE que la Cour ont manifestement méconnu le sens et la portée du principe de proportionnalité consacré par le TUE, en analysant ce programme comme un pur acte de politique monétaire et en s'abstenant de tenir compte de ses effets sur la politique budgétaire relevant de la compétence des États membres.

Dans la conception allemande, qui est la plus aboutie au plan théorique, l'*ultra vires* procède d'une violation caractérisée du principe de la compétence d'attribution par l'Union, par un acte qui entraîne un glissement structurellement significatif dans le système de répartition des compétences entre elle et les États membres, au détriment de ces derniers. L'existence de ce contrôle est explicitement justifiée par la préoccupation de ne pas transférer aux institutions de l'Union le pouvoir de réviser les traités ou d'étendre ses compétences, ce que seuls les États membres, qualifiés de « maîtres des traités », peuvent faire. Cette éventualité, qu'elle qualifie de « fort rare » compte tenu des garanties dont l'action de l'Union est entourée, doit être prévenue autant que possible « de manière coopérative et avec considération mutuelle ». L'*ultra vires* est donc une arme de dernier recours qui

ne peut être dégainée qu'après renvoi préjudiciel, c'est-à-dire, en quelque sorte, après avoir donné à la Cour de justice une chance de respecter et de faire respecter le principe de la compétence d'attribution dévolue à l'Union (77). La Cour de Karlsruhe dit s'astreindre en principe à suivre l'interprétation que la Cour de justice donne du droit de l'Union en lui reconnaissant, « dans une certaine mesure, un droit à l'erreur », mais elle n'admet pas que les traités soient « interprétés d'une manière qui n'est tout simplement plus compréhensible et qui est donc objectivement arbitraire » (78).

Ce vocabulaire, comme l'état d'esprit qu'il traduit, ne sont clairement pas les vôtres. Le dialogue des juges peut sans doute être « rugueux et sans complaisance », pour emprunter les mots de Jean-Marc Sauvé (79), mais jamais, dans vos décisions, y compris celles qui ont fait suite aux quelques 150 questions préjudicielles que vous avez posées à la Cour depuis une vingtaine d'années, y compris lorsque ses réponses pouvaient susciter une certaine perplexité, y compris, bien entendu, après que la Cour de justice vous a reproché d'avoir placé la France en manquement dans le dossier du précompte mobilier (80), jamais vous ne vous êtes autorisé à porter un jugement de valeur ou même un regard critique sur les raisonnements tenus par la Cour de justice - c'est là, tout au plus, le monopole mesquin de vos rapporteurs publics. Jamais vous ne lui avez contesté le rôle que lui reconnaît l'article 19 du Traité sur l'Union européenne d'assurer « le respect du droit dans l'interprétation et l'application des traités ». Jamais vous ne vous êtes érigés en organe de contrôle de son activité, pour lui reprocher d'avoir mal fait son travail. Nous ne vous inviterons pas à emprunter cette voie (81), ce que le Conseil constitutionnel n'a, pour sa part, jamais fait (82).

Notre réticence ne tient pas à nos qualités de gentleman du droit, vous l'aurez compris.

Ce n'est pas davantage votre positionnement institutionnel qui nous dissuade de mettre en oeuvre un tel contrôle, d'autant que vous êtes aussi, dans votre champ de compétence, une cour constitutionnelle.

Ce n'est pas non plus la base légale qui manque, à notre avis. L'article 88-1 de la Constitution (83) définit la participation de la République à l'Union européenne comme un choix libre d'exercer certaines de ses compétences avec les autres États membres dans le cadre défini par le Traité de Lisbonne, c'est-à-dire *dans la limite des compétences dévolues à l'Union*. La délimitation des compétences de l'Union est régie par le principe d'attribution posé à l'article 5 du TUE. En vertu de l'article 13 de ce traité, toute institution de l'Union doit agir « dans les limites des attributions qui lui sont conférées dans les traités, conformément aux procédures, conditions et fins prévues par ceux-ci ». Il serait tout à fait possible de construire un contrôle *ultra vires* sur ces bases. Si une institution de l'Union autre que la Cour de justice méconnaît cette règle, c'est en principe à cette dernière d'y remédier. Mais personne ne peut garantir que la Cour, dont les décisions sont insusceptibles de recours, assurera correctement le respect du principe d'attribution. Et on sait que pour tracer sereinement une frontière, il est toujours préférable d'être deux, de part et d'autre.

Enfin, nous ne pensons pas non plus que vous soyez, par principe, prisonnier d'une *force obligatoire* irrépressible des arrêts de la Cour s'attachant au dispositif de ses arrêts et aux motifs qui en constituent le soutien nécessaire (84). Il entre en effet dans votre office de délimiter la *portée que revêt, pour vous comme pour l'administration, l'autorité de la chose jugée par d'autres juridictions*.

C'est ce que vous faites tant pour les juridictions pénales et civiles, de manière différenciée (85), que pour le Conseil constitutionnel, en interprétant l'article 62 de la Constitution (86), ou encore pour les arrêts de la Cour européenne des droits de l'homme, dont vous avez défini la portée en droit administratif dans cette formation solennelle (87). Rien ne justifie de raisonner différemment pour la Cour de justice, qui n'est pas votre Cour suprême.

C'est vous qui avez accepté l'autorité absolue des arrêts annulant ou constatant l'invalidité des actes de droit dérivé, y compris à la demande d'une autre juridiction, nationale ou étrangère, dans la logique de la jurisprudence *Foto-Frost* (88). C'est encore vous qui, abandonnant votre jurisprudence *ONIC* (89), avez admis que l'interprétation du traité et des actes de droit dérivé par la Cour de justice s'impose à vous, alors

même qu'elle ne fait pas l'objet du renvoi préjudiciel (90). Et c'est vous qui, dans la même décision, en avez fixé des limites, en prenant soin de relever dans une incise que « la Cour était compétente pour donner [cette interprétation] en vertu du a) et du b) de l'article 234 du Traité CE » : il ne faut pas y voir la trace d'un contrôle *ultra vires*, au sens allemand du terme, mais une délimitation de la portée de l'autorité de la chose jugée par la Cour à l'aune de la compétence d'attribution qui lui est reconnue par les traités. Vous en avez fait application dans ce précédent en rappelant qu'il appartient au juge national, saisi du principal, de qualifier les faits à la lumière de l'arrêt de la Cour, dans la logique de sa propre jurisprudence (91). Alors que celle-ci avait cru pouvoir trancher le litige de fond à votre place, vous avez souverainement effectué ce travail, comme l'explique la chronique cosignée par Claire Landais et prémonitoirement intitulée : « Ni capitulation, ni rébellion : dialogue » (92).

En l'occurrence, cette soupape de compétence ainsi comprise n'est d'aucune utilité : la Cour de justice s'est bien livrée à une interprétation du droit de l'Union à votre demande, comme elle peut et doit le faire. Cela étant, l'élargissement de ce raisonnement au cas où la Cour a conféré à un acte de droit dérivé une portée excédant le champ du droit de l'Union serait tout à fait envisageable conceptuellement.

Ce sont deux autres raisons qui nous conduisent à ne pas vous proposer de le faire aujourd'hui (93).

La première, sans doute surmontable, tient à la *difficulté de fixer précisément les limites* d'un contrôle *ultra vires* à l'allemande. La logique de l'arrêt *PSPP*, qui consiste à reprocher à la Cour de justice d'avoir incorrectement manié le principe de proportionnalité, ouvre la voie à une remise en cause systématique de ses arrêts pour les motifs les plus variés (94).

L'argumentation du gouvernement est révélatrice de cette difficulté. Il nous paraîtrait périlleux de reprocher à la Cour d'avoir fait du hors-piste ici. Il y a bien longtemps que, sans que personne ne s'en émeuve plus, l'interprétation qu'elle donne des actes de droit dérivé est susceptible d'avoir des incidences sur la sécurité nationale, la sécurité publique ou la santé publique. Elle juge constamment que le seul fait qu'une mesure nationale a été prise à ces fins n'entraîne pas l'inapplicabilité du droit de l'Union et ne dispense pas les États membres du respect nécessaire de ce droit, notamment des libertés de circulation et d'établissement (95). C'est d'ailleurs précisément la raison pour laquelle l'article 4 du TUE oblige l'Union, y compris la Cour de justice, à respecter « les fonctions essentielles de l'État, notamment celles qui ont pour objet d'assurer son intégrité territoriale, de maintenir l'ordre public et de sauvegarder la sécurité nationale » : cette stipulation, qui s'adresse aux institutions de l'Union dans l'exercice de leurs compétences, présuppose nécessairement que leur action puisse avoir un impact sur ces enjeux. Du reste, ces questions régaliennes ne sont pas soustraites de manière générale à la compétence du législateur européen : à titre d'exemple, l'article 83 du Traité sur le fonctionnement de l'Union européenne (TFUE) lui permet d'adopter des directives fixant des règles minimales en matière de criminalité transfrontière particulièrement grave, y compris le terrorisme.

La *seconde raison* est plus décisive à nos yeux : *nous ne pensons pas que vous ayez besoin d'une telle innovation*. Votre boîte à outils contient déjà, et d'assez longue date, un instrument adapté à la situation, conçu initialement pour un autre usage et dont vous ne faites pas une utilisation immodérée, mais dont l'assise juridique et la logique nous paraissent incontestables. Il consiste, non pas à critiquer la solution de la Cour au regard des règles s'imposant à elle, mais simplement, au stade de sa réception en droit interne, à refuser de la transcrire servilement parce qu'elle se heurte à un obstacle constitutionnel de fond. C'est ce que nous appellerons la « clause de sauvegarde *Arcelor* ». Le gouvernement vous demande, à titre subsidiaire, d'en faire application. Il nous faut vous en rappeler l'origine et la logique, ce qui demande, hélas, un peu de concentration.

2° L'article 88-1 de la Constitution consacre, vous le savez, l'existence d'un ordre juridique intégré de l'Union européenne, distinct de l'ordre juridique international, pour reprendre les termes du Conseil constitutionnel que vous avez déjà fait vôtre (96). Il a explicitement tiré de cet article la reconnaissance du *principe de primauté du droit de l'Union* et l'obligation corollaire pour le législateur de *transposer en droit interne les directives de l'Union comme de respecter les règlements lorsqu'une loi a pour objet d'y adapter le droit interne* (97). Sans vous

référer expressément à la primauté du droit de l'Union, vous avez fait de même, à la suite de la décision *SCEA du Chéneau* du Tribunal des conflits (98), en jugeant que le *respect du droit de l'Union européenne* constitue une obligation découlant de l'article 88-1, dont il résulte un principe d'effectivité qui implique que le juge national chargé d'appliquer les dispositions du droit de l'Union a l'obligation d'en assurer le plein effet en laissant au besoin inappliquée, de sa propre autorité (99), toute disposition contraire (100), et même tout engagement international contraire, à tout le moins à un règlement européen (101).

Cette exigence constitutionnelle n'est toutefois pas supérieure aux autres. Sans doute le principe de primauté du droit de l'Union a-t-il été constamment réaffirmé par la Cour de justice (102), avec de rares tempéraments (103), avec pour conséquence l'injonction expressément faite au juge national de laisser inappliquée une disposition *constitutionnelle* contraire au droit de l'Union (104). Mais ce qui vaut dans l'ordre européen, du point de vue de la Cour de justice, pour les besoins de la construction du marché intérieur et de la convergence des règles du jeu à l'échelle européenne dont elle a la charge (105), n'est plus vrai dans l'ordre interne, où, comme l'ont rappelé vos décisions *Sarran et Levacher* et *SNIP* (106), *la norme suprême est la Constitution*. Le Conseil constitutionnel a même jugé que cet article 88-1 confirmait lui-même la place de la Constitution au sommet de l'ordre juridique interne (107).

Il en résulte que le droit de l'Union n'est pas soustrait au respect de la Constitution. S'agissant du droit primaire, c'est le Conseil constitutionnel qui s'en assure, lorsqu'il est saisi sur le fondement de l'article 54. S'agissant des actes de droit dérivé de l'Union, la difficulté tient au rôle particulier dévolu par les traités à la Cour de justice de l'Union dans le contrôle de leur validité, et au risque de contrariétés de jurisprudence. Le contrôle de constitutionnalité a donc été adapté dans ses modalités, afin d'assurer le plus harmonieusement possible l'intégration de l'ordre juridique européen à l'ordre interne. Ce contrôle fait l'objet d'une *délégation européenne, assortie d'une clause de sauvegarde*.

Pour la bonne compréhension de ce qui suit, il faut rappeler que le contrôle de légalité suppose de confronter une disposition-source à la norme de référence invoquée par le requérant. Cette disposition-source n'est pas toujours l'acte formellement attaqué. Si un acte administratif ou une loi critiqué se borne à réitérer ou à tirer les conséquences nécessaires d'une norme supérieure (108), c'est cette dernière qui doit être regardée comme la disposition réellement en débat (109). C'est *l'original qui se cache derrière la copie*. Un peu comme s'il était reproché à un agent d'accomplir un acte qu'il a consigne expresse d'exécuter : dans ce cas, il faut adresser ses récriminations au supérieur hiérarchique.

Lorsqu'une loi se borne à tirer les conséquences nécessaires d'un règlement auquel elle adapte le droit interne, ou de dispositions précises et inconditionnelles d'une directive qu'elle a pour objet de transposer, la disposition-source, celle qui est réellement visée, c'est donc ce règlement ou cette directive. Et lorsqu'un requérant soutient devant le Conseil constitutionnel qu'une telle loi est contraire à la Constitution, il l'invite donc à se faire juge de la conformité de ce règlement ou de cette directive à la Constitution. Dans ce cas, après s'être assuré que la loi a été adoptée selon une procédure conforme à la Constitution, qu'elle n'est pas manifestement incompatible avec le règlement ou la directive - ce dont il résulterait une méconnaissance de l'article 88-1 - et que le législateur n'est pas resté en deçà de la compétence que lui reconnaît l'article 34 de la Constitution, il s'en remet en principe, pour le respect des exigences constitutionnelles de fond, au contrôle des juges du droit de l'Union que sont les juridictions administratives et judiciaires et la Cour de justice. Autrement dit, le contrôle de constitutionnalité ne disparaît pas, mais il est, dans cette mesure, transporté dans l'ordre juridique européen et placé *in fine* sous la bonne garde de la Cour de Luxembourg (110). Le policier constitutionnel renvoie le plaignant vers le gendarme communautaire, pour autant qu'ils appliquent les mêmes règles.

Car telle est bien sûr la limite de cette forme de sous-traitance du contrôle de constitutionnalité : lorsqu'est en cause *une règle ou un principe inhérent à l'identité constitutionnelle de la France* (111) - autrement dit lorsqu'une norme constitutionnelle (112) n'a pas d'homologue européen -, le Conseil constitutionnel s'assure de son respect par la loi donc, en réalité, par la directive (113). C'est sous cette réserve, que les tables analytiques de jurisprudence du Conseil constitutionnel dénomment « *clause de sauvegarde* », que l'article 88-1

peut être regardé comme consacrant le principe de primauté du droit de l'Union, selon les termes de sa décision n° 2004-505 DC du 19 novembre 2004 (114).

Concrètement, cela signifie que *le Conseil constitutionnel s'autorise à laisser inappliqué le droit de l'Union, dans des cas résiduels* (115) *et qu'il n'a d'ailleurs jamais illustrés* (116). Ce faisant, il a adopté ce qui est un quasi standard européen, puisque de nombreuses autres cours constitutionnelles ont mis en place un filet de sécurité comparable, souvent connu sous le nom de « théorie des contre-limites » (117). Cette soupape, disons-le, n'est pas l'instrument d'un repli nationaliste, d'un réflexe idéologique de souveraineté ou d'une fierté juridictionnelle mal placée : elle est d'abord un outil pour faire respecter la norme fondamentale dont tout procède, y compris le choix de l'État de participer à la construction européenne ; et elle est aussi une garantie d'efficacité du dialogue des juges, sur la base d'un rapport de forces équilibré (118).

Vous vous êtes directement inspirés de cette jurisprudence constitutionnelle pour bâtir, il y a près de quinze ans maintenant, la « clause de sauvegarde *Arcelor* » (119).

Dans cette affaire, vous étiez saisi d'un moyen critiquant la conformité à la Constitution d'un décret transposant les dispositions précises et inconditionnelles d'une directive. Le débat portait donc sur la constitutionnalité de la directive elle-même, qui était la disposition-source. Dans une telle configuration, vous examinez s'il existe une règle ou un principe du droit de l'Union qui, eu égard à sa nature et à sa portée, tel qu'il est interprété par la jurisprudence de la Cour de justice, garantit par son application l'effectivité du respect de l'exigence constitutionnelle invoquée. Si une telle règle existe, le contrôle de constitutionnalité est « transporté » dans l'ordre juridique de l'Union : cela vous conduit, en cas de difficulté sérieuse, à poser à la Cour de justice la question de savoir si la directive est conforme à cette norme européenne d'effet équivalent. Si tel est le cas, alors la directive est aussi présumée conforme à la Constitution et le moyen dirigé contre le décret qui la transpose fidèlement doit être écarté. À l'inverse, si l'ordonnancement juridique européen ne contient pas de norme équivalente, vous procédez à un examen de constitutionnalité classique qui peut aboutir à annuler le décret, c'est-à-dire à laisser la directive inappliquée (120). Vous avez, par la suite, discrètement transposé ce raisonnement à l'acte réglementaire qui se borne à adapter le droit national à un règlement européen, à l'instar de ce que fait le Conseil constitutionnel (121). *Vous vous reconnaissez donc vous aussi la faculté de mettre à l'écart un règlement ou une directive, et la jurisprudence de la Cour de justice qui l'accompagne le cas échéant*.

Vous observerez que la clause de sauvegarde que vous avez alors aménagée est plus large (122) *que celle du Conseil constitutionnel, en tous les cas telle qu'il l'a appliquée jusqu'à présent*. En effet, vous ne vous contentez pas de vérifier que la norme constitutionnelle invoquée trouve son pendant formel dans l'ordre juridique européen, comme le font vos voisins de Montpensier (123). Au-delà de « l'identité nominale », vous vous assurez d'une « équivalence réelle » (124) : la *portée* qui lui est conférée par la Cour de justice, en l'état de sa jurisprudence, doit être comparable à celle qui lui est donnée en droit national. C'est logique : ce qui compte, en la matière comme pour le contrôle de constitutionnalité des lois « telles qu'interprétées » par les juridictions compétentes, c'est la portée réelle d'une norme. S'il existe un décalage, s'il n'y a plus superposition des règles constitutionnelle et européenne, le contrôle autonome de constitutionnalité trouve de nouveau à s'appliquer pour « ce qui dépasse » (125).

3° Il ne vous aura pas échappé que la configuration procédurale du présent litige n'est pas celle de la décision *Arcelor*.

Les requérants ne critiquent nullement la constitutionnalité des dispositions réglementaires litigieuses, ni celles de la loi où se loge, on l'a dit, l'obligation de conservation - ce qu'ils n'auraient pu faire, dans ce second cas, que par la voie d'une question prioritaire de constitutionnalité (QPC) (126). Ils soulèvent exclusivement des moyens d'inconventionnalité, principalement contre la loi. Et *c'est le défendeur qui oppose à ces moyens une exception d'inconstitutionnalité*, visant les engagements européens dont les requérants se prévalent. C'est, trivialement, une défense antimissile : loin de reprocher quoi que ce soit à la loi, l'État vous demande de l'appliquer telle qu'elle est, au motif que la norme européenne qui la vise - le missile - serait elle-même contraire à la

Constitution. Ce n'est donc pas la conformité à la Constitution de la loi qui est en cause (127), ce qui poserait un problème de loi-écran, mais bien celle de la directive *e-privacy* et du RGPD. Vous êtes donc conviés à opérer le même contrôle de constitutionnalité adapté que dans l'affaire *Arcelor*.

Vous pourriez être gênés, il est vrai, par un effet « à rebours » de ce contrôle de constitutionnalité, lorsqu'est en cause une loi, et non un décret. En écartant une directive au motif qu'elle priverait de garanties une exigence constitutionnelle spécifique, vous donneriez à penser, de façon présomptueuse, que le législateur ne pourrait, sans méconnaître la Constitution, faire le choix, ultérieurement, d'appliquer cette directive.

Ce serait là, à notre avis, commettre une erreur de perspective.

Ce qui vous est demandé par les requérants, dans cette configuration, c'est de mettre à l'écart une législation existante sur le fondement du droit dérivé de l'Union. Et c'est l'exercice de ce contrôle de conventionnalité qui, en évinçant la loi, pourrait conduire à priver de garantie les exigences constitutionnelles tels que vous les interprétez et qui s'imposent à vous. En refusant d'appliquer le droit dérivé dans une telle hypothèse, vous ne dites rien de ce que le législateur pourrait faire ou non à l'avenir au regard de la Constitution. Ce n'est pas votre rôle. Vous vous bornez, pour ce qui vous concerne, à affirmer que la Constitution ne vous permet pas de faire droit au moyen d'inconventionnalité. C'est, en d'autres termes, une « contre-limite » de votre propre office. Vous disposez naturellement d'une entière latitude pour l'introduire. À défaut de dispositions précises dans la Constitution, c'est vous, en effet, qui définissez les conditions et limites du contrôle de conventionnalité. Vous n'avez pas eu besoin d'une autorisation constitutionnelle expresse pour adopter la décision *Nicolo* et donner son plein effet à l'article 55 de la Constitution. Vous n'en avez pas besoin non plus pour suivre notre proposition et donner son plein effet au reste de la Constitution.

Nous ne croyons pas, en outre, que cette construction se heurte à un quelconque *problème de compétence*, à tout le moins en l'espèce. Rappelons que vous vous refusez en principe à contrôler la conformité des engagements internationaux de la France à la Constitution (128). Vous vous efforcez seulement d'en donner l'interprétation la plus conforme à la Constitution, dans la limite de ce qu'autorise la lettre du texte et en tenant compte de l'intention de son auteur (129).

Vous avez surmonté la difficulté dans *Arcelor*, en acceptant le principe du contrôle de constitutionnalité d'une directive à la Constitution, comme vous y invitait Mattias Guyomar. Ce dernier avançait à cette fin deux motifs :

- d'une part, « la transposition d'une directive ne constitue une obligation constitutionnelle que si et dans la mesure où elle respecte, dans son contenu, les règles et principes de valeur constitutionnelle ». Cet argument, tiré de la suprématie de la Constitution dans l'ordre interne, est généralisable : ce n'est pas seulement la transposition d'une directive qui constitue une exigence constitutionnelle, c'est plus largement son respect. Or la directive comme le règlement ne sont « respectables » que s'ils respectent eux-mêmes le bloc de constitutionnalité (130) ;

- le second argument est qu'« il n'existe pas, dans notre ordre interne, de juge chargé de s'assurer de la constitutionnalité des directives à l'occasion de leur transposition directe par le pouvoir réglementaire » : ce constat, décisif, est transposable au cas dans lequel la disposition réglementaire attaquée est prise pour l'application d'une loi. C'est à tout le moins certain lorsque, comme ici (131), la directive ou le règlement n'impose pas au législateur de modifier le droit national, mais se borne à lui ouvrir une faculté - encadrée. Le Conseil constitutionnel, qu'il soit saisi de la loi dans le cadre de son contrôle *a priori* ou en QPC, ne contrôle pas la conventionnalité d'une telle loi ; il n'est pas amené à confronter la loi à l'acte de droit dérivé. Par conséquent, il n'est jamais conduit à vérifier que cet acte de droit dérivé ne se heurte pas lui-même à la Constitution (132). À l'occasion d'un litige portant sur la légalité d'un décret pris pour l'application d'une telle loi, vous êtes bien les seuls à pouvoir vous assurer qu'en écartant cette loi en raison de sa contrariété avec une directive ou un règlement, vous ne privez pas du même coup de garantie une exigence constitutionnelle spécifique.

Une dernière difficulté, propre à l'espèce, mérite d'être mentionnée sur ce point : c'est la question de savoir si vous ne vous heurtez pas à un « traité-écran ». Comme on l'a dit, la Cour de justice a ici interprété la directive *e-privacy* et le RGPD « à la lumière de la Charte des droits fondamentaux ». Cette méthode d'interprétation pèse d'un poids particulier dans notre affaire, car on est enclin à croire que les auteurs de ces textes n'avaient jamais envisagé que leur créature puisse leur échapper à ce point. En témoigne d'ailleurs la position de la Commission européenne et de quinze gouvernements devant la Cour, tendant à ce qu'elle abandonne ou tempère la jurisprudence *Télé2*. De même, la censure de la directive de 2006 dans l'arrêt *Digital Rights Ireland* sur le fondement de la Charte donne du crédit à l'idée que son mode d'emploi serait en réalité l'ombre portée de la Charte, c'est-à-dire d'un traité. La Cour indique d'ailleurs, au point 109 de sa décision d'octobre dernier, qu'en adoptant la directive *e-privacy*, le législateur de l'Union a « concrétisé » les droits garantis par les articles 7 et 8 de la Charte.

Pour autant, elle n'énonce pas que cette directive et le RGPD se borneraient à tirer les conséquences nécessaires de la Charte. Elle se contente de les interpréter dans le sens le plus conforme à celle-ci. Nous ne croyons donc pas que la disposition-source se trouverait dans la Charte elle-même et que vous soyez ainsi conduit à confronter un traité à la Constitution(133).

La configuration de l'espèce appelle en conséquence la mise en oeuvre d'un contrôle de même nature que celui qui a été imaginé dans *Arcelor* :

- il y a lieu d'examiner d'abord s'il existe, dans le droit de l'Union, une norme d'effet équivalent à la règle constitutionnelle invoquée par le défendeur. Le cas échéant, il vous faudrait y confronter l'acte de droit dérivé. C'est ce que vous feriez, d'ailleurs, si le défendeur soulevait plus directement une exception d'invalidité de la directive invoquée au regard du droit primaire ;

- et, dans la négative, vous devez confronter la directive et le règlement, tels qu'interprétés par la Cour, à cette règle constitutionnelle spécifique et, le cas échéant, écarter le droit de l'Union.

Il va de soi que la mise en oeuvre de cette clause de sauvegarde ne peut être qu'exceptionnelle, parce que le respect du droit de l'Union constitue aussi une exigence constitutionnelle, on l'a dit, et parce que vous ne pouvez ignorer qu'elle expose la France à une action en manquement voire à une crise politique. Nous vous invitons à respecter quelques lignes directrices dans cet exercice.

En premier lieu, vous devez faire un usage raisonnable de la condition *d'équivalence des protections*, lorsqu'une norme est formellement protégée constitutionnellement et conventionnellement. Il faut concevoir les prises de position de la Cour de justice dans l'interprétation et l'application des textes comme formant un tableau, pointilliste ou abstrait, à distance duquel vous devez vous tenir pour en saisir l'impression d'ensemble. Vous devez vous satisfaire de ce qu'une exigence est garantie « en général » et « pour l'essentiel de la même façon », pour reprendre la formulation de la Cour de Karlsruhe(134). On perçoit bien le risque d'un glissement vers une équivalence toujours plus concrète et précise, qui consisterait à examiner pour chaque affaire si le résultat auquel est parvenu la Cour de justice sur le fondement du droit de l'Union correspond précisément à celui qui découle des normes constitutionnelles selon votre propre analyse. Vous autoriseriez le défendeur à rediscuter systématiquement du bien-fondé de ses arrêts devant vous(135). Il en résulterait une forme de *relativisme juridique permanent*, où ce qu'on croyait acquis à l'aune d'un droit pourrait toujours être rediscuté sur le fondement d'un autre. Vous ouvririez la boîte de Pandore de l'insécurité juridique, de l'imprévisibilité des règles, et, de là, de l'ineffectivité des droits et de tous ces maux juridiques qui rongent déjà nos sociétés et la compétitivité de notre économie. Cette retenue que nous préconisons ne doit naturellement pas vous interdire de mettre en évidence une différence de cadre d'analyse, et pas seulement d'appréciation, derrière une solution unique dont les effets vous paraîtraient aberrants - un peu comme une dénaturation en cassation peut être le révélateur d'une erreur de droit.

En deuxième lieu, vous devez, pour autant que la lettre du droit dérivé et les énonciations des arrêts de la Cour

vous le permettent, *privilégier une logique de conciliation par leur interprétation conforme aux exigences constitutionnelles*. C'est toujours cette voie que vous privilégiez en présence d'un conflit entre normes supérieures. Le constat d'échec du dialogue des juges, nous dirions même, désormais, du concert des juges, ne peut être qu'une solution de dernier recours (136).

En troisième lieu, nous pensons que vous ne pouvez actionner la clause de sauvegarde, en dernier recours, que si vous êtes *saisi d'un moyen en ce sens*. Il est vrai que le débat porte sur l'applicabilité du droit dérivé invoqué, plutôt que sur sa validité. Or il appartient en principe au juge de déterminer d'office la norme applicable au litige dont il est saisi. Mais ce principe ne vaut pas pour le jeu des exceptions, lorsqu'elles ne sont pas elles-mêmes d'ordre public (137). C'est tout le sens de la vénérable jurisprudence *Morgane* en matière d'inconventionnalité de la loi : alors même qu'est en cause l'applicabilité de la loi au litige, vous ne soulevez pas d'office sa contrariété à un engagement international ou européen. Nous ne voyons pas la logique qu'il y aurait à secourir d'office un défendeur qui s'abstiendrait de lancer la contre-attaque constitutionnelle contre un moyen d'inconventionnalité du requérant. En dépit de son importance, le débat de constitutionnalité n'a jamais été, en lui-même, d'ordre public devant le juge de l'excès de pouvoir (138). Par ailleurs, il nous semble matériellement difficile de contrôler d'office la conformité à la Constitution de tout acte de droit dérivé invoqué, le cas échéant interprété par tout arrêt préjudiciel. Il est préférable de laisser le défendeur prendre l'initiative et la responsabilité d'ouvrir ce débat délicat, par une argumentation qui se devra d'être circonstanciée et solidement étayée, comme en l'espèce.

En quatrième lieu, vous ne devez, le cas échéant, écarter le droit de l'Union que *dans la stricte mesure du nécessaire*. Vous devez en effet veiller à respecter autant que possible le principe de coopération loyale figurant à l'article 4 du Traité sur l'Union européenne, en vous abstenant de toute décision susceptible de « mettre en péril la réalisation des objectifs de l'Union ». À nos yeux, toutefois, cette expression est plus circonscrite que celle de méconnaissance du droit de l'Union : elle peut vous servir de guide pour apprécier le principe et la portée de la « dérogation » que vous vous autorisez à pratiquer (139). En l'occurrence, par exemple, les objectifs poursuivis par l'Union à travers la directive *e-privacy* consistent à unifier le marché intérieur des services de communications électroniques en respectant un standard élevé de protection de la vie privée ; son considérant 14 précise que « L'harmonisation devrait être limitée aux exigences nécessaires pour garantir que la promotion et le développement de nouveaux services et réseaux de communications électroniques entre États membres ne sont pas entravés » (140). Nous ne voyons pas bien en quoi le droit français constituerait une entrave au développement des réseaux et services, d'autant que la compensation dont bénéficient les opérateurs permet de prévenir toute distorsion de concurrence. Et l'obligation de conservation des données n'a, depuis vingt ans, jamais été identifiée comme une entrave à la liberté de circulation et d'établissement des personnes, pas même celle des terroristes.

Enfin, vous ne devez pas perdre de vue que votre légitimité de juge national n'est pas supérieure à celle du juge européen, et faire preuve en conséquence de retenue dans la confrontation entre l'acte de droit dérivé et les exigences constitutionnelles invoquées en défense. Sans exiger une incompatibilité manifeste, vous devez disposer d'une certitude suffisante pour vous autoriser à écarter le droit de l'Union, plutôt que de laisser cette responsabilité soit au constituant, soit au législateur européen, soit encore, si nécessaire, aux États membres en tant que parties aux traités.

4° Si l'on adopte ce cadre de référence, il y a lieu d'examiner si les normes invoquées en l'espèce par le gouvernement font l'objet en droit de l'Union d'une *protection équivalente* à celle que leur accorde la Constitution. Sont en jeu la sauvegarde des intérêts fondamentaux de la nation, au nombre desquels figurent l'indépendance de la nation et l'intégrité du territoire (141), l'objectif de prévention des atteintes à l'ordre public, notamment celle des atteintes à la sécurité des personnes et des biens et la lutte contre le terrorisme (142), et l'objectif de recherche des auteurs d'infractions (143), notamment pénales.

a) La plupart du temps, le Conseil constitutionnel mobilise les objectifs de valeur constitutionnelle à titre de justifications des atteintes portées à l'exercice de droits ou de libertés constitutionnellement garantis (144),

comme le font usuellement les juridictions européennes. Mais c'est parce que le débat contentieux se présente le plus souvent ainsi devant lui.

Contrairement à ce qu'on lit parfois, ces objectifs ne sont pas dépourvus d'autonomie normative et ils peuvent, à eux seuls, fonder des censures, comme les principes constitutionnels (145). Les exemples sont multiples, tant dans la jurisprudence du Conseil constitutionnel (146) que dans la vôtre, à propos par exemple de l'objectif d'intelligibilité de la norme (147). Même si les objectifs liés à la sécurité n'en offrent pas d'illustration explicite, à notre connaissance (148), la même logique doit prévaloir. Le Conseil constitutionnel a du reste qualifié la sauvegarde de l'ordre public d'« exigence constitutionnelle » (149) et jugé qu'elle « implique notamment que soit assurée la protection des personnes » (150). Dans la même logique, il a fait obligation au législateur de fixer les « règles appropriées » tendant à la réalisation de l'objectif de valeur constitutionnelle de protection de la santé publique (151). Nous relevons par ailleurs que le Conseil constitutionnel ne se borne pas à examiner si une loi élargissant les pouvoirs de coercition ou d'investigation des autorités administratives ou judiciaires ne porte pas une atteinte manifestement excessive au droit au respect de la vie privée : il s'assure que le législateur n'a pas opéré une « conciliation manifestement déséquilibrée » entre le droit au respect de la vie privée et ces objectifs (152). Cette formulation n'exclut nullement que le déséquilibre manifeste puisse résulter des insuffisances de la loi pour garantir la sécurité. S'il prenait fantaisie au législateur de dépénaliser le meurtre ou le viol, nous doutons fort que le Conseil constitutionnel ne trouverait rien à y redire. Cette obligation d'agir existe aussi dans votre jurisprudence : vous exigez de l'autorité investie du pouvoir de police qu'elle prenne toute mesure pour prévenir une atteinte à l'ordre public (153). Il y a bien longtemps (154) que vous contrôlez, sans texte exprès, la légalité des refus d'édicter des mesures de police nécessaires à la préservation de l'ordre public (155) et que vous réparez les préjudices nés de la carence de l'autorité de police, dans le cadre, désormais, d'un régime de faute simple (156).

La normativité des objectifs de prévention des atteintes à l'ordre public et de recherche des auteurs d'infractions s'impose d'autant plus qu'ils sont constamment regardés par le Conseil constitutionnel comme « nécessaires à la sauvegarde de principes et de droits de valeur constitutionnelle » (157). Il a même pu juger que, sans l'ordre public, « l'exercice des libertés ne saurait être assuré » (158). Car à travers eux, c'est tout le corpus des droits fondamentaux qui est en jeu (159). Le débat qui vous est soumis aujourd'hui n'est donc pas tant un conflit entre liberté et sécurité qu'un conflit interne au droit au respect de la vie privée : ce droit est directement atteint par la conservation et, plus encore, l'accès aux données par les autorités administratives et judiciaires ; mais il serait également en péril si les forces de sécurité ne disposaient plus des moyens d'exercer leurs missions, car, alors, votre vie privée pourrait être piétinée en toute impunité par les criminels et les délinquants, les vrais.

C'est ce qu'exprime parfaitement la Déclaration de 1789 : on sait qu'une « société dans laquelle la garantie des droits n'est pas assurée (...) n'a point de constitution », selon son article 16 ; on connaît moins son article 12 selon lequel « la garantie des droits de l'homme et du citoyen nécessite une force publique ». Il en découle nécessairement que cette dernière doit disposer des moyens d'exercer cette mission (160), moyens non seulement financiers - comme le prévoit explicitement l'article 13 de la Déclaration - mais aussi juridiques et opérationnels.

Soyons clair : notre propos ne consiste pas à dégager prétoriennement *un droit constitutionnel à la sécurité* qu'on ne trouve ni dans notre Constitution écrite, contrairement à nombre d'autres (161), ni dans la jurisprudence du Conseil constitutionnel, au titre des principes fondamentaux reconnus par les lois de la République. Du point de vue constitutionnel, vous avez le droit de vivre dans un environnement équilibré et respectueux de votre santé (162), vous avez aussi le droit à la sécurité matérielle (163), notamment à la sécurité sociale (164), et dans une certaine mesure à la sécurité juridique (165), mais le « droit fondamental » à la sécurité n'est proclamé, modestement, que par l'article L. 111-1 du code de la sécurité intérieure (166). Vous n'y voyez donc pas une liberté fondamentale qu'il vous appartiendrait de protéger en référé-liberté (167). Et le Conseil constitutionnel a de son côté jugé que l'objectif de sauvegarde de l'ordre public ne pouvait en lui-même être invoqué à l'appui d'une question prioritaire de constitutionnalité (168).

Pour autant, cet objectif est parfaitement invocable en combinaison avec le ou les droits ou libertés garantis par la Constitution qu'il vise à protéger, comme le droit au respect de la vie privée ou la sauvegarde de la dignité de la personne humaine, qui protège le droit à la vie (169). En outre, et surtout, le fait qu'une personne ne puisse se prévaloir d'un tel objectif à l'occasion d'un contentieux individuel n'enlève rien aux obligations qu'il fait peser sur le législateur, sur le pouvoir réglementaire, et sur vous-même, dans le cadre de votre contrôle de conventionnalité.

b) *Il reste à déterminer si le droit de l'Union garantit l'effectivité du respect des exigences constitutionnelles ainsi comprises*.

Il faut rendre cette justice à la Cour de Luxembourg : alors qu'initialement, elle ne voyait dans la lutte contre le terrorisme (170) et la criminalité grave (171) que des objectifs d'intérêt général pouvant justifier des limitations aux droits fondamentaux, de même que la protection de la sécurité publique contribuant à la protection des droits et libertés d'autrui (172), son arrêt du 6 octobre 2020 énonce, en s'inspirant explicitement de la jurisprudence de la Cour européenne des droits de l'homme (173), que le droit au respect de la vie privée et familiale peut créer dans le chef des États certaines *obligations positives* d'agir pour lutter efficacement contre les infractions qui la menacent, en particulier pour les mineurs et les autres personnes vulnérables (174). Mais ces obligations sont conçues de manière étroite et résiduelle : en pratique, la Cour ne nous semble les faire jouer ici qu'en ce qui concerne les adresses *IP*, lorsqu'elle entend préserver les capacités opérationnelles de lutte contre la pédopornographie. Et son arrêt montre que ces obligations positives ne sont pas d'une nature distincte des objectifs d'intérêt généraux : elles constituent de simples facteurs de limitation de l'exercice des droits fondamentaux. Pour les raisons théoriques et psychologiques que nous avons essayé d'identifier précédemment, elle néglige largement que l'incapacité de l'État à lutter contre les menaces qui pèsent sur lui et sa population est elle aussi de nature à compromettre purement et simplement l'exercice de ces mêmes droits (175). Comme nous allons nous efforcer de le montrer, le mode d'emploi auquel elle est parvenue le démontre clairement, à nos yeux.

Au fond, notre conviction est que, structurellement, le droit de l'Union ne peut pas accorder à la sauvegarde de la sécurité nationale et à la recherche des auteurs d'infractions le même niveau de garantie que la Constitution - et cette conviction s'étend, bien entendu et presque *a fortiori*, à l'exigence constitutionnelle de « nécessaire libre disposition de la force armée », même si ce n'est pas le sujet du jour (176). D'une part, parce que l'article 4 du TUE prévoit que la responsabilité de la sécurité nationale relève des seuls États membres. D'autre part, parce que ce même article se borne à prescrire à l'Union de *respecter* « les fonctions essentielles de l'État, notamment celles qui ont pour objet d'assurer son intégrité territoriale, de maintenir l'ordre public et de sauvegarder la sécurité nationale ». *Respecter n'est pas garantir*. La Cour se doit de tenir compte de ces considérations lorsqu'elle apprécie la proportionnalité de l'ingérence - c'est ce qu'elle a fait ici, en particulier en aménageant une soupape pour la sauvegarde de la sécurité nationale - mais elle n'en est pas la gardienne (177). C'est le juge national, qui plus est lorsqu'il se nomme Conseil d'État, qui doit veiller à ce que soit assurée la sauvegarde de la sécurité nationale et de la sécurité publique, sans laquelle, à terme, il n'y a tout simplement plus d'État. Assumons le raccourci jusqu'au bout : s'il n'y a plus d'État, il n'y a plus d'État membre, donc il n'y a plus de construction européenne, non plus (178). On rappellera au passage à celles et ceux qui nous suspecteraient de souverainisme que les autorités nationales ne contribuent pas seulement à la sécurité de la France. Elles jouent un rôle-clé dans celle de l'Europe et au-delà, tant à travers les mécanismes de coopération policière et judiciaire qu'en luttant contre une criminalité qui ne respecte aucune frontière.

***

VI. - *Il est grand temps de passer aux travaux pratiques*. Nous aborderons successivement les trois catégories de données auxquelles la Cour a appliqué des régimes différents : 1° celles que nous qualifierions d'administratives, notamment l'identité civile de l'utilisateur ; 2° les adresses *IP* ; et 3° les autres données de connexion, ce qui vise essentiellement les données relatives aux communications effectuées et les données de localisation.

1° Comme on l'a vu, les *données d'identité civile*, c'est-à-dire les noms et prénoms, ainsi que les adresses postales et électroniques et les numéros de téléphone attachés à un compte, peuvent faire l'objet d'une obligation de conservation généralisée et indifférenciée sans limite de durée. À cette catégorie, vous pourrez prendre sur vous de rattacher les autres informations relatives au contrat ou au compte de l'abonné, ainsi que les données de paiement mentionnées au 4° de l'article 1er du décret de 2011, sur lesquelles vous n'avez pas interrogé la Cour. Il s'agit seulement du type de paiement utilisé par le créateur d'un contenu en ligne pour s'acquitter de son abonnement internet et/ou de ses frais d'hébergement, de la référence de la transaction, de sa date et de son heure, ainsi que de son montant. Les numéros de carte bancaire ne font pas partie des données obligatoirement conservées.

Ces données administratives ne sont pas relatives au trafic et elles ne révèlent rien de la localisation des communications passées. Le principe de confidentialité posé par la directive *e-privacy* leur est, en toute rigueur, inapplicable. En tout état de cause, ni ce texte, ni l'article 23 du RGPD ne font obstacle à ce que ces données soient obligatoirement conservées à des fins de sécurité nationale ou publique, *a fortiori* seulement un an, dans la mesure où l'ingérence dans la vie privée des internautes est très limitée. La solution est suffisamment certaine pour vous dispenser d'une nouvelle question préjudicielle.

2° S'agissant à présent des *adresses IP associées à la source d'une communication,* vous vous heurtez à une première difficulté, qui est du reste commune à l'ensemble des données de trafic et de localisation. Elle tient au choix de la Cour de *ranger les motifs d'ingérence dans des cases apparemment étanches*, en introduisant une différence de nature entre la criminalité et les menaces de sécurité publique « en général » et celles qui sont « graves ». Seules ces dernières justifient la conservation généralisée et indifférenciée des adresses *IP*. Les requérants soutiennent que la Cour exige ainsi des États qu'ils appliquent le principe de proportionnalité de façon abstraite, en adoptant des mesures législatives définissant ces notions, énumérant limitativement les infractions pénales méritant cette qualification ou définissant des seuils de déclenchement.

Précisons à titre liminaire que la restriction ainsi prévue par la jurisprudence de la Cour est dépourvue d'incidence sur l'ampleur des données que les opérateurs doivent stocker. Elle n'intéresse que l'accès. En effet, dès lors qu'il est logiquement et matériellement impossible pour les opérateurs, comme du reste pour les services, de savoir par avance quelles adresses *IP* seront utiles pour la lutte contre la criminalité grave, et celles qui ne le seraient que pour la criminalité « ordinaire », il faut nécessairement que toutes les adresses *IP* soient conservées. Par conséquent, l'exigence selon laquelle la conservation doit avoir pour finalité la lutte contre la criminalité grave n'a d'incidence pratique qu'au stade de l'accès : ce dernier ne sera possible que pour ce motif. Ce résultat est cohérent avec la règle jurisprudentielle que nous avons rappelée, selon laquelle l'accès aux données relatives au trafic est en lui-même une ingérence grave, qui ne peut être autorisée que pour des motifs graves et non pour la lutte contre la criminalité « ordinaire ». Le détour par la conservation apparaît donc inutile ici car l'ingérence que constitue l'obligation de conserver, et les risques associés, seront de toute façon subis du seul fait que les données seront stockées par les opérateurs.

Cela étant dit, nous ne lisons pas l'arrêt de la Cour comme imposant impérativement, à peine de méconnaissance du droit de l'Union, que le législateur pré-définisse de manière abstraite les cas dans lesquels l'accès aux adresses *IP* pourra avoir lieu. Certes, une classification préalable est sans doute satisfaisante pour la prévisibilité et la clarté de la règle. Mais elle est problématique à mettre en oeuvre.

Il n'y a certes aucune difficulté à inclure les crimes et à exclure les contraventions. L'exercice est plus délicat pour les délits. Assurément, la délinquance en bande organisée, pour laquelle l'autorité judiciaire dispose dès l'enquête préliminaire de pouvoirs d'investigation extrêmement étendus prévus au titre XXV du code de procédure pénale, mérite d'être rangée dans la criminalité grave. Pour la généralité des délits, on pourrait songer à fixer un seuil de peine encourue à partir duquel la « criminalité » devient grave au sens du droit de l'Union. Le seuil de trois ans est évoqué dans les écritures du gouvernement, en référence à plusieurs dispositifs existants, notamment les perquisitions contraintes (179) et les interceptions judiciaires (180), réputées toutefois plus intrusives que l'accès en temps différé aux données (181). À dire vrai, nous aurions tendance à considérer que,

dès l'instant qu'un délit est puni d'une peine d'emprisonnement, c'est nécessairement que l'infraction qu'il entend réprimer est grave, car on ne met pas en prison quelqu'un pour des faits « non graves »(182).

Cela étant, on voit bien que le q*uantum* de la peine encourue n'est qu'un indice de la gravité des faits qu'il s'agit de rechercher et poursuivre. Le vol d'un oeuf comme d'un boeuf est passible de trois ans d'emprisonnement, et même de cinq ans s'il est commis en réunion ; or on imagine mal que des données de connexion puissent être systématiquement exploitées pour réprimer une telle infraction. La gravité des agissements dépend, au-delà du quantum de la peine encourue, des circonstances de chaque infraction et de l'ampleur des préjudices subis par la société et par la victime.

Et au-delà même de l'infraction proprement dite motivant une réquisition donnée, c'est plus largement la finalité qu'elle poursuit qui doit être prise en considération, conformément aux principes les mieux établis du droit des traitements de données à caractère personnel. Il est donc périlleux d'exclure par principe l'accès aux données pour des infractions punis d'une peine faible, alors que leur recherche peut s'inscrire dans des investigations plus larges portant sur une suspicion d'infraction plus grave. Pour reprendre un exemple évoqué en séance orale d'instruction, un vol à la tire de 20 € dans le métro parisien peut être l'oeuvre facétieuse d'un *pickpocket* occasionnel ou celle d'une filière organisée exploitant des enfants. Dans ce second cas, l'accès aux données de connexion est parfaitement légitime.

Nous ajouterons qu'une classification figée risque fort d'inciter les services d'enquête à une surenchère dans les qualifications pénales retenues pour justifier la réquisition, afin de « passer la barre », en particulier si l'accès intervient à un stade précoce de la procédure. L'ingérence dans la vie privée sera subie de toute façon, même si les éléments recueillis venaient finalement à être écartés dans la suite de la procédure.

Dans ces conditions, si des présomptions de gravité ou de non-gravité peuvent parfaitement et opportunément être posées par le législateur, le cadre juridique devra nécessairement comporter, fût-ce à titre de voiture-balai, un *examen concret, au cas par cas, de la proportionnalité de l'ingérence* au regard du motif justifiant la réquisition(183). C'est précisément ce que prévoit le droit français :

- *pour les enquêtes pénales*, le 6e alinéa du III de l'article préliminaire du code de procédure pénale, issu de la loi justice de 2019, subordonne toute mesure portant atteinte à la vie privée à sa proportionnalité à la gravité de l'infraction(184). Il n'y a là que la codification de la jurisprudence constante de la chambre criminelle, notamment à l'aune de la Convention européenne(185) ;

- *pour les services de renseignement*, l'article L. 801-1 du code de la sécurité intérieure pose une exigence de proportionnalité dans la mise en oeuvre des techniques de renseignement, que le Conseil constitutionnel a expressément relevée dans sa décision sur la loi « renseignement » de 2015(186), en plaçant le contrôle de son respect entre les mains de la CNCTR(187) et du Conseil d'État.

La règle du contrôle préalable à l'accès, que pose par ailleurs la Cour, permet de garantir concrètement la proportionnalité de la mesure.

Nous vous proposons ainsi de vous satisfaire de ce qui n'est, ni plus ni moins, que l'application normale du principe de proportionnalité, principe général du droit de l'Union rappelé par l'article 15 de la directive *e-privacy* et l'article 23 du RGPD, sans nécessairement enfermer le législateur et les acteurs dans une typologie ou une échelle de gravité prédéfinie. Nous y sommes encouragé par l'idée, défendue par les avocats généraux dans leurs conclusions sur les affaires *Ministerio fiscal* (188) et *H.K.* (189), que la criminalité grave est une notion contingente et multi-factorielle, dont les contours doivent être laissés à la main des États membres, dans le cadre de leur compétence de principe en matière pénale(190), et non une notion autonome du droit de l'Union.

Nous vous proposons donc de juger que la conservation et l'accès peuvent être imposés pour la poursuite d'infractions pénales qui doivent être suffisamment graves, au regard de l'ingérence qu'elles constituent, afin de

respecter le principe de proportionnalité. Au regard des pratiques existantes, il est vraisemblable que la jurisprudence de la Cour va conduire à rehausser quelque peu le niveau d'exigence des autorités en charge du contrôle de l'accès.

Vous observerez que la même logique doit valoir pour les manquements graves aux législations sectorielles, dès lors que le principe de proportionnalité est d'application générale : l'Autorité de la concurrence peut recueillir les données de connexion pertinentes pour confondre les protagonistes du fameux « cartel national du jambon », pas pour caractériser une entente sur le prix de la paupiette entre les bouchers-charcutiers de Laon.

Quant à la durée de conservation des adresses *IP*, d'un an, l'argumentation cursive des requérants ne nous convainc pas qu'elle ne serait pas justifiée. C'est la durée que proposait le Conseil d'État dans son rapport *Internet et les réseaux numériques* de 1998, en appelant de ses voeux l'obligation de conservation consacrée par la loi de 2000 et reprise dans la *LCEN*. C'est cette même durée que la CNIL a admise de manière générale pour l'article R. 10-13, après quelques hésitations(191).

Au total, les dispositions législatives et réglementaires en litige ne nous paraissent pas méconnaître le droit de l'Union ainsi interprété, s'agissant des adresses *IP*.

3° Nous en venons au plat de résistance, concernant les *autres données relatives au trafic, dont le détail des communications téléphoniques, et les données de localisation*. L'architecture retenue par la Cour nous conduit à aborder distinctement la conservation à des fins de sauvegarde de la sécurité nationale et la lutte contre la criminalité.

a) La directive *e-privacy* explicite la notion de « sécurité nationale » par celle de « sûreté de l'État ». La Cour définit cet objectif comme la protection des « fonctions essentielles de l'État et [des] intérêts fondamentaux de la société », ce qui inclut « la prévention et la répression d'activités de nature à déstabiliser gravement les structures constitutionnelles, politiques, économiques ou sociales fondamentales d'un pays, et en particulier à menacer directement la société, la population ou l'État en tant que tel, telles que notamment des activités de terrorisme ».

Au regard des missions dévolues aux services de renseignement par l'article L. 811-3 du code de la sécurité intérieure, entrent sans discussion possible dans cette définition la défense de l'indépendance nationale, de l'intégrité du territoire et de la défense nationale (1°)(192), la prévention de toute forme d'ingérence étrangère - c'est le contre-espionnage (2°), la prévention du terrorisme (4°), la prévention des atteintes à la forme républicaine du gouvernement (a. du 5°) et la prévention de la prolifération des armes de destruction massive (7°). On peut se laisser aisément convaincre pour la défense des intérêts majeurs de la politique étrangère et l'exécution des engagements européens et internationaux de la France (2°), ainsi que des intérêts économiques, industriels et scientifiques majeurs de la France (3°) - d'autant que le considérant 11 de la directive de 2002 inclut dans la sécurité nationale les activités de sûreté « concourant à la prospérité économique de l'État ». On peut davantage hésiter pour les autres rubriques(193), en particulier la prévention des violences collectives de nature à porter gravement atteinte à la paix publique (c. du 5°)(194) et la prévention de la criminalité et de la délinquance organisées (6°)(195), qui représentent à elles deux environ 1/3 des techniques de renseignement mises en oeuvre.

L'article L. 811-3 les qualifie d'intérêts fondamentaux de la nation ; nous comprenons que c'est dans la mesure où les agissements visés sont de nature à affecter les intérêts fondamentaux de la nation que les services de renseignement ont vocation à intervenir. C'est à tout le moins certain pour ce qui concerne les services spécialisés : l'article L. 811-2 du CSI précise qu'ils ont pour mission de collecter et d'exploiter des renseignements relatifs aux enjeux géopolitiques et stratégiques ainsi qu'aux menaces et aux risques « susceptibles d'affecter la vie de la nation ». C'est plus discutable pour les services du second cercle en tant qu'ils poursuivent ces finalités. Toutefois, il existe, en pratique, une très grande porosité entre les finalités et les actions menées par les uns et les autres, et nous craignons qu'une dissociation des régimes ne soit à la fois artificielle et complexe dans sa mise

en oeuvre. Par ailleurs, à partir du moment où la conservation généralisée et indifférenciée serait admise au titre de certains items, les inconvénients associés à cette ingérence seraient supportés de toute façon.

Rappelons aussi qu'il est de jurisprudence européenne constante qu'il appartient aux États membres de définir leurs intérêts essentiels de sécurité nationale (196), ce qui vous donne une certaine liberté de lecture de l'arrêt. C'est la raison pour laquelle, non sans hésitation, nous vous proposons de rattacher la défense de l'ensemble des intérêts fondamentaux énumérés à l'article L. 811-3 à la sauvegarde de la sécurité nationale. En revanche, la « promotion » de ces intérêts, également mentionnée à cet article, ne nous paraît pas devoir relever de la « sauvegarde de la sécurité nationale » ; nous ne sommes pas certains, du reste, que les données de connexion soient utilisées à cette fin en pratique.

S'agissant des enquêtes pénales, peuvent à tout le moins y être inclus les atteintes aux intérêts fondamentaux de la nation figurant au titre I^er^ du livre IV du code pénal, les actes de terrorisme réprimés par les dispositions de son titre II et les infractions relatives à la prolifération des vecteurs d'armes de destruction massive mentionnées dans le code de la défense (197).

Indépendamment de ce débat d'ordre terminologique sur les contours de la « sécurité nationale », il vous faut surtout *arbitrer entre deux lectures radicalement différentes de l'arrêt de la Cour* en ce qui concerne l'injonction de conservation généralisée et indifférenciée en cas de menace grave pour la sécurité nationale. Pour les requérants, la Cour aurait entendu se référer à une forme d'état d'urgence très circonscrit dans le temps, et qui correspondrait peu ou prou au niveau « Urgence attentat » du plan *Vigipirate*, c'est-à-dire au cas de la menace d'attaque imminente ou à la suite immédiate d'un attentat terroriste. À titre d'exemple, l'injonction aurait pu être prise le 29 octobre dernier, à la suite de l'attentat de la basilique Notre-Dame de Nice, et prendre fin le 5 mars dernier. C'est ainsi que le concevait l'avocat général dans notre affaire, en évoquant « des situations réellement exceptionnelles, caractérisées par une menace imminente ou par un risque extraordinaire justifiant la déclaration officielle d'une situation d'urgence dans un État membre ». On ne peut pas absolument exclure que la Cour l'ait suivi, puisqu'elle a pris soin de préciser que la conservation dans ce cadre « ne saurait présenter un caractère systématique ». Or les menaces qui pèsent sur la France ne sont ni récentes ni éphémères, ce que la Cour ne pouvait ignorer.

Le gouvernement défend quant à lui l'idée que, tant que cette menace grave existe, fût-elle un état permanent à une échéance longue, la conservation généralisée doit pouvoir être imposée.

La seule lecture de l'arrêt qui soit conforme aux exigences constitutionnelles invoquées est celle du gouvernement. Nous peinons sincèrement à imaginer une injonction stroboscopique circonscrite aux quelques mois qui suivent un attentat terroriste, alors que l'identification et l'arrestation des responsables supposent d'accéder à des données concernant des communications antérieures au gel qui serait ainsi ordonné, de la préparation de l'attentat à son déroulement lui-même. Plus largement, l'action des services de renseignement consiste précisément à anticiper et déjouer la survenance de risques majeurs par une surveillance au long cours et permanente, y compris des « signaux faibles ». Il ne fait guère de sens d'attendre que la menace grave se matérialise sous la forme d'un attentat précis, ou soit sur le point de se réaliser, pour leur permettre d'avoir accès à l'ensemble des données permettant de caractériser une telle menace et de la prévenir. Ajoutons que le dispositif à éclipses suggéré par les requérants nous semble difficilement gérable pour les opérateurs.

Nous interprétons aussi l'arrêt comme autorisant que les données conservées de manière généralisée pour un motif donné de sécurité nationale - par exemple le terrorisme - puissent être accessibles pour d'autres motifs du même niveau de gravité - par exemple la surveillance du développement d'un programme nucléaire militaire par un pays qui n'y est pas autorisé. Au point 166 de son arrêt, la Cour rappelle ainsi que l'accès ne peut être justifié que par « l'objectif d'intérêt général » pour lequel la conservation a été imposée aux opérateurs, et l'illustre en raisonnant au regard des trois niveaux de gravité, qu'elles qualifient d'« objectifs » : lutte contre la criminalité « ordinaire », lutte contre la criminalité grave et sauvegarde de la sécurité nationale. Autrement dit, la sécurité nationale forme un tout et il n'y a pas lieu de descendre au niveau de granularité des rubriques de l'article L. 811-

3 du CSI.

Si vous nous suivez, vous ne pourrez que constater l'existence d'une menace grave, « réelle et actuelle », et *a fortiori* « prévisible » comme l'admet la Cour, pesant sur la sécurité nationale, tant à la date des décrets attaqués qu'à celle de votre décision. Il n'est pas besoin de s'étendre très longuement sur ce point. Les décrets ont été pris, pour l'un, quelques mois après l'attentat de Charlie Hebdo et dans la foulée de l'attaque du Thalys ; pour les autres, quelques semaines après les attentats du Bataclan. En enjambant les années 2016 à 2019, dont, entre autres, le carnage sur la promenade des Anglais, l'assassinat du père Hamel à Saint-Etienne-du-Rouvray, le double meurtre de la gare Saint-Charles ou l'attentat du marché de Noël de Strasbourg, on déplore six attaques terroristes en 2020, dont l'assassinat de Samuel Paty, et deux actions déjouées, comme ce fut encore le cas en mars dernier. Nous vivons depuis le 5 mars au niveau *Vigipirate* « Sécurité renforcée - risque d'attentat » qui témoigne d'un niveau élevé de la menace terroriste.

Au-delà du terrorisme, le gouvernement fait aussi état de façon circonstanciée, exemples à l'appui, de cas réitérés de trahison et d'intelligence avec des puissances étrangères hostiles susceptibles d'avoir des conséquences très graves, d'espionnage industriel et d'attaques informatiques pilotées ou soutenues par des États et visant des cibles sensibles, y compris des hôpitaux. Peut-être plus que tout autre État membre, la France est une cible en raison de son potentiel économique et scientifique, de ses capacités militaires et de ses opérations extérieures, et, tout simplement, des valeurs qu'elle incarne et qu'elle porte sur la scène internationale. S'y ajoute le durcissement de la violence politique, militante et identitaire, capitalisant sur la recrudescence des mouvements sociaux et des manifestations et se livrant à des actions para-terroristes comme le sabotage d'infrastructures.

Au fond, s'il n'y avait pas de menace grave pour la sécurité nationale, notre pays ne consacrerait pas de tels moyens au fonctionnement de ses services de renseignement - au moins 2 milliards d'euros par an (198). Et même si on s'habitue à tout, paraît-il, ce n'est pas parce qu'une menace est durable qu'elle n'est plus grave.

Dans la mesure où la Cour de justice n'exige pas que la menace grave soit constatée formellement dans l'acte d'injonction de conservation, il n'y a aucune difficulté à admettre que les dispositions législatives et réglementaires litigieuses valent injonction, en tant qu'elles portent sur la sauvegarde de la sécurité nationale. Par ailleurs, cette injonction est soumise à un contrôle juridictionnel effectif, comme le montre la présente affaire : c'est le vôtre à travers la contestation de la légalité des dispositions réglementaires, à l'appui de laquelle la conventionnalité de la loi peut être critiquée.

La seule aspérité tient au *caractère illimité dans le temps de cette injonction*. Au regard des énonciations claires de l'arrêt de la Cour, on ne peut se satisfaire de ce que le gouvernement est tenu d'abroger le dispositif s'il devient illégal, conformément à la jurisprudence *Alitalia* codifiée (199), ni même d'un mécanisme de tacite reconduction. Il n'est pas équivalent, y compris au regard du droit au recours, de l'obliger formellement à prendre une nouvelle mesure à échéance régulière, dont nous pensons qu'elle devrait être, tout au plus, annuelle. En soi, l'obligation d'un réexamen périodique ne porte aucune atteinte aux objectifs de valeur constitutionnelle.

Pour terminer sur cette finalité, la *durée de la conservation obligatoire,* fixée à un an, nous paraît limitée à ce qui est strictement nécessaire dès lors qu'elle permet de retracer des contacts et des déplacements pendant une période cohérente avec la préparation d'actions de déstabilisation de l'État, comme un attentat terroriste. On la retrouve dans de nombreuses législations européennes, l'Italie ayant quant à elle opté pour une durée de six ans.

Il en résulte que, pour cette finalité, la seule illégalité dont sont entachés l'article R. 10-13 du code des procédures civiles d'exécution (CPCE) et le décret du 25 février 2011 tient à leur caractère pérenne. Il faut et il suffit, pour respecter les exigences de la Cour, qu'ils organisent leur propre sortie de vigueur.

Si l'effort de lecture de l'arrêt que nous vous proposons vous paraît hors de portée, notre solution subsidiaire est

d'activer la clause de sauvegarde pour sécuriser la conservation généralisée des données à cette fin.

b) Pour ce qui concerne à présent la *lutte contre la criminalité grave*, au sens où nous l'avons entendu, les choses se compliquent puisque, comme nous l'avons précédemment rappelé, l'arrêt de la Cour condamne la conservation généralisée et indifférenciée des données de trafic et de localisation, hors adresses *IP*.

Or éclairé par l'instruction dynamique menée par votre 10e chambre, nous avons acquis l'intime conviction que la *disponibilité* des données de trafic et de localisation passées, sur une période suffisante, est, ou au moins est devenue, en l'état actuel des techniques, une condition nécessaire de l'effectivité de cette mission de l'État, donc une garantie du respect des objectifs de valeur constitutionnelle invoqués.

On ne peut certainement pas se satisfaire des deux catégories de données « sanctuarisées » par la Cour.

L'identification d'un utilisateur à partir d'un numéro de téléphone ou d'un autre identifiant est sans doute précieuse - elle représentait plus de 400 000 réquisitions en 2020 et environ deux tiers des accès en temps différé par les services de renseignement, en y incluant le recensement des numéros d'abonnement d'un utilisateur désigné. Mais l'utilisation de téléphones pré-payés ou à usage unique - les fameux « téléphones de guerre » - ou encore celle d'un nom d'emprunt ou d'un pseudonyme lors de l'ouverture de la ligne, la prive peu ou prou de son utilité, lorsqu'elle est prise isolément. Et elle ne permet ni la localisation, ni l'identification des contacts, ni la détermination d'une chronologie, pas plus que la connaissance des différentes cartes *SIM* utilisées dans un même appareil.

L'adresse IP (200), quant à elle, permet seulement de retracer des connexions à des sites internet. Et on sait que sa fiabilité est sujette à caution du fait de l'utilisation aisée des VPN ou d'autres méthodes de « brouillage » (201). Les services qui se sont exprimés lors de la séance orale d'instruction ont confirmé unanimement que cette information, à elle seule, était d'une faible valeur informationnelle.

Les autres données de connexion, si elles ne sont pas nécessairement décisives à elles seules, sont très souvent déterminantes, en combinaison les unes avec les autres et, le cas échéant, avec des éléments physiques, pour initier et orienter les recherches, corroborer ou infirmer des hypothèses et, le cas échéant, justifier la mise en oeuvre de techniques plus intrusives. Connaître les contacts téléphoniques et électroniques d'un suspect, réguliers ou au moment d'une infraction, peut permettre de mettre en évidence une bande organisée ou des complicités ; savoir qu'un suspect a guetté les allers et venues autour d'un pâté de maisons où il n'avait aucune raison particulière de se trouver et où des cambriolages ont été perpétrés est un élément précieux pour la conduite des investigations ; le bornage du même téléphone à des endroits où se sont produit des viols ou des agressions sexuelles est un indice clé. Il est toutefois important d'insister encore sur le fait qu'une donnée de connexion, quelle qu'elle soit, n'est pas nécessairement fiable lorsqu'elle est prise isolément ; c'est le croisement de plusieurs données qui peut offrir des certitudes, y compris en détectant l'existence de manoeuvres de contournement ou de dissimulation.

Il convient d'ajouter que ces données ne servent pas seulement à incriminer, mais aident aussi à disculper : il n'est pas rare qu'un suspect en mal d'alibi solide soit mis hors de cause grâce au bornage de son téléphone. Elles permettent aussi d'enquêter sur des disparitions inquiétantes indépendamment ou en amont de toute infraction.

Ces informations ne sont pas raisonnablement substituables. La criminalité et la délinquance laissent de moins en moins de traces physiques - et la cybercriminalité, aucune. En tout état de cause, le recours exclusif à des méthodes traditionnelles d'investigation nécessiteraient des moyens humains considérables que notre pays ne peut s'offrir dans les proportions qui seraient nécessaires pour compenser la perte de capacités opérationnelles enregistrées. En outre, il n'est pas certain qu'il y ait beaucoup à gagner, du point de vue des libertés, à un recours accru aux écoutes téléphoniques et aux autres interceptions de contenus, à la sonorisation de domiciles et à la pose de caméras. Du reste, l'efficacité des interceptions se réduit à mesure que se généralise le chiffrement de

bout en bout des échanges, en particulier sur les messageries instantanées comme *Whatsapp* et *Signal*. Quant à l'exploitation des données contenues dans les téléphones, que les requérants suggèrent à titre de solution de rechange, elle suppose que les équipements aient été saisis ou soient spontanément présentés, et que les données n'aient pas été effacées ou altérées.

Ces données de connexion ne sont pas simplement, pour reprendre les termes des requérants, une « aubaine technologique », pas plus que ne l'ont été les outils développés par la police technique et scientifique après l'interdiction du marquage au fer rouge des criminels en 1832, qui permettait d'identifier les récidivistes. Il en va de l'accès à ces données comme du développement de la photographie signalétique, de la dactylotechnie - l'étude des empreintes digitales - et, désormais, des analyses ADN. Il s'agit de répondre aux menaces du XXI^{e} siècle avec des outils du XXI^{e} siècle, pour satisfaire les exigences du corps social du XXI^{e} siècle. On peut apprécier le charme désuet des interrogatoires de l'inspecteur Columbo ou du commissaire Maigret, ou les improbables déductions de Sherlock Holmes à partir d'une trace de chaussure ou d'une enveloppe cachetée. Mais dans la vraie vie, les gens veulent qu'on mette les criminels hors d'état de nuire en exploitant les traces de chaussures et les enveloppes cachetées des temps modernes que sont ces données de connexion.

Nous serions bien en peine, il est vrai, de vous indiquer du haut de ce pupitre le seuil en deçà duquel le taux d'élucidation deviendrait socialement inacceptable. Pour les victimes elles-mêmes, c'est évidemment 100 %. Pour votre culture générale, ce taux s'élevait respectivement à 70 et 93 % pour la police et la gendarmerie en 2018, pour les seuls homicides. Nous nous bornerons modestement à relever, à titre d'élément de contexte un peu grossier, que le sentiment d'insécurité tend plutôt à croître qu'à se réduire, si l'on se réfère aux enquêtes d'opinion, et que le sentiment d'impunité ne semble pas en voie d'extinction. Les statistiques de la délinquance des dernières années sont particulièrement préoccupantes en ce qui concerne les atteintes aux personnes (202).

Au total, non seulement le dépérissement des preuves électroniques contrarierait *l'accoutumance des services* qui les utilisent, avec le risque redoutable d'une escalade dans les techniques utilisées, ou, pire, celui de rejeter certaines pratiques dans la clandestinité, et celle des juridictions de jugement, habituées à trouver ces éléments probants dans les dossiers - le gouvernement vous indique qu'elles exigent quasi-systématiquement désormais la production des données de localisation des suspects. Mais c'est aussi la *confiance des citoyens dans l'efficacité de ces autorités* qui en serait durement ébranlée.

Précisons bien qu'il ne s'agit pas, dans notre esprit, d'ériger la disponibilité des données de connexion au rang constitutionnel. On peut parfaitement imaginer que des évolutions technologiques relèguent cette technique d'investigation à l'arrière-plan. Le législateur peut aussi décider d'un équilibre différent en modifiant les conditions de recours à d'autres outils s'il estime qu'ils présentent un rapport bénéfices/risques plus favorable. Notre propos est de dire qu'en retirant sèchement et uniquement cette garantie, ici et maintenant, c'est le *mikado* pénal qui s'écroule.

Un argument fort peut troubler cette conviction. C'est celui du *droit comparé*. Sans doute la France n'est-elle pas isolée dans le concert européen, c'est un euphémisme. On l'a dit, plus de la moitié des États membres sont intervenus devant la Cour pour l'inviter à assouplir sa jurisprudence en raison de ses conséquences opérationnelles. Certains ont plaidé pour une obligation de conservation généralisée de l'ensemble des données, d'autres, avec la Commission, de certaines catégories de données jugées prioritaires. L'abstention des autres États est probablement moins le signe d'une indifférence qu'une marque de discrétion. L'Italie, par exemple, ne s'est pas manifestée, alors qu'elle s'est dotée de l'une des législations les plus dures du continent. Plusieurs États, dont l'Allemagne (203), la Finlande (204) et la Suède (205), ont entrepris de resserrer l'obligation de conservation, selon le cas, sur des finalités plus circonscrites, des catégories de données moins nombreuses et une durée de conservation plus courte, sans pour autant renoncer au principe de la conservation généralisée.

Cela étant, il existe bien des États membres où cette obligation de conservation générale a été supprimée. Le gouvernement mentionne la Roumanie, l'Autriche et les Pays-Bas. C'est aussi le cas en Slovénie. Par ailleurs, les

juridictions allemandes ne semblent pas se contenter du resserrement législatif opéré en 2017 ; c'est la raison pour laquelle votre homologue outre-Rhin a prudemment posé une nouvelle question préjudicielle à la Cour de justice. Or nous n'avons pas connaissance d'une explosion de la criminalité dans ces pays. Il vous est en outre indiqué par les requérants que les États-Unis n'auraient pas recours à une telle obligation, privilégiant le recueil des données spontanément conservées par les opérateurs.

Il reste que cet argument de droit comparé ne peut être manié qu'avec la plus grande précaution. Il supposerait une analyse d'ensemble des textes et surtout des pratiques, des opérateurs comme des services, permettant de vérifier que la levée de l'obligation n'a pas trouvé sa contrepartie dans des *gentleman agreements*, ou que les remèdes apportés ne sont pas pires que le mal, en particulier en termes d'intrusion dans la vie privée. Il faudrait aussi disposer d'une évaluation documentée de l'incidence de leur évolution sur l'activité des services. Le gouvernement vous indique ainsi que le service de sécurité suédois *Sapö* a publiquement déploré l'impact de ces restrictions sur ses capacités opérationnelles (206). Les Pays-Bas, où une juridiction de *district* a déclaré la loi contraire au droit de l'Union en 2015, ont de leur côté engagé une réflexion pour réintroduire une telle obligation de conservation généralisée, dont ils ont par ailleurs plaidé la nécessité devant la Cour de justice.

Les éléments fournis ne nous ont pas paru suffisants pour conférer à cet argument un caractère dirimant, en l'état.

Si vous nous suivez, il vous faudra encore rechercher si la jurisprudence de la Cour permet néanmoins d'assurer, d'une manière ou d'une autre, *cette nécessaire disponibilité des données* pour la lutte contre les infractions graves.

En premier lieu, l'instruction a fait clairement ressortir *l'impossibilité de s'en remettre à la conservation volontaire des données de connexion par les opérateurs pour leurs besoins propres* :

- d'une part, *il ne s'agit pas exactement des mêmes données ni de la même durée de conservation*. Les opérateurs télécom ne conservent pas, ou très peu de temps, les données de localisation (207), qui présentent rarement un intérêt pour la facturation, les données relatives aux appels reçus, qu'on ne paye pas, et celles, de plus en plus nombreuses en proportion, relatives aux appels sortants entrant intégralement dans des forfaits illimités - puisqu'ils sont sans incidence sur le montant de la facture. Les quatre derniers numéros des personnes appelées ne sont normalement conservés qu'à la demande expresse du client, en vertu de l'article D. 98-5 du CPCE (208). Le numéro de téléphone de l'émetteur des appels reçus par l'abonné, ainsi que les numéros IMEI et IMSI qui permettent d'identifier respectivement le téléphone et la carte *SIM* utilisés, ne sont stockés que quelques jours à un mois pour la résolution des incidents. S'agissant des fournisseurs d'accès à internet, qui se rémunèrent principalement par un abonnement forfaitaire, les données techniques sont rarement nécessaires aux opérations commerciales, et certaines d'entre elles peuvent être conservées pour l'analyse de la qualité de service et les opérations de sécurité des réseaux, pour une durée inférieure à trois mois, et qui est en pratique plus courte. Un régime de conservation purement volontaire aurait donc un impact opérationnel lourd, et même dirimant pour des infractions occultes ou révélées tardivement ;

- d'autre part, la disponibilité de ces données est largement *tributaire de la politique commerciale de chaque entreprise*. Un opérateur peut parfaitement souhaiter valoriser, sur le plan marketing, des pratiques d'effacement rapide pour s'afficher comme le meilleur défenseur de la vie privée de ses clients. La présence de *Free* parmi les requérants et la différence de tonalité des observations présentées par la fédération française des télécoms montrent que les positionnements commerciaux ne sont pas alignés, laissant augurer des angles morts affectant la complétude des informations et privant potentiellement d'intérêt les réquisitions, qui sont souvent adressées à tous les opérateurs. C'est précisément et explicitement pour s'affranchir de cette dépendance aux pratiques commerciales des fournisseurs d'accès et opérateurs télécom que le législateur est intervenu il y a vingt ans ;

- enfin, l'instruction a fait ressortir que les données stockées dans les entrepôts dédiés aux réquisitions font

l'objet d'un *formatage et de traitements techniques* selon des modalités convenues avec l'État pour les rendre plus rapidement et plus facilement exploitables par les autorités accédantes, moyennant compensation financière. Ce n'est pas le cas des données brutes conservées pour les besoins propres des opérateurs. Il est évident que l'ergonomie et la rapidité du recueil, comme l'exploitabilité des données fournies, sont des conditions essentielles de l'efficacité opérationnelle des services d'enquête compte tenu de leurs moyens et de leurs contraintes de fonctionnement.

En deuxième lieu, l'idée de *conservation ciblée* par zones géographiques ou catégories de personnes préalablement identifiées procède, il faut le dire, d'une conception purement théorique du principe de proportionnalité, sans grand rapport avec la réalité opérationnelle.

L'instruction, y compris d'ailleurs les propres observations de *Free*, fait ressortir *l'impossibilité technique de procéder à un ciblage géographique fiable de la conservation*, en particulier sur des sites sensibles comme ceux que cite la Cour. L'internet et la téléphonie fixe, *via* une *box*, ne sont localisables qu'avec l'adresse *IP* ; or on a vu qu'il était possible, avec des VPN, de simuler des connexions à distance, de là où se trouvent les serveurs utilisés. Quant à la téléphonie mobile, elle fonctionne grâce à des relais qui couvrent, selon la densité du maillage, quelques centaines de mètres en zone urbaine et quelques dizaines de kilomètres en zone rurale. Certains aléas peuvent en outre conduire le téléphone à « borner » sur une antenne plus éloignée mais sans obstacle intercalaire : c'est la raison pour laquelle, sans le savoir, vous pouvez solliciter deux antennes situées à plusieurs centaines de mètres de distance en faisant quelques pas dans votre appartement. Le gouvernement vous précise de surcroît, sans être contredit, que, pour des raisons techniques, les seules données de connexion qui seraient nécessairement conservées sont celles qui se rapportent à des communications intégralement réalisées dans la zone « surveillée ». *Free* ajoute, au surplus, qu'elle réalise des opérations de réseau conduisant à modifier aléatoirement les identifiants des antennes-relais, les « cellules », ce qui empêcherait toute traçabilité géographique des données de connexion.

À l'impasse technique s'ajoute *l'inanité opérationnelle*. La criminalité et la délinquance ne sont pas pré-localisables - après tout, on a même trouvé des djihadistes à Lunel, dans l'Hérault. Ces menaces sont au contraire diffuses et potentiellement omniprésentes. Il est d'ailleurs assez fréquent qu'une réquisition porte sur l'ensemble du territoire national. Les malfaiteurs, quant à eux, s'adapteraient rapidement à ce zonage prévisible, façon « chat perché ». Ajoutons qu'il ne serait guère acceptable, moralement sinon juridiquement, de justifier la conservation des données de personnes par le seul fait qu'elles résident dans des zones caractérisées par une plus forte criminalité ou une plus forte délinquance.

Le *ciblage personnel* est lui aussi problématique sur un plan technique, s'il est question d'obliger les opérateurs à conserver les données de catégories de personnes définies selon des critères généraux qu'ils ne peuvent mettre en oeuvre. Les données de trafic et de localisation ne disent rien, par elles-mêmes, de la dangerosité d'une personne. Le seul dispositif envisageable techniquement semble être celui dans lequel l'État fournirait lui-même la liste des individus dont les données doivent être conservées. Encore faudrait-il établir cette liste sur la base de critères non discriminatoires. On songe, par exemple, aux personnes fichées S ou aux multi-récidivistes. Mais on se heurterait là encore à la réalité opérationnelle : d'une part, il sera aisé pour les plus avisés, en particulier les personnes qui pensent être surveillées, de dissimuler leur identité ou de changer d'équipement ou de carte *SIM*. Un tel subterfuge ne peut être démasqué qu'en disposant justement d'autres données de connexion, qui n'auront pas été conservées sous le même nom ; d'autre part, au-delà des « *usual suspects* » défavorablement connus des services, ces derniers sont dans l'impossibilité logique d'identifier par avance les personnes qui sont susceptibles de passer à l'acte, en tous les cas jusqu'à ce que notre monde ressemble à l'univers de *Minority Report*. Il n'y aura alors plus même besoin de données de connexion pour arrêter ceux dont on sait par avance qu'ils vont commettre un méfait.

Enfin, nous sommes, pour notre part, très circonspect, et même inquiet, à l'idée qu'une liste complète des sites géographiques et des personnes « sous surveillance » puisse être ainsi partagée avec les opérateurs. L'accès au coup par coup dans une vaste base de données indifférenciée est nettement moins révélateur de la doctrine de

renseignement ou d'investigation et limite le risque d'un usage abusif d'informations sensibles, voire classifiées, par les agents des opérateurs.

En troisième et dernier lieu, en lui-même, le *gel des données via* le dispositif de « conservation rapide » n'est, par construction, efficace que pour les données qui existent encore ou seront ultérieurement produites. Il est utile pour remonter une filière à partir de l'identification d'un suspect. Mais l'absence d'antériorité le rend quasiment inutile pour élucider des infractions passées.

Pris isolément comme globalement, ces outils ne garantissent pas la nécessaire disponibilité des données de connexion aux fins d'assurer la sauvegarde de l'ordre public et la recherche des auteurs d'infractions.

***

VII. - À bien y regarder, nous pensons toutefois qu'il y a place pour construire un dispositif viable et aussi respectueux que possible des exigences de la Cour, en combinant les différentes souplesses offertes par l'arrêt, avec l'audace interprétative qui nous caractérise aujourd'hui.

Si vous admettez que l'État puisse légalement enjoindre aux opérateurs de conserver de manière généralisée et indifférenciée l'ensemble des données de connexion pour les besoins de la sauvegarde de la sécurité nationale, alors les données dont les services d'enquête ont besoin existeront. Cette existence est, bien entendu, la première condition de leur disponibilité.

Elle ne se suffit toutefois pas à elle-même. Car, comme on l'a dit, la jurisprudence de la Cour exclut qu'on puisse y accéder directement à des fins de lutte contre la criminalité grave, conformément à la règle de concordance. L'entrepôt de données est là, mais sa porte ne s'ouvre qu'à ceux pour qui il a été constitué. Toutefois, l'arrêt du 6 octobre 2020 n'exclut pas, et même envisage à notre avis, que la conservation rapide à des fins de lutte contre la criminalité grave puisse se greffer sur ce lac de données « sécurité nationale ». Elle indique en effet au point 164 de l'arrêt du 6 octobre que la finalité de la conservation rapide doit être précisée dans la loi « dans la mesure où [elle] ne correspond plus à celles pour lesquelles les données ont été collectées et conservées initialement ». Elle semble ainsi admettre une forme de « déclassement » du motif de conservation, qui apparaît justifié dès l'instant que la conservation rapide n'est pas elle-même généralisée et indifférenciée, mais porte sur des personnes ou des infractions bien identifiées - c'est la logique du bassin de rétention. Ainsi articulée avec le régime de conservation pour les besoins de la sécurité nationale, la conservation rapide pourra porter non seulement sur les données futures, mais aussi sur les données passées, avec la même profondeur d'un an, et avec le champ d'application large admis par la Cour qui permet de geler les données des suspects, des victimes ou des tiers dès l'instant qu'elles peuvent contribuer à l'élucidation de l'infraction, mais aussi de sanctuariser les données se rapportant à telle ou telle zone géographique - par exemple la liste des numéros de téléphone ayant « borné » dans un secteur.

Deux objections viennent immédiatement aux esprits critiques :

- la première, d'ordre opérationnel, c'est la *précarité* d'une telle solution. Elle n'est viable que s'il y a eu injonction de conserver au titre de la sécurité nationale et que cette injonction est légale, donc qu'il y ait une menace grave pour la sécurité nationale. Mais nous vous proposons de l'assumer et de l'intégrer à votre raisonnement en jugeant que les objectifs de valeur constitutionnelle ne sont pas privés des garanties nécessaires pour autant que et aussi longtemps que ces conditions sont remplies. Ce serait votre jurisprudence *Solange* à vous. Il y aura matière à réexamen des obligations pesant sur les autorités nationales le jour où le lac de données « sécurité nationale » sera asséché, c'est-à-dire que plus aucune menace grave ne pèsera sur la sécurité nationale de la France - avec tout l'optimisme qui nous caractérise, nous ne serons sans doute plus de ce monde. Plus vraisemblablement, la directive *e-privacy* sera remplacée d'ici quelques mois ou années par un règlement dont le projet a fait l'objet d'un accord au sein du Conseil en février dernier, après de laborieuses négociations. Son article 2 prévoit, comme à notre avis la jurisprudence de la Cour l'autorise (209), l'exclusion

pure et simple des traitements réalisés par les opérateurs à la demande des autorités publiques à des fins de sauvegarde de la sécurité nationale. Il est donc fort possible que la question de l'existence des données ne se pose plus d'ici quelques temps et que le gouvernement ne soit donc plus contraint d'édicter un décret annuel pour enjoindre aux opérateurs de conserver les données à cette fin (210). Cette objection pourrait donc tomber d'elle-même.

- la seconde objection, c'est *l'artificialité* de cette solution. Elle est double :

> d'abord, elle subordonne à l'existence d'une menace pour la sécurité nationale l'efficacité de la lutte contre la criminalité grave quelle qu'elle soit, y compris des meurtres de droit commun. Mais il ne faut pas oublier que, par-delà les catégories que la Cour de justice a cru devoir identifier, il existe souvent un continuum opérationnel entre elles, entre les individus du « bas du spectre » et du « haut du spectre », entre le terrorisme et la délinquance et la criminalité organisées qui le financent ou avec lequel elle entretient les liens les plus divers. Dès lors qu'il n'y a pas nécessairement d'étanchéité et d'indépendance opérationnelles, il n'y a rien d'excessivement choquant à créer un lien de dépendance juridique ;

> la seconde incongruité apparente tient à ce que l'ingérence particulièrement grave que constitue l'obligation de conservation généralisée et indifférenciée est consommée de toute façon, à partir du moment où les données sont stockées quelque part. On ne voit pas en quoi la possibilité d'accès direct ouverte à l'autorité judiciaire pour la lutte contre la criminalité grave l'aggraverait et ce qu'apporterait de ce point de vue la conservation rapide, à la différence de l'accès immédiat. Mais c'est la logique du raisonnement de la Cour. Et nous voyons tout de même un *intérêt opérationnel* à ce détour par la conservation rapide. Elle permet de loger la procédure de contrôle préalable pour l'accès aux données par ailleurs exigée par la jurisprudence européenne, sans risque de dépérissement des preuves. Au lieu d'accéder directement aux données, les services peuvent demander aux opérateurs de surseoir à leur effacement, le temps d'obtenir le feu vert de l'autorité compétente pour les recueillir. Ce régime de conservation rapide n'est donc pas une complication inutile ou une manoeuvre de contournement de l'interdiction de la conservation généralisée : c'est, à notre avis, le dispositif pertinent pour concilier au mieux les exigences en présence.

Nous pensons qu'ainsi interprétée et en l'état de la menace pesant sur la France, la jurisprudence de la Cour ne prive pas de garantie les objectifs de valeur constitutionnelle invoqués. Si, toutefois, vous estimiez ce détour par la conservation rapide impossible ou vain, nous vous inviterions à titre subsidiaire à activer la clause de sauvegarde afin de préserver la conservation généralisée et indifférenciée des données de connexion aux fins de lutte contre la criminalité grave.

Précisons que ce régime devrait aussi s'appliquer aux services de renseignement si vous décidiez que certaines des finalités mentionnées à l'article L. 811-3 ne relèvent pas de la sécurité nationale, mais « seulement » de la prévention des menaces graves contre la sécurité publique.

***

VIII. - Le dernier moyen relatif à la conservation reproche aux dispositions législatives de l'autoriser pour des *personnes bénéficiant d'un « secret professionnel »*. Dans son arrêt *Digital Rights Ireland*, la Cour de justice avait formulé le même reproche à l'endroit de la directive de 2006 qu'elle a invalidée (pt 58). Nous ne pensons pas qu'il faille et qu'on puisse en déduire que cette conservation serait proscrite par principe, alors surtout qu'elle ne porte, en elle-même, aucune atteinte au secret professionnel, mais se borne à la rendre possible matériellement. Une telle interdiction serait difficilement praticable car elle supposerait de tenir à jour en permanence une liste des personnes protégées dont les opérateurs devraient s'abstenir de stocker les données de connexion. Et elle serait surtout inacceptable parce qu'il est évidemment impossible d'opérer le départ, au stade de la conservation, entre celles des données de ces personnes qui sont couvertes par ce secret, parce qu'elles s'inscrivent dans l'exercice de leurs fonctions « protégées », et les autres, et parce qu'on ne voit pas pourquoi on reconnaîtrait aux intéressés une forme d'immunité numérique, alors qu'elles peuvent parfaitement se livrer à

des agissements répréhensibles.

C'est dans l'accès que leur protection a vocation à être opposée. C'est précisément ce à quoi procède l'article L. 821-7 du code de la sécurité intérieure, pour certaines catégories de personnes particulièrement protégées : les parlementaires, les magistrats, les avocats et les journalistes ne peuvent faire l'objet d'une technique de renseignement à raison de l'exercice de leur mandat ou de leur profession. En-dehors de celles-ci, il est prévu que la CNCTR, qui doit obligatoirement être consultée préalablement à toute mise en oeuvre, même en cas d'urgence absolue, se réunit en formation plénière pour examiner la demande, et qu'elle assure un contrôle étroit et systématique de la transcription des renseignements collectés. Nous n'identifions donc aucune difficulté.

***

IX. - *Il nous faut à présent vous entretenir des questions situées en aval de la conservation des données*. Nous commencerons par les griefs communs aux quatre techniques de renseignement en litige, puis nous aborderons la question spécifique du champ d'application des deux techniques de recueil de données en temps réel, avant de nous pencher sur la technique dite de l'algorithme.

1° La première question commune est aussi la plus problématique. On l'a dit : contrairement à la Cour européenne des droits de l'homme, en l'état de sa jurisprudence, la Cour de justice a posé en principe que tout accès aux données de connexion, en temps différé comme en temps réel, devait être précédé d'un *contrôle préalable* d'une juridiction ou d'une autorité administrative indépendante dotée d'un pouvoir contraignant. Il n'en va différemment qu'en cas d'urgence dûment justifiée, auquel cas le contrôle doit intervenir à bref délai.

Or la procédure organisée par le code de la sécurité intérieure ne répond pas complètement à ces exigences.

En principe, la CNCTR est systématiquement saisie des demandes de mise en oeuvre des techniques de renseignement. Elle n'émet qu'un avis simple. Si le Premier ministre passe outre un avis défavorable de la Commission, cette dernière peut saisir la formation spécialisée du Conseil d'État en vue de faire annuler l'autorisation et ordonner la destruction des renseignements irrégulièrement collectés (211). Plus largement, la Commission, qui dispose d'un accès permanent, complet et direct à l'ensemble des données collectées, peut, à tout moment, adresser au Premier ministre une recommandation tendant à l'interruption de la mise en oeuvre d'une technique (art. L. 833-6). Là encore, la formation spécialisée peut être saisie d'un refus d'obtempérer du Premier ministre.

En cas d'urgence absolue et uniquement pour les finalités mentionnées à l'article L. 821-5, notamment la prévention du terrorisme, le Premier ministre peut autoriser immédiatement la mise en oeuvre d'une technique, à charge pour lui d'en saisir *a posteriori* la CNCTR qui pourra lui enjoindre d'y mettre fin dans les mêmes conditions.

L'ensemble de ce régime ne soulève pas de difficulté en cas d'urgence dûment justifiée au sens de la jurisprudence de la Cour - qu'il s'agisse d'un cas d'urgence absolue visé à l'article L. 821-5 ou d'une urgence « simple » - puisqu'un contrôle *a posteriori* est possible à l'initiative de la Commission. Dès l'instant qu'elle est en désaccord avec la position du Premier ministre, il lui revient d'en saisir immédiatement la formation spécialisée, et il appartient à cette dernière de statuer dans les plus brefs délais, afin de se conformer aux exigences posées par la Cour.

En revanche, en l'absence d'urgence, le contrôle n'est pas préalable puisque rien n'empêche que l'accès intervienne avant même que la Commission ait pu saisir le Conseil d'État et, *a fortiori*, avant que ce dernier se soit prononcé.

Les exigences du droit de l'Union sur ce point ne contreviennent pas aux objectifs de valeur constitutionnelle

invoquées. Le législateur peut parfaitement organiser la procédure pour prévoir un contrôle préalable hors urgence, soit en dotant la CNCTR d'un pouvoir d'avis conforme (212), soit en prévoyant qu'en cas de passé-outre un avis défavorable, la technique ne peut être effectivement mise en oeuvre avant que le contentieux devant la formation spécialisée soit purgé.

Cette difficulté concerne non seulement les trois techniques consistant en un accès direct aux données, mais aussi celle de l'algorithme en tant qu'elle prévoit, au IV de l'article L. 851-3, la possibilité d'un recueil des données ayant donné lieu à une alerte, pour vérification, dans les mêmes conditions que pour l'accès direct aux données de connexion conservées.

Les deux décrets restant en litige sont donc illégaux sur ce point (213).

2° S'agissant des *personnes susceptibles d'accéder aux données de connexion*, l'arrêt *Digital Rights Ireland* dont se prévalent les requérants s'est borné à reprocher à la directive de 2006 de ne pas avoir fixé de critère objectif permettant de limiter au strict nécessaire le nombre de personnes disposant d'une autorisation d'accès et de réutilisation.

Or il résulte de l'article L. 811-4 du CSI et des dispositions réglementaires attaquées que, d'une part, chacune des techniques ne peut être mise en oeuvre que par les services expressément autorisés à le faire, et seulement pour les finalités limitativement énumérées ; d'autre part, au sein de chacun de ces services, seuls les agents individuellement désignés et habilités par le ministre ou, par délégation, par le directeur dont ils relèvent, peuvent y procéder. Enfin, le principe de proportionnalité rappelé par l'article L. 801-1 du même code impose de limiter le nombre d'habilitations au strict nécessaire, ce que vous pourriez opportunément rappeler : il ne saurait évidemment être question d'habiliter l'ensemble du personnel de la DGSI ou de la DGSE. Dans ces conditions, les articles 7 et 8 de la Charte des droits fondamentaux ne sont pas méconnus.

3° En ce qui concerne *l'information des personnes* dont les données de connexion sont recueillies, la Cour l'a exigée au nom du droit au recours, dans l'arrêt *Télé2*, « dès le moment où cette communication n'est pas susceptible de compromettre les enquêtes » (214). Vos chambres réunies l'ont invitée à réexaminer ce point en tenant compte des possibilités de recours devant la formation spécialisée du Conseil d'État. La Cour n'a répondu que pour l'accès en temps réel. Mais sa réponse est sans doute de portée générale, et elle témoigne discrètement d'un assouplissement puisque cette information ne doit intervenir, comme on l'a dit, que « pour autant et dès le moment où cette communication n'est pas susceptible de compromettre les missions qui incombent » aux autorités. Elle envisage donc expressément l'éventualité que cette information n'intervienne jamais (215).

Ces exigences nous paraissent respectées par le droit interne. Le V de l'article 32 de la loi du 6 janvier 1978 applicable à la date des décrets attaqués, dont les dispositions sont désormais reprises en substance à son article 116, écarte l'obligation d'information pour les traitements mis en oeuvre pour le compte de l'État et intéressant la sûreté de l'État et la sécurité publique, *dans la mesure où une telle limitation est nécessaire au respect des fins poursuivies par le traitement*. On ne peut rien reprocher à la loi, ni au décret. Il appartient aux services de respecter l'obligation d'information pesant sur eux, pour autant qu'elle ne met pas en péril leur action. En pratique, il est vraisemblable que cette nécessité ne cèdera que dans des cas marginaux : on peut songer aux erreurs sur la personne ou aux « fausses alertes » issues de l'algorithme. Il est légitime, dans ce cas, que la personne concernée sache que ses données de connexion ont été recueillies et s'assure qu'elles ne sont plus traitées.

Pour le surplus, c'est-à-dire dans tous les cas où les services sont soustraits à toute obligation d'information spontanée des personnes concernées, le droit au recours est garanti par la possibilité offerte à ces dernières de présenter à la CNCTR une demande tendant à la vérification qu'aucune technique de renseignement n'est irrégulièrement mise en oeuvre à son égard et, si elle n'en est pas satisfaite, de saisir la formation spécialisée du Conseil d'État (216).

4° Les requérants, se plaçant là encore sur le terrain de la contrariété au droit de l'Union, mettent enfin en cause la *durée de quatre ans pendant laquelle les services de renseignement peuvent conserver les données* recueillies auprès des opérateurs, en vertu de l'article L. 822-2 du CSI. Mais ce traitement de données subséquent, totalement étranger à l'activité des opérateurs, relève du cadre juridique afférent à sa finalité propre. Or les traitements de données mises en oeuvre par les services de renseignement, dont les activités relèvent de la sauvegarde de la sécurité nationale, échappent au champ d'application du droit de l'Union, comme le rappellent clairement le paragraphe 2 de l'article 2 du RGPD, éclairé par son considérant 16, et le paragraphe 3 de l'article 2 de la directive police-justice, éclairée par son considérant 14. Ils sont régis par le titre IV de la loi du 6 janvier 1978, comme tous les traitements « intéressant la sûreté de l'État et la défense ». Le moyen est donc inopérant.

5° Vous pourrez opposer la même réponse aux moyens tirés de *l'absence de contrôle préalable sur l'exploitation des données par les services de renseignement et sur les transferts de ces données à l'étranger*, qui se situent en aval et ne sont pas régis par le droit de l'Union.

***

X. - *Nous en venons à une problématique propre aux deux techniques d'accès en temps réel, qui touche à leur champ d'application*. Qu'il s'agisse de la géolocalisation en temps réel, c'est-à-dire de l'accès aux seules données de localisation des équipements, ou de l'accès en temps réel à l'ensemble des données de connexion, c'est-à-dire tant aux données de trafic qu'aux données de localisation, la Cour n'en a admis le principe qu'à condition qu'elles soient limitées aux personnes « à l'égard desquelles il existe une raison valable de soupçonner qu'elles sont impliquées d'une manière ou d'une autre dans des activités de terrorisme ».

1° En ce qui concerne la seconde technique, tel était assurément le cas dans la version initiale de l'article L. 851-2, en vigueur à la date des décrets attaqués, puisque l'accès était circonscrit aux données des personnes préalablement identifiées comme présentant une menace terroriste.

Mais les requérants relèvent que cet article a été modifié postérieurement pour étendre l'accès aux données « lorsqu'il existe des raisons sérieuses de penser qu'une ou plusieurs personnes appartenant à l'entourage de la personne concernée par l'autorisation sont susceptibles de fournir des informations au titre de la finalité qui motive l'autorisation ».

Cette modification (217) a été faite en deux temps :

- une loi du 21 juillet 2016 avait prévu cette extension, mais à la suite d'une question prioritaire de constitutionnalité soulevée par les mêmes requérants à l'appui d'une contestation du refus d'abroger le décret n° 2016-67 qu'ils avaient par ailleurs suscité (218), le Conseil constitutionnel a censuré ces dispositions au motif que la technique pouvait porter sur un nombre élevé de personnes, sans que leur lien avec la menace soit nécessairement étroit, faute pour le législateur d'avoir prévu que le nombre d'autorisations simultanément en vigueur devrait être limité (219) ;

- une loi du 30 octobre 2017 en a tiré les conséquences en réintroduisant cette extension, assortie d'un contingentement des autorisations susceptibles d'être simultanément délivrées.

À office inchangé, vous n'êtes pas tenu de vous prononcer sur la conformité au droit de l'Union de cette extension postérieure aux décrets attaqués, bien que la Cour ait cru devoir citer l'article L. 851-2 en vigueur. Vous pourriez toutefois souhaiter éclairer le gouvernement sur ce point alors qu'un projet de loi relatif au renseignement est en cours d'élaboration, qui pourrait d'ailleurs étendre le champ des données susceptibles d'être recueillies en temps réel.

Sauf à vous imposer un délibéré façon « nuit du droit », nous ne pouvons pas décemment vous exposer aussi

longuement qu'il le faudrait les raisons pour lesquelles nous pensons que vous pourriez faire évoluer votre office sur ce point. Disons simplement qu'aucun obstacle de principe ne s'oppose à nos yeux à ce que vous transposiez, en l'enrichissant, le raisonnement de la décision *Stassen* de vos 2e et 7e chambres réunies du 28 février 2020 (220) au contentieux du recours en excès de pouvoir contre un décret. Vous pourriez admettre que le requérant puisse demander et obtenir, à défaut de l'annulation *ab initio*, son abrogation à partir de la date de votre décision et même son annulation à compter d'une date postérieure à son édiction, si le décret est devenu illégal à compter de cette date. On pourrait d'ailleurs imaginer, en sens inverse, que l'annulation pour un motif de fond (221) soit circonscrite à la période antérieure à sa « régularisation », par une forme d'application automatique de la jurisprudence *AC !* En l'occurrence, il serait aisé de déceler de telles conclusions dans les écritures dont vous êtes saisis, à partir du moment où les requérants articulent un moyen invoquant précisément la nouvelle version de l'article L. 851-2.

Plus modestement, et sans rien changer à votre office, vous pourriez recourir ici à un *obiter dictum*, qui ne serait pas du tout inédit dans votre jurisprudence (222), si vous souhaitiez éclairer les parties prenantes quant à la conformité au droit de l'Union de ce dispositif.

À la lumière des objectifs de valeur constitutionnelle invoqués, nous n'interprétons pas l'arrêt de la Cour comme exigeant de démontrer que la personne visée soit impliquée personnellement et directement dans une organisation ou une démarche terroriste - bref, qu'elle constitue elle-même une menace. Le point 189 de son arrêt tempère d'ailleurs l'idée d'implication en énonçant que « seules peuvent être concernées les personnes présentant un lien avec l'objectif de prévention du terrorisme ». Vous pourriez reprendre la condition posée par le Conseil constitutionnel en 2017, lorsqu'il a fixé les limites de ce dispositif, selon laquelle seules les personnes présentant un « lien étroit » avec un individu représentant une menace terroriste peuvent faire l'objet de cette technique (223). Le contingentement des autorisations, que le Conseil a estimé indispensable pour assurer le respect de la Constitution, constitue un puissant facteur de régulation à cet égard. À partir du moment où ce lien étroit est caractérisé, on peut considérer qu'il y a une forme d'implication au sens où l'entend la Cour (224). Et dans la mesure où la surveillance doit cesser dès l'instant qu'elle n'est pas indispensable au suivi de la cible, l'ingérence ne nous semble pas disproportionnée.

2° L'effort de lecture est plus grand pour ce qui concerne la *géolocalisation en temps réel* (225).

Une précision technique liminaire : il ne s'agit plus seulement du bornage du téléphone, dont on a vu la relative imprécision, mais aussi de l'exploitation des coordonnées GPS transmises *via* le réseau satellitaire par les applications installées sur le terminal. Concrètement, cette technique permet de suivre un point sur une carte, avec une précision de l'ordre d'une dizaine de mètres (226).

La Cour s'est manifestement méprise en indiquant que cette technique était limitée à la prévention du terrorisme en droit français (227), c'est-à-dire en alignant le champ d'application de l'article L. 851-4 sur celui de l'article L. 851-2. Près des deux tiers des demandes de mise en oeuvre de cette technique, qui ne cesse de monter en puissance (228), sont étrangères au terrorisme, et portent en particulier sur la criminalité et la délinquance organisées et sur la prévention des violences collectives. Vous observerez d'ailleurs que le recours à cette technique n'est pas contingenté, contrairement à l'accès en temps réel aux données de connexion. Au-delà, la géolocalisation en temps réel est aussi utilisée abondamment par l'autorité judiciaire. L'article 230-32 du code de procédure pénale l'autorise dans son principe pour toute enquête ou instruction portant sur un crime ou un délit puni d'au moins trois ans d'emprisonnement. Ce régime, précisons-le, est loin d'être propre à la France (229).

Nous ne pouvons croire que la Cour a entendu condamner l'usage de cette technique d'investigation devenue extrêmement courante, en-dehors des affaires de terrorisme. Elle est certes plus attentatoire aux libertés que la bonne vieille filature physique, et comparable à celle de la pose d'une balise. Mais elle reste moins intrusive qu'une interception téléphonique, comme l'a expressément jugé la Cour européenne des droits de l'homme qui n'a jamais circonscrit son périmètre autorisé au terrorisme (230).

La première option est de lire l'arrêt comme n'ayant pas entendu limiter cette technique à la prévention du terrorisme, mais seulement comme exigeant qu'elle ne soit mise en oeuvre, en matière de terrorisme, qu'à l'égard des personnes impliquées dans de telles activités. Le raisonnement serait ainsi transposable aux autres cas d'usage : la géolocalisation en temps réel serait possible à l'égard des personnes impliquées dans des activités de criminalité organisée, mais pas pour les contacts occasionnels de bandits de grand chemin. Nous vous proposons cette lecture à titre principal car nous ne comprenons pas ce qui, dans la directive *e-privacy* ou le RGPD, permettrait de justifier une restriction au terrorisme.

La seconde option, plus pure mais moins diplomatique, consiste à prendre la Cour aux mots et à activer la clause de sauvegarde, ce qui s'imposerait ici compte tenu des conséquences majeures qui s'attacheraient à l'impossibilité pour les services de renseignement de suivre le parcours de gros bonnets de la drogue autrement qu'en posant un mouchard sur leur voiture ou en dépêchant des équipes de surveillance physique, à leurs risques et périls d'ailleurs. Plus encore, par effet de rebond, on ne pourrait qu'être préoccupé de l'incapacité ou de l'extrême difficulté dans laquelle se trouveraient les services d'enquêtes de retrouver et de suivre à la trace des cambrioleurs en série, des fugitifs ou des kidnappeurs d'enfants.

***

. - Nous terminons l'examen de fond par les moyens spécifiques à la *technique de l'algorithme*, qui sort largement indemne de l'examen luxembourgeois.

Ce régime est prévu à l'article L. 851-3 du CSI, à titre expérimental. Le gouvernement a toutefois annoncé son intention de le pérenniser. Il consiste en une analyse automatisée massive du flux de données de connexion permettant de détecter le plus précocement possible des signaux de faible intensité susceptibles de révéler une menace terroriste, dans un contexte marqué par la très forte augmentation du nombre d'« objectifs » à surveiller, la rapidité croissante du passage à l'acte et des moyens d'analyse humains comptés. Les traitements que les opérateurs sont tenus de mettre en oeuvre à ce titre, sur la base du paramétrage défini par les services de renseignement en fonction des techniques et comportements observés de manière récurrente chez les auteurs d'actes terroristes, ne peuvent permettre par eux-mêmes l'identification des personnes. Selon le IV de l'article L. 851-3, une autorisation spécifique est nécessaire pour lever l'anonymat et recueillir les données pertinentes, qui doivent être détruites sous soixante jours si elles ne contiennent pas d'éléments sérieux confirmant l'existence d'une menace terroriste.

Tout en y voyant une ingérence « particulièrement grave » dans les droits fondamentaux, la Cour admet le principe de ce dispositif sous réserve du respect de quatre conditions :

- il doit être prévu et défini dans sa portée par la loi ;

- il doit exister une menace grave pesant sur la sécurité nationale et la durée du traitement (231) doit être limitée au strict nécessaire, comme l'injonction de conservation généralisée aux mêmes fins ;

- la mise en oeuvre de la technique doit faire l'objet d'un contrôle juridictionnel, qui n'est pas nécessairement préalable ;

- enfin, cette technique doit être entourée de garanties matérielles et procédurales permettant d'assurer le respect du principe de proportionnalité, notamment la définition de modèles et critères spécifiques, fiables, non discriminatoires, ne reposant pas exclusivement sur des données dites « sensibles », et un réexamen régulier de ces modèles et critères comme des bases de données utilisées.

Ces conditions sont remplies, moyennant une interprétation du I de l'article L. 851-3 conforme au droit de l'Union.

La mise en oeuvre de cette technique est obligatoirement précédée d'un avis de la CNCTR qui doit s'assurer, d'une part, de l'existence d'une menace grave pour la sécurité nationale la justifiant et, d'autre part, de la licéité et de la qualité de l'algorithme lui-même, notamment au regard des exigences posées par la Cour. La Commission peut saisir le Conseil d'État si le Premier ministre passe outre un avis défavorable. En outre, par dérogation au droit commun, la durée de l'autorisation initiale est limitée à deux mois, et non quatre. Le renouvellement suppose de présenter une nouvelle demande, qui doit exposer les raisons pour lesquelles il est justifié et comporter un relevé du nombre d'identifiants signalés par le traitement automatisé et une analyse de la pertinence de ces signalements. Le renouvellement est soumis à la même procédure de contrôle, *via* la CNCTR. Cette dernière dispose d'un accès permanent aux bases de données utilisées et elle est donc en mesure de s'assurer de leur fiabilité et de leur actualité. L'ensemble de ces garanties avait convaincu le Conseil constitutionnel de ne pas censurer cette technique en 2015.

Le I de l'article L. 851-3 nous paraît donc à l'abri du reproche d'inconventionnalité, de même que le décret de 2016, qui seul y fait référence, d'ailleurs fugacement. Il n'avait pas à en dire plus, étant précisé que les règles générales de mise en oeuvre ont été fixées par le Premier ministre dans une décision classifiée du 27 avril 2017 reprenant l'ensemble des observations formulées par la CNCTR, selon le rapport parlementaire d'information sur le bilan de la loi renseignement de 2015.

Au final, comme nous l'avons dit, le seul reproche qu'on peut adresser à la technique de l'algorithme porte sur l'absence de contrôle préalable au recueil de données de connexion nominatives, prévue au IV de l'article L. 851-3.

***

. - Si vous nous avez suivi dans ce parcours de bosses, sinon du combattant, il vous faudra prononcer les annulations suivantes :

- d'une part, celle du refus d'abroger le I de l'article R. 10-13 du CPCE et les 1° et 2° de l'article 1er du décret du 25 février 2011 en tant, d'une part, qu'ils permettent la mise en oeuvre de l'obligation de conservation généralisée et indifférenciée des données relatives au trafic, à l'exclusion de l'adresse *IP* attribuée à la source de chaque connexion, et des données de localisation, pour des motifs autres que la sauvegarde de la sécurité nationale et, d'autre part, en tant qu'ils prévoient une telle obligation pour ce dernier motif sans limite de temps, donc sans examen périodique de l'existence d'une menace grave, actuelle ou prévisible, pour la sécurité nationale ;

- d'autre part, l'annulation des décrets du 11 décembre 2015 et du 29 janvier 2016 en tant qu'ils permettent la mise en oeuvre des techniques de renseignement mentionnées aux articles L. 851-1, L. 851-2 et L. 851-4 du code de la sécurité intérieure, ainsi que le recueil des données dans le cadre de la technique de l'algorithme prévu au IV de l'article L. 851-3, sans contrôle préalable d'une juridiction ou d'une autorité administrative indépendante dotée d'un pouvoir contraignant, en dehors d'une urgence dûment justifiée.

***

. - Il restera alors à déterminer les conséquences de ces annulations.

La Cour de justice a entendu assurer l'application immédiate des exigences qu'elle a posées dans son arrêt du 6 octobre. Elle s'est opposée à toute limitation dans le temps des effets d'une déclaration d'inconventionnalité d'une loi imposant aux opérateurs la conservation généralisée et indifférenciée des données.

En l'espèce, les annulations que nous vous proposons n'impliquent ni ne permettent aux opérateurs de procéder à l'effacement de la moindre donnée à l'avenir, puisque la sauvegarde de la sécurité nationale exige qu'ils les conservent dans les mêmes conditions qu'aujourd'hui. Elles impactent uniquement l'accès, pour l'avenir, et la

possibilité pour les services de continuer à stocker et exploiter les données collectées par le passé.

1° S'agissant du contentieux du refus d'abroger, il n'y a pas matière à modulation dans le temps à proprement parler. Vous n'êtes pas juge des effets produits par la mesure dans le passé, mais seulement de l'avenir de la mesure elle-même - ce qui explique votre office. Toutefois, votre injonction ne saurait aboutir elle-même à priver de garantie les exigences constitutionnelles. Vous devez donc ménager au gouvernement le temps nécessaire pour qu'il adapte le cadre juridique aux exigences du droit de l'Union. Nous vous invitons en conséquence à enjoindre à l'État de procéder aux abrogations ou modifications nécessaires dans le délai de six mois qu'il réclame.

Précisons tout de même que le dispositif supplétif que nous envisageons pour la lutte contre la criminalité grave nous semble déjà pouvoir fonctionner. Certes, les dispositions du code de procédure pénale, comme d'ailleurs celles du code de la sécurité intérieure, n'évoquent à aucun moment la conservation rapide des données de connexion. On ne trouve au deuxième alinéa de l'article 60-2 du premier code qu'une procédure de gel des données relatives au *contenu des correspondances*, sur autorisation du juge des libertés et de la détention. Mais il n'y a guère de difficulté à considérer que les dispositions du premier alinéa du même article 60-2, qui autorisent l'accès, permettent *a fortiori* de demander simplement le gel. Cette lecture est, du reste, la seule conforme à la Convention de Budapest à laquelle la France est partie : celle-ci lui fait en effet obligation de prévoir dans sa législation les mesures permettant d'ordonner la conservation rapide des données relatives au trafic (232). *Free* a d'ailleurs produit plusieurs exemples de réquisition portant sur la conservation provisoire de données, et non sur l'accès, et il semble qu'il y est notamment recouru lorsque le délai de conservation d'un an touche à sa fin (233). Cela étant, il n'est pas exclu que le juge judiciaire porte un autre regard sur la question (234) et nous vous invitons donc à ne pas vous aventurer sur ses terres.

2° S'agissant des décrets, vous n'êtes pas contraints par l'interdiction de la modulation résultant de l'arrêt du 6 octobre, qui ne porte que sur l'obligation de conservation généralisée et indifférenciée. N'est en cause ici que la problématique de l'accès, et plus particulièrement du contrôle de l'accès. Pour autant, la faculté de modulation ne peut être utilisée qu'à titre exceptionnel et en présence d'une nécessité impérieuse, comme le juge votre décision d'assemblée *Association nationale des opérateurs détaillants en énergie* du 19 juillet 2017 (235).

Il n'est évidemment concevable ni de priver les services de renseignement d'une source d'informations aussi précieuse du jour au lendemain, ni de les contraindre à effacer les données irrégulièrement collectées par le passé, alors que la continuité de la surveillance est l'une des conditions cardinales de son efficacité. De telles conséquences seraient totalement disproportionnées au regard du motif d'annulation retenu.

C'est particulièrement vrai pour le passé, alors que les rapports publics de la CNCTR font ressortir que le Premier ministre n'est jamais passé outre un avis défavorable de celle-ci. Autrement dit, la faille du dispositif de contrôle justifiant l'annulation n'a jamais eu la moindre conséquence pratique. Vous pourriez même en déduire qu'il n'y a, par conséquent, pas matière à modulation. Afin d'éviter tout débat sur ce point à l'avenir, nous vous proposons néanmoins, par sécurité, de regarder comme définitifs les effets produits par l'illégalité des dispositions réglementaires litigieuses antérieurement à leur annulation, sous réserve des actions contentieuses engagées à la date de votre décision.

Pour l'avenir, nous vous invitons à assortir votre annulation d'un régime transitoire supplétif afin d'assurer le respect du droit de l'Union, comme vous l'avez fait dans votre décision d'assemblée *Vassilikiotis* (236). Vous pourrez prévoir que les dispositions réglementaires ne pourront être légalement appliquées qu'à condition qu'une technique de renseignement autorisée par le Premier ministre en dépit d'un avis défavorable de la CNCTR ne puisse être mise en oeuvre, sauf urgence dûment justifiée, sans que la Commission ait été mise à même de saisir la formation spécialisée du Conseil d'État - c'est-à-dire ait disposé d'un délai raisonnable pour ce faire (237) - et, le cas échéant, avant que la formation spécialisée ait statué - ce qu'il lui appartient de faire à bref délai. Le droit de l'Union ne nous semble pas imposer, en revanche, que la CNCTR soit tenue de saisir le Conseil d'État, par le biais de son président ou d'au moins trois membres comme le prévoit l'article L. 833-8. S'ils y

renoncent, le contrôle préalable n'en est pas moins exercé. Là encore, même si cela peut sembler superflu, vous pourriez, par sécurité, différer votre annulation de six mois, le temps que les textes soient adaptés, afin de n'introduire aucune perturbation dans le dispositif.

Vous pourrez enfin mettre à la charge de l'État la somme de 3 000 € au profit de chaque association requérante et de 1 500 € pour chacune des sociétés du groupe *Free*, au titre des dispositions de l'article L. 761-1 du code de justice administrative, et rejeter le surplus des conclusions dont vous êtes saisi.

***

Monsieur le président, Mesdames, Messieurs,

Lorsqu'il y a quinze ans presque jour pour jour, cette institution nous ouvrait ses portes, nous nous savions investi du pouvoir, immense mais heureusement collégial, de priver d'effet la volonté exprimée par la représentation nationale. Nous nous étions alors promis de n'en faire usage qu'avec tact et mesure.

Notre légitimité pour vous proposer d'écarter une loi inconventionnelle n'est pas discutable dans son principe. Elle repose sur la volonté implicite du constituant et un office ancien et indispensable du juge administratif, et sur les garanties fortes que comporte le statut qui est le nôtre. Accessoirement, elle se nourrit du privilège plus personnel d'avoir été formé dans une grande école de service public et d'avoir pu apprendre le métier en côtoyant les meilleurs.

Mais pour honorer la confiance placée en lui, le juge, quelles que soient ses qualités, doit savoir rester à sa juste place, avec la claire conscience de la légitimité qui s'attache à la loi. Elle ne découle pas seulement de l'onction démocratique dont bénéficient les parlementaires qui l'adoptent ; elle est aussi, on l'oublie, celle des femmes et des hommes qui l'ont façonnée, à commencer par celles et ceux qui en ont éprouvé et exprimé le besoin au contact du terrain et de la « vraie vie » de nos concitoyens, dans ce qu'elle a de plus beau et dans ce qu'elle a de plus dur.

Alors que nous nous apprêtons à quitter ce pupitre, c'est cette promesse de retenue que nous entendons tenir, en vous invitant à ne pas détruire une oeuvre guidée par la préoccupation de protéger au mieux les citoyens, mais à la rendre meilleure. Il ne s'agit pas ici de prendre parti pour ou contre la vie privée, ou pour ou contre la construction européenne. Quel que soit le sens de votre décision, ces enjeux, auxquels nous sommes profondément attaché, seront affectés, directement ou indirectement. Il s'agit de fixer, en l'état et en conscience, le point d'équilibre d'un écosystème dont l'actualité ne cesse de démontrer la grande fragilité. Celui que nous vous proposons est parfaitement discutable. Mais nous ne croyons pas qu'il trahisse la volonté du peuple français au nom duquel vous allez rendre la justice.

Tel est le sens de toutes nos conclusions.

Annexe

Conseil d'État, assemblée, 21 avril 2021, n° 393099 et autres

French Data Network et autres

(*Extraits*)

1. Les associations et sociétés requérantes contestent les dispositions réglementaires imposant aux opérateurs de communications électroniques, aux fournisseurs d'accès à internet et aux hébergeurs de contenus de conserver de façon généralisée et indifférenciée, pour une durée d'un an, les données de trafic et de localisation

de l'ensemble de leurs utilisateurs ainsi que leurs données d'identité civile et certaines données relatives à leurs comptes et aux paiements qu'ils effectuent en ligne. Elles contestent également les dispositions réglementaires permettant aux services de renseignement de recueillir et d'opérer des traitements sur ces données. Sous le n° 393099, les associations French Data Network, La Quadrature du Net et la Fédération des fournisseurs d'accès à internet associatifs demandent l'annulation de la décision implicite de rejet née du silence gardé par le Premier ministre sur leur demande tendant à l'abrogation de l'article R. 10-13 du code des postes et des communications électroniques et du décret du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne. 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 n° 394922, du décret du 28 septembre 2015 portant désignation des services spécialisés de renseignement et, sous le n° 397851, du décret du 29 janvier 2016 relatif aux techniques de recueil de renseignement. Sous le n° 397844, l'association Igwan.net demande l'annulation pour excès de pouvoir 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 même code. Sous les n^{os} 424717 et 424718, les sociétés Free Mobile et Free demandent l'annulation de la décision implicite de rejet née du silence gardé par le Premier ministre sur leur demande tendant à l'abrogation de l'article R. 10-13 du code des postes et des communications électroniques. Par ses décisions n° 393099 et n^{os} 394922, 394925, 397844, 397851 du 26 juillet 2018, le Conseil d'État, statuant au contentieux, a écarté les moyens invoqués devant lui autres que ceux tirés de la méconnaissance du droit de l'Union européenne et a sursis à statuer jusqu'à ce que la Cour de justice de l'Union européenne se soit prononcée sur les questions préjudicielles dont il l'a saisie. Par un arrêt en date du 6 octobre 2020, rendu dans les affaires jointes C-511/18, C-512/18 et C-520/18, la Cour de justice s'est prononcée sur ces questions.

2. Les requêtes présentent à juger des questions communes. Il y a lieu de les joindre pour statuer par une seule décision.

Sur le cadre juridique des litiges :

En ce qui concerne les exigences inhérentes à la hiérarchie des normes :

3. En vertu de l'article 88-1 de la Constitution : « La République participe à l'Union européenne constituée d'États qui ont choisi librement d'exercer en commun certaines de leurs compétences en vertu du traité sur l'Union européenne et du traité sur le fonctionnement de l'Union européenne, tels qu'ils résultent du traité signé à Lisbonne le 13 décembre 2007 ». Selon le paragraphe 3 de l'article 4 du Traité sur l'Union européenne : « En vertu du principe de coopération loyale, l'Union et les États membres se respectent et s'assistent mutuellement dans l'accomplissement des missions découlant des traités. / Les États membres prennent toute mesure générale ou particulière propre à assurer l'exécution des obligations découlant des traités ou résultant des actes des institutions de l'Union. / Les États membres facilitent l'accomplissement par l'Union de sa mission et s'abstiennent de toute mesure susceptible de mettre en péril la réalisation des objectifs de l'Union ». La seconde phrase du paragraphe 1 de l'article 19 du même traité assigne à la Cour de justice de l'Union européenne la mission d'assurer « le respect du droit dans l'interprétation et l'application des traités ».

4. Le respect du droit de l'Union constitue une obligation tant en vertu du Traité sur l'Union européenne et du traité sur le fonctionnement de l'Union européenne qu'en application de l'article 88-1 de la Constitution. Il emporte l'obligation de transposer les directives et d'adapter le droit interne aux règlements européens. En vertu des principes de primauté, d'unité et d'effectivité issus des traités, tels qu'ils ont été interprétés par la Cour de justice de l'Union européenne, le juge national, chargé d'appliquer les dispositions et principes généraux du droit de l'Union, a l'obligation d'en assurer le plein effet en laissant au besoin inappliquée toute disposition contraire, qu'elle résulte d'un engagement international de la France, d'une loi ou d'un acte administratif.

5. Toutefois, tout en consacrant l'existence d'un ordre juridique de l'Union européenne intégré à l'ordre juridique

interne, dans les conditions mentionnées au point précédent, l'article 88-1 confirme la place de la Constitution au sommet de ce dernier. Il appartient au juge administratif, s'il y a lieu, de retenir de l'interprétation que la Cour de justice de l'Union européenne a donnée des obligations résultant du droit de l'Union la lecture la plus conforme aux exigences constitutionnelles autres que celles qui découlent de l'article 88-1, dans la mesure où les énonciations des arrêts de la Cour le permettent. Dans le cas où l'application d'une directive ou d'un règlement européen, tel qu'interprété par la Cour de justice de l'Union européenne, aurait pour effet de priver de garanties effectives l'une de ces exigences constitutionnelles, qui ne bénéficierait pas, en droit de l'Union, d'une protection équivalente, le juge administratif, saisi d'un moyen en ce sens, doit l'écarter dans la stricte mesure où le respect de la Constitution l'exige.

6. Il en résulte, d'une part, que, dans le cadre du contrôle de la légalité et de la constitutionnalité des actes réglementaires assurant directement la transposition d'une directive européenne ou l'adaptation du droit interne à un règlement et dont le contenu découle nécessairement des obligations prévues par la directive ou le règlement, il appartient au juge administratif, saisi d'un moyen tiré de la méconnaissance d'une disposition ou d'un principe de valeur constitutionnelle, de rechercher s'il existe une règle ou un principe général du droit de l'Union européenne qui, eu égard à sa nature et à sa portée, tel qu'il est interprété en l'état actuel de la jurisprudence du juge de l'Union, garantit par son application l'effectivité du respect de la disposition ou du principe constitutionnel invoqué. Dans l'affirmative, il y a lieu pour le juge administratif, afin de s'assurer de la constitutionnalité de l'acte réglementaire contesté, de rechercher si la directive que cet acte transpose ou le règlement auquel cet acte adapte le droit interne est conforme à cette règle ou à ce principe général du droit de l'Union. Il lui revient, en l'absence de difficulté sérieuse, d'écarter le moyen invoqué, ou, dans le cas contraire, de saisir la Cour de justice de l'Union européenne d'une question préjudicielle, dans les conditions prévues par l'article 167 du Traité sur le fonctionnement de l'Union européenne. En revanche, s'il n'existe pas de règle ou de principe général du droit de l'Union garantissant l'effectivité du respect de la disposition ou du principe constitutionnel invoqué, il revient au juge administratif d'examiner directement la constitutionnalité des dispositions réglementaires contestées.

7. D'autre part, lorsqu'il est saisi d'un recours contre un acte administratif relevant du champ d'application du droit de l'Union et qu'est invoqué devant lui le moyen tiré de ce que cet acte, ou les dispositions législatives qui en constituent la base légale ou pour l'application desquelles il a été pris, sont contraires à une directive ou un règlement européen, il appartient au juge administratif, après avoir saisi le cas échéant la Cour de justice d'une question préjudicielle portant sur l'interprétation ou la validité de la disposition du droit de l'Union invoquée, d'écarter ce moyen ou d'annuler l'acte attaqué, selon le cas. Toutefois, s'il est saisi par le défendeur d'un moyen, assorti des précisions nécessaires pour en apprécier le bien-fondé, tiré de ce qu'une règle de droit national, alors même qu'elle est contraire à la disposition du droit de l'Union européenne invoquée dans le litige, ne saurait être écartée sans priver de garanties effectives une exigence constitutionnelle, il appartient au juge administratif de rechercher s'il existe une règle ou un principe général du droit de l'Union européenne qui, eu égard à sa nature et à sa portée, tel qu'il est interprété en l'état actuel de la jurisprudence du juge de l'Union, garantit par son application l'effectivité de l'exigence constitutionnelle invoquée. Dans l'affirmative, il lui revient, en l'absence de difficulté sérieuse justifiant une question préjudicielle à la Cour de justice, d'écarter cette argumentation avant de faire droit au moyen du requérant, le cas échéant. Si, à l'inverse, une telle disposition ou un tel principe général du droit de l'Union n'existe pas ou que la portée qui lui est reconnue dans l'ordre juridique européen n'est pas équivalente à celle que la Constitution garantit, il revient au juge administratif d'examiner si, en écartant la règle de droit national au motif de sa contrariété avec le droit de l'Union européenne, il priverait de garanties effectives l'exigence constitutionnelle dont le défendeur se prévaut et, le cas échéant, d'écarter le moyen dont le requérant l'a saisi.

8. En revanche, et contrairement à ce que soutient le Premier ministre, il n'appartient pas au juge administratif de s'assurer du respect, par le droit dérivé de l'Union européenne ou par la Cour de justice elle-même, de la répartition des compétences entre l'Union européenne et les États membres. Il ne saurait ainsi exercer un contrôle sur la conformité au droit de l'Union des décisions de la Cour de justice et, notamment, priver de telles décisions de la force obligatoire dont elles sont revêtues, rappelée par l'article 91 de son règlement de

procédure, au motif que celle-ci aurait excédé sa compétence en conférant à un principe ou à un acte du droit de l'Union une portée excédant le champ d'application prévu par les traités.

En ce qui concerne les exigences constitutionnelles invoquées en défense par l'État :

9. Il est soutenu en défense que les dispositions du droit national contestées au motif qu'elles seraient contraires au droit de l'Union européenne ne sauraient être écartées sans priver de garanties effectives les objectifs de valeur constitutionnelle de sauvegarde des intérêts fondamentaux de la nation, de prévention des atteintes à l'ordre public et de recherche des auteurs d'infractions pénales et de lutte contre le terrorisme. Il ressort en effet de l'article 12 de la Déclaration des droits de l'homme et du citoyen de 1789 que la garantie des droits de l'homme et du citoyen, sans laquelle une société n'a point de constitution selon l'article 16 de la même Déclaration, nécessite une force publique. La sauvegarde des intérêts fondamentaux de la nation, la prévention des atteintes à l'ordre public, notamment celle des atteintes à la sécurité des personnes et des biens, la lutte contre le terrorisme, ainsi que la recherche des auteurs d'infractions pénales constituent des objectifs de valeur constitutionnelle, nécessaires à la sauvegarde de droits et de principes de même valeur, qui doivent être conciliés avec l'exercice des libertés constitutionnellement garanties, au nombre desquelles figurent la liberté individuelle, la liberté d'aller et venir et le respect de la vie privée.

10. Selon le paragraphe 2 de l'article 4 du Traité sur l'Union européenne, il appartient à l'Union, y compris à la Cour de justice de l'Union européenne, de respecter l'identité nationale des États membres, « inhérente à leurs structures fondamentales politiques et constitutionnelles », ainsi que « les fonctions essentielles de l'État, notamment celles qui ont pour objet d'assurer son intégrité territoriale, de maintenir l'ordre public et de sauvegarder la sécurité nationale », cette dernière restant « de la seule responsabilité des États membres ». Aux termes du paragraphe 1 de l'article 52 de la Charte des droits fondamentaux de l'Union européenne : « Toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui ». Il ressort de la jurisprudence de la Cour de justice de l'Union européenne, d'une part, que les objectifs de protection de la sécurité nationale et de lutte contre la criminalité grave, qui contribuent à la protection des droits et des libertés d'autrui, sont au nombre des objectifs d'intérêt général reconnus par l'Union, comme tels susceptibles de justifier des limitations aux droits garantis par la Charte en vertu de son article 52, et, d'autre part, que si l'article 6 de la Charte, qui garantit le droit à la sûreté, ne saurait être interprété comme imposant aux pouvoirs publics une obligation d'adopter des mesures spécifiques en vue de réprimer des infractions pénales, il découle de ses articles 3, 4 et 7, qui garantissent le droit au respect de l'intégrité de la personne, l'interdiction de la torture et des peines et traitements inhumains ou dégradants et le respect de la vie privée et familiale, des obligations positives à la charge de l'État, incluant la mise en place de règles permettant une lutte effective contre certaines infractions pénales. Toutefois, les exigences constitutionnelles mentionnées au point 9, qui s'appliquent à des domaines relevant exclusivement ou essentiellement de la compétence des États membres en vertu des traités constitutifs de l'Union, ne sauraient être regardées comme bénéficiant, en droit de l'Union, d'une protection équivalente à celle que garantit la Constitution.

[...]

Décide :

Article 1er : Sont annulées les décisions du Premier ministre refusant d'abroger l'article R. 10-13 du code des postes et des communications électroniques et le décret du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne, en tant que ces dispositions réglementaires, d'une part, ne limitent pas les finalités de l'obligation de conservation généralisée et indifférenciée des données de trafic et de localisation autres que les données d'identité civile, les coordonnées de contact et de paiement, les données relatives aux contrats et aux comptes et

les adresses *IP* à la sauvegarde de la sécurité nationale et, d'autre part, ne prévoient pas un réexamen périodique de l'existence d'une menace grave, réelle et actuelle ou prévisible pour la sécurité nationale.

Article 2 : Il est enjoint au Premier ministre de procéder à cette abrogation dans un délai de six mois à compter de la présente décision.

Article 3 : Les décrets du 11 décembre 2015 et du 29 janvier 2016 sont annulés en tant seulement qu'ils permettent la mise en oeuvre des dispositions des articles L. 851-1, L. 851-2, L. 851-4 et du IV de l'article L. 851-3 du code de la sécurité intérieure sans contrôle préalable par une autorité administrative indépendante dotée d'un pouvoir d'avis conforme ou une juridiction, en dehors des cas d'urgence dûment justifiée.

Article 4 : La requête n° 394922 est rejetée.

Article 5 : L'État versera la somme de 3 000 € à l'association La Quadrature du Net, 3 000 € à l'association French Data Network, 3 000 € à la Fédération des fournisseurs d'accès à internet associatifs, 3 000 € à l'association Igwan.net, 1 500 € à la société Free Mobile et 1 500 € à la société Free au titre de l'article L. 761-1 du code de justice administrative.

Article 6 : Le surplus des conclusions des requêtes est rejeté.

Article 7 : La présente décision sera notifiée aux associations La Quadrature du Net, French Data Network, Igwan.net, à la Fédération des fournisseurs d'accès à internet associatifs, à la société Free Mobile, à la société Free, au Premier ministre, au ministre de l'économie, des finances et de la relance, à la ministre des armées, au ministre de l'intérieur, au garde des sceaux, ministre de la justice, à Privacy International et au Center for Democracy and Technology.

Copie en sera adressée à la Fédération française des télécoms.

Mots clés :
DROIT EUROPEEN * Droit de l'Union européenne * Primauté du droit de l'Union * Constitution * Clause de sauvegarde
DROITS FONDAMENTAUX ET PRINCIPES GENERAUX * Informatique et libertés * Fichiers * Droits et libertés fondamentaux * Droit au respect de la vie privée * Données personnelles

(1) V. égal. la chronique d'A. Roblot-Troizier, *infra* p. 576.

(2) Selon les chiffres communiqués par le gouvernement, 1,8 million en 2017, 2,2 millions en 2018, 2,4 millions en 2019 et 2,5 millions en 2020, sans compter les réquisitions ne transitant pas par la PNIJ (notamment celles opérées par les sociétés Deveryware et Elektron, ainsi que les réquisitions auprès des fournisseurs d'accès à internet qui ne sont pas connectés à cette plateforme).

(3) Directive 97/66/CE du Parlement européen et du Conseil du 15 déc. 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications.

(4) CJCE, 18 janv. 2001, aff. C-151/00, *Commission des Communautés européennes* c/ *France*, D. 2001. 522. Le défaut de transposition portait notamment sur l'art. 7 relatif à l'obligation d'effacement ou d'anonymisation des données de trafic et de localisation.

(5) Loi n° 2001-1062 du 15 nov. 2001 relative à la sécurité quotidienne.

(6) Art. 10 de la loi n° 2004-669 du 9 juill. 2004.

(7) C'est-à-dire au plus tard jusqu'à l'expiration du délai de prescription de l'action en paiement ou en remboursement fixé à un an par l'art. L. 34-2 du même code.

(8) V. l'exposé des motifs de l'amendement n° 9 déposé par le gouvernement en nouvelle lecture au Sénat, et le rapport fait au nom de la Commission des lois constitutionnelles, de la législation et de l'administration générale de la République par M. B. Le Roux, enregistré le 24 oct. 2001, n° 3352.

(9) V. le 2° de l'art. L. 39-3 du même code. Le 1. du VI de l'art. 6 de la *LCEN* prévoit quant à lui une peine d'un an d'emprisonnement et de 250 000 € d'amende en cas de non conservation des éléments d'information visés au II de cet article.

(10) Le Conseil constitutionnel s'est ainsi assuré que ces dispositions énoncent « avec précision la nature et les conditions de conservation et de communication » des données de connexion et il a écarté en conséquence le grief d'incompétence négative (Cons. const., 27 déc. 2001, n° 2001-457 DC, consid. 6 à 9, D. 2002. 1945, obs. D. Ribes, qui valide le droit de communication des agents des douanes, de l'administration fiscale et des enquêteurs de la COB, devenue AMF ; V. aussi, Cons. const., 24 juill. 2015, n° 2015-478 QPC, *Association French Data Network et autres*, consid. 11 à 14, AJDA 2015. 1514 ; D. 2015. 1647, et les obs. ; *ibid*. 2016. 1461, obs. N. Jacquinot et A. Mangiavillano, jugeant que les « données de connexion » accessibles aux services de renseignement sont suffisamment définies par l'art. L. 34-1).

(11) V. l'art. 1er de la loi n° 2000-719 du 1er août 2000 qui a introduit un art. 43-9 dans la loi n° 86-1067 du 30 sept. 1986 relative à la liberté de communication.

(12) Art. L. 96 G du Livre des procédures fiscales, qui s'est substitué à l'art. L. 83 du même livre.

(13) Art. L. 450-3-3 du code de commerce, issu de l'art. 212 de la loi n° 2019-486 du 22 mai 2019 (dite loi *PACTE*).

(14) Art. 65 *quinquies* du code des douanes.

(15) Art. L. 621-10-2 du code monétaire et financier.

(16) Art. 14 de la loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet.

(17) Art. 24 de la loi n° 2013-1168 du 18 déc. 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.

(18) Art. L. 8113-5-2 du code du travail : seules les données permettant l'identification des personnes proposant un travail une prestation ou une activité relevant du travail illégal sont accessibles au système d'inspection du travail.

(19) Art. L. 34-1-1 du CPCE, issu de l'art. 6 de la loi n° 2006-64 du 23 janv. 2006 relative à la lutte contre le terrorisme et portant diverses dispositions relatives à la sécurité et aux contrôles frontaliers.

(20) Loi n° 2015-912 du 24 juill. 2015 relative au renseignement

(21) Il s'agit des informations énumérées au 2° du I de l'art. R. 851-5 du CSI. Elles ne font pas l'objet d'une obligation de

conservation par les opérateurs, mais sont traitées par eux et accessibles en temps réel. C'est le cas des données de localisation GPS, de données d'acheminement permettant de détecter le recours à des techniques d'anonymisation ou à des réseaux privés virtuels (VPN), des *logins* et mots de passe renseignés ou encore des certificats électroniques.

(22) CE, 10 déc. 2012, n° 317074, *Ministre du budget, des comptes publics et de la fonction publique c/ Société Rhodia*, Lebon T. p. 632.

(23) Vous avez notamment entrepris de cantonner la portée des décisions avant dire droit dans votre décision d'assemblée du 27 mars 2015, n° 382083, *Commission nationale des comptes de campagne et des financements politiques*, Lebon p. 128 ; AJDA 2015. 660 ; *ibid*. 981, chron. J. Lessi et L. Dutheillet de Lamothe ; RFDA 2015. 598, note R. Rambaud.

(24) CE, 13 juin 2016, n° 372721, *Coulibaly et Mas*, Lebon T. p. 615-902 ; AJDA 2016. 1210 ; v. aussi CE, 20 oct. 2016, n° 395105, *La Cimade et autres*, AJDA 2016. 2358 ; D. 2017. 261, obs. O. Boskovic, S. Corneloup, F. Jault-Seseke, N. Joubert et K. Parrot ; Constitutions 2016. 671, chron. C. Pouly ; CE, 13 avr. 2016, n° 394114, *CIMADE*, AJDA 2016. 1667.

(25) CE, sect., 11 juill. 2011, n° 320735-320854, *Société d'équipement du département de Maine-et-Loire (SODEMEL) c/ Ministre de l'intérieur, de l'outre-mer, des collectivités territoriales de l'immigration*, Lebon p. 346 ; AJDA 2012. 449, note N. Foulquier ; *ibid*. 2011. 1406 ; AJDI 2011. 806, obs. R. Hostiou ; *ibid*. 2012. 22, chron. S. Gilbert ; *ibid*. 2015. 25, chron. S. Gilbert ; RDI 2011. 519, obs. P. Soler-Couteaux.

(26) Le maniement de cette exception d'inconventionnalité suppose d'identifier de façon méticuleuse la disposition législative affectée et la mesure dans laquelle elle l'est, sans vous arrêter aux choix rédactionnels du législateur et, en particulier, sans égard pour sa cohabitation éventuelle avec d'autres dispositions dans un même article ou un même alinéa. Il y a lieu par ailleurs d'arbitrer au cas par cas entre deux types de contrôle : le contrôle abstrait, qui conduit le cas échéant à annuler l'acte réglementaire attaqué s'il se trouve privé purement et simplement de sa base légale en raison d'une contrariété pleine et entière aux engagements européens ou internationaux de la France, ou seulement en tant qu'il régit ou ne régit pas telle ou telle situation, ou en tant qu'il comporte ou ne comporte pas telle ou telle disposition ; et le contrôle concret (v. CE, sect., 10 nov. 2010, n° 314449, *Commune de Palavas-les-Flots et Commune de Lattes*, Lebon p. 429 ; AJDA 2010. 2183 ; *ibid*. 2416, chron. D. Botteghi et A. Lallet ; D. 2010. 2842, obs. R. Grand ; AJCT 2010. 163, obs. J.-D. Dreyfus ; RFDA 2011. 124, concl. N. Boulouis ; Constitutions 2011. 81, obs. P. De Baecke ; RTD civ. 2011. 501, obs. P. Deumier ; CE, ass., 31 mai 2016, n° 396848, *Gonzalez-Gomez*, Lebon p. 208, concl. A. Bretonneau ; AJDA 2016. 1092 ; *ibid*. 1398, chron. L. Dutheillet de Lamothe et G. Odinet ; D. 2016. 1470, obs. M.-C. de Montecler ; *ibid*. 1472, note H. Fulchiron ; *ibid*. 1477, note B. Haftel ; *ibid*. 2017. 729, obs. F. Granet-Lambrechts ; *ibid*. 781, obs. J.-C. Galloux et H. Gaumont-Prat ; *ibid*. 935, obs. RÉGINE ; *ibid*. 1011, obs. H. Gaudemet-Tallon et F. Jault-Seseke ; AJ fam. 2016. 439, obs. C. Siffrein-Blanc ; *ibid*. 360, obs. A. Dionisi-Peyrusse ; RFDA 2016. 740, concl. A. Bretonneau ; *ibid*. 754, note P. Delvolvé ; RTD civ. 2016. 578, obs. P. Deumier ; *ibid*. 600, obs. J. Hauser ; *ibid*. 802, obs. J.-P. Marguénaud ; *ibid*. 834, obs. J. Hauser ; RTD eur. 2017. 319, obs. D. Ritleng), si l'acte lui-même « tient debout » tel qu'il est écrit et que la difficulté se loge le cas échéant dans certaines de ses modalités d'application. Il est possible d'annuler l'acte en tant qu'il permet la mise en oeuvre d'une loi inconventionnelle sous tel ou tel aspect (v. par ex. : CE, 7 juin 2006, n° 285576, *Association AIDES*, Lebon p. 282 ; AJDA 2006. 1189 ; *ibid*. 2233, note H. Rihal ; D. 2007. 2192, obs. A. Gouttenoire et L. Brunet ; Dr. soc. 2006. 1037, concl. C. Devys ; RDSS 2006. 1047, note L. Gay : annulation d'un décret en tant qu'il met en oeuvre des dispositions législatives pour une catégorie de personnes. V. aussi, CE, 6 avr. 2007, n° 282390, *Comité Harkis et vérité*, Lebon T. p. 639-648 ; AJDA 2007. 833 ; CE, 16 juin 2008, n° 300636-300637, *Association La Cimade*, Lebon p. 218 ; AJDA 2008. 1232) ou d'assortir le rejet du moyen d'une réserve d'interprétation ou d'indications à destination des autorités en charge de sa mise en oeuvre afin de garantir le respect des engagements de la France au stade de son application pratique.

(27) À l'exclusion de la direction du renseignement militaire et de *Tracfin*.

(28) Vous observerez d'ailleurs que, même si l'accès est évidemment vain en l'absence de conservation des données, la disparition de toute obligation de conservation à des fins régaliennes ne priverait pas de portée juridique les dispositions

organisant leur recueil, puisque les services de renseignement pourraient continuer à puiser dans les données spontanément conservées par les opérateurs pour leurs besoins propres.

(29) La géolocalisation en temps réel n'implique pas de conservation (sinon un instant de raison) puisque les données sont transmises en même temps qu'elles sont traitées pour l'acheminement de la communication.

(30) CSI, 2° du I de l'art. R. 851-5.

(31) CSI, 2nd al. de l'art. L. 821-1.

(32) CSI, art. L. 871-7.

(33) CSI, art. L. 833-8.

(34) CSI, art. L. 871-1 et s.

(35) La primauté du droit de l'Union ne met pas en échec l'autorité de la chose jugée, en principe (v. notamment : CJCE, 3 sept. 2009, aff. C-2/08, *Amministrazione dell'Économia e delle Finanze*, RTD eur. 2010. 113, chron. L. Coutron ; Rev. UE 2015. 370, étude G. Eckert).

(36) V. respectivement, pour l'enquête de flagrance, l'enquête préliminaire et l'instruction, les art. 60-2 (1er al.), 77-1-2 et 99-4 de ce code.

(37) V. les arrêts C-151/00 (18 janv. 2001, *Commission des Communautés européennes* c/ *France*, D. 2001. 522), C-211/02 et C-350/02.

(38) Directive 2002/58/CE du Parlement européen et du Conseil du 12 juill. 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques).

(39) CEDH, 4 déc. 2008, n° 30562/04 et 30566/04, *Marper c/ Royaume-Uni*, § 67, AJDA 2009. 872, chron. J.-F. Flauss ; D. 2010. 604, obs. J.-C. Galloux et H. Gaumont-Prat ; AJ pénal 2009. 81, obs. G. Roussel ; RFDA 2009. 741, étude S. Peyrou-Pistouley ; RSC 2009. 182, obs. J.-P. Marguénaud.

(40) CJUE, 8 avr. 2014, aff. C-293/12 et C-594/12, *Digital Rights Ireland Ltd contre Minister for Communications, Marine and Natural Resources e.a. et Kärntner Landesregierung e.a.,* AJDA 2014. 773 ; *ibid*. 1147, chron. M. Aubert, E. Broussy et H. Cassagnabère ; D. 2014. 1355, et les obs., note C. Castets-Renard ; *ibid*. 2317, obs. J. Larrieu, C. Le Stanc et P. Tréfigny ; Légipresse 2014. 265 et les obs. ; RTD eur. 2014. 283, édito. J.-P. Jacqué ; *ibid*. 283, édito. J.-P. Jacqué ; *ibid*. 2015. 117, étude S. Peyrou ; *ibid*. 168, obs. F. Benoît-Rohmer ; *ibid*. 786, obs. M. Benlolo-Carabot.

(41) V. notamment la chronique de jurisprudence de la CJUE à l'AJDA 2021. 387.

(42) N° 388134, Dalloz IP/IT 2016. 313, obs. O. Henrard.

(43) CJUE, 2 oct. 2018, aff. C-207/16, AJDA 2018. 2280, chron. P. Bonneville, E. Broussy, H. Cassagnabère et C. Gänser ;

D. 2018. 1913 ; AJ pénal 2018. 584, obs. B. Nicaud .

(44) Aff. C-511/18, C-512/18 et C-520/18, AJDA 2020. 1880 ; D. 2021. 406, et les obs. , note M. Lassalle ; *ibid*. 2020. 2262, obs. J. Larrieu, C. Le Stanc et P. Tréfigny ; AJ pénal 2020. 531 ; Dalloz IP/IT 2021. 46, obs. E. Daoud, I. Bello et O. Pecriaux ; Légipresse 2020. 671, étude W. Maxwell ; *ibid*. 2021. 240, étude N. Mallet-Poujol ; RTD eur. 2021. 175, obs. Brunessen Bertrand ; *ibid*. 181, obs. Brunessen Bertrand .

(45) CJUE, 6 oct. 2020, aff. C-623/17, AJDA 2021. 387, chron. P. Bonneville, C. Gänser, S. Markarian et A. Iljic ; AJ pénal 2020. 531, obs. B. Nicaud ; Dalloz IP/IT 2021. 46, obs. E. Daoud, I. Bello et O. Pecriaux ; RTD eur. 2021. 175, obs. Brunessen Bertrand .

(46) Aff. C-746/18, D. 2021. 470 .

(47) Sont en outre exclues, comme vous avez pris sur vous de le juger en 2018, à juste titre, les opérations réalisées par l'État qui n'impliquent aucun traitement de la part des opérateurs et qui ne présentent donc pas la moindre adhérence avec la directive *e-privacy*.

(48) L'État est en réalité un « destinataire » des données, selon la terminologie consacrée.

(49) Dans son arrêt *LQDN*, la Cour justifie la différence de jurisprudence avec l'arrêt *Parlement c/ Conseil et Commission* du 30 mai 2006 (C-317/04 et C-318/04) D. 2006. 1560, obs. E. Pahlawan-Sentilhes ; AJ pénal 2006. 369, obs. C. Saas ; RSC 2006. 684, chron. L. Idot ; RTD eur. 2006. 535, note V. Michel par la différence de rédaction de la directive *e-privacy*, qui n'exclut que les « activités » de l'État, là où la directive 95/46 excluait tous les « traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État », sans opérer de distinction en fonction de l'auteur du traitement de données concerné (pt 101). Du reste, cette exclusion n'est plus d'actualité depuis le RGPD (pt 102) : cela signifie, au passage, que tout traitement de données à caractère personnel réalisé par un particulier, fût-ce pour les besoins d'activités régaliennes, relève désormais du droit de l'Union.

(50) Au pt 205 de son arrêt du 6 oct. 2020, la Cour semble également rattacher les services de messagerie sur internet à la catégorie des « services de communications électroniques » régis par la directive *e-privacy*, en se référant aux pts 35 et 38 de son arrêt *Google* du 13 juin 2019 (C-193/18, D. 2019. 1285 ; Dalloz IP/IT 2019. 413, obs. C. Crichton). Cet arrêt retient pourtant la solution inverse, puisqu'il est jugé que le service de messagerie sur internet *Gmail* ne peut être qualifié de « service de communications électroniques » au sens de l'art. 2 de la directive-cadre 2002/21/CE du 7 mars 2002 (auquel renvoie la directive *e-privacy*) faute de consister entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques. Nous relevons à cet égard que, contrairement à son homologue allemande désavouée par la CJUE dans cet arrêt, l'ARCEP considère de longue date que les fournisseurs de messagerie électronique n'entrent pas dans cette catégorie, ce qui explique qu'ils n'ont déposé aucune déclaration sur le fondement de l'art. L. 33-1 du CPCE (v. son avis n° 2010-0764 du 6 juill. 2010). Il faut probablement comprendre le « dès lors » figurant au pt 205 de l'arrêt *LQDN* comme signifiant que les services de messagerie relèvent de la directive *e-privacy* s'ils assument la responsabilité de la transmission des signaux (à l'instar d'un service comme *SkypeOut* dans lequel, en vertu d'accords passés avec des fournisseurs de services de télécommunications, l'opérateur assume la responsabilité de la transmission des signaux vis-à-vis de ses clients, moyennant rémunération : CJUE, 5 juin 2019, aff. C-142/18, *Skype Communications SARL*, D. 2019. 1227 ; Dalloz IP/IT 2019. 413, obs. C. Crichton). Sous cette réserve, nous pensons que le premier et le troisième al. du II de l'art. 6 de la *LCEN*, relatifs à la conservation et à l'accès judiciaire aux données des créateurs de contenus, n'est pas applicable à ces services, en l'état. Ils n'offrent pas un « accès » à des services de communication au public en ligne (FAI) ni n'assurent le stockage de signaux, d'écrits, d'images, de sons ou de messages « pour mise à disposition du public par des services de communication au public en ligne » (hébergeurs). On peut hésiter à y voir des éditeurs de services de communication au public en ligne, cette dernière étant définie par le IV de l'art. 1er de la *LCEN* (auquel renvoie le 23° de l'art. L. 32 du CPCE) comme « toute transmission, sur demande individuelle, de données numériques n'ayant pas un caractère de correspondance privée, par un procédé de communication électronique permettant un échange réciproque d'informations entre l'émetteur et le récepteur ». Il semble, à la lecture du II de l'art. L. 32-3 du CPCE, que les opérateurs de messagerie électronique sont des « fournisseurs de services de communication au public en ligne permettant à leurs utilisateurs d'échanger des correspondances ». Autrement dit, si l'activité de messagerie proprement dite n'est pas un service de communication au public en ligne, les opérateurs pris dans leur ensemble relèvent de cette catégorie, laquelle n'est pas soumise à l'obligation de conservation prévue par la *LCEN*.

Cette lecture est conforme aux travaux préparatoires de la loi du 1er août 2000 (v. le rapport fait au nom de la commission des affaires culturelles, familiales et sociales sur le projet de loi par M. D. Mathus, n° 2238, 8 mars 2000). L'état du droit doit toutefois évoluer. L'art. 2 de la directive 2018/1972 du Parlement européen et du Conseil du 11 déc. 2018 établissant le code des communications électroniques européen (qui remplace la directive-cadre 2002/21/CE à laquelle fait référence la directive *e-privacy*) inclut depuis le 21 déc. 2020 les services de « communications interpersonnelles » dans les services de communications électroniques. La France tarde à la transposer.

(51) En raison de l'effet potentiellement dissuasif des mesures étatiques sur l'utilisation des moyens de communication.

(52) Pt 119.

(53) La fédération française des télécoms mentionne aussi l'accès contrôlé avec personnel habilité, les réseaux indépendants et non reliés à internet, les clefs d'authentification forte pour accéder aux serveurs, une gestion rigoureuse des mots de passe, une traçabilité des accès, le chiffrement de certaines bases...

(54) Il est à cet égard édifiant de lire, dans les conclusions de l'avocat général sur l'affaire *Télé2* que « (...) les risques d'accès abusif ou illégal aux données conservées n'ont rien de théorique. D'une part, le risque d'accès abusif par les autorités compétentes doit être mis en rapport avec les nombres extrêmement élevés de demandes d'accès évoqués dans les observations soumises à la Cour. Dans le contexte du régime suédois, Tele2 Sverige a indiqué qu'elle recevait environ 10 000 demandes d'accès par mois, nombre qui n'inclut pas les demandes reçues par d'autres fournisseurs actifs sur le territoire suédois. En ce qui concerne le régime du Royaume-Uni, M. Watson a reproduit des nombres extraits d'un rapport officiel faisant état de 517 236 autorisations et de 55 346 autorisations orales urgentes pour la seule année 2014. D'autre part, le risque d'accès illégal, par toute personne, est consubstantiel à l'existence même de bases de données conservées sur des supports informatiques ». À aucun moment l'occurrence du risque n'est évoquée, sur la base d'éléments concrets. Un tel raisonnement condamnerait un nombre extrêmement élevé de bases de données très sensibles.

(55) Art. 226-18 du code pénal.

(56) Cette logique irrigue largement le droit positif depuis quelques années maintenant comme en atteste, par ex., le fait que, de plus en plus, les entreprises doivent non seulement s'abstenir de commettre une infraction, mais aussi démontrer, à peine de sanction, par exemple qu'elles ont pris toutes les mesures de conformité permettant d'éviter qu'une infraction soit commise en leur sein.

(57) Pt 122.

(58) Pt 111.

(59) V. sur ce point l'arrêt *Ministerio fiscal*.

(60) Il ressort des éléments fournis par le gouvernement que, conformément à la doctrine de la CNCTR (délibération n° 1/2016 du 14 janv. 2016) qui analyse les *URL* comme des données mixtes (de connexion et de contenu), seul le protocole (*http* par ex.) et le nom de domaine (*youtube.com*) peuvent être connus, et non le chemin d'accès (par ex., celui de la vidéo visionnée sur *YouTube*). Un projet de loi est en cours d'élaboration pour permettre de mettre en oeuvre des traitements algorithmiques sur les *URL* complètes.

(61) La convention définit les données relatives au trafic comme « toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent ». On peut considérer que cette définition couvre l'ensemble des communications électroniques (internet et téléphonie).

(62) Loi n° 2005-493 du 19 mai 2005 autorisant l'approbation de la Convention sur la cybercriminalité et du Protocole

additionnel à cette convention relatif à l'incrimination d'actes de nature raciste ou xénophobe commis par le biais de systèmes informations, et décret n° 2006-580 du 23 mai 2006 portant publication de la Convention sur la cybercriminalité.

(63) La Convention de Budapest fait obligation aux États de prévoir cette conservation rapide pour une durée maximale de 90 jours, éventuellement renouvelable, non seulement pour prévenir (son préambule indique que la convention « est nécessaire pour prévenir les actes » visés, « en facilitant la détection, l'investigation et la poursuite »), rechercher et poursuivre les infractions relevant de la cybercriminalité, mais, plus largement, pour sauvegarder les preuves électroniques de toute infraction pénale. Il résulte du c. du 2. de l'art. 14 de la Convention que la conservation rapide peut permettre la collecte des preuves électroniques de toute infraction pénale (et non pas seulement des infractions commises au moyen d'un système informatique ou relevant de la cybercriminalité au sens des art. 2 à 11 de la Convention).

(64) V. l'art. 21.

(65) Naturellement, en-dehors des périodes couvertes par cette injonction spécifique, la sauvegarde de la sécurité nationale peut tout à fait justifier, *a fortiori*, la conservation ciblée ou rapide des données dans les conditions que nous avons décrites précédemment.

(66) Pt. 138.

(67) Arrêt *H.K. c/ Prokuratuur* du 2 mars 2021, pt 29 : « la Cour a jugé qu'un tel accès ne peut être octroyé que pour autant que ces données aient été conservées par ces fournisseurs d'une manière conforme audit art. 15, § 1 (v., en ce sens, arrêts du 6 oct. 2020, C-511/18, C-512/18 et C-520/18, *La Quadrature du Net e.a.*, pt 167) ».

(68) V. aussi l'arrêt *H.K. c/ Prokuratuur*, pt 31.

(69) Arrêt *H.K. c/ Prokuratuur*.

(70) V. l'arrêt *Télé2*, pt 120 et l'arrêt *H.K.,* pt 51. L'arrêt *LQDN et autres* ne rappelle cette exigence que pour l'accès en temps réel.

(71) Sur ce point, là encore, la Cour de justice se montre plus exigeante que la Cour de Strasbourg. Cette dernière se contente, à ce jour, d'un contrôle *a posteriori*, notamment à travers les nullités invocables dans la procédure pénale.

(72) Pt 121 de l'arrêt *Télé2* et pt 190 de l'arrêt *LQDN et autres* pour ce qui concerne l'accès en temps réel.

(73) Rapport d'information de la mission d'information commune sur l'évaluation de la loi du 24 juill. 2015 relative au renseignement, n° 3069, enregistré le 10 juin 2020, présenté par M. G. Larrivé, président, et MM. Kervran et Mis, rapporteurs.

(74) Arrêt du *Højesteret* sur le Traité de Maastricht cité par L. Coutron, « Contentieux de l'Union européenne - Quand la réitération de l'effet direct horizontal du principe de non-discrimination en raison de l'âge passe mal : du rififi avec la Cour suprême danoise ! », RTD eur. 2017. 389 : les tribunaux danois « ne peuvent [néanmoins] pas se voir privés du pouvoir d'examiner la question de savoir si un acte juridique communautaire outrepasse les limites de l'abandon de souveraineté effectué par la loi sur l'adhésion. Les juridictions danoises doivent donc tenir un acte communautaire pour inapplicable au Danemark dans l'hypothèse extraordinaire où l'on constaterait, avec toute la certitude requise, qu'un acte communautaire dont la validité a été confirmée par la Cour de justice repose sur une mise en oeuvre du traité exorbitante de l'abandon de souveraineté effectué par la loi sur l'adhésion ».

(75) Cour const. tchèque, 31 janv. 2012, Pl. ÚS 5/12, *Régime de pensions slovaque*, commenté par A. Levade dans la revue

Constitutions 2012. 292. L'arrêt se fonde à la fois sur l'incompétence au regard des transferts consentis et sur l'atteinte à l'identité constitutionnelle tchèque.

(76) *Højesteret*, 6 déc. 2016, aff. 15/2014, *Dansk Industri (DI)*, agissant pour *Ajos/Succession Rasmussen*.

(77) Arrêt *Honeywell* du 6 juill. 2010, 2 *BvR* 2661/06 et arrêt *OMT* du 21 juin 2016, 2 *BvR* 2728/13.

(78) Pt 118.

(79) L'autorité du droit de l'Union européenne : le point de vue des juridictions constitutionnelles et suprêmes, discours prononcé le 19 oct. 2017 au Congrès du 25e anniversaire de l'Académie de droit européen (ERA) à Trèves.

(80) CJUE, 4 oct. 2018, aff. C-416/17, *Commission* c/ *France*, AJDA 2018. 1933 ; *ibid*. 2280, chron. P. Bonneville, E. Broussy, H. Cassagnabère et C. Gänser ; D. 2019. 240, note P.-A. Cazau ; RFDA 2019. 139, note A. Iliopoulou-Penot ; RTD eur. 2019. 423, obs. A. Maitrot de la Motte ; *ibid*. 474, obs. L. Coutron.

(81) V. pour une critique virulente de l'arrêt, notamment en ce qu'il prétend imposer son interprétation du droit de l'Union à la Cour de justice : D-U Galetta et J. Ziller, « Les violations flagrantes et délibérées du droit de l'Union par l'arrêt "inintelligible" et "arbitraire" du *Bundesverfassungsgericht* dans l'affaire *Weiss* », RTD eur. 2020. 855. V. aussi C. Blumann, « Quelques enseignements de l'arrêt du *Bundesverfassungsgericht* du 5 mai 2020 sur les fondamentaux du droit de l'Union européenne », RTD Europe 2020. 889, qui observe que la Cour de Karlsruhe a reproché à la BCE puis à la Cour de justice d'avoir mal appliqué le principe de proportionnalité, qui régit l'exercice des compétences de l'Union, et non le principe d'attribution.

(82) En dépit de l'ambiguïté de la décision *Isoglucose* de 1977 et des débats qui l'ont précédée. Cette décision juge que les répercussions de la répartition des compétences opérée par un règlement communautaire entre les institutions communautaires et les autorités nationales au regard tant des conditions d'exercice de la souveraineté nationale que du jeu des règles de l'art. 34 de la Constitution relatives au domaine de la loi « ne sont que la conséquence d'engagements internationaux souscrits par la France qui sont entrés dans le champ de l'article 55 de la Constitution ». Selon un commentateur : « la formule laisse un doute sur ce que pourrait être l'attitude du Conseil au cas où le règlement, ou toute autre décision communautaire, excéderait la compétence de la Communauté et, par suite, la portée de l'engagement international » (L. Dubouis, « Le juge français et le conflit entre norme constitutionnelle et norme européenne », *Mélanges Boulouis,* 1991, p. 205 à 219, spéc. p. 209). Le délibéré au Conseil constitutionnel indique que : « Pour la rédaction de la décision, il conviendra de faire apparaître qu'il s'agit de l'application pure et simple de traités et non de leur extension ».

(83) Nous ne croyons pas possible, en revanche, de mobiliser le principe de subsidiarité, auquel l'art. 88-6 confère une valeur constitutionnelle, et qui renvoie au principe énoncé à l'art. 5 du Traité sur l'Union européenne, lequel régit l'exercice (et non la délimitation) des compétences et limite l'intervention de l'Union, dans les compétences partagées, au cas où les objectifs de l'action envisagée seraient mieux atteints au niveau européen qu'au niveau national. Le contrôle *ultra vires* de la Cour de Karlsruhe ne nous paraît d'ailleurs pas fondé sur ce principe, repris à l'art. 23 de la *Grundgesetz* (V. *contra* : C. Langenfeld, La jurisprudence récente de la Cour constitutionnelle allemande relative au droit de l'Union européenne, titre VII, n° 2, avr. 2019).

(84) Cette force obligatoire n'est formellement affirmée qu'à l'art. 91 du règlement de procédure dont la Cour s'est dotée. Mais elle a défini dans ses arrêts la portée de la chose qu'elle juge (CJUE, 15 nov. 2012, aff. C-456/11, *Gothaer et al. c/ Samskip*, pt 40, D. 2013. 1503, obs. F. Jault-Seseke ; *ibid*. 2293, obs. L. d'Avout et S. Bollée ; Rev. crit. DIP 2013. 686, note M. Nioche ; CJCE, 1er juin 2006, aff. C-442/03 P et C-471/03 P, *P & O European Ferries SA et a.*, pt 44).

(85) Rappelons au passage que vous avez constamment reconnu cette autorité de la chose jugée aux jugements judiciaires statuant incompétemment (CE, 19 déc. 1924, *Compagnie des phosphates de Constantine*, Lebon ; CE, ass., 16 mars 1945, *Dauriac*, Lebon p. 93).

(86) Vous jugez que l'autorité de chose jugée attachée aux motifs qui sont le soutien nécessaire du dispositif d'une décision du Conseil constitutionnel ne s'étend pas à l'interprétation d'une autre loi, même conçue en termes analogues (CE, sect., 22 juin 2007, n° 288206, *Lesourd*, Lebon p. 253, concl. T. Olson ; AJDA 2007. 2130, chron. J. Boucher et B. Bourgeois-Machureau ; AJFP 2007. 295, et les obs. ; RFDA 2007. 1077, concl. T. Olson ; *ibid*. 1283, chron. A. Roblot-Troizier).

(87) CE, ass., 30 juill. 2014, n° 358564, *Vernes*, Lebon p. 260, concl. S. von Coester ; AJDA 2014. 1580 ; *ibid*. 1929, chron. J. Lessi et L. Dutheillet de Lamothe ; RFDA 2014. 945, concl. S. von Coester ; RSC 2015. 369, obs. J.-M. Brigant.

(88) CE, 1er oct. 2015, n° 373018-373022-373023, *Société Melitta France et autres*, Lebon T. p. 577 ; AJDA 2015. 1836.

(89) CE, sect, 26 juill. 1985, n° 42204, *Office national interprofessionnel des céréales*, Lebon p. 233.

(90) CE, ass., 11 déc. 2006, n° 234560, *Société De Groot En Slot Allium BV, Société Bejo Zaden BV*, Lebon p. 512, concl. F. Seners ; AJDA 2007. 136, chron. C. Landais et F. Lenica ; D. 2007. 994, note O. Steck ; RFDA 2007. 372, concl. F. Séners ; RTD civ. 2007. 299, obs. P. Remy-Corlay ; RTD eur. 2007. 473, étude F. Dieu ; *ibid*. 2008. 835, chron. D. Ritleng, A. Bouveresse et J.-P. Kovar.

(91) CJCE, 13 déc. 1990, aff. C-42/90, *Bellon*, pt 6 ; CJCE, 24 oct. 2002, aff. C-121/00, pt 21, RSC 2003. 156, obs. L. Idot. V. sur la question : F. Dieu, « Le Conseil d'État face à l'autorité des interprétations données par la CJCE dans le cadre d'un renvoi préjudiciel : une position délicate », RTD eur. 2007. 473.

(92) AJDA 2007. 136.

(93) Étant ajouté que, s'il était envisagé de le faire, il faudrait en toute rigueur adresser à la Cour de justice une nouvelle question préjudicielle. Car loin d'envisager l'éventualité d'un contrôle *ultra vires* dans la décision de renvoi de 2018, les chambres réunies ont au contraire admis l'applicabilité de la directive *e-privacy* en appliquant la jurisprudence *Télé2* sur ce point.

(94) En l'occurrence, par ex., on pourrait soutenir que la Cour ne pouvait définir dans le menu détail un régime unique de conservation et d'accès aux données de connexion à l'échelle de l'Union, sans ménager d'espace aux législateurs nationaux, alors que le § 2 de l'art. 4 du Traité sur l'Union européenne lui fait obligation de respecter « l'identité nationale » des États membres, « inhérente à leurs structures fondamentales politiques et constitutionnelles ». Certains de ces arrêts traduisent une plus grande prise en considération de ces exigences par la Cour que dans notre affaire. V. pour un exemple typique : CJCE, 14 oct. 2004, aff. C-36/02, *Omega Spielhallen- und Automatenaufstellungs-GmbH* c/ *Oberbürgermeisterin der Bundesstadt Bonn*, AJDA 2005. 152, note A. Von Walter ; D. 2004. 2833 ; RTD eur. 2005. 867, chron. C. Prieto, dans lequel elle autorise les États membres à interdire l'exploitation commerciale de jeux de simulation d'homicides en tenant compte du « niveau de protection de la dignité humaine que la constitution nationale a entendu assurer sur le territoire de la République fédérale d'Allemagne ». V. aussi, à propos de l'interdiction du port des titres de noblesse en Autriche : CJUE, 22 déc. 2010, aff. C-208/09, *Sayn-Wittgenstein*, pts 92-94, AJDA 2011. 264, chron. M. Aubert, E. Broussy et F. Donnat ; Constitutions 2011. 332, obs. A. Levade ; RTD civ. 2011. 98, obs. J. Hauser ; RTD eur. 2011. 571, obs. E. Pataut.

(95) CJCE, 11 nov. 1981, aff. C-203/80, *Casati* ; CJCE, 4 juin 1992, aff. C-13/91 et C-113/91, *Debus* ; CJUE, 4 juin 2013, aff. C-300/11, *ZZ*, pt 38, AJDA 2013. 1684, chron. M. Aubert, E. Broussy et H. Cassagnabère ; D. 2013. 1412 ; RFDA 2014. 335, chron. C. Mayeur-Carpentier, L. Clément-Wilz et F. Martucci ; RTD eur. 2014. 478-XXXVI, obs. L. Coutron ; CJUE, 20 mars 2018, aff. C-187/16, *Commission c/ Autriche*, pts 75 et 76 ; CJUE, 2 avr. 2020, aff. C-715/17, C-718/17 et C-719/17, *Commission c/ Pologne, Hongrie et République tchèque*, pts 143 et 170.

(96) V. en dernier lieu : CE, ass., 19 juill. 2019, n° 424216-424217, *Association des Américains accidentels*, Lebon p. 296, concl. A. Lallet ; AJDA 2019. 1543 ; *ibid*. 1986, chron. C. Malverti et C. Beaufils ; D. 2020. 1262, obs. W. Maxwell et C. Zolynski ; RFDA 2019. 891, concl. A. Lallet.

(97) Cons. const., 12 juin 2018, n° 2018-765 DC, consid. 2 et 3, AJDA 2018. 1191 ; D. 2019. 1248, obs. E. Debaets et N. Jacquinot ; RTD eur. 2018. 830, obs. D. Ritleng ; Cons. const., 25 oct. 2019, n° 2019-810 QPC, *Société Air France*, consid. 7, AJDA 2020. 185, note F. Brunet ; *ibid*. 2019. 2155 ; D. 2019. 2097, et les obs. ; *ibid*. 2020. 1324, obs. E. Debaets et N. Jacquinot ; JT 2019, n° 225, p. 11, obs. X. Delpech ; RFDA 2020. 184, note M. Carpentier ; Constitutions 2019. 583, Décision.

(98) T. confl., 17 oct. 2011, n° 3828-3829, *SCEA du Chéneau* c/ *INAPORC* c/ *Cherel* c/ *CNIEL*, Lebon p. 698 ; AJDA 2012. 27, chron. M. Guyomar et X. Domino ; *ibid*. 2011. 2041 ; D. 2011. 3046, et les obs., note F. Donnat ; *ibid*. 2012. 244, obs. N. Fricero ; RFDA 2011. 1122, concl. J.-D. Sarcelet ; *ibid*. 1129, note B. Seiller ; *ibid*. 1136, note A. Roblot-Troizier ; *ibid*. 2012. 339, étude J.-L. Mestre ; *ibid*. 377, chron. L. Clément-Wilz, F. Martucci et C. Mayeur-Carpentier ; Constitutions 2012. 294, obs. A. Levade ; RTD civ. 2011. 735, obs. P. Remy-Corlay ; RTD eur. 2012. 135, étude D. Ritleng .

(99) Cette expression est curieuse car le moyen tiré de la contrariété au droit de l'Union n'est pas d'ordre public (CE, 11 janv. 1991, n° 90995, *SA « Morgane »*, Lebon p. 9 ; AJDA 1991. 149 ; *ibid*. 111, chron. E. Honorat et R. Schwartz ; RFDA 1991. 652, concl. M.-D. Hagelsteen ; CE, 28 juill. 1993, n° 118717, *Bach*, Lebon).

(100) CE, sect., 23 mars 2012, n° 331805, *Fédération Sud Santé sociaux*, Lebon p. 102, concl. C. Landais ; AJDA 2012. 620 ; *ibid*. 1583, note E. Marc ; D. 2012. 1012, obs. S. Brondel ; Just. & cass. 2013. 118, concl. C. Landais ; RDT 2012. 376, obs. H. Tissandier ; RFDA 2012. 429, concl. C. Landais ; *ibid*. 961, chron. C. Mayeur-Carpentier, L. Clément-Wilz et F. Martucci ; Constitutions 2012. 294, obs. A. Levade ; RTD eur. 2012. 926, obs. D. Ritleng . Vous aviez auparavant dégagé, sans nuances, une « obligation pour les autorités nationales d'assurer l'application du droit communautaire », que vous aviez d'ailleurs distinguée des « exigences inhérentes à la hiérarchie des normes » (CE, sect., 3 déc. 1999, n° 164789-165122, *Association ornithologique et mammalogique de Saône-et-Loire et Rassemblement des opposants à la chasse*, Lebon p. 379, concl. F. Lamy ; AJDA 2000. 170 ; *ibid*. 120, chron. M. Guyomar et P. Collin ; D. 2000. 272, note G. Toulemonde ; RFDA 2000. 59, concl. F. Lamy ; *ibid*. 664, note L. Favoreu ; *ibid*. 668, note B. Genevois ; *ibid*. 676, note D. de Béchillon ; *ibid*. 678, note G. Carcassonne ; RTD civ. 2000. 194, obs. R. Libchaber).

(101) CE, ass., 19 juill. 2019, n° 424216-424217, *Association des Américains accidentels,* préc. Cette solution peut sembler comporter une adhérence avec la jurisprudence Fédération nationale de la libre pensée. En effet, la primauté du droit de l'Union (sous réserve de la suprématie constitutionnelle) est une exigence constitutionnelle, découlant de l'art. 88-1. Par suite, la confrontation de l'engagement international au profit du droit de l'Union pourrait s'analyser comme un contrôle de constitutionnalité de cet engagement. Mais ce serait commettre l'erreur de perspective décrite par J. Boucher dans ses conclusions sur la décision *Kandyrine* : il ne s'agit pas ici d'apprécier la validité d'un traité au regard d'une norme supérieure, mais simplement de définir la norme applicable au litige dont le juge administratif est saisi, à la lumière des exigences constitutionnelles.

(102) Les formulations, elles, ont pu varier : « L'invocation d'atteintes portées soit aux droits fondamentaux tels qu'ils sont formulés par la Constitution d'un État membre soit aux principes d'une structure constitutionnelle nationale ne saurait affecter la validité d'un acte de la Communauté ou son effet sur le territoire de cet État membre » (CJCE, 17 déc. 1970, aff. 11/70, *Internationale Handelsgesellschaft*, Rev. UE 2015. 562, étude S. Van Raepenbusch ; CJCE, 2 juill. 1996, aff. C-473/93, *Commission c/ Luxembourg*, Dr. soc. 1997. 510, chron. S. Van Raepenbusch . « Il ne saurait être admis que des règles de droit national, fussent-elles d'ordre constitutionnel, portent atteinte à l'unité et à l'efficacité du droit de l'Union » (CJUE, 8 sept. 2010, aff. C-409/06, *Winner Wetten GmbH*, AJDA 2010. 2305, chron. M. Aubert, E. Broussy et F. Donnat ; Rev. UE 2015. 562, étude S. Van Raepenbusch).

(103) La primauté s'efface ainsi, de manière temporaire, pour l'application de mesures conservatoires exigées par la situation, le temps que la Cour se prononce sur la validité d'un règlement ou d'une directive (CJCE, 9 nov. 1995, aff. C-465/93, *Atlanta Fruchthandelsgesellschaft mbH* c/ *Bundesamt für Ernährung und Forstwirtschaft*, AJDA 1996. 273, chron. H. Chavrier, E. Honorat et G. de Bergues ; D. 1995. 256 ; RTD eur. 1996. 77, étude R. Mehdi ; Rev. UE 2015. 370, étude G. Eckert), pour respecter le principe de l'autorité de la chose jugée, de sorte qu'une juridiction nationale n'a pas à écarter des règles

de procédure internes pour réexaminer ou annuler une décision de justice passée en force de chose jugée, bien qu'elle soit contraire au droit de l'Union (CJCE, 16 mars 2006, aff. C-234/04, *Kapferer* c/ *Schlank & Schick GmbH*, AJDA 2006. 634 ; *ibid*. 2271, chron. E. Broussy, F. Donnat et C. Lambert ; D. 2006. 1247 ; Rev. crit. DIP 2007. 140, note S. Francq ; RTD civ. 2006. 728, obs. P. Remy-Corlay, réaffirmée par CJCE, 3 sept. 2009, aff. C-2/08, RTD eur. 2010. 113, chron. L. Coutron ; Rev. UE 2015. 370, étude G. Eckert ; cette solution a seulement été écartée en matière de compatibilité des aides d'État au traité : CJCE, 18 juill. 2007, aff. C-119/05, *Ministero dell'industria, del Commercio e dell'Artigianato* c/ *Lucchini SpA*, AJDA 2007. 1500 ; *ibid*. 2248, chron. E. Broussy, F. Donnat et C. Lambert ; Rev. UE 2015. 370, étude G. Eckert), ou encore pour prévenir toute violation du principe de légalité des délits et des peines en raison d'un défaut de précision de la loi ou au motif de l'application rétroactive d'une loi pénale plus sévère à des faits antérieurs et des procédures en cours (CJUE, 8 sept. 2015, aff. C-105/14, *MAS, MB*, RTD eur. 2016. 77, obs. D. Berlin ; *ibid*. 2017. 739, étude Nicoletta Perlo, rendu à la suite d'un bras de fer avec la Cour constitutionnelle italienne dans l'affaire *Tarrico* (v. le savant commentaire d'E. Dubout, « La primauté du droit de l'Union et le passage au pluralisme constitutionnel », RTD eur. 2018. 563). D'une certaine manière, l'absence d'engagement de la responsabilité de l'État à raison d'une violation non manifeste du droit de l'Union par une juridiction nationale statuant en dernier ressort peut aussi s'analyser comme une forme de tempérament (CJCE, 30 sept. 2003, aff. C-224/01, *Gerhard Köbler* c/ *Autriche*, AJDA 2003. 2146, chron. J.-M. Belorgey, S. Gervasoni et C. Lambert ; *ibid*. 2004. 315, chron. J.-M. Belorgey, S. Gervasoni et C. Lambert ; *ibid*. 423, étude J. Courtial ; D. 2003. 2546, et les obs. ; RSC 2004. 178, chron. L. Idot ; RTD eur. 2015. 232, obs. C. Yannakopoulos ; *ibid*. 232, obs. C. Yannakopoulos ; CE, 18 juin 2008, n° 295831, *Gestas*, Lebon ; AJDA 2008. 1237 ; RFDA 2008. 755, concl. C. de Salins ; *ibid*. 1178, note D. Pouyaud).

(104) V. pour une telle injonction : CJCE, 22 mai 2003, aff. C-462/99, *Connect Austria*, RTD eur. 2004. 669, chron. L. Idot ; *ibid*. 2005. 131, chron. J.-B. Blaise et L. Idot .

(105) Sous réserve des modestes tempéraments que la cour elle-même y apportés (v. *supra* note 103).

(106) CE, ass., 30 oct. 1998, n° 200286-200287, *Sarran et Levacher et autres*, Lebon p. 368 ; AJDA 1998. 1039 ; *ibid*. 962, chron. F. Raynaud et P. Fombeur ; *ibid*. 2014. 114, chron. P. Fombeur ; D. 2000. 152, note E. Aubin ; RFDA 1998. 1081, concl. C. Maugüé ; *ibid*. 1094, note D. Alland ; *ibid*. 1999. 57, étude L. Dubouis ; *ibid*. 67, note B. Mathieu et M. Verpeaux ; *ibid*. 77, étude O. Gohin ; RTD civ. 1999. 232, obs. N. Molfessis ; CE, 3 déc. 2001, n° 226514, *Syndicat national de l'industrie pharmaceutique et autres*, Lebon T. p. 790-1078-1198 ; AJDA 2002. 1219, étude A.-L. Valembois ; RTD eur. 2003. 197, étude C. Castaing . La Cour de cassation a repris la logique de l'arrêt *Sarran*, tout en semblant réserver le cas de l'Union européenne (Cass., ass. plén., 2 juin 2000, n° 99-60.274, *M^elle^ Fraisse*, Bull ass. plén, n° 4, p. 7 ; D. 2000. 865, note B. Mathieu et M. Verpeaux ; *ibid*. 2001. 1636, chron. B. Beignier et S. Mouton ; RTD civ. 2000. 672, obs. R. Libchaber).

(107) Cons. const., 9 août 2012, n° 2012-653 DC. AJDA 2012. 1717, étude M. Lombard, S. Nicinski et E. Glaser ; RFDA 2012. 1043, étude E. Oliva ; Constitutions 2012. 562, obs. P. Bachschmidt ; *ibid*. 575, obs. A. Levade ; *ibid*. 628, obs. A. Barilari ; RTD eur. 2012. 855, note J. Roux ; Rev. UE 2012. 565, édito. F. Chaltiel

(108) Ce qui ne peut être le cas que si cette norme est inconditionnelle.

(109) Ce qui peut conduire à écarter le moyen de légalité comme inopérant si la norme invoquée s'avère d'un rang inférieur à la « disposition-source » ainsi identifiée ou lorsqu'elles sont d'un niveau égal - en jugeant que l'une a entendu déroger à l'autre - à quelques exceptions près. Il en va ainsi des règles de forme et procédure que l'administration a pu se prescrire à elle-même par une disposition de même rang (v. en dernier lieu : CE, 11 oct. 2017, n° 403855, *Syndicat éducation populaire - UNSA*, Lebon T. p. 434-758 ; AJDA 2017. 1984 dans la ligne de CE, ass., 19 mai 1983, n° 23127-23181-23182, *Club sportif et familial de la Fève*, Lebon p. 205), de la confrontation entre deux engagements internationaux, qui se résout conformément au mode d'emploi issu de votre décision d'assemblée *Kandyrine de Brito Paiva* du 23 déc. 2011 (n° 303678, Lebon p. 623, concl. J. Boucher ; AJDA 2012. 4 ; *ibid*. 201, chron. X. Domino et A. Bretonneau ; D. 2012. 98, et les obs. ; Just. & cass. 2012. 117, concl. J. Boucher ; RFDA 2012. 1, concl. J. Boucher ; *ibid*. 19, avis G. Guillaume ; *ibid*. 26, note D. Alland ; *ibid*. 377, chron. L. Clément-Wilz, F. Martucci et C. Mayeur-Carpentier ; *ibid*. 455, chron. H. Labayle, F. Sudre, X. Dupré de Boulois et L. Milano ; *ibid*. 2013. 417, chron. C. Santulli ; Constitutions 2012. 295, obs. A. Levade ;

RTD eur. 2012. 929, obs. D. Ritleng), et de celle de deux règles issues du droit de l'Union soulevant une difficulté sérieuse, ce qui vous oblige à en saisir la Cour de justice de l'Union européenne afin de déterminer laquelle des deux doit prévaloir. À l'inverse, lorsque la norme invoquée reste supérieure à la « disposition-source », vous écartez le moyen comme irrecevable lorsque vous estimez ne pas être compétent pour procéder à la confrontation. Tel est le cas du contrôle de constitutionnalité des lois - c'est le fameux « écran législatif », et de celui des engagements internationaux de la France - c'est le « traité-écran » - expression rappelée par J. Boucher dans ses conclusions sur l'affaire *Kandyrine de Brito Paiva* (cette incompétence vaut non seulement lorsque l'acte attaqué est le décret de publication de l'engagement international, mais aussi lorsqu'il se borne à tirer les conséquences nécessaires de cet engagement international : v. par ex. la décision *Association des américains accidentels*). Échappe également à votre compétence l'invalidation du droit dérivé de l'Union au regard du droit primaire, dont la Cour de justice a le monopole - toute difficulté sérieuse en la matière devant lui être renvoyée.

(110) La jurisprudence rendue à propos de l'art. 88-2 relatif au mandat d'arrêt européen, qui a donné lieu à un renvoi préjudiciel du Conseil constitutionnel à la CJUE afin de déterminer si la décision-cadre guidait la plume du législateur ou si elle lui laissait une marge d'appréciation permettant d'y loger un contrôle de constitutionnalité, ne s'explique que par la rédaction très particulière de cette disposition constitutionnelle. Le Constituant s'en est expressément remis aux actes pris par l'Union européenne dans ce domaine. On peut du reste se demander s'il n'y aurait pas place également, en la matière, pour la réserve de l'identité constitutionnelle de la France, dès lors que le consentement donné par le Constituant peut difficilement s'interpréter comme un blanc-seing absolu.

(111) Initialement, la clause de sauvegarde était limitée aux « dispositions expresses contraires de la Constitution » (décision n° 2004-496 DC du 10 juin 2004, consid. 7). AJDA 2004. 1534 , note J. Arrighi de Casanova ; *ibid*. 1937 ; *ibid*. 1385, tribune P. Cassia ; *ibid*. 1497, tribune M. Verpeaux ; *ibid*. 1537, note M. Gautier et F. Melleray , note D. Chamussy ; *ibid*. 2261, chron. J.-M. Belorgey, S. Gervasoni et C. Lambert ; D. 2005. 199 , note S. Mouton ; *ibid*. 2004. 1739, chron. B. Mathieu ; *ibid*. 3089, chron. D. Bailleul ; *ibid*. 2005. 1125, obs. V. Ogier-Bernaud et C. Severino ; RFDA 2004. 651, note B. Genevois ; *ibid*. 2005. 465, étude P. Cassia ; RTD civ. 2004. 605, obs. R. Encinas de Munagorri ; RTD eur. 2004. 583, note J.-P. Kovar ; *ibid*. 2005. 597, étude E. Sales Mais il ressort du commentaire autorisé de cette décision que cette notion renvoyait à une norme constitutionnelle écrite propre à la Constitution française (J.-E. Schoettl, « Le nouveau régime juridique de la communication en ligne devant le Conseil constitutionnel », LPA, n° 122, 18 juin 2004). Si la condition du caractère écrit a été abandonnée par la suite, cette décision jetait déjà les bases de la jurisprudence actuelle.

(112) Sans qu'on sache très bien, en l'état de sa jurisprudence, si cette norme doit revêtir une importance particulière au sein du bloc de constitutionnalité. La notion d'« identité constitutionnelle », à laquelle la doctrine rattache couramment la forme républicaine du gouvernement ou le principe de laïcité, pourrait le laisser entendre.

(113) Cons. const., 27 juill. 2006, n° 2006-540 DC , consid. 17 à 20 D. 2006. 2157, chron. C. Castets-Renard ; *ibid*. 2878, chron. X. Magnon ; *ibid*. 2007. 1166, obs. V. Bernaud, L. Gay et C. Severino ; RTD civ. 2006. 791, obs. T. Revet ; *ibid*. 2007. 80, obs. R. Encinas de Munagorri ; Cons. const., 17 déc. 2010, n° 2010-79 QPC . AJDA 2011. 638 ; RFDA 2011. 353, étude G. Eveillard ; Constitutions 2011. 53, obs. A. Levade ; *ibid*. 581, chron. V. Tchen ; Rev. crit. DIP 2011. 1, étude D. Simon Il en va différemment, bien entendu, si le constituant y a consenti. Initialement, le Conseil constitutionnel avait jugé que la directive pouvait être tenue en échec par une disposition expresse contraire de la Constitution (Cons. const., 10 juin 2004, n° 2004-496 DC) AJDA 2004. 1534 , note J. Arrighi de Casanova ; *ibid*. 1937 ; *ibid*. 1385, tribune P. Cassia ; *ibid*. 1497, tribune M. Verpeaux ; *ibid*. 1537, note M. Gautier et F. Melleray , note D. Chamussy ; *ibid*. 2261, chron. J.-M. Belorgey, S. Gervasoni et C. Lambert ; D. 2005. 199 , note S. Mouton ; *ibid*. 2004. 1739, chron. B. Mathieu ; *ibid*. 3089, chron. D. Bailleul ; *ibid*. 2005. 1125, obs. V. Ogier-Bernaud et C. Severino ; RFDA 2004. 651, note B. Genevois ; *ibid*. 2005. 465, étude P. Cassia ; RTD civ. 2004. 605, obs. R. Encinas de Munagorri ; RTD eur. 2004. 583, note J.-P. Kovar ; *ibid*. 2005. 597, étude E. Sales . De même, le Conseil constitutionnel, saisi au titre de l'art. 54 de la Constitution des stipulations d'un accord international qui doit être signé tant par l'Union européenne que par chacun des États membres de celle-ci, mais qui relève d'une compétence exclusive de l'Union européenne, limite son contrôle au respect d'une règle ou d'un principe inhérent à l'identité constitutionnelle de la France (Cons. const., 31 juill. 2017, n° 2017-749 DC , *Accord économique et commercial global entre le Canada, d'une part, et l'Union européenne et ses États membres, d'autre part*). AJDA 2017. 2008 , note B. Bonnet ; D. 2017. 1656, et les obs. ; *ibid*. 2378, point de vue J. Roux

(114) C'est ce qui explique d'ailleurs que le Conseil constitutionnel n'ait pas estimé nécessaire de réviser la Constitution préalablement à la ratification de feu le Traité établissant une Constitution pour l'Europe.

(115) Le commentaire aux *Cahiers* de la décision du 19 nov. 2004 indique que la « porte constitutionnelle » a été ouverte aux « neuf dixièmes » à la réception immédiate du droit communautaire dans l'ordre juridique interne.

(116) L'assemblée générale du Conseil d'État a en revanche rattaché à l'identité constitutionnelle de la France le droit d'asile constitutionnel, dans un avis non public mais mis en ligne sur le site du GISTI (avis portant sur l'application de la notion de « pays tiers sûr »).

(117) Dans le cadre de son contrôle du respect de l'identité constitutionnelle (*Identitätskontrolle*), la Cour constitutionnelle fédérale allemande se reconnaît la faculté de confronter aussi bien un acte réglementaire qu'un acte individuel, pris en vertu du droit de l'Union, aux normes intangibles limitativement énumérées au troisième al. de l'art. 79 de la même Loi fondamentale et auxquelles même une révision constitutionnelle ne pourrait déroger, selon la clause dite d'éternité : l'organisation fédérale, la participation des *Länder* à la législation nationale, le respect de la dignité humaine ou encore le principe de démocratie, dont découle notamment le droit pour chaque citoyen de faire respecter la souveraineté nationale, notamment la souveraineté budgétaire de l'Allemagne, en interdisant aux autorités allemandes de procéder à des transferts de compétences ou de prendre des décisions qui videraient de sa substance le processus démocratique à l'échelon national du fait de l'approfondissement de l'intégration européenne. En Espagne, la primauté du droit de l'Union s'entend sous réserve de sa compatibilité avec les principes fondamentaux de l'État social et démocratique de droit établi par la Constitution nationale (déclaration n° 1/2004 du 13 déc. 2004 du Tribunal constitutionnel espagnol). En Italie, la théorie des « contre-limites » met en échec la primauté du droit de l'Union dans le cas où seraient violés les principes fondamentaux de l'ordonnancement constitutionnel italien ou les droits inaliénables de la personne humaine (Cour const., 18 déc. 1973, n° 183 ; 22 oct. 2014, n° 238, concernant l'affaire *Taricco* qui a finalement conduit la Cour de justice à adapter sa jurisprudence : CJUE, 8 sept. 2015, aff. C-105/14, RTD eur. 2016. 77, obs. D. Berlin ; *ibid*. 2017. 739, étude Nicoletta Perlo). Le Conseil d'État grec a quant à lui affirmé la supériorité de la Constitution sur le droit de l'Union (CE n° 3242/2004 du 16 nov. 2004). À l'époque où le Royaume-Uni était encore membre de l'Union européenne, la Cour suprême estimait elle aussi que le *Bill of rights*, qui se rattache à l'identité constitutionnelle britannique, devrait primer sur le *European Communities Act*, qui incorporait en droit britannique les traités européens (V. l'arrêt *HS2 c/ Secretaire d'État au transport* [2014] UKSC 3).

(118) V. pour cette présentation l'intéressant article de J.-P. Jacqué, « La Cour de justice de l'Union européenne et la théorie des contre limites », http://www.droit-union-europeenne.be/432984946.

(119) CE, ass., 8 févr. 2007, n° 287110, *Société Arcelor Atlantique et Lorraine*, Lebon p. 55, concl. M. Guyomar ; AJDA 2007. 577, chron. F. Lenica et J. Boucher ; *ibid*. 1097, tribune P. Cassia ; D. 2007. 2272, note M. Verpeaux ; *ibid*. 1166, obs. V. Bernaud, L. Gay et C. Severino ; *ibid*. 2742, chron. P. Deumier ; RDI 2007. 130, obs. L. Fonbaustier ; RFDA 2007. 384, concl. M. Guyomar ; *ibid*. 564, note A. Levade ; *ibid*. 578, note X. Magnon ; *ibid*. 596, chron. T. Rambaud et A. Roblot-Troizier ; *ibid*. 789, note M. Canedo-Paris ; *ibid*. 2008. 780, chron. T. Haas et C. Santulli ; Constitutions 2010. 58, obs. A. Levade ; RTD civ. 2007. 299, obs. P. Remy-Corlay ; RTD eur. 2007. 378, note P. Cassia ; *ibid*. 2008. 835, chron. D. Ritleng, A. Bouveresse et J.-P. Kovar. Vous avez tiré toutes les conséquences de la jurisprudence constitutionnelle en matière de QPC : en l'absence de mise en cause d'une règle ou d'un principe inhérent à l'identité constitutionnelle de la France, il n'appartient pas au Conseil d'État de renvoyer au Conseil constitutionnel la QPC dirigée contre des dispositions législatives se bornant à tirer les conséquences nécessaires de dispositions précises et inconditionnelles d'une directive (CE, 14 sept. 2015, n° 389806, *Société NotreFamille.com*, Lebon T. p. 576-848 ; AJDA 2015. 2441, note F. Rassu ; D. 2015. 2214, obs. J. Larrieu, C. Le Stanc et P. Tréfigny ; RTD com. 2016. 123, obs. F. Pollaud-Dulian ; RTD eur. 2017. 313, obs. D. Ritleng).

(120) Vous avez par la suite réitéré ce mode d'emploi, en abandonnant au passage, très logiquement, la référence à l'art. 55 de la Constitution : CE, 7 févr. 2020, n° 388649, *Confédération paysanne et autres*, Lebon p. 25, concl. L. Cytermann ; AJDA 2020. 327 ; *ibid*. 1972, note N. Pauthe ; D. 2020. 1012, obs. V. Monteillet et G. Leray ; AJ fam. 2020. 146, obs. A. Dionisi-Peyrusse.

(121) V. *a contrario* : CE, 8 juill. 2020, n° 428271-428276-429018-429469, *Association de défense des ressources marines et Fédération nationale de la plaisance et des pêches en mer*. Lebon. Cette décision juge aussi logiquement que, lorsque le décret intervient dans le cadre de la marge d'appréciation de l'État, et non pour la transposition de stipulations ou dispositions inconditionnelles, le contrôle de constitutionnalité du décret s'effectue normalement.

(122) Vous n'êtes pas allés, en revanche, jusqu'à consacrer la méthodologie de l'avis de l'assemblée générale du Conseil d'État du 26 sept. 2002, *Décision-cadre du Conseil de l'Union européenne du 13 juin 2002 relative au mandat d'arrêt européen*, n° 368.282, *Rapport public 2003*, p. 192) consistant à vérifier qu'une décision-cadre à transposer (ou une directive) ne comporte pas de dispositions contraires à la Constitution ou à des principes de valeur constitutionnelle, mettant en cause les droits et libertés constitutionnellement garantis ou portant atteinte aux conditions essentielles d'exercice de la souveraineté nationale.

(123) V. à propos du respect de la vie privée : Cons. const., 29 juill. 2004, n° 2004-499 DC, consid. 7 et 8, D. 2005. 1132 ; *ibid*. 1125, obs. V. Ogier-Bernaud et C. Severino ; RFDA 2005. 465, étude P. Cassia ; pour le principe d'égalité et la liberté d'entreprendre (Cons. const., 26 juill. 2018, n° 2018-768 DC, consid. 12 et 38 à 40, RDT 2018. 666, étude V. Champeil-Desplats).

(124) Nous empruntons ces notions au très intéressant article de M. Blanquet, « La protection de l'identité constitutionnelle de la France », *in La Constitution européenne de la France*, Dalloz.

(125) Vous observerez, à cet égard, que la Cour de justice a elle-même posé des limites à cette logique du « mieux-disant ». Non seulement elle n'admet pas que les dispositions précises et inconditionnelles d'une directive puissent être mises à l'écart sur le fondement d'une Constitution nationale, comme vous l'envisagez. Mais même lorsque le droit de l'Union laisse aux États membres une certaine marge de manoeuvre dans sa mise en oeuvre, elle considère qu'un État membre ne peut appliquer des standards nationaux de protection des droits fondamentaux dans la mise en oeuvre des actes de droit dérivé par la législation et la réglementation nationales, que si cette application ne compromet pas le niveau de protection prévu par la Charte, telle qu'interprétée par la Cour, ni la primauté, l'unité et l'effectivité du droit de l'Union, ce qui tend à faire des droits fondamentaux garantis par le droit de l'Union à la fois des planchers et des plafonds (CJUE, 26 févr. 2013, aff. C-617/10 , *Aklagaren* c/ *Hans Akerberg Fransson*, pt 29, AJDA 2013. 1154, chron. M. Aubert, E. Broussy et H. Cassagnabère ; AJ pénal 2013. 270 , note C. Copain ; RFDA 2013. 1231, chron. C. Mayeur-Carpentier, L. Clément-Wilz et F. Martucci ; RTD civ. 2014. 312, obs. L. Usunier ; RTD eur. 2013. 267, note D. Ritleng ; *ibid*. 2015. 184, obs. F. Benoît-Rohmer ; *ibid*. 235, obs. L. d'Ambrosio et D. Vozza et CJUE, 26 févr. 2013, aff. C-399/11, *Stefano Melloni* c/ *Ministerio Fiscal*, pts 55 s., AJDA 2013. 1154, chron. M. Aubert, E. Broussy et H. Cassagnabère ; D. 2013. 711 ; AJ pénal 2013. 350, obs. J. Lelieur ; Constitutions 2013. 184, obs. A. Levade ; RTD eur. 2013. 267, note D. Ritleng ; *ibid*. 812, chron. P. Beauvais ; *ibid*. 2015. 166, obs. F. Benoît-Rohmer ; *ibid*. 235, obs. L. d'Ambrosio et D. Vozza ; Rev. UE 2015. 277, étude D. Ritleng ; *ibid*. 562, étude S. Van Raepenbusch ; v. aussi, CJUE, 24 sept. 2019, aff. C-507/17, *Google LLC* c/ *Commission nationale de l'informatique et des libertés*, pt 72, AJDA 2019. 1839 ; *ibid*. 2291, chron. P. Bonneville, C. Gänser et S. Markarian ; D. 2020. 515 , note T. Douville ; *ibid*. 2019. 2022, note J.-L. Sauron ; *ibid*. 2266, obs. J. Larrieu, C. Le Stanc et P. Tréfigny ; *ibid*. 2020. 951, obs. S. Clavel et F. Jault-Seseke ; *ibid*. 1262, obs. W. Maxwell et C. Zolynski ; *ibid*. 1970, obs. L. d'Avout, S. Bollée et E. Farnoux ; Dalloz IP/IT 2019. 631, obs. N. Martial-Braz ; Légipresse 2019. 515 et les obs. ; Rev. crit. DIP 2020. 874, Eclairages A. d'Ornano ; RTD eur. 2020. 311, obs. F. Benoît-Rohmer ; *ibid*. 316, obs. F. Benoît-Rohmer).

(126) L'écran législatif joue aussi lorsque le décret se borne à tirer les conséquences nécessaires de la loi (CE, 6 déc. 2012, n° 347870-347871, *Société Air Algérie*, Lebon p. 398 ; AJDA 2012. 2373, chron. X. Domino et A. Bretonneau ; RFDA 2013. 367, chron. C. Mayeur-Carpentier, L. Clément-Wilz et F. Martucci ; *ibid*. 417, chron. C. Santulli ; *ibid*. 653, note P. Cassia ; *ibid*. 663, chron. A. Roblot-Troizier et G. Tusseau ; RTD eur. 2013. 384, obs. L. Grard ; *ibid*. 871, obs. D. Ritleng). Cette décision porte sur le cas de la transposition législative de dispositions précises et inconditionnelles d'une directive. Mais la solution vaut a fortiori lorsque la loi est le fruit d'un pouvoir d'appréciation de l'État membre. Dans ce cas, il faut, pour le requérant, soulever un moyen d'inconventionnalité de la loi, pour ce qui concerne les droits et libertés garantis par le droit de l'Union (et s'il s'agit d'une transposition de directive inconditionnelle ou une adaptation à un règlement, il faudra soutenir que l'acte de droit dérivé, où se loge réellement la disposition litigieuse, est contraire au droit primaire) et une QPC, pour ce qui concerne l'identité constitutionnelle de la France, à supposer qu'elle renferme bien un droit ou une liberté - ce qui devrait le plus souvent être le cas.

(127) On imagine d'ailleurs assez mal l'État soulever ici une QPC, sauf à rechercher audacieusement une forme de validation de son argumentation par le Conseil constitutionnel en vue de fragiliser la critique de conventionnalité élevée par les requérants.

(128) CE, 9 juill. 2010, n° 327663 et autres, *Fédération nationale de la libre pensée (FNLP)*, Lebon p. 268, concl. R. Keller ; AJDA 2010. 1397 ; *ibid*. 1635 ; *ibid*. 1950 ; *ibid*. 1635, chron. S.-J. Liéber et D. Botteghi, note A. Legrand ; D. 2010. 2868, obs. O. Boskovic, S. Corneloup, F. Jault-Seseke, N. Joubert et K. Parrot ; RFDA 2010. 980, concl. R. Keller ; *ibid*. 995, note T. Rambaud et A. Roblot-Troizier ; *ibid*. 2011. 173, chron. C. Santulli ; v. aussi, CE, ass., 23 déc. 2011, n° 303678, *Kandyrine de Brito Paiva*, préc. Cette incompétence vaut non seulement lorsque l'acte attaqué est le décret de publication de l'engagement international, mais aussi lorsqu'il se borne à tirer les conséquences nécessaires de cet engagement international (v. par ex. la décision *Association des Américains accidentels*). Il faut bien avouer que les justifications théoriques de l'angle mort qui en résulte sont fragiles (pour leur présentation : D. Botteghi et S-J. Lieber, « De deux questions de droit international public et d'une question de procédure contentieuse », AJDA 2010. 1635). Elle ne peut en tous les cas être trouvée dans la seule règle *Pacta sunt servanda*, dont découlerait une forme d'immunité juridictionnelle des engagements antérieurement souscrits, puisqu'il est admis qu'un engagement international doit être laissé inappliqué s'il est contraire à un règlement européen (V. la même décision *Association des Américains accidentels*). Il en résulte d'ailleurs, paradoxalement, que le droit de l'Union est mieux garanti que le droit constitutionnel, comme c'était le cas de manière générale avant la mise en place de la QPC. À notre avis, le seul argument recevable est celui qui tire de la Constitution, notamment de son art. 54, la volonté du constituant de ne pas investir le juge administratif de la mission de contrôler la conformité des traités à la Constitution.

(129) Dans son article de référence sur le Conseil d'État et l'interprétation de la loi (RFDA 2002. 877), le président Genevois ne hiérarchise pas les techniques d'interprétation téléologique (intention du législateur) et d'interprétation conforme aux normes supérieures, même s'il relève que la seconde occupe une place croissante dans le raisonnement du juge administratif.

(130) On se gardera toutefois de donner trop de portée à cet argument : en allant jusqu'au bout de cette logique, il faudrait aussi considérer que l'obligation de respecter les traités, qui découle du principe *Pacta sunt servanda* issu du 14e al. du Préambule de 1946, et la supériorité de leur autorité sur celle des lois, conférée par l'art. 55 de la Constitution, ne valent que sous réserve de leur conformité à la Constitution, ce qui vous conduirait à effectuer ce contrôle et à abandonner la jurisprudence *Fédération nationale de la libre pensée*...

(131) L'art. 15 de la directive *e-privacy* se borne à ouvrir une faculté de dérogation aux États-membres.

(132) La même conclusion devrait être tirée, à notre avis, pour une loi ayant pour objet de transposer une directive (que ses dispositions soient précises et inconditionnelles ou non) ou d'adapter le droit interne à un règlement. Certes, dans ce cadre, le Conseil constitutionnel exerce, au stade du contrôle *a priori*, un contrôle de l'incompatibilité manifeste entre la loi et l'acte de droit dérivé, sur le fondement de l'art. 88-1. Et dans ce cadre, le gouvernement pourrait tout à fait se prévaloir de la méconnaissance de l'identité constitutionnelle de la France par la directive. Mais ce contrôle résiduel ne s'exerce plus au stade de la QPC, car l'obligation de transposition des directives découlant de l'art. 88-1 n'est pas au nombre des droits et libertés que la Constitution garantit (Cons. const., 17 déc. 2010, n° 2010-79 QPC) AJDA 2011. 638 ; RFDA 2011. 353, étude G. Eveillard ; Constitutions 2011. 53, obs. A. Levade ; *ibid*. 581, chron. V. Tchen ; Rev. crit. DIP 2011. 1, étude D. Simon. Et cette configuration est théorique : la difficulté constitutionnelle surgira le plus souvent au stade aval de l'interprétation de la directive ou du règlement par la CJUE, et non dès son adoption par le législateur européen, souvent avec l'accord de la France.

(133) En tout état de cause, nous pensons d'ailleurs qu'il y aurait place dans ce cas pour un aménagement de votre jurisprudence *Fédération nationale de la libre pensée* afin de vous assurer que la portée effective que la jurisprudence de la Cour de justice confère à une stipulation des traités ne contredit pas la Constitution. Contrairement aux juridictions nationales, qui doivent donner une interprétation des traités conforme à la Constitution, et notamment faire leur la lecture que le Conseil constitutionnel a pu en donner dans le cadre de son contrôle pré-ratification, le cas échéant, la Cour de justice est libre de sa lecture du droit primaire. Or comme l'indiquait le commentaire aux *Cahiers* de la décision du Conseil constitutionnel de 2004 sur la Constitution pour l'Europe, si la Charte des droits fondamentaux n'appelait aucune révision constitutionnelle, « il est (...) clair que toute interprétation jurisprudentielle future des Cours de Luxembourg ou de Strasbourg allant au-delà des dispositions de la Charte ou restreignant la portée de ses clauses de limitation particulières ou générales conduirait à altérer les données au vu desquelles s'est prononcé le Conseil constitutionnel pour arriver à la conclusion que la deuxième partie du traité n'appelait pas de révision ». Le Conseil constitutionnel ne pouvant pas se faire justice lui-même puisqu'il ne peut être saisi postérieurement à la ratification, personne d'autre que vous ne pourrait y remédier, nous semble-t-il. Nous laissons ces dernières élucubrations à l'usage des générations futures.

(134) *BVerfG*, 7 juin 2000, *Solange III*, 2 *BvL* 1/97, RTD eur. 2001. 155.

(135) S'agissant par exemple du droit au déréférencement des contenus sur les moteurs de recherche, qui conduit à mettre en balance le respect de la vie privée, d'un côté, et la liberté d'expression et d'entreprendre, de l'autre, vous pourriez, saisi d'un moyen de défense en ce sens, être amené à définir des règles du jeu différentes de celles que la Cour de justice a dégagées, et non plus seulement à appliquer la jurisprudence européenne au cas particulier qui vous est soumis, ce qui est votre rôle normal de juge de droit commun du droit de l'Union.

(136) Nous pensons que vous disposez d'une certaine marge d'interprétation des arrêts préjudiciels. L'art. 104 du règlement de procédure de la Cour de justice exclut, dans sa relation avec les juridictions de renvoi, l'application de l'art. 158 qui prévoit qu'en cas de difficulté sur le sens et la portée d'un arrêt ou d'une ordonnance, il appartient à la Cour de l'interpréter. Dans le cadre du mécanisme préjudiciel, le § 2 de l'art. 104 confie aux juridictions nationales le soin d'apprécier si elles s'estiment suffisamment éclairées par une décision préjudicielle. Si ce n'est pas le cas, il convient de saisir à nouveau la Cour. C'est donc le juge national qui doit au premier chef porter une appréciation.

(137) V. aussi, à propos de la subdélégation illégale du pouvoir réglementaire : CE, 17 nov. 2010, n° 320827, *Société Arthus consulting*, Lebon T. p. 607-920 ; AJDA 2011. 337, concl. M. Vialettes.

(138) Il l'est par exception, s'agissant de l'incompétence du pouvoir réglementaire intervenant dans le domaine de la loi.

(139) On rappellera au passage que le Danemark et l'Irlande bénéficient de clauses d'*opt-out* dans le domaine de l'espace de liberté, de sécurité et de justice, sans qu'à notre connaissance, la construction européenne s'en soit trouvée compromise.

(140) Ce considérant 14 précise : « Il convient d'harmoniser les dispositions législatives, réglementaires et techniques adoptées par les États membres en ce qui concerne la protection des données à caractère personnel, de la vie privée et des intérêts légitimes des personnes morales dans le secteur des communications électroniques afin d'éviter de créer des obstacles au marché intérieur des communications électroniques conformément à l'article 14 du traité ».

(141) Cons. const., 10 nov. 2011, n° 2011-192 QPC, consid. 20, AJDA 2011. 2206 ; D. 2011. 2721, édito. F. Rome ; Cons. const., 10 nov. 2016, n° 2016-738 DC, consid. 20 à 23, D. 2017. 1328, obs. N. Jacquinot et R. Vaillant.

(142) Cons. const., 7 août 2020, n° 2020-805 DC, *Loi instaurant des mesures de sûreté à l'encontre des auteurs d'infractions terroristes à l'issue de leur peine*, AJDA 2020. 2319, note M. Verpeaux ; *ibid*. 1817, tribune V. Goesel-Le Bihan ; D. 2020. 1869, note G. Beaussonie ; *ibid*. 1623 et les obs. ; *ibid*. 1853, chron. J. Pradel ; *ibid*. 2407, point de vue C. Duvert ; RSC 2020. 986, obs. A. Botton.

(143) Cons. const., 2 mars 2004, n° 2004-492 DC. D. 2004. 2756, obs. B. de Lamy ; *ibid*. 956, chron. M. Dobkine ; *ibid*. 1387, chron. J.-E. Schoettl ; *ibid*. 2005. 1125, obs. V. Ogier-Bernaud et C. Severino ; RSC 2004. 725, obs. C. Lazerges ; *ibid*. 2005. 122, étude V. Bück ; RTD civ. 2005. 553, obs. R. Encinas de Munagorri

(144) V. parmi d'innombrables exemples : Cons. const., 9 juin 2011, n° 2011-631 DC, *Loi relative à l'immigration, à l'intégration et à la nationalité*, consid. 78, AJDA 2011. 1174 ; *ibid*. 1936, étude O. Lecucq ; JA 2011, n° 442, p. 7, obs. S.Z.-D. ; *ibid*., n° 442, p. 9, obs. L.T. ; Constitutions 2011. 581, chron. V. Tchen ; *ibid*. 2012. 63, obs. A. Levade ; Cons. const., 9 oct. 2014, n° 2014-420/421 QPC, consid. 9, D. 2014. 2278, note A. Botton ; AJ pénal 2014. 574, note J.-B. Perrier.

(145) Comme l'indique P. de Montalivet dans son article consacré aux objectifs de valeur constitutionnelle publié aux *Cahiers du Conseil constitutionnel* n° 20 de juin 2006, « le Conseil constitutionnel considère que le législateur est soumis à l'interdiction de méconnaître les objectifs, ce qui signifie qu'il ne doit pas adopter de dispositions allant à leur encontre. Ainsi,

chaque objectif implique certaines interdictions pesant sur le législateur. Contrairement à certaines affirmations doctrinales, le Conseil sanctionne la violation des objectifs, confirmant leur juridicité ».

(146) Il en va ainsi, par exemple, de l'objectif de pluralisme des quotidiens d'information politique et générale (n° 86-210 DC du 29 juill. 1986) ou de l'objectif d'accessibilité et d'intelligibilité de la loi (Cons. const., 29 déc. 2005, n° 2005-530 DC, *Loi de finances pour 2006*, AJDA 2006. 13 ; D. 2006. 826, obs. V. Ogier-Bernaud et C. Severino).

(147) V. par ex. : CE, ass., 24 mars 2006, n° 288460-288465-288474-288485, *Société KPMG et Société Ernst & Young Audit et autres*, Lebon p. 154 ; AJDA 2006. 1028, chron. C. Landais et F. Lenica ; *ibid*. 841, tribune B. Mathieu ; *ibid*. 897, tribune F. Melleray ; D. 2006. 1224 ; *ibid*. 1190, chron. P. Cassia ; *ibid*. 1226, point de vue R. Dammann ; Rev. sociétés 2006. 583, note P. Merle ; RFDA 2006. 463, concl. Y. Aguila ; *ibid*. 483, note F. Moderne ; RTD civ. 2006. 527, obs. R. Encinas de Munagorri). Sur ce dernier sujet, nous nous permettrons de renvoyer le lecteur à notre article en hommage au président Stirn, « Le droit simple », *in La scène juridique : harmonies en mouvement*, Dalloz, 2019.

(148) Vous semblez hésiter sur l'opérance du moyen tiré de la méconnaissance des objectifs de prévention des atteintes à l'ordre public et de recherche des auteurs d'infractions, que vous avez déjà écarté au fond, « en tout état de cause » (CE, 23 févr. 2005, n° 264712-265248, 265281 et 265343, *Association pour la transparence et la moralité des marchés publics (ATMMP)*, Lebon p. 71 ; AJDA 2005. 668, note J.-D. Dreyfus ; RFDA 2005. 483, concl. D. Casas ; RTD eur. 2006. 301, chron. D. Ritleng ; Rev. UE 2015. 434, étude P. Bourdon).

(149) V. par ex., la décision Cons. const., 9 juin 2011, n° 2011-631 DC, *Loi relative à l'immigration, à l'intégration et à la nationalité*, consid. 64, AJDA 2011. 1174 ; *ibid*. 1936, étude O. Lecucq ; JA 2011, n° 442, p. 7, obs. S.Z.-D. ; *ibid*., n° 442, p. 9, obs. L.T. ; Constitutions 2011. 581, chron. V. Tchen ; *ibid*. 2012. 63, obs. A. Levade.

(150) Cons. const., 25 juill. 1991, n° 91-294 DC, consid. 17, AJDA 1991. 659, étude B. Néel ; D. 1991. 617, note L. Hamon ; RFDA 1992. 173, note G. Vedel ; RTD eur. 1992. 187, note X. Prétot.

(151) Cons. const., 22 janv. 1990, n° 89-269 DC. Dans sa décision n° 86-217 DC du 18 sept. 1986 (consid. 9), il a exigé du législateur qu'il assure la garantie des objectifs de valeur constitutionnelle de sauvegarde de l'ordre public et de respect de la liberté d'autrui.

(152) V. précisément à propos de l'accès administratif aux données de connexion par les services de renseignement : Cons. const., 23 juill. 2015, n° 2015-713 DC, *Loi relative au renseignement*, consid. 51 à 53, 55 et 56, AJDA 2015. 1513 ; D. 2016. 1461, obs. N. Jacquinot et A. Mangiavillano ; à propos de la saisie de données informatiques : Cons. const., 2 déc. 2016, n° 2016-600 QPC, consid. 7 à 13, AJDA 2016. 2348 ; D. 2016. 2467, et les obs. ; *ibid*. 2017. 1328, obs. N. Jacquinot et R. Vaillant ; Constitutions 2016. 720, chron. ; *ibid*. 2017. 121, chron. O. Le Bot ou encore : Cons. const., 12 mai 2010, n° 2010-605 DC, *Loi relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne*, consid. 25, AJDA 2010. 1048 ; D. 2010. 1321, note A. Levade ; *ibid*. 1229, chron. P. Fombeur ; *ibid*. 1234, chron. P. Cassia et E. Saulnier-Cassia ; *ibid*. 1495, chron. V. Lasserre-Kiesow et P. Le More ; RFDA 2010. 458, note P. Gaïa ; Constitutions 2010. 363, obs. A.-M. Le Pourhiet ; *ibid*. 387, obs. A. Levade ; Rev. crit. DIP 2011. 1, étude D. Simon ; RTD civ. 2010. 499, obs. P. Deumier ; Cons. const., 18 oct. 2010, n° 2010-55 QPC, consid. 6, AJDA 2011. 649, chron. S. Nicinski, M. Lombard et E. Glaser ; Cons. const., 13 mars 2003, n° 2003-467 DC, consid. 27. D. 2004. 1273, obs. S. Nicot ; RSC 2003. 614, obs. V. Bück ; *ibid*. 616, obs. V. Bück

(153) CE, ass., 27 oct. 1995, n° 136727, *Commune de Morsang-sur-Orge*, Lebon p. 372, concl. P. Frydman ; AJDA 1995. 942 ; *ibid*. 878, chron. J.-H. Stahl et D. Chauvaux ; *ibid*. 2014. 106, chron. M. Franc ; D. 1995. 257 ; RFDA 1995. 1204, concl. P. Frydman.

(154) Sur la question de la date de naissance de cette obligation, nous renvoyons au très intéressant article de F. Melleray, « L'obligation de prendre des mesures de police initiale », AJDA 2005. 71. Plutôt qu'à l'arrêt *Lemonnier* ou à la décision

Doublet, il propose de rattacher cette obligation au pouvoir de substitution du préfet posé à l'origine par l'art. 99 du 5 avr. 1884.

(155) CE, 8 juill. 1992, n° 80775, *Ville de Chevreuse*, Lebon p. 281.

(156) CE, 28 nov. 2003, n° 238349, *Commune de Moissy Cramayel* c/ *Bellonga*, Lebon p. 464 ; AJDA 2004. 988, note C. Deffigier.

(157) Cons. const., 10 nov. 2016, n° 2016-738 DC, D. 2017. 1328, obs. N. Jacquinot et R. Vaillant. On trouve aussi dans de nombreuses décisions une référence à la « protection » de principes et de droits de valeur constitutionnelle (v. par ex. : Cons. const., 22 mars 2012, n° 2012-652 DC, *Loi relative à la protection de l'identité*, AJDA 2012. 623).

(158) Cons. const., 25 janv. 1985, n° 85-187 DC.

(159) Selon P. de Montalivet (*op. cit.*) : « Les objectifs de valeur constitutionnelle ne sont pas des droits mais des buts assignés par la Constitution au législateur, qui constituent des conditions objectives d'effectivité des droits fondamentaux constitutionnels. Ils découlent des droits et libertés et servent à en déterminer la portée exacte. Ils servent moins à les limiter qu'à les protéger. La « clef d'interprétation » des objectifs réside ainsi dans l'effectivité des droits et libertés ».

(160) Le Conseil constitutionnel n'a pas explicité la portée de cette disposition autrement qu'en interdisant la délégation de compétences de police administrative générale à des personnes privées (Cons. const., 10 mars 2011, n° 2011-625 DC, *Loi d'orientation et de programmation pour la performance de la sécurité intérieure*, consid. 18, AJDA 2011. 532 ; *ibid*. 1097, note D. Ginocchi ; D. 2011. 1162, chron. P. Bonfils ; *ibid*. 2012. 1638, obs. V. Bernaud et N. Jacquinot ; AJCT 2011. 182, étude J.-D. Dreyfus ; Constitutions 2011. 223, obs. A. Darsonville ; *ibid*. 581, chron. V. Tchen ; RSC 2011. 728, chron. C. Lazerges ; *ibid*. 789, étude M.-A. Granger ; *ibid*. 2012. 227, obs. B. de Lamy ; Cons. const., 16 juin 2017, n° 2017-637 QPC, *Association nationale des supporters*, consid. 4 et 5, AJDA 2017. 1257 ; D. 2017. 1253 ; Constitutions 2017. 347, Décision ; *ibid*. 456, chron. L. Domingo).

(161) V. A. Vidal-Naquet, « La sécurité en droit constitutionnel : non-dit ou non-être ? », https://halshs.archives-ouvertes.fr/halshs-02112622/document.

(162) Art. 1er de la Charte de l'environnement.

(163) 11e al. du Préambule de 1946.

(164) Le droit à la protection sociale est garanti par la Constitution (Cons. const., 23 janv. 1987, n° 86-225 DC, consid. 16 et 17).

(165) Art. 16 de la Déclaration de 1789 tel qu'interprété par la décision n° 2010-2 QPC du 11 juin 2010, consid. 21 à 23. (AJDA 2010. 1178 ; D. 2010. 1976, obs. I. Gallmeister, note D. Vigneau ; *ibid*. 1980, note V. Bernaud et L. Gay ; *ibid*. 2011. 2565, obs. A. Laude ; *ibid*. 2012. 297, chron. N. Maziau ; RFDA 2010. 696, C. de Salins ; RDSS 2010. 127, obs. R. Pellet ; Constitutions 2010. 391, obs. A. Levade ; *ibid*. 403, obs. P. De Baecke ; *ibid*. 427, obs. X. Bioy ; RTD civ. 2010. 517, obs. P. Puig). Les tables analytiques évoquent directement la sécurité juridique.

(166) Qui codifie l'art. 1er de la loi n° 95-73 du 21 janv. 1995 d'orientation et de programmation relative à la sécurité. Y est aussi affirmé le devoir de l'État d'assurer la sécurité en veillant, sur l'ensemble du territoire de la République, à la défense des institutions et des intérêts nationaux, au respect des lois, au maintien de la paix et de l'ordre publics, à la protection des personnes et des biens.

(167) CE, 20 juill. 2001, n° 236196, *Commune de Mandelieu-La-Napoule*, Lebon p. 388.

(168) Cons. const., 17 oct. 2014, n° 2014-422 QPC, *Chambre syndicale des cochers chauffeurs CGT-taxis* [Voitures de tourisme avec chauffeur], AJDA 2015. 226, note A. Haquet ; D. 2014. 2046 ; *ibid*. 2015. 1457, obs. L. Gay et A. Mangiavillano ; Constitutions 2015. 378, chron. M.-A. Granger. Le Conseil refuse ainsi d'ouvrir la voie à un pur recours en carence du législateur sur ce point, comme il en existe dans d'autres systèmes juridiques (v. sur ce point le commentaire de l'art. L. 111-1 du CSI édité par Dalloz, citant l'exemple du Portugal).

(169) Cons. const., 2 juin 2017, n° 2017-632 QPC, *Union nationale des associations de familles de traumatisés crâniens et de cérébro-lésés*, consid. 4 et 6, AJDA 2017. 1143 ; *ibid*. 1908, note X. Bioy ; D. 2017. 1194, obs. F. Vialla ; *ibid*. 1307, point de vue A. Batteur ; *ibid*. 2018. 765, obs. J.-C. Galloux et H. Gaumont-Prat ; *ibid*. 1344, obs. E. Debaets et N. Jacquinot ; AJ fam. 2017. 379, obs. A. Dionisi-Peyrusse ; RDSS 2017. 1035, note D. Thouvenin ; Constitutions 2017. 342, Décision.

(170) CJCE, 3 sept. 2008, aff. C-402/05 P et C-415/05 P, *Kadi et Al Barakaat International Foundation c/ Conseil et Commission*, pt 363, D. 2009. 1118, note D. Delcourt ; RFDA 2008. 1204, note P. Cassia et F. Donnat ; RSC 2009. 75, étude H. Rouidi ; *ibid*. 197, obs. L. Idot ; RTD eur. 2009. 161, note J. P. Jacqué ; *ibid*. 2015. 301, étude D. Burriez.

(171) CJUE, 23 nov. 2010, aff. C-145/09, *Baden Württemberg* c/ *Tsakouridis*, pts 46-47, AJDA 2010. 2240 ; *ibid*. 2011. 264, chron. M. Aubert, E. Broussy et F. Donnat ; RTD eur. 2011. 604, obs. S. Robin-Olivier ; Rev. UE 2013. 45, chron. E. Sabatakakis.

(172) CJUE, gde ch., 26 juill. 2017, avis 1/15, *Projet d'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers*, pt 149, D. 2017. 1655, obs. E. Autier ; JT 2017, n° 201, p. 12, obs. X. Delpech.

(173) À propos de l'art. 8 de la Convention protégeant la vie privée, la Cour européenne a jugé à plusieurs reprises que « une dissuasion effective contre des actes graves mettant en jeu des valeurs fondamentales et des aspects essentiels de la vie privée appelle des dispositions pénales efficaces », le cas échéant de la part du législateur (CEDH, 2 déc. 2008, n° 2872/02, *K.U. c/ Finlande*, pt 45).

(174) Pt 126.

(175) Dans ses conclusions sur l'affaire *LQDN et autres*, l'avocat général C. Sánchez-Bordona indique d'ailleurs que « On pourrait profiter de l'opportunité offerte par les présentes demandes de décision préjudicielle pour proposer plus clairement la recherche d'un équilibre entre, d'une part, le droit à la sécurité et, d'autre part, le droit à la vie privée et le droit à la protection des données à caractère personnel. Cela permettrait d'éviter les critiques selon lesquelles les seconds seraient favorisés au détriment du premier ». Mais il ne conclut pas réellement sur ce point, ajoutant même que « si la préservation du principe de confidentialité des données est primordiale dans une société démocratique, l'importance de la sécurité au sein de cette société ne doit pas être sous-estimée » (c'est nous qui soulignons). Cette formulation témoigne bien de la hiérarchisation des priorités. La Cour ne nous semble de toute façon pas avoir réellement donné suite à l'idée de rééquilibrage évoquée.

(176) Cons. const., 27 févr. 2015, n° 2014-450 QPC, consid. 6. AJDA 2015. 424 ; D. 2015. 492 ; AJFP 2015. 244, comm. J.-C. Videlin

(177) Cette analyse n'est pas démentie par la jurisprudence du Conseil constitutionnel qui a admis que la Charte des droits fondamentaux ne requérait pas de révision constitutionnelle, notamment parce que la clause de limitation qui figure à son

art. 52 devait s'interpréter à la lumière de l'obligation de respecter ces mêmes fonctions essentielles de l'État. Dire que la Constitution n'est pas nécessairement méconnue en raison de cette interprétation ne signifie pas qu'elle ne peut jamais l'être, ce que rappelle le commentaire aux cahiers que nous avons cité.

(178) Y compris celle d'une Europe du renseignement que porte en germe le nouveau Collège du renseignement en Europe.

(179) Art. 76 du code de procédure pénale (C. pr. pén.).

(180) C. pr. pén., art. 60-4 et 100.

(181) V. pour une intéressante discussion sur ce seuil de trois ans, les conclusions de l'avocat général Saugmansgaard Øe sur l'affaire *Ministerio fiscal* (pts 116 à 120) citant les arrêts *Kennedy* du 18 mai 2010 et *Roman Zakharov* du 4 déc. 2015 de la CEDH, et dans lesquelles il plaide, précisément, pour ne pas définir la criminalité grave à l'aune de la seule peine encourue.

(182) Il est vrai toutefois qu'il y a loin de la peine d'emprisonnement prévue par le code pénal à la peine de prison effectivement exécutée...

(183) Et cet examen a vocation, à notre avis, à jouer « dans les deux sens », si le législateur fixe un seuil de gravité : il doit permettre de s'opposer à l'accès aux données de connexion pour une infraction située « au-delà » du seuil mais qui apparaît vénielle (vol d'une pomme sur un étalage) et à l'inverse, il peut justifier de « repêcher » une réquisition pour une infraction située « en deçà » du seuil lorsque sa gravité propre ou la finalité poursuivie par le service le justifie.

(184) L'art. 39-3 du code de procédure pénale assigne par ailleurs au procureur de la République la mission de contrôler la légalité des moyens mis en oeuvre par les enquêteurs et la proportionnalité des actes d'investigation au regard de la nature et de la gravité des faits.

(185) V. par ex., à propos de la géolocalisation en temps réel : Crim., 6 janv. 2015, n° 14-84.822, au Bull.

(186) Cons. const., 23 juill. 2015, n° 2015-713 DC, consid. 11. AJDA 2015. 1513 ; D. 2016. 1461, obs. N. Jacquinot et A. Mangiavillano

(187) L'art. L. 833-5 du CSI fait obligation à la CNCTR de vérifier que la mesure respecte l'art. L. 801-1.

(188) Pt 93 s.

(189) Pt 91 s.

(190) Selon l'art. 83 du TFUE, c'est seulement lorsque l'harmonisation du droit pénal est indispensable pour la mise en oeuvre efficace d'une politique de l'Union, dans un domaine préalablement harmonisé, que l'Union peut adopter des directives visant à établir des règles minimales relatives à la définition des infractions pénales et des sanctions dans le domaine concerné.

(191) Les opérateurs, de nombreuses associations et, dans un premier temps, la CNIL (délibération n° 03-056 du 9 déc. 2003), ainsi que le G29 (recommandation de 1999, réitérée en 2003), avaient plaidé pour une durée de conservation de trois mois. La CNIL s'est finalement rallié à la durée d'un an (délibération n° 2005-254 du 10 nov. 2005). Dans l'avis qu'elle a rendu le 20 déc. 2007 sur le projet de décret d'application de la *LCEN* (n° 2007-391), elle n'évoque même pas du tout cette question de la durée de conservation.

(192) Ce triptyque est l'explicitation de la notion de « sécurité nationale » qui figurait dans la loi avant 2015 (CSI, art. L. 241-2 , repris dans le projet de loi initial), mais dans une acception évidemment plus étroite que celle de la Cour de justice.

(193) C'est aussi le cas pour la prévention des actions tendant au maintien ou à la reconstitution de groupements dissous en application de l'art. L. 212-1 du CSI, en tant que seraient visés des groupements ne constituant pas une menace pour la sécurité nationale (cas notamment des groupements provoquant à la discrimination ou à la haine contre une personne ou un groupe de personnes pour l'un des motifs discriminatoires mentionnés).

(194) La CNCTR se montre « particulièrement vigilante sur ce point » puisqu'elle « considère toutefois que cette finalité ne saurait être interprétée comme permettant la pénétration d'un milieu syndical ou politique ou la limitation du droit constitutionnel de manifester ses opinions, y compris extrêmes, tant que le risque d'une atteinte grave à la paix publique n'est pas avéré » (CNCTR, premier rapport d'activité 2015/2016, p. 31, rappelé dans le rapport 2018, p. 67).

(195) Cette notion renvoie aux incriminations pénales énumérées à l'art. 706-73 du code de procédure pénale, précisées par la jurisprudence de la Cour de cassation. De manière générale, le Conseil constitutionnel a estimé, dans sa décision n° 2015-713 DC du 23 juill. 2015, que les finalités retenues par le législateur faisaient référence soit à des incriminations pénales existantes, soit à des dispositions du code de la sécurité intérieure, du code des douanes ou du code de la défense. Il a en conséquence écarté le grief selon lequel elles seraient insuffisamment définies.

(196) Arrêt *Privacy international*, pt 44.

(197) Art. L. 2339-14 à L. 2339-18.

(198) Ce chiffre est issu du rapport de la délégation parlementaire au renseignement de 2015. Depuis lors, les crédits alloués aux services ont sensiblement augmenté.

(199) CRPA, art. L. 243-2 .

(200) L'adresse *IP* dynamique du visiteur d'un site ne suffit pas nécessairement à le retrouver puisqu'elle change, notamment, à chaque reconnexion de la *box* : il faut qu'elle soit horodatée et accompagnée du fuseau horaire, du protocole et du port utilisés (v. en ce sens le référentiel des prestations de la PNIJ). La Cour de justice elle-même ne dit pas autre chose dans son arrêt *Breyer c/ Allemagne* du 19 oct. 2016 (aff. C-582/14, D. 2016. 2215 ; Dalloz IP/IT 2017. 120, obs. G. Péronne et E. Daoud), en ce qu'elle juge qu'une adresse *IP* dynamique ne constitue une donnée à caractère personnel à l'égard d'un responsable de traitement que s'il dispose des moyens légaux lui permettant de faire identifier la personne concernée grâce aux informations supplémentaires dont dispose le fournisseur d'accès à Internet de cette personne.

(201) Le gouvernement cite les *Carrier-Grade Network Address Translation* qui permettent à plusieurs utilisateurs de détenir la même adresse *IP* au même moment, indépendamment de leur localisation.

(202) SSMSI, *Insécurité et délinquance en 2019 : bilan statistique*, sept. 2020.

(203) Les données de trafic sont conservées pour une durée maximale de 10 semaines et les durées de localisation de 4 semaines, pour la lutte contre les infractions pénales les plus graves (terrorisme, criminalité organisée...).

(204) Les données sont conservées 6 mois pour la téléphonie par internet, 9 mois pour le trafic internet classique et 12 mois pour la téléphonie mobile.

(205) L'obligation de conservation est limitée à ce qui est strictement nécessaire à la lutte contre la criminalité grave ;

certaines données ne peuvent plus être conservées ; les durées de conservation, variables selon les catégories de données, ont été revues à la baisse.

(206) Selon un récent rapport réalisé pour la Commission européenne, non versé au débat contradictoire, les autorités autrichiennes semblent se satisfaire de la situation (*Study on the retention of electronic communications non-content data for law enforcement purposes*, Milieu, sept. 2020, p. 112).

(207) Le gouvernement évoque « quelques jours », pour le contrôle des fraudes.

(208) V. l'arrêté du 31 déc. 2013 relatif aux factures des services de communications électroniques et à l'information du consommateur sur la consommation au sein de son offre.

(209) La Cour indique clairement, aux pts 100 et 101 de son arrêt du 6 oct. 2020, que l'inclusion des réquisitions de « sécurité » dans le champ de la directive *e-privacy* s'explique par sa rédaction, qui exclut les « activités » de l'État en matière régalienne, c'est-à-dire des traitements dont l'État est le responsable de traitement, et non les traitements imposés par l'État aux opérateurs et dont ces derniers sont responsables - ce qui est le cas de la conservation et de la communication des données. À l'inverse, c'est parce que l'ancienne directive 95/46 excluait de son champ d'application l'ensemble des traitements, quel qu'en soit l'auteur, ayant pour objet la sécurité publique, la défense ou la sûreté de l'État, que la Cour a jugé qu'échappaient aux règles posées par ce texte les transferts de données des compagnies aériennes aux autorités publiques (CJCE, 30 mai 2006, aff. C-317/04 et C-318/04, *Parlement c/ Conseil et Commission*).

(210) En revanche, s'agissant de la lutte contre la criminalité grave, le projet de règlement prévoit seulement en ses art. 6 et 7 d'assouplir à la marge les conditions de conservation, mais il est peu probable que la rédaction choisie appelle une jurisprudence sensiblement plus accommodante de la Cour, à la lumière de la Charte.

(211) CJA, art. L. 773-7 et R. 773-26.

(212) Il faudrait sans doute, dans ce cas, prévoir que le Premier ministre peut saisir lui-même la formation spécialisée pour surmonter l'opposition de la CNCTR.

(213) Cette question se pose également pour l'accès judiciaire, et dans des termes nettement plus problématiques. L'arrêt *H.K.*, qui confirme sur ce point l'arrêt *Télé2*, condamne clairement le dispositif français, en ce qu'il prévoit, comme son homologue estonien, une autorisation du procureur de la République préalablement à l'accès pendant l'enquête de flagrance ou l'enquête préliminaire. Ce dernier n'est pas considéré en effet comme un tiers indépendant, apte à opérer le contrôle préalable exigé par la Cour. Il faudrait donc, en toute rigueur, que l'accès soit autorisé par le juge des libertés et de la détention. Or on imagine assez mal que ce dernier examine 2 à 2,5 millions de réquisitions par an...

(214) Pt 121.

(215) Ce qui est d'ailleurs le cas sous l'empire de l'art. 13 de la directive police-justice, transposé au II de l'art. 107 de la loi du 6 janv. 1978 : le responsable de traitement peut non seulement retarder et limiter la fourniture des informations sur le traitement, mais encore ne pas y procéder du tout, dès lors et aussi longtemps qu'une mesure de cette nature est nécessaire et proportionnée dans une société démocratique, en tenant dûment compte des droits fondamentaux et des intérêts légitimes de la personne physique concernée pour les besoins des enquêtes et de la protection de la sécurité publique et de la sécurité nationale. Le § 4 de l'art. 13 de la directive autorise même l'adoption de mesures pour placer des catégories entières de traitements dans ce régime dérogatoire.

(216) V. respectivement les art. L. 833-4 et L. 841-1 du CSI.

(217) Dont la CNCTR indique dans son rapport 2019 qu'elle a renouvelé l'intérêt opérationnel de cette technique, jusque-là

peu utilisée (p. 35).

(218) V. CE, 17 mai 2017, n° 405792, *La Quadrature du Net et autres*, préc.

(219) Cons. const., 4 août 2017, n° 2017-648 QPC. AJDA 2017. 1642 ; D. 2017. 1657, et les obs. ; *ibid*. 2018. 1344, obs. E. Debaets et N. Jacquinot ; Constitutions 2017. 452, chron. O. Le Bot ; *ibid*. 499, Décision

(220) N° 433886, Lebon p. 63, concl. G. Odinet ; AJDA 2020. 489 ; D. 2021. 388, obs. C. de droit et d'économie du sport (OMIJ-CDES) ; RFDA 2020. 469, concl. G. Odinet .

(221) Le cas du vice de légalité externe est plus complexe. En cas de vice de forme ou de procédure, vous avez admis, en matière de versement de subvention, que l'administration puisse régulariser un tel vice en prenant une nouvelle décision (CE, sect., 1er juill. 2016, n° 363047-363134, *Commune d'Emerainville et syndicat d'agglomération nouvelle de Marne-la-Vallée-Val-Maubuée*, Lebon p. 291, concl. V. Daumas ; AJDA 2016. 1365 ; *ibid*. 1859, chron. L. Dutheillet de Lamothe et G. Odinet ; JA 2016, n° 546, p. 13, obs. S. Damarey ; AJCT 2017. 46, obs. O. Didriche ; RFDA 2017. 289, concl. V. Daumas). Cette solution pourrait être étendue en toutes matières, comme le proposait V. Daumas dans ses conclusions. Mais en l'absence de tout acte de régularisation, il nous paraît impossible de circonscrire l'annulation à une période donnée, sauf à faire application de la jurisprudence *AC !* en mettant en balance la gravité du vice et celle des conséquences de l'annulation.

(222) V. par ex. : CE, 21 mars 2001, n° 208541, *Mme Mathio Emma Essaka*, Lebon p. 150.

(223) Telle était l'intention du législateur, puisqu'il ressort des travaux préparatoires de la loi de 2017 qu'il a entendu prescrire à la CNCTR et au Premier ministre de vérifier l'intensité et la régularité des liens entre le terroriste « en puissance » et la personne susceptible de faire l'objet du recueil de données.

(224) Il ne s'agit pas de présumer que toute personne en lien étroit avec un terroriste est censée connaître ses noirs desseins et en est donc un complice, mais de considérer qu'une telle personne est, volontairement ou involontairement (c'est-à-dire fût-ce en étant instrumentalisée), impliquée dans de telles activités à partir du moment où elle échange régulièrement avec lui.

(225) Curieusement, le II de l'art. R. 851-5 du CSI ne prévoit le recueil des données techniques « permettant de localiser les équipements terminaux » (mentionnées au a du 2° du I du même art.) que pour l'accès en temps réel aux données de connexion (CSI, art. L. 851-2) et l'analyse algorithmique (art. L. 851-3), mais non pour la géolocalisation en temps réel (art. L. 851-4). En toute rigueur, cette dernière technique devrait donc reposer sur les données de localisation prévues à l'art. R. 10-13, qui sont les données de « bornage », peu précises comme on l'a dit, alors que les données de localisation du a du 2° du I englobent des données traitées mais non conservées par les opérateurs, comme les coordonnées GPS des smartphones transmises automatiquement à des serveurs distants par les logiciels embarqués (le cas échéant à des fins commerciales ou publicitaires).

(226) Cette précision peut toutefois varier en fonction de l'environnement, notamment en milieu urbain.

(227) V. le pt 188 : « Si l'objectif de prévention du terrorisme que poursuit la réglementation nationale en cause au principal (...) », réglementation qui porte aussi bien sur l'accès en temps réel aux données de connexion qu'à la seule géolocalisation en temps réel.

(228) Le rapport 2019 de la CNCTR fait état de 7 601 demandes de géolocalisations en temps réel en 2019, contre 2 426 en 2016, soit une augmentation de 213 % !

(229) V. pour une analyse (un peu ancienne) de droit comparé, l'étude d'impact du projet de loi relatif à la géolocalisation du

20 déc. 2013.

(230) CEDH, 2 sept. 2010, n° 35623/05, *Uzun* c/ *Allemagne*, D. 2011. 724, obs. S. Lavric, note H. Matsopoulou ; RSC 2011. 217, obs. D. Roets.

(231) La Cour évoque par erreur la « durée de la conservation » au pt 177.

(232) Seules les techniques mentionnées aux art. 20 (collecte en temps réel) et 21 (interception de données relatives au contenu) sont facultatives, et seulement à certaines conditions mentionnées au § 3 de l'art. 14.

(233) Le même raisonnement pourrait valoir pour les autorités administratives disposant d'un droit d'accès en vertu de la loi. On ne peut toutefois exclure que la Cour de justice se montre plus souple en présence d'obligations de conservation et de procédures d'accès destinées à assurer l'effectivité du droit de l'Union dans certains domaines. C'est la question posée par la Cour de cassation à propos de la recherche des manquements d'initiés par l'AMF. On peut aussi songer au droit d'accès de l'Autorité de la concurrence.

(234) Curieusement, alors que l'arrêt *Télé2* de 2016 ouvrait déjà une brèche, rares semblent être les parties et surtout les avocats qui se sont prévalus de cette cause potentielle de nullité, à ce stade. Vous n'avez été informé que d'un arrêt de la cour d'appel d'Aix-en-Provence se prononçant sur la question (en balayant l'argumentation d'un revers de manche). Cet arrêt est frappé de pourvoi.

(235) N° 370321, Lebon p. 255 ; AJDA 2017. 1477 ; *ibid*. 1879, chron. G. Odinet et S. Roussel ; RFDA 2017. 1099, note S. de La Rosa ; RTD com. 2017. 853, obs. F. Lombard ; RTD eur. 2018. 397, obs. E. Muller.

(236) CE, ass., 29 juin 2001, n° 213229, *Vassilikiotis*, Lebon p. 303, concl. F. Lamy ; AJDA 2001. 1051 ; *ibid*. 1046, chron. M. Guyomar et P. Collin. V. aussi pour un régime supplétif faisant suite à une annulation « en tant que » (et non « en tant que ne pas ») : CE, 31 juill. 2019, n° 428530-428564, *Association La Cimade et autres*, préc.

(237) Celle-ci doit être communiquée « sans délai » à la commission (CSI, art. L. 821-4, 3e al.) et indiquer les motifs pour lesquels l'avis défavorable n'a pas été suivi (2e al.).

Copyright 2021 - Dalloz – Tous droits réservés

ARRÊT DE LA COUR (grande chambre)
15 juillet 2021 (*)
« Renvoi préjudiciel – Protection de la sécurité et de la santé des travailleurs – Aménagement du temps de travail – Membres des forces armées – Applicabilité du droit de l'Union – Article 4, paragraphe 2, TUE – Directive 2003/88/CE – Champ d'application – Article 1er, paragraphe 3 – Directive 89/391/CEE – Article 2, paragraphe 2 – Activités des militaires – Notion de "temps de travail" – Période de garde – Litige relatif à la rémunération du travailleur »
Dans l'affaire C-742/19,
ayant pour objet une demande de décision préjudicielle au titre de l'article 267 TFUE, introduite par le Vrhovno sodišče (Cour suprême, Slovénie), par décision du 10 septembre 2019, parvenue à la Cour le 10 octobre 2019, dans la procédure
B. K.
contre
Republika Slovenija (Ministrstvo za obrambo),
LA COUR (grande chambre),
composée de M. K. Lenaerts, président, Mme R. Silva de Lapuerta, vice-présidente, MM. J.-C. Bonichot, M. Vilaras, E. Regan et N. Piçarra, présidents de chambre, MM. T. von Danwitz, M. Safjan, D. Šváby, S. Rodin, Mme K. Jürimäe, MM. C. Lycourgos (rapporteur), P. G. Xuereb, Mme L. S. Rossi et M. I. Jarukaitis, juges,
avocat général : M. H. Saugmandsgaard Øe,
greffier : Mme R. Şereş, administratrice,
vu la procédure écrite et à la suite de l'audience du 21 septembre 2020,
considérant les observations présentées :
– pour B. K., par Me M. Pukšič, odvetnik,
– pour le gouvernement slovène, par Mmes A. Grum et A. Dežman Mušič, en qualité d'agents,
– pour le gouvernement allemand, par M. J. Möller et Mme S. Eisenberg, en qualité d'agents,
– pour le gouvernement espagnol, par M. S. Jiménez García, en qualité d'agent,
– pour le gouvernement français, par Mmes A.-L. Desjonquères, E. de Moustier et N. Vincent ainsi que par MM. T. Stehelin et A. Ferrand, en qualité d'agents,
– pour la Commission européenne, par Mme B. Rous Demiri ainsi que par MM. N. Ruiz García et M. van Beek, en qualité d'agents,
ayant entendu l'avocat général en ses conclusions à l'audience du 28 janvier 2021,
rend le présent
Arrêt
1 La demande de décision préjudicielle porte sur l'interprétation de l'article 2 de la directive 2003/88/CE du Parlement européen et du Conseil, du 4 novembre 2003, concernant certains aspects de l'aménagement du temps de travail (JO 2003, L 299, p. 9).
2 Cette demande a été présentée dans le cadre d'un litige opposant B. K. à la Republika Slovenija (Ministrstvo za obrambo) [République de Slovénie (ministère de la Défense)] au sujet d'un complément de rémunération au titre d'heures supplémentaires.
Le cadre juridique
Le droit de l'Union
La directive 76/207/CEE
3 L'article 3, paragraphe 1, de la directive 76/207/CEE du Conseil, du 9 février 1976, relative à la mise en œuvre du principe de l'égalité de traitement entre hommes et femmes en ce qui concerne l'accès à l'emploi, à la formation et à la promotion professionnelles, et les conditions de travail (JO 1976, L 39, p. 40), disposait :
« L'application du principe de l'égalité de traitement implique l'absence de toute discrimination fondée sur le sexe dans les conditions d'accès, y compris les critères de sélection, aux emplois ou postes de travail, quel qu'en soit le secteur ou la branche d'activité, et à tous les niveaux de la hiérarchie professionnelle. »
La directive 89/391/CEE
4 L'article 2 de la directive 89/391/CEE du Conseil, du 12 juin 1989, concernant la mise en œuvre de mesures visant à promouvoir l'amélioration de la sécurité et de la santé des travailleurs au travail (JO 1989, L 183, p. 1), prévoit :
« 1. La présente directive s'applique à tous les secteurs d'activités, privés ou publics (activités industrielles, agricoles, commerciales, administratives, de service, éducatives, culturelles, de loisirs, etc.).

2. La présente directive n'est pas applicable lorsque des particularités inhérentes à certaines activités spécifiques dans la fonction publique, par exemple dans les forces armées ou la police, ou à certaines activités spécifiques dans les services de protection civile s'y opposent de manière contraignante.
Dans ce cas, il y a lieu de veiller à ce que la sécurité et la santé des travailleurs soient assurées, dans toute la mesure du possible, compte tenu des objectifs de la présente directive. »

La directive 89/656/CEE

5 L'article 1er de la directive 89/656/CEE du Conseil, du 30 novembre 1989, concernant les prescriptions minimales de sécurité et de santé pour l'utilisation par les travailleurs au travail d'équipements de protection individuelle (troisième directive particulière au sens de l'article 16 paragraphe 1 de la directive 89/391/CEE) (JO 1989, L 393, p. 18), dispose :

« 1. La présente directive, qui est la troisième directive particulière au sens de l'article 16 paragraphe 1 de la directive 89/391/CEE, fixe des prescriptions minimales de sécurité et de santé pour l'utilisation par les travailleurs au travail d'équipements de protection individuelle.

2. Les dispositions de la directive 89/391/CEE s'appliquent pleinement à l'ensemble du domaine visé au paragraphe 1, sans préjudice de dispositions plus contraignantes et/ou spécifiques contenues dans la présente directive. »

6 L'article 2 de cette directive est ainsi libellé :

« 1. Aux fins de la présente directive, on entend par équipement de protection individuelle tout équipement destiné à être porté ou tenu par le travailleur en vue de le protéger contre un ou plusieurs risques susceptibles de menacer sa sécurité ou sa santé au travail, ainsi que tout complément ou accessoire destiné à cet objectif.

2. Sont exclus de la définition visée au paragraphe 1 :

[...]

c) les équipements de protection individuelle des militaires, des policiers et des personnes des services de maintien de l'ordre ;

[...] »

La directive 2003/88

7 L'article 1er, paragraphe 3, premier alinéa, de la directive 2003/88 énonce :

« La présente directive s'applique à tous les secteurs d'activités, privés ou publics, au sens de l'article 2 de la directive 89/391/CEE, sans préjudice des articles 14, 17, 18 et 19 de la présente directive. »

8 Aux termes de l'article 2 de cette directive, intitulé « Définitions » :

« Aux fins de la présente directive, on entend par :

1. "temps de travail" : toute période durant laquelle le travailleur est au travail, à la disposition de l'employeur et dans l'exercice de son activité ou de ses fonctions, conformément aux législations et/ou pratiques nationales ;

2. "période de repos" : toute période qui n'est pas du temps de travail ;

[...] ».

9 L'article 17, paragraphe 3, de ladite directive prévoit :

« Conformément au paragraphe 2 du présent article, il peut être dérogé aux articles 3, 4, 5, 8 et 16 :

[…]

b) pour les activités de garde, de surveillance et de permanence caractérisées par la nécessité d'assurer la protection des biens et des personnes, notamment lorsqu'il s'agit de gardiens ou de concierges ou d'entreprises de gardiennage ;

c) pour les activités caractérisées par la nécessité d'assurer la continuité du service ou de la production [...] ;

[...] »

La directive 2013/35/UE

10 L'article 1er de la directive 2013/35/UE du Parlement européen et du Conseil, du 26 juin 2013, concernant les prescriptions minimales de sécurité et de santé relatives à l'exposition des travailleurs aux risques dus aux agents physiques (champs électromagnétiques) (vingtième directive particulière au sens de l'article 16, paragraphe 1, de la directive 89/391/CEE) et abrogeant la directive 2004/40/CE (JO 2013, L 179, p. 1), dispose :

« 1. La présente directive, qui est la vingtième directive particulière au sens de l'article 16, paragraphe 1, de la directive 89/391/CEE, fixe des prescriptions minimales en matière de protection des travailleurs contre les risques pour leur santé et leur sécurité résultant ou susceptibles de résulter d'une exposition à des champs électromagnétiques au travail.

[...]
6. Sans préjudice des dispositions plus contraignantes ou plus spécifiques de la présente directive, la directive 89/391/CEE continue à s'appliquer intégralement à l'ensemble du domaine visé au paragraphe 1. »
11 L'article 10, paragraphe 1, de cette directive énonce :
« Par dérogation à l'article 3, mais sans préjudice de l'article 5, paragraphe 1, les dispositions suivantes s'appliquent :
[...]
b) les États membres peuvent autoriser la mise en œuvre d'un système de protection équivalent ou plus spécifique pour le personnel travaillant dans des installations militaires opérationnelles ou participant à des activités militaires, y compris des exercices militaires internationaux conjoints, pour autant qu'il permette de prévenir les effets nocifs pour la santé et les risques pour la sécurité ;
[...] »

Le droit slovène

12 L'article 46 de la Kolektivna pogodba za javni sektor (convention collective pour le secteur public), dans sa version applicable au litige au principal (Uradni list RS, n° 57/2008 et suivants), disposait que les agents publics ont droit à une indemnité d'astreinte à hauteur de 20 % du taux horaire du traitement de base, sans que ces périodes d'astreinte soient considérées comme du temps de travail.
13 Les motifs de cette convention collective exposaient ce qui suit :
« L'astreinte signifie que l'agent public doit pouvoir être joint pour pouvoir se rendre au travail en dehors de son temps de travail. L'astreinte doit être imposée par écrit. Le montant de l'indemnité d'astreinte est le même, indépendamment du fait que l'agent public est soumis à astreinte de jour, de nuit, un jour ouvrable, un dimanche ou un jour férié. »
14 L'article 5 du Zakon o obrambi (loi sur la défense), du 20 décembre 1994 (Uradni list RS, n° 82/94), dans sa rédaction applicable au litige au principal (ci-après le « ZObr »), prévoit, à son point 14, que le militaire est, au sens de cette loi, une personne qui exerce une fonction militaire et précise, à son point 14 bis, que le travailleur est, au sens de ladite loi, le militaire, le civil qui travaille à titre professionnel dans l'armée ou une autre personne qui, à titre professionnel, remplit des missions administratives ou techniques spécialisées au ministère.
15 Selon l'article 51 du ZObr, un militaire peut, dans certaines conditions, utiliser les armes pour effectuer des gardes.
16 L'article 97č du ZObr, relatif au service de garde, énonce :
« (1) Les gardes durent, en règle générale, 24 heures ininterrompues.
(2) Les militaires qui exercent un service de garde sont considérés comme travaillant pendant le temps de travail partagé. Les heures pendant lesquelles ils n'effectuent pas de travail effectif sont considérées non comme du temps de travail, mais comme une période d'astreinte sur le lieu de travail.
(3) L'obligation professionnelle journalière pendant la garde ne saurait aller au-delà de 12 heures. En cas d'événement exceptionnel ou de nécessité d'achever une mission entamée, le temps de travail des militaires peut exceptionnellement se prolonger, mais, à cette occasion, les heures travaillées au-delà des 12 heures de travail effectif déjà effectuées sont considérées comme des heures supplémentaires.
(4) L'exercice du service de garde ne peut durer de manière ininterrompue plus de sept jours. Les militaires ont droit à une pause de repos sur le lieu où ils effectuent la garde, en ce que 12 heures leur sont reconnues comme du temps de travail ordinaire et les 12 heures restantes sont considérées comme une période d'astreinte. »
17 Selon l'article 97e du ZObr, relative à l'astreinte :
« (1) L'astreinte est le temps pendant lequel le travailleur doit être en disponibilité pour travailler sur son lieu de travail, en un lieu déterminé ou à la maison.
(2) La période d'astreinte n'est pas incluse dans le compte des heures d'obligations professionnelles hebdomadaires ou mensuelles. Si le travailleur doit, pendant la période d'astreinte, effectivement travailler, ces heures de travail effectif sont incluses dans le compte des heures d'obligations professionnelles hebdomadaires ou mensuelles.
(3) Le ministre détermine les cas et les modes d'exercice de l'astreinte dans les espaces professionnels, en un endroit déterminé ou à la maison. Les cas et les modes d'exercice de l'astreinte dans l'armée sont déterminés par le chef d'état-major.
(4) L'astreinte en un lieu déterminé est assimilée à l'astreinte sur le lieu de travail. »

18 Les Pravila službe v Slovenski vojski (règlement de service dans l'armée slovène) (Uradni list RS, nº 84/09) définissent la notion de « garde » dans les termes suivants :

« La garde est considérée comme une mission de combat en temps de paix [...], au cours de laquelle un soldat de garde peut également faire usage des armes et de la force létale conformément aux dispositions de l'article 51 du ZObr. La garde est effectuée dans des blocs de temps (dans le cadre d'une période de 7 jours avec une présence permanente c'est-à-dire de 24 heures par jour de présence au lieu de travail) en vue de l'organisation adéquate du travail. La garde est organisée au niveau de l'unité militaire qui veille également à ce que les personnes au sein d'une même unité soient soumises de manière égale à la charge d'assurer les gardes. La garde a une importance militaire et stratégique spécifique. Assurer la disponibilité opérationnelle continue est une tâche fondamentale de l'armée en temps de paix. Afin d'assurer un niveau adéquat de préparation en temps de paix, l'armée assure des forces permanentes et des mesures permanentes pour intervenir. Les forces permanentes permettent d'assurer une capacité ininterrompue et les possibilités pour l'armée d'intervenir militairement et non militairement sur terre, en mer et dans les airs en République de Slovénie. Les forces de défense constituent une partie des forces permanentes.

La garde est assurée par une unité armée ou un groupe de militaires qui assure la protection physique des personnes, des installations, des actifs et du territoire. [...]

Les obligations générales des personnes de garde sont de protéger et de défendre avec vigilance ce qui leur est confié (installations, personnes, etc.), de ne pas lâcher leur arme des mains et d'être constamment prêts à en faire usage, de ne pas quitter le poste de garde jusqu'à ce que quelqu'un les ait remplacés, de n'autoriser personne en dehors d'un supérieur, un commandant adjoint ou un commandant de garde, un officier de service ou un responsable de la surveillance à s'approcher du poste de garde ou du bâtiment protégé ou de se déplacer en un endroit interdit. Les personnes de garde doivent en outre arrêter les personnes ainsi que cela est déterminé pour certains postes de garde et maintenir le contact et ne communiquer qu'avec le commandant de la garde et les autres organes de la garde, et informer le commandant de la garde en cas de perturbation ou d'incendie à proximité, lorsqu'il existe une menace pour l'objet protégé ou les forces en raison de catastrophes naturelles ou d'autres catastrophes, lorsqu'elles tombent malades ou ont besoin de toute autre forme d'assistance.

Les forces de sécurité assurent la sécurité des installations, des documents, des personnes, des armes et équipements militaires, des munitions et autres matériels contre diverses formes de menace. [...] »

Le litige au principal et les questions préjudicielles

19 Au cours de la période allant du mois de février 2014 au mois de juillet 2015, B. K. a effectué, en sa qualité de sous-officier de l'armée slovène, un « service de garde » ininterrompu de sept jours par mois au cours duquel il devait être joignable et présent en permanence au sein de la caserne où il était affecté. Ce « service de garde » comprenait à la fois des périodes au cours desquelles B. K. devait exercer une activité de surveillance effective et des périodes durant lesquelles ce dernier n'était tenu que de demeurer à la disposition de ses supérieurs. En cas de venue inopinée de la police militaire, d'un groupe d'inspection ou d'un groupe d'intervention, il devait en faire mention sur le formulaire d'enregistrement et remplir les missions que lui imposaient ses supérieurs.

20 Le ministère de la Défense a considéré que, pour chacun de ces jours de « service de garde », huit heures devaient être considérées comme étant du temps de travail, de sorte qu'il a versé à B. K. le traitement ordinaire correspondant pour ces huit heures de travail. Au titre des autres heures, B. K. n'a bénéficié que d'une indemnité d'astreinte à hauteur de 20 % du traitement de base.

21 B. K. a saisi les juridictions slovènes d'un recours tendant à ce que lui soient payées, en tant qu'heures de travail supplémentaires, les heures pendant lesquelles, au cours du « service de garde », il n'avait exercé aucune activité effective au service de son employeur, mais avait été contraint de demeurer à la disposition de ses supérieurs, au sein de la caserne en étant éloigné de sa résidence et de sa famille.

22 Son recours ayant été rejeté en première instance et en appel, B. K. a introduit un recours en révision devant la juridiction de renvoi.

23 Cette dernière relève, en premier lieu, que, conformément à l'article 1er, paragraphe 3, de la directive 2003/88, lu en combinaison avec l'article 2 de la directive 89/391, la directive 2003/88 ne s'applique pas lorsque des particularités inhérentes à certaines activités spécifiques dans la fonction publique s'y opposent de manière contraignante. La juridiction de renvoi considère, en se référant à l'arrêt du 5 octobre 2004, Pfeiffer e.a. (C-397/01 à C-403/01, EU:C:2004:584), que cette exception n'a été prévue que pour assurer le bon fonctionnement des services qui sont absolument nécessaires à la protection de la sécurité, de la santé et de l'ordre publics en cas d'événements d'une gravité exceptionnelle, lorsqu'il n'est pas possible de planifier le temps de travail des groupes d'intervention et de secours.

24 La juridiction de renvoi fait observer que, en l'occurrence, B. K. a effectué son travail ordinaire, à savoir un « service de garde » en temps de paix, de manière régulière, sans qu'il y ait eu, au cours de la période en cause au principal, la moindre circonstance imprévisible ou le moindre événement exceptionnel. Ainsi, selon cette juridiction, la planification du temps de travail de l'intéressé n'était aucunement impossible.

25 Ladite juridiction se demande toutefois si l'exception prévue à l'article 2 de la directive 89/391 peut être invoquée de manière générale à l'égard des militaires en temps de paix et des travailleurs du secteur de la défense.

26 En deuxième lieu, à supposer que la directive 2003/88 s'applique en l'occurrence, la juridiction de renvoi s'interroge sur le point de savoir si les périodes pendant lesquelles, au cours de son « service de garde », B. K. n'exerçait aucune activité effective au service de son employeur mais était tenu de demeurer au sein de la caserne, à la disposition de ses supérieurs, doivent être considérées comme étant du « temps de travail » au sens de l'article 2 de cette directive.

27 Après avoir souligné que cette question pourrait appeler une réponse affirmative, cette juridiction relève que, en droit slovène, de telles périodes sont exclues du temps de travail, au même titre que les périodes durant lesquelles un militaire est tenu de demeurer à son domicile, et qu'un même niveau de rémunération est prévu pour ces deux périodes, ce qui ne serait pas, selon ladite juridiction, conforme à la directive 2003/88.

28 Dans ces conditions, le Vrhovno sodišče (Cour suprême, Slovénie) a décidé de surseoir à statuer et de poser à la Cour les questions préjudicielles suivantes :

« 1) L'article 2 de la directive [2003/88] s'applique-t-il également aux travailleurs qui travaillent dans le domaine de la défense et aux militaires qui effectuent des gardes en temps de paix ?

2) L'article 2 de la directive [2003/88] fait-il obstacle à une réglementation nationale en vertu de laquelle les périodes d'astreinte des travailleurs qui travaillent dans l'armée, effectuées sur le lieu de travail ou en un endroit déterminé (mais pas à domicile) et la présence des militaires qui travaillent dans le domaine de la défense en périodes de garde, lorsque ces militaires n'effectuent pas de travail effectif, mais doivent être physiquement présents dans la caserne, ne sont pas incluses dans le temps de travail ? »

Sur les questions préjudicielles

Sur la recevabilité

29 Par ses questions préjudicielles, la juridiction de renvoi cherche, en substance, à déterminer si certaines périodes au cours desquelles tant les militaires que le personnel civil actif dans le domaine de la défense sont tenus de demeurer à la disposition de leurs supérieurs en cas de besoin peuvent être considérées comme étant du « temps de travail », au sens de l'article 2 de cette directive.

30 Or, il est constant que le litige au principal concerne uniquement un militaire. Il convient dès lors de constater que, en ce qu'elles portent sur la situation du personnel civil actif dans le domaine de la défense, les questions préjudicielles n'ont aucun rapport avec l'objet du litige au principal et sont, partant, en vertu d'une jurisprudence constante, irrecevables (arrêt du 2 février 2021, Consob, C-481/19, EU:C:2021:84, point 29 et jurisprudence citée).

Sur la première question

31 À titre liminaire, il convient de rappeler que, selon une jurisprudence constante de la Cour, dans le cadre de la procédure de coopération entre les juridictions nationales et la Cour instituée à l'article 267 TFUE, il appartient à celle-ci de donner au juge national une réponse utile qui lui permette de trancher le litige dont il est saisi. Dans cette optique, il incombe, le cas échéant, à la Cour de reformuler les questions qui lui sont soumises. En outre, la Cour peut être amenée à prendre en considération des normes du droit de l'Union auxquelles le juge national n'a pas fait référence dans l'énoncé de sa question (arrêt du 7 août 2018, Smith, C-122/17, EU:C:2018:631, point 34 et jurisprudence citée).

32 À cet égard, il y a lieu de relever, d'une part, que, afin de déterminer si, comme le demande la juridiction de renvoi, l'article 2 de la directive 2003/88 est applicable à une activité de garde assurée par un militaire en temps de paix, telle que le « service de garde » effectué par B. K. dans les conditions mentionnées au point 19 du présent arrêt, il convient d'examiner si une telle activité relève du champ d'application de cette directive, lequel est fixé non par son article 2 mais par son article 1er, paragraphe 3.

33 D'autre part, la juridiction de renvoi part de la prémisse selon laquelle le litige au principal relève du champ d'application du droit de l'Union. Néanmoins, dans la mesure où ce litige concerne un militaire, il convient d'examiner, au préalable, si, comme l'ont soutenu les gouvernements français et espagnol, le droit de l'Union n'a pas vocation à régir l'aménagement du temps de travail des militaires au motif que cet aménagement relèverait des modalités d'organisation des forces armées des États membres, lesquelles

seraient, par leur nature même, exclues du champ d'application de ce droit, conformément à l'article 4, paragraphe 2, TUE.

34 Dans ces conditions, afin de donner à la juridiction de renvoi une réponse utile qui lui permette de trancher le litige dont elle est saisie, il convient de reformuler la première question et de considérer que, par celle-ci, cette juridiction demande, en substance, si l'article 1er, paragraphe 3, de la directive 2003/88, lu à la lumière de l'article 4, paragraphe 2, TUE, doit être interprété en ce sens que l'activité de garde exercée par un militaire en temps de paix est exclue du champ d'application de cette directive.

35 En premier lieu, il convient de vérifier si l'article 4, paragraphe 2, TUE impose d'exclure l'intégralité des membres des forces armées du champ d'application du droit de l'Union et notamment des règles sur l'aménagement du temps de travail.

36 Aux termes de cet article 4, paragraphe 2, l'Union respecte, d'une part, l'égalité des États membres devant les traités ainsi que leur identité nationale, inhérente à leurs structures fondamentales politiques et constitutionnelles et, d'autre part, les fonctions essentielles de l'État, notamment celles qui ont pour objet d'assurer son intégrité territoriale, de maintenir l'ordre public et de sauvegarder la sécurité nationale. Cette même disposition précise que la sécurité nationale reste de la seule responsabilité de chaque État membre.

37 À cet égard, il y a lieu de relever que les missions principales des forces armées des États membres, que sont la préservation de l'intégrité territoriale et la sauvegarde de la sécurité nationale, figurent explicitement parmi les fonctions essentielles de l'État que l'Union doit respecter, en vertu de l'article 4, paragraphe 2, TUE.

38 Il ressort d'ailleurs de la jurisprudence de la Cour que les choix d'organisation militaire des États membres qui ont pour objet la défense de leur territoire ou de leurs intérêts essentiels ne sont pas régis, en tant que tels, par le droit de l'Union (voir, en ce sens, arrêt du 11 mars 2003, Dory, C-186/01, EU:C:2003:146, point 35).

39 Cela étant, il ne découle pas du respect dû par l'Union aux fonctions essentielles de l'État, consacré à l'article 4, paragraphe 2, TUE, que les décisions des États membres relatives à l'organisation de leurs forces armées échapperaient au champ d'application du droit de l'Union, en particulier lorsque sont en cause des règles relatives à l'aménagement du temps de travail.

40 En effet, selon une jurisprudence constante de la Cour, bien qu'il appartienne aux seuls États membres de définir leurs intérêts essentiels de sécurité et d'arrêter les mesures propres à assurer leur sécurité intérieure et extérieure, y compris les décisions relatives à l'organisation de leurs forces armées, le seul fait qu'une mesure nationale a été prise aux fins de la protection de la sécurité nationale ne saurait entraîner l'inapplicabilité du droit de l'Union et dispenser les États membres du respect nécessaire de ce droit (voir, en ce sens, arrêts du 26 octobre 1999, Sirdar, C-273/97, EU:C:1999:523, point 15 ; du 11 janvier 2000, Kreil, C-285/98, EU:C:2000:2, point 15, ainsi que du 6 octobre 2020, Privacy International, C-623/17, EU:C:2020:790, point 44 et jurisprudence citée). Il doit en aller de même des mesures nationales adoptées aux fins de la protection de l'intégrité territoriale d'un État membre.

41 Par ailleurs, comme l'a relevé, en substance, M. l'avocat général aux points 44 et 45 de ses conclusions, cette affirmation n'est pas contredite par l'arrêt du 11 mars 2003, Dory (C-186/01, EU:C:2003:146).

42 En effet, alors que l'instauration d'un service militaire obligatoire, qui était en cause dans l'affaire ayant donné lieu à cet arrêt, ne constitue pas une question appréhendée par le droit de l'Union, l'aménagement du temps de travail est une matière qui a été harmonisée, en vertu de l'article 153, paragraphe 2, TFUE, par le biais de la directive 2003/88.

43 Toutefois, si le respect dû par l'Union aux fonctions essentielles de l'État n'implique pas de soustraire intégralement l'aménagement du temps de travail des militaires au champ d'application du droit de l'Union, il n'en demeure pas moins que l'article 4, paragraphe 2, TUE requiert que l'application aux militaires des règles du droit de l'Union relatives à cet aménagement ne soit pas de nature à entraver le bon accomplissement de ces fonctions essentielles. Dès lors, ces règles ne sauraient être interprétées d'une manière telle qu'elles empêcheraient les forces armées d'accomplir leurs missions et qu'elles porteraient atteinte, par voie de conséquence, aux fonctions essentielles de l'État que sont la préservation de son intégrité territoriale et la sauvegarde de la sécurité nationale.

44 Il s'ensuit que les spécificités que chaque État membre confère au fonctionnement de ses forces armées doivent être dûment prises en considération par le droit de l'Union, que ces spécificités résultent, entre autres, des responsabilités internationales particulières assumées par cet État membre, des conflits ou des menaces auxquels il est confronté, ou encore du contexte géopolitique dans lequel cet État évolue.

45 Ainsi, l'application des dispositions du droit de l'Union et, plus particulièrement, de celles relatives à l'aménagement du temps de travail ne saurait empêcher l'accomplissement des missions spécifiques que chaque État membre confie, compte tenu de ses contraintes et de ses responsabilités propres, à ses forces armées, en vue de préserver son intégrité territoriale ou de sauvegarder sa sécurité nationale.
46 Il découle de l'ensemble des considérations qui précèdent que l'article 4, paragraphe 2, TUE n'a pas pour effet d'exclure l'aménagement du temps de travail de l'ensemble des militaires du champ d'application du droit de l'Union.
47 En deuxième lieu, il convient de rappeler que la directive 2003/88 a pour objet de fixer des prescriptions minimales destinées à améliorer les conditions de vie et de travail des travailleurs par un rapprochement des réglementations nationales concernant, notamment, la durée du temps de travail. Cette harmonisation au niveau de l'Union européenne en matière d'aménagement du temps de travail vise à garantir une meilleure protection de la sécurité et de la santé des travailleurs, en faisant bénéficier ceux–ci de périodes minimales de repos – notamment journalier et hebdomadaire – ainsi que de périodes de pause adéquates, et en prévoyant une limite maximale à la durée hebdomadaire de travail [arrêt du 9 mars 2021, Radiotelevizija Slovenija (Période d'astreinte dans un lieu reculé), C-344/19, EU:C:2021:182, point 25 et jurisprudence citée].
48 Par ailleurs, les dispositions de la directive 2003/88 précisent le droit fondamental à une limitation de la durée maximale du travail et à des périodes de repos journalier et hebdomadaire expressément consacré à l'article 31, paragraphe 2, de la charte des droits fondamentaux de l'Union européenne (ci-après la « Charte ») et doivent, dès lors, être interprétées à la lumière de ce dernier (arrêt du 17 mars 2021, Academia de Studii Economice din București, C-585/19, EU:C:2021:210, point 37 et jurisprudence citée). Il s'ensuit notamment que ces dispositions ne sauraient faire l'objet d'une interprétation restrictive au détriment des droits que le travailleur tire de cette directive [arrêt du 9 mars 2021, Radiotelevizija Slovenija (Période d'astreinte dans un lieu reculé), C-344/19, EU:C:2021:182, point 27 et jurisprudence citée].
49 À cet égard, il ressort de la jurisprudence de la Cour que, aux fins de l'application de la directive 2003/88, la notion de « travailleur » doit être définie selon des critères objectifs qui caractérisent la relation de travail en considération des droits et des devoirs des personnes concernées. Or, la caractéristique essentielle de la relation de travail est la circonstance qu'une personne accomplit, pendant un certain temps, en faveur d'une autre et sous la direction de celle-ci, des prestations en contrepartie desquelles elle reçoit une rémunération. Il s'ensuit qu'une relation de travail suppose l'existence d'un lien de subordination entre le travailleur et son employeur. L'existence d'un tel lien doit être appréciée dans chaque cas particulier en fonction de tous les éléments et de toutes les circonstances caractérisant les relations entre les parties (arrêt du 20 novembre 2018, Sindicatul Familia Constanța e.a., C-147/17, EU:C:2018:926, points 41 et 42 ainsi que jurisprudence citée).
50 En l'occurrence, il est constant que, au cours de la période en cause au principal, B. K. percevait une rémunération et se trouvait, en sa qualité de sous-officier de l'armée slovène, dans un lien de subordination par rapport à son employeur, au sens du point précédent. Il s'ensuit que la directive 2003/88 a, a priori, vocation à s'appliquer à sa situation.
51 En troisième lieu, il convient de déterminer si les activités des forces armées en général ou, à tout le moins, certaines d'entre elles doivent être exclues du champ d'application de la directive 2003/88 en vertu de son article 1er, paragraphe 3, lu à la lumière de l'article 4, paragraphe 2, TUE.
52 L'article 1er, paragraphe 3, de la directive 2003/88 définit le champ d'application de celle-ci par renvoi à l'article 2 de la directive 89/391. Aux termes de l'article 2, paragraphe 1, de cette dernière directive, celle-ci s'applique à « tous les secteurs d'activités, privés ou publics ».
53 Toutefois, l'article 2, paragraphe 2, de la directive 89/391 prévoit, à son premier alinéa, que celle-ci n'est pas applicable lorsque des particularités inhérentes à certaines activités spécifiques dans la fonction publique, notamment dans les forces armées, ou à certaines activités spécifiques dans les services de protection civile, s'y opposent de manière contraignante, et précise, à son second alinéa, que, dans un tel cas, la sécurité et la santé des travailleurs doivent être assurées, dans toute la mesure du possible, compte tenu des objectifs de ladite directive.
54 Il convient, dès lors, de déterminer si les activités des forces armées en général ou, à tout le moins, certaines d'entre elles doivent être exclues du champ d'application de la directive 2003/88 au motif qu'elles relèveraient de l'exception prévue à l'article 2, paragraphe 2, premier alinéa, de la directive 89/391, en tenant dûment compte de la nécessité d'interpréter ledit champ d'application à la lumière de l'article 4, paragraphe 2, TUE.

55 Il ressort de la jurisprudence de la Cour que l'article 2, paragraphe 2, premier alinéa, de la directive 89/391 doit recevoir une interprétation qui limite sa portée à ce qui est strictement nécessaire à la sauvegarde des intérêts qu'il permet aux États membres de protéger (arrêts du 5 octobre 2004, Pfeiffer e.a., C-397/01 à C-403/01, EU:C:2004:584, point 54, ainsi que du 30 avril 2020, Készenléti Rendőrség, C-211/19, EU:C:2020:344, point 32).

56 En outre, le critère utilisé à l'article 2, paragraphe 2, premier alinéa, de la directive 89/391 pour exclure certaines activités du champ d'application de cette directive et, partant, de celui de la directive 2003/88 est fondé non pas sur l'appartenance des travailleurs à l'un des secteurs de la fonction publique visés à cette disposition, considéré dans sa globalité, mais exclusivement sur la nature spécifique de certaines missions particulières exercées par les travailleurs des secteurs visés par cette disposition, nature qui justifie une exception aux règles en matière de protection de la sécurité et de la santé des travailleurs, en raison de la nécessité absolue de garantir une protection efficace de la collectivité (arrêt du 20 novembre 2018, Sindicatul Familia Constanţa e.a., C-147/17, EU:C:2018:926, point 55 ainsi que jurisprudence citée).

57 Figure au nombre des particularités inhérentes de ces activités spécifiques qui justifient, en vertu de l'article 2, paragraphe 2, premier alinéa, de la directive 89/391, une exception aux règles en matière de protection de la sécurité et de la santé des travailleurs le fait qu'elles ne se prêtent pas, par leur nature, à une planification du temps de travail (arrêt du 20 novembre 2018, Sindicatul Familia Constanţa e.a., C-147/17, EU:C:2018:926, point 64 ainsi que jurisprudence citée).

58 L'article 2, paragraphe 2, premier alinéa, de la directive 89/391 permet ainsi de préserver l'efficacité des activités spécifiques de la fonction publique dont la continuité est indispensable pour assurer l'exercice effectif des fonctions essentielles de l'État. Cette exigence de continuité doit être appréciée en tenant compte de la nature spécifique de l'activité considérée (arrêt du 20 novembre 2018, Sindicatul Familia Constanţa e.a., C-147/17, EU:C:2018:926, points 65 et 66 ainsi que jurisprudence citée).

59 À cet égard, d'une part, la Cour a jugé que l'exigence de continuité des services actifs dans les domaines de la santé, la sécurité et l'ordre publics ne fait pas obstacle à ce que, lorsqu'elles ont lieu dans des conditions normales, les activités de ces services puissent être organisées, en ce compris quant aux horaires de travail de leurs employés, si bien que l'exception prévue à l'article 2, paragraphe 2, premier alinéa, de la directive 89/391 n'est applicable à de tels services que dans des circonstances d'une gravité et d'une ampleur exceptionnelles, telles que des catastrophes naturelles ou technologiques, des attentats ou des accidents majeurs, qui nécessitent l'adoption de mesures indispensables à la protection de la vie, de la santé ainsi que de la sécurité de la collectivité, et dont la bonne exécution serait compromise si toutes les règles énoncées par la directive 2003/88 devaient être respectées. Dans de tels cas, il convient de reconnaître une priorité absolue à l'objectif de protection de la population, au détriment du respect des dispositions de cette directive, lesquelles peuvent provisoirement être méconnues au sein desdits services (voir, en ce sens, arrêts du 20 novembre 2018, Sindicatul Familia Constanţa e.a., C-147/17, EU:C:2018:926, point 67, ainsi que du 30 avril 2020, Készenléti Rendőrség, C-211/19, EU:C:2020:344, point 42 et jurisprudence citée).

60 D'autre part, la Cour a jugé que certaines activités particulières de la fonction publique présentent, même lorsqu'elles sont exercées dans des conditions normales, des caractéristiques à ce point spécifiques que leur nature s'oppose, de manière contraignante, à une planification du temps de travail respectueuse des prescriptions imposées par la directive 2003/88 (arrêt du 20 novembre 2018, Sindicatul Familia Constanţa e.a., C-147/17, EU:C:2018:926, point 68).

61 Tel est, en particulier, le cas des activités qui, afin de remplir efficacement l'objectif d'intérêt général qui leur est assigné, ne peuvent être exercées que de manière continue et par un seul et même travailleur, sans qu'il soit possible d'instaurer un système de rotation permettant d'accorder, à intervalles réguliers, audit travailleur, le droit à des heures ou à des jours de repos après qu'il a effectué un certain nombre d'heures ou de jours de travail (voir, en ce sens, arrêts du 20 novembre 2018, Sindicatul Familia Constanţa e.a., C-147/17, EU:C:2018:926, points 70 à 74, ainsi que du 30 avril 2020, Készenléti Rendőrség, C-211/19, EU:C:2020:344, points 43 et 44).

62 De telles activités doivent être intégralement exclues, en vertu de l'article 2, paragraphe 2, premier alinéa, de la directive 89/391, du champ d'application de la directive 2003/88.

63 En l'occurrence, il convient de déterminer dans quelle mesure la jurisprudence rappelée aux points 57 à 61 du présent arrêt est applicable aux activités des membres des forces armées, étant entendu que, comme il a été souligné aux points 43 et 45 de cet arrêt, il convient de veiller à ce que l'application à

ceux-ci de la directive 2003/88 n'affecte pas le bon accomplissement des fonctions essentielles des États membres, au sens de l'article 4, paragraphe 2, TUE.

64 À cet égard, il convient, premièrement, de relever que l'article 2, paragraphe 2, premier alinéa, de la directive 89/391 ne saurait être interprété en ce sens que les membres des forces armées des États membres sont exclus, dans leur intégralité et en permanence, du champ d'application de la directive 2003/88.

65 En effet, ainsi qu'il a été rappelé aux points 55, 56 et 58 du présent arrêt, bien qu'il vise à préserver l'exercice effectif des fonctions essentielles de l'État, l'article 2, paragraphe 2, premier alinéa, de la directive 89/391 doit être interprété restrictivement et a pour objet de faire échapper au champ d'application de cette directive et, par voie de conséquence, à celui de la directive 2003/88 non pas certains secteurs de la fonction publique, considérés dans leur globalité, mais seulement certaines catégories d'activités dans ces secteurs, en raison de leur nature spécifique.

66 Or, d'une part, la Cour a déjà jugé que l'article 2, paragraphe 2, premier alinéa, de la directive 89/391 ne peut justifier l'exclusion intégrale du personnel non civil des administrations publiques du champ d'application de cette directive (voir, en ce sens, arrêt du 12 janvier 2006, Commission/Espagne, C-132/04, non publié, EU:C:2006:18, points 30 à 40).

67 Du reste, et comme M. l'avocat général l'a relevé, en substance, à la note de bas de page 88 de ses conclusions, les exceptions spécifiques à l'égard des militaires, qui sont expressément prévues tant à l'article 2, paragraphe 2, sous c), de la directive 89/656 qu'à l'article 10, paragraphe 1, sous b), de la directive 2013/35, auraient été inutiles si l'article 2, paragraphe 2, premier alinéa, de la directive 89/391 avait exclu, de façon générale, les membres des forces armées du champ d'application de cette dernière directive. En effet, cet article 2, paragraphe 2, premier alinéa, détermine également le champ d'application des directives 89/656 et 2013/35, ainsi qu'il ressort, respectivement, de l'article 1er, paragraphe 2, de la directive 89/656 et de l'article 1er, paragraphe 6, de la directive 2013/35.

68 D'autre part, comme M. l'avocat général l'a également relevé, en substance, aux points 82 et 83 de ses conclusions, il ne saurait être considéré que l'intégralité des activités exercées par les militaires présentent des particularités telles que celles-ci s'opposent à toute planification du temps de travail respectueuse des exigences imposées par la directive 2003/88.

69 Au contraire, certaines activités susceptibles d'être exercées par les membres des forces armées, comme celles liées notamment à des services d'administration, d'entretien, de réparation, de santé, de maintien de l'ordre ou de poursuite des infractions, ne sauraient être exclues, dans leur intégralité, du champ d'application de la directive 2003/88.

70 En effet, il est constant que de telles activités relèvent, en principe, du champ d'application de cette directive lorsqu'elles sont exercées, dans des conditions similaires, par des travailleurs de la fonction publique n'ayant pas le statut de militaire.

71 Or, il convient de rappeler que l'exception prévue à l'article 2, paragraphe 2, premier alinéa, de la directive 89/391 est applicable, de la même manière, à tous les travailleurs qui exercent des activités spécifiques identiques au service de la collectivité (voir, en ce sens, arrêt du 20 novembre 2018, Sindicatul Familia Constanţa e.a., C-147/17, EU:C:2018:926, point 59).

72 Par ailleurs, s'il est vrai que tout militaire est soumis à une exigence de disponibilité de nature telle qu'il doit être en mesure d'être projeté en opération dans un très bref délai, l'application à ce militaire des règles prévues par la directive 2003/88, au cours des activités visées au point 69 du présent arrêt, n'est cependant pas de nature à contrarier le respect effectif d'une telle exigence de disponibilité, à tout le moins tant que ces activités ne sont pas exercées dans le cadre d'une opération militaire, en ce compris au cours de sa préparation immédiate.

73 Cela étant, deuxièmement, il découle, d'une part, de la jurisprudence rappelée au point 59 du présent arrêt que, lorsque les membres des forces armées sont confrontés à des circonstances d'une gravité et d'une ampleur exceptionnelles, au sens de cette jurisprudence, les activités de ceux-ci sont exclues du champ d'application de la directive 2003/88, en vertu de son article 1er, paragraphe 3, lu en combinaison avec l'article 2, paragraphe 2, premier alinéa, de la directive 89/391.

74 Il en va ainsi lorsque, eu égard à la gravité et à l'ampleur de l'ensemble des circonstances pertinentes, il apparaît qu'il est impossible de protéger la population tout en organisant les activités des forces armées de telle manière que chacun de leurs membres puisse bénéficier des garanties prévues par la directive 2003/88 en matière de durée du temps de travail et du temps de repos, notamment par un mécanisme de rotation des effectifs (voir, par analogie, arrêt du 30 avril 2020, Készenléti Rendőrség C-211/19, EU:C:2020:344, points 47 à 50).

75 D'autre part, il peut être déduit de la jurisprudence rappelée au point 60 du présent arrêt que certaines catégories d'activités militaires échappent, dans leur intégralité, au champ d'application de la directive 2003/88, lorsque ces activités sont à ce point spécifiques qu'elles s'opposent de manière contraignante et permanente au respect des exigences imposées par cette directive.

76 Tel est le cas des activités exercées par des membres des forces armées qui, en raison de leurs hautes qualifications ou du caractère extrêmement sensible des tâches qui leur sont assignées, ne peuvent que très difficilement être remplacés par d'autres membres des forces armées, au moyen d'un système de rotation permettant de garantir tout à la fois le respect des périodes maximales de travail et des périodes de repos prévues par la directive 2003/88 et le bon accomplissement des missions essentielles qui leur sont imparties.

77 Troisièmement, il importe de relever que tous les militaires appelés à prêter leur concours aux opérations impliquant un engagement militaire des forces armées d'un État membre, que celles-ci se déploient, de façon permanente ou occasionnelle, à l'intérieur de ses frontières ou à l'extérieur de celles-ci, exercent une activité qui, en vertu de l'article 1er, paragraphe 3, de la directive 2003/88, lu en combinaison avec l'article 2, paragraphe 2, premier alinéa, de la directive 89/391, et à la lumière de l'article 4, paragraphe 2, TUE, doit, par sa nature même, être exclue, dans son intégralité, du champ d'application de la directive 2003/88.

78 En effet, le respect des exigences imposées par la directive 2003/88 au cours de ces opérations ferait peser un risque considérable sur le succès de celles-ci, succès qui suppose de pouvoir exiger un engagement total, au cours de longues périodes, des membres des forces armées impliqués, et, par voie de conséquence, sur le bon accomplissement des fonctions essentielles de sauvegarde de la sécurité nationale ou de préservation de l'intégrité territoriale des États membres.

79 Dans ce cadre, il convient d'avoir égard à l'éventuelle interdépendance existant non seulement entre lesdites opérations, mais aussi entre celles-ci et d'autres activités exercées par les membres des forces armées, auxquelles l'application des règles de cette directive, en imposant aux autorités concernées de mettre en place un système de rotation ou de planification du temps de travail, ne pourrait se faire qu'au détriment de ces mêmes opérations, contrairement aux exigences de l'article 4, paragraphe 2, TUE. Partant, si cela s'avère nécessaire au bon accomplissement des opérations militaires proprement dites, il ne saurait être exclu que certaines activités des forces armées qui n'y ont pas trait directement échappent également, pour la durée de ces opérations, au champ d'application de la directive 2003/88.

80 En outre, l'article 1er, paragraphe 3, de la directive 2003/88, lu en combinaison avec l'article 2, paragraphe 2, premier alinéa, de la directive 89/391, et à la lumière de l'article 4, paragraphe 2, TUE, impose tout autant d'exclure du champ d'application de la directive 2003/88 l'ensemble des activités qui relèvent soit de la formation initiale des militaires, à laquelle il convient d'assimiler le service militaire obligatoire, soit des entraînements opérationnels auxquels les membres des forces armées sont, par la suite, régulièrement astreints.

81 En effet, comme l'a relevé le gouvernement français, afin de garantir l'efficacité opérationnelle des forces armées, les militaires doivent pouvoir être confrontés, au cours de leur formation initiale et de leur entraînement opérationnel, à des situations qui permettent de reproduire au plus près les conditions, y compris les plus extrêmes, dans lesquelles les opérations militaires proprement dites se déroulent. Or, un tel objectif légitime ne pourrait être atteint si les règles relatives à l'aménagement du temps de travail, prévues par la directive 2003/88, devaient être respectées au cours de cette formation initiale et de ces entraînements opérationnels.

82 Du reste, en imposant aux militaires de telles exigences de formation et d'entraînement, les États membres veillent également à ce que la santé et la sécurité de ces militaires soient au mieux protégées au cours des opérations des forces armées proprement dites, dans la mesure où ces exigences permettent à ceux-ci d'acquérir et de conserver un niveau élevé d'endurance face à des conditions de vie dégradées.

83 La circonstance que la formation initiale, les entraînements opérationnels et les opérations militaires proprement dites ont lieu en temps de paix n'est pas de nature à infirmer la conclusion selon laquelle ces activités doivent être intégralement exclues du champ d'application de la directive 2003/88. En effet, les missions qui sont assumées par les forces armées afin d'assurer la préservation de la sécurité nationale et de l'intégrité du territoire doivent pouvoir être pleinement réalisées, même en temps de paix.

84 Il importe d'ajouter qu'il relève de la seule responsabilité de chacun des États membres, compte tenu, notamment, des menaces auxquelles il est confronté, des responsabilités internationales qui lui sont propres ou du contexte géopolitique spécifique dans lequel il évolue, de procéder aux opérations militaires qu'il juge appropriées et de déterminer l'intensité de la formation initiale et des entraînements

opérationnels qu'il estime utiles au bon accomplissement desdites opérations, sans qu'un contrôle de la Cour à cet égard soit envisageable, de telles questions devant être considérées comme échappant au champ d'application du droit de l'Union, comme il a été relevé au point 38 du présent arrêt.

85 En l'occurrence, il appartient à la juridiction de renvoi de déterminer si l'activité de garde assurée par B. K. relève d'une des hypothèses visées aux points 73 à 83 du présent arrêt. Dans la négative, cette activité devra être considérée comme étant soumise au champ d'application de la directive 2003/88. À cet égard, il ne saurait être exclu, au vu du dossier dont dispose la Cour, que cette juridiction puisse considérer que l'activité de garde en cause au principal constitue une opération militaire proprement dite, de sorte qu'elle échappe au champ d'application de cette directive.

86 Enfin, il y a lieu de préciser que, même lorsque des militaires exercent des activités qui relèvent pleinement du champ d'application de la directive 2003/88, celle-ci contient, contrairement à ce que soutient le gouvernement français, des exceptions aux droits qu'elle instaure, susceptibles d'être invoquées par les États membres à l'égard de ces militaires.

87 Il en va, en tout cas, ainsi de l'article 17, paragraphe 3, sous b) et c), de ladite directive, qui permet, en substance, de déroger, sous certaines conditions, aux articles 3, 4, 5, 8 et 16 de celle-ci, tant pour les activités de garde, de surveillance et de permanence caractérisées par la nécessité d'assurer la protection des biens et des personnes que pour les activités caractérisées par la nécessité d'assurer la continuité du service ou de la production.

88 Il résulte de l'ensemble des considérations qui précèdent que l'article 1er, paragraphe 3, de la directive 2003/88, lu à la lumière de l'article 4, paragraphe 2, TUE, doit être interprété en ce sens qu'une activité de garde exercée par un militaire est exclue du champ d'application de cette directive :

– soit lorsque cette activité intervient dans le cadre de sa formation initiale, d'un entraînement opérationnel ou d'une opération militaire proprement dite,

– soit lorsqu'elle constitue une activité à ce point particulière qu'elle ne se prête pas à un système de rotation des effectifs permettant d'assurer le respect des exigences de ladite directive,

– soit lorsqu'il apparaît, au vu de l'ensemble des circonstances pertinentes, que cette activité est exécutée dans le cadre d'événements exceptionnels, dont la gravité et l'ampleur nécessitent l'adoption de mesures indispensables à la protection de la vie, de la santé ainsi que de la sécurité de la collectivité et dont la bonne exécution serait compromise si l'ensemble des règles énoncées par ladite directive devaient être respectées,

– soit lorsque l'application de ladite directive à une telle activité, en imposant aux autorités concernées de mettre en place un système de rotation ou de planification du temps de travail, ne pourrait se faire qu'au détriment du bon accomplissement des opérations militaires proprement dites.

Sur la seconde question

89 À titre liminaire, il y a lieu de préciser que, dans le cadre de la réponse à la deuxième question posée par la juridiction de renvoi, l'expression « période de garde » sera utilisée afin de désigner l'ensemble des périodes au cours desquelles le militaire, durant son activité de garde, demeure uniquement à la disposition de ses supérieurs, sans exercer effectivement une activité de surveillance.

90 Par ailleurs, il convient de souligner qu'il ressort de la décision de renvoi que le litige au principal concerne exclusivement la rémunération, en tant qu'heures supplémentaires, des périodes de garde assurées par B. K.

91 Partant, afin de donner une réponse utile à la juridiction de renvoi, il convient de reformuler la seconde question et de considérer que, par celle-ci, la juridiction de renvoi cherche, en substance, à savoir si l'article 2 de la directive 2003/88 doit être interprété en ce sens qu'il impose qu'une période de garde au cours de laquelle le militaire est tenu de demeurer au sein de la caserne où il est affecté mais n'y accomplit pas de travail effectif soit considérée comme étant du temps de travail, aux fins de la fixation de la rémunération due à ce militaire pour une telle période.

92 Il importe encore de préciser que la réponse à cette question ne sera pertinente pour le litige au principal que dans le cas où la juridiction de renvoi devrait aboutir à la conclusion que l'activité de garde en cause au principal n'est pas exclue du champ d'application de la directive 2003/88.

93 Sous le bénéfice de ces précisions liminaires, il convient, en premier lieu, de rappeler que relève de la notion de « temps de travail », au sens de la directive 2003/88, l'intégralité des périodes de garde au cours desquelles les contraintes imposées au travailleur sont d'une nature telle qu'elles affectent objectivement et très significativement la faculté, pour ce dernier, de gérer librement, au cours de ces périodes, le temps pendant lequel ses services professionnels ne sont pas sollicités et de consacrer ce temps à ses propres intérêts. Inversement, lorsque les contraintes imposées au travailleur au cours d'une période de garde

déterminée n'atteignent pas un tel degré d'intensité et lui permettent de gérer son temps et de se consacrer à ses propres intérêts sans contraintes majeures, seul le temps lié à la prestation de travail qui est, le cas échéant, effectivement réalisée au cours d'une telle période constitue du « temps de travail », aux fins de l'application de cette directive [arrêt du 9 mars 2021, Radiotelevizija Slovenija (Période d'astreinte dans un lieu reculé), C-344/19, EU:C:2021:182, points 37 et 38 ainsi que jurisprudence citée].

94 S'agissant des périodes de garde effectuées sur des lieux de travail qui, comme en l'occurrence, ne se confondent pas avec le domicile du travailleur, le facteur déterminant pour considérer que les éléments caractéristiques de la notion de « temps de travail », au sens de la directive 2003/88, sont présents est le fait que le travailleur est contraint d'être physiquement présent sur le lieu déterminé par l'employeur et de s'y tenir à la disposition de ce dernier pour pouvoir immédiatement fournir ses services en cas de besoin, étant précisé que le lieu de travail doit être compris comme tout lieu où le travailleur est appelé à exercer une activité sur ordre de son employeur, y compris lorsque ce lieu n'est pas l'endroit où il exerce habituellement son activité professionnelle. Dès lors qu'au cours d'une telle période de garde, le travailleur doit rester éloigné de son environnement social et familial et bénéficie d'une faible latitude pour gérer le temps pendant lequel ses services professionnels ne sont pas sollicités, l'intégralité de celle-ci doit être qualifiée de « temps de travail », au sens de cette directive, indépendamment des prestations de travail réellement effectuées par le travailleur au cours de ladite période [arrêt du 9 mars 2021, Radiotelevizija Slovenija (Période d'astreinte dans un lieu reculé), C-344/19, EU:C:2021:182, points 33 à 35 et jurisprudence citée].

95 Il résulte de ce qui précède que, à supposer que la directive 2003/88 s'y applique, une période de garde imposée à un militaire qui implique sa présence continue sur son lieu de travail doit être considérée comme étant du temps de travail, au sens de l'article 2, point 1, de cette directive, lorsque ce lieu de travail ne se confond pas avec son domicile.

96 En deuxième lieu, il importe toutefois de rappeler que, exception faite de l'hypothèse particulière relative au congé annuel payé, visée à l'article 7, paragraphe 1, de la directive 2003/88, cette directive se borne à réglementer certains aspects de l'aménagement du temps de travail afin d'assurer la protection de la sécurité et de la santé des travailleurs, de sorte que, en principe, elle ne trouve pas à s'appliquer à la rémunération des travailleurs [arrêt du 9 mars 2021, Radiotelevizija Slovenija (Période d'astreinte dans un lieu reculé), C-344/19, EU:C:2021:182, point 57 et jurisprudence citée].

97 Partant, le mode de rémunération des travailleurs au titre des périodes de garde qu'ils effectuent relève non pas de la directive 2003/88 mais des dispositions pertinentes du droit national. Cette directive ne s'oppose, par conséquent, pas à l'application d'une réglementation d'un État membre, d'une convention collective de travail ou d'une décision d'un employeur qui, aux fins de la rémunération d'un service de garde, prend en compte de manière différente les périodes au cours desquelles des prestations de travail sont réellement effectuées et celles durant lesquelles aucun travail effectif n'est accompli, même lorsque ces périodes doivent être considérées, dans leur intégralité, comme du « temps de travail » aux fins de l'application de ladite directive [arrêt du 9 mars 2021, Radiotelevizija Slovenija (Période d'astreinte dans un lieu reculé), C-344/19, EU:C:2021:182, point 58 ainsi que jurisprudence citée].

98 Il découle de l'ensemble des considérations qui précèdent que l'article 2 de la directive 2003/88 doit être interprété en ce sens qu'il ne s'oppose pas à ce qu'une période de garde au cours de laquelle un militaire est tenu de demeurer au sein de la caserne où il est affecté mais n'y accomplit pas de travail effectif soit rémunérée d'une manière différente qu'une période de garde au cours de laquelle il effectue des prestations de travail effectif.

Sur les dépens

99 La procédure revêtant, à l'égard des parties au principal, le caractère d'un incident soulevé devant la juridiction de renvoi, il appartient à celle-ci de statuer sur les dépens. Les frais exposés pour soumettre des observations à la Cour, autres que ceux desdites parties, ne peuvent faire l'objet d'un remboursement.

Par ces motifs, la Cour (grande chambre) dit pour droit :

1) **L'article 1er, paragraphe 3, de la directive 2003/88/CE du Parlement européen et du Conseil, du 4 novembre 2003, concernant certains aspects de l'aménagement du temps de travail, lu à la lumière de l'article 4, paragraphe 2, TUE, doit être interprété en ce sens qu'une activité de garde exercée par un militaire est exclue du champ d'application de cette directive :**

– **soit lorsque cette activité intervient dans le cadre de sa formation initiale, d'un entraînement opérationnel ou d'une opération militaire proprement dite,**

– **soit lorsqu'elle constitue une activité à ce point particulière qu'elle ne se prête pas à un système de rotation des effectifs permettant d'assurer le respect des exigences de ladite directive,**

– **soit lorsqu'il apparaît, au vu de l'ensemble des circonstances pertinentes, que cette activité est exécutée dans le cadre d'événements exceptionnels, dont la gravité et l'ampleur nécessitent l'adoption de mesures indispensables à la protection de la vie, de la santé ainsi que de la sécurité de la collectivité et dont la bonne exécution serait compromise si l'ensemble des règles énoncées par ladite directive devaient être respectées,**

– **soit lorsque l'application de ladite directive à une telle activité, en imposant aux autorités concernées de mettre en place un système de rotation ou de planification du temps de travail, ne pourrait se faire qu'au détriment du bon accomplissement des opérations militaires proprement dites.**

2) **L'article 2 de la directive 2003/88 doit être interprété en ce sens qu'il ne s'oppose pas à ce qu'une période de garde au cours de laquelle un militaire est tenu de demeurer au sein de la caserne où il est affecté mais n'y accomplit pas de travail effectif soit rémunérée d'une manière différente qu'une période de garde au cours de laquelle il effectue des prestations de travail effectif.**

CE, 17 déc. 2021, n° 437125

Vu la procédure suivante :
Par une requête et trois nouveaux mémoires, enregistrés au secrétariat du contentieux du Conseil d'Etat les 25 décembre 2019, 5 juillet 2020, 1er octobre et 11 novembre 2021, M. G... Q... demande au Conseil d'Etat :
1°) d'annuler pour excès de pouvoir la décision par laquelle le ministre de l'intérieur a rejeté sa demande tendant à ce qu'il prenne les mesures nécessaires pour l'application à la gendarmerie des dispositions de l'article 6 de la directive 2003/88/CE du Parlement européen et du Conseil du 4 novembre 2003 concernant certains aspects de l'aménagement du temps de travail ;
2°) d'enjoindre au ministre de l'intérieur de prendre les mesures nécessaires dans un délai de deux mois, sous astreinte de 100 euros par jour de retard.
Vu les autres pièces du dossier ;
Vu :
- la Constitution ;
- le traité sur l'Union européenne ;
- le traité sur le fonctionnement de l'Union européenne ;
- la directive 89/391/CEE du Conseil du 12 juin 1989 ;
- la directive 2003/88/CE du Parlement européen et du Conseil du 4 novembre 2003 ;
- le code de la défense ;
- le code de la sécurité intérieure ;
- le code général de la propriété des personnes publiques ;
- la circulaire n° 17400/GEND/DOE/SPSPSR/BSP du 4 novembre 2013 ;
- l'instruction n° 36132/GEND/DOE/SDSPSR/BSP du 8 juin 2016 ;
- l'instruction n° 35000/GEND/DSF du 13 décembre 2018 ;
- la circulaire n° 49500/GEND/DOE/SDSPSR/BSP du 10 juillet 2019 ;
- la circulaire n° 42000/GEND/DOE/SDSPSR/BSP du 16 mars 2021 ;
- l'arrêt de la Cour de justice de l'Union européenne du 9 mars 2021, RJ c/ Stadt Offenbach am Main (C-580/19) ;
- l'arrêt de la Cour de justice de l'Union européenne du 15 juillet 2021, B.K. c/ Republika Slovenija (Ministrstvo za obrambo) (C-742/19) ;
- le code de justice administrative ;

Après avoir entendu en séance publique :
- le rapport de M. Alexis Goin, auditeur,
- les conclusions de Mme Mireille Le Corre, rapporteure publique ;

Considérant ce qui suit :

1. M. Q..., sous-officier de gendarmerie affecté dans la gendarmerie départementale, a demandé au ministre de l'intérieur de prendre les mesures nécessaires pour assurer l'application à la gendarmerie des dispositions de l'article 6 de la directive 2003/88/CE du Parlement européen et du Conseil du 4 novembre 2003, limitant la durée hebdomadaire du temps de travail. Par une lettre du 18 décembre 2019, le directeur général de la gendarmerie nationale, agissant par délégation de signature du ministre de l'intérieur, a refusé de faire droit à cette demande. M. Q... demande l'annulation pour excès de pouvoir de cette décision. Eu égard à son intérêt à agir, sa requête doit être regardée comme ne contestant cette décision qu'en tant qu'elle concerne la gendarmerie départementale.

2. Aux termes de l'article 6 de la directive du 4 novembre 2003 : " Les Etats membres prennent les mesures nécessaires pour que, en fonction des impératifs de protection de la sécurité et de la santé des travailleurs : / a) la durée hebdomadaire du travail soit limitée au moyen de dispositions législatives, réglementaires ou administratives (...) ; / b) la durée moyenne de travail pour chaque période de sept jours n'excède pas quarante-huit heures, y compris les heures supplémentaires. " En application des dispositions des articles 16, 17 et 19 de cette directive, le respect de cette durée hebdomadaire peut être vérifié sur une période de référence allant jusqu'à six mois pour, notamment, les activités de garde, de surveillance et de permanence ou caractérisées par la nécessité d'assurer la continuité du service. M. Q... soutient que la réglementation applicable dans la gendarmerie départementale méconnaît les objectifs de l'article 6 de la directive du 4 novembre 2003.

3. Saisi d'un moyen tiré de la méconnaissance de l'obligation de transposer les directives dans le cadre d'un litige dirigé contre le refus de l'autorité administrative de prendre les mesures de transposition d'une disposition d'une directive, il incombe au juge administratif de vérifier si ces mesures relèvent de la compétence de l'autorité qui a été saisie de la demande et si les textes législatifs ou réglementaires en vigueur n'assurent pas une transposition

suffisante et conforme de la disposition en cause. Le juge de l'excès de pouvoir apprécie la légalité d'un tel refus au regard des règles applicables et des circonstances prévalant à la date de sa décision.

4. Les ministres des armées et de l'intérieur soutiennent, en défense, d'une part, que la demande de M. Q..., qui tend, selon eux, à l'annulation d'une décision individuelle relative à son temps de travail, ne relève pas de la compétence de premier et dernier ressort du Conseil d'Etat et, d'autre part, que les exigences constitutionnelles de nécessaire libre disposition de la force armée et de sauvegarde des intérêts fondamentaux de la Nation, au nombre desquels figurent l'indépendance de la Nation et l'intégrité du territoire, s'opposent à ce qu'il soit fait droit aux conclusions de la requête.

Sur l'exception d'incompétence du Conseil d'Etat soulevée par les ministres :

5. Aux termes de l'article R. 311-1 du code de justice administrative : " Le Conseil d'Etat est compétent pour connaître en premier et dernier ressort : (...) / 2° Des recours dirigés contre les actes réglementaires des ministres et des autres autorités à compétence nationale et contre leurs circulaires et instructions de portée générale ; (...) ".

6. Les décisions refusant de prendre un acte réglementaire doivent elles-mêmes être regardées comme de nature réglementaire. Par suite, le Conseil d'Etat est compétent pour connaître de telles décisions lorsqu'elles sont prises par les ministres. La requête de M. Q... étant dirigée contre le refus du ministre de l'intérieur de prendre des mesures relatives au temps de travail, qui relèvent de son pouvoir réglementaire d'organisation du service, et ne tendant pas, contrairement à ce que soutiennent les ministres, à l'annulation d'une décision individuelle relative à son temps de travail, elle relève de la compétence de premier et dernier ressort du Conseil d'Etat.

Sur le cadre juridique :

En ce qui concerne les exigences inhérentes à la hiérarchie des normes :

7. En vertu de l'article 88-1 de la Constitution : " La République participe à l'Union européenne constituée d'Etats qui ont choisi librement d'exercer en commun certaines de leurs compétences en vertu du traité sur l'Union européenne et du traité sur le fonctionnement de l'Union européenne, tels qu'ils résultent du traité signé à Lisbonne le 13 décembre 2007 ". Selon le paragraphe 3 de l'article 4 du traité sur l'Union européenne : " En vertu du principe de coopération loyale, l'Union et les Etats membres se respectent et s'assistent mutuellement dans l'accomplissement des missions découlant des traités. / Les Etats membres prennent toute mesure générale ou particulière propre à assurer l'exécution des obligations découlant des traités ou résultant des actes des institutions de l'Union. / Les Etats membres facilitent l'accomplissement par l'Union de sa mission et s'abstiennent de toute mesure susceptible de mettre en péril la réalisation des objectifs de l'Union ". La seconde phrase du paragraphe 1 de l'article 19 du même traité assigne à la Cour de justice de l'Union européenne la mission d'assurer " le respect du droit dans l'interprétation et l'application des traités ".

8. Le respect du droit de l'Union constitue une obligation tant en vertu du traité sur l'Union européenne et du traité sur le fonctionnement de l'Union européenne qu'en application de l'article 88-1 de la Constitution. Il emporte l'obligation de transposer les directives et d'adapter le droit interne aux règlements européens. En vertu des principes de primauté, d'unité et d'effectivité issus des traités, tels qu'ils ont été interprétés par la Cour de justice de l'Union européenne, le juge national, chargé d'appliquer les dispositions et principes généraux du droit de l'Union, a l'obligation d'en assurer le plein effet en laissant au besoin inappliquée toute disposition contraire, qu'elle résulte d'un engagement international de la France, d'une loi ou d'un acte administratif.

9. Toutefois, tout en consacrant l'existence d'un ordre juridique de l'Union européenne intégré à l'ordre juridique interne, dans les conditions mentionnées au point précédent, l'article 88-1 confirme la place de la Constitution au sommet de ce dernier. Il appartient au juge administratif, s'il y a lieu, de retenir de l'interprétation que la Cour de justice de l'Union européenne a donnée des obligations résultant du droit de l'Union la lecture la plus conforme aux exigences constitutionnelles autres que celles qui découlent de l'article 88-1, dans la mesure où les énonciations des arrêts de la Cour le permettent. Dans le cas où l'application d'une directive ou d'un règlement européen, tel qu'interprété par la Cour de justice de l'Union européenne, aurait pour effet de priver de garanties effectives l'une de ces exigences constitutionnelles, qui ne bénéficierait pas, en droit de l'Union, d'une protection équivalente, le juge administratif, saisi d'un moyen en ce sens, doit l'écarter dans la stricte mesure où le respect de la Constitution l'exige.

10. Il en résulte, d'une part, que, dans le cadre du contrôle de la légalité et de la constitutionnalité des actes réglementaires assurant directement la transposition d'une directive européenne ou l'adaptation du droit interne à

un règlement et dont le contenu découle nécessairement des obligations prévues par la directive ou le règlement, il appartient au juge administratif, saisi d'un moyen tiré de la méconnaissance d'une disposition ou d'un principe de valeur constitutionnelle, de rechercher s'il existe une règle ou un principe général du droit de l'Union européenne qui, eu égard à sa nature et à sa portée, tel qu'il est interprété en l'état actuel de la jurisprudence du juge de l'Union, garantit par son application l'effectivité du respect de la disposition ou du principe constitutionnel invoqué. Dans l'affirmative, il y a lieu pour le juge administratif, afin de s'assurer de la constitutionnalité de l'acte réglementaire contesté, de rechercher si la directive que cet acte transpose ou le règlement auquel cet acte adapte le droit interne est conforme à cette règle ou à ce principe général du droit de l'Union. Il lui revient, en l'absence de difficulté sérieuse, d'écarter le moyen invoqué, ou, dans le cas contraire, de saisir la Cour de justice de l'Union européenne d'une question préjudicielle, dans les conditions prévues par l'article 267 du traité sur le fonctionnement de l'Union européenne. En revanche, s'il n'existe pas de règle ou de principe général du droit de l'Union garantissant l'effectivité du respect de la disposition ou du principe constitutionnel invoqué, il revient au juge administratif d'examiner directement la constitutionnalité des dispositions réglementaires contestées.

11. D'autre part, lorsqu'il est saisi d'un recours contre un acte administratif relevant du champ d'application du droit de l'Union et qu'est invoqué devant lui le moyen tiré de ce que cet acte, ou les dispositions législatives qui en constituent la base légale ou pour l'application desquelles il a été pris, sont contraires à une directive ou un règlement européen, il appartient au juge administratif, après avoir saisi le cas échéant la Cour de justice d'une question préjudicielle portant sur l'interprétation ou la validité de la disposition du droit de l'Union invoquée, d'écarter ce moyen ou d'annuler l'acte attaqué, selon le cas. Toutefois, s'il est saisi par le défendeur d'un moyen, assorti des précisions nécessaires pour en apprécier le bien-fondé, tiré de ce qu'une règle de droit national, alors même qu'elle est contraire à la disposition du droit de l'Union européenne invoquée dans le litige, ne saurait être écartée sans priver de garanties effectives une exigence constitutionnelle, il appartient au juge administratif de rechercher s'il existe une règle ou un principe général du droit de l'Union européenne qui, eu égard à sa nature et à sa portée, tel qu'il est interprété en l'état actuel de la jurisprudence du juge de l'Union, garantit par son application l'effectivité de l'exigence constitutionnelle invoquée. Dans l'affirmative, il lui revient, en l'absence de difficulté sérieuse justifiant une question préjudicielle à la Cour de justice, d'écarter cette argumentation avant de faire droit au moyen du requérant, le cas échéant. Si, à l'inverse, une telle disposition ou un tel principe général du droit de l'Union n'existe pas ou que la portée qui lui est reconnue dans l'ordre juridique européen n'est pas équivalente à celle que la Constitution garantit, il revient au juge administratif d'examiner si, en écartant la règle de droit national au motif de sa contrariété avec le droit de l'Union européenne, il priverait de garanties effectives l'exigence constitutionnelle dont le défendeur se prévaut et, le cas échéant, d'écarter le moyen dont le requérant l'a saisi.

En ce qui concerne les exigences constitutionnelles invoquées en défense par les ministres :

12. Aux termes de l'article 5 de la Constitution : " Le Président de la République veille au respect de la Constitution. Il assure, par son arbitrage, le fonctionnement régulier des pouvoirs publics ainsi que la continuité de l'Etat. / Il est le garant de l'indépendance nationale, de l'intégrité du territoire et du respect des traités. ". Selon son article 15 : " Le Président de la République est le chef des armées. Il préside les conseils et les comités supérieurs de la défense nationale. ". Aux termes de son article 20 : " Le Gouvernement détermine et conduit la politique de la nation. / Il dispose de l'administration et de la force armée. / (...) ". Selon son article 21 : " Le Premier ministre dirige l'action du Gouvernement. Il est responsable de la défense nationale. (...) ".

13. Il résulte de ce qui précède que la Constitution garantit la nécessaire libre disposition de la force armée, ainsi que l'a jugé le Conseil constitutionnel par ses décisions n° 2014-432 QPC du 28 novembre 2014 et n° 2014-450 QPC du 27 février 2015. A la lumière des exigences constitutionnelles inhérentes à la sauvegarde des intérêts fondamentaux de la Nation, au premier rang desquels figurent l'indépendance nationale et l'intégrité du territoire, qui en sont la finalité, cette libre disposition de la force armée implique que soit assurée la disponibilité, en tout temps et en tout lieu, des forces armées.

14. Selon le paragraphe 2 de l'article 4 du traité sur l'Union européenne, il appartient à l'Union, y compris à la Cour de justice de l'Union européenne, de respecter l'identité nationale des Etats membres, " inhérente à leurs structures fondamentales politiques et constitutionnelles ", ainsi que " 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 ", cette dernière restant " de la seule responsabilité des Etats membres ". La Cour de justice de l'Union européenne a dit pour droit, dans son arrêt du 15 juillet 2021, B.K. c/ Republika Slovenija (Ministrstvo za obrambo) (C-742/19), que l'Union respecte, d'une part, l'identité nationale des Etats membres, inhérente à leurs structures fondamentales politiques et constitutionnelles et, d'autre part, 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, celle-ci relevant de la seule responsabilité de chaque Etat membre. La Cour a rappelé que les missions principales des forces armées des Etats membres, que sont la préservation de l'intégrité territoriale et la sauvegarde de la sécurité nationale, figuraient explicitement parmi les fonctions essentielles de l'Etat que l'Union doit respecter, en vertu de l'article 4, paragraphe 2, du traité sur l'Union européenne. La Cour a ainsi précisé que les règles du droit de l'Union ne sauraient être interprétées d'une manière telle qu'elles empêcheraient les forces armées d'accomplir leurs missions et souligné à cet égard que les spécificités que chaque Etat membre confère au fonctionnement de ses forces armées devaient être dûment prises en considération, que ces spécificités résultent, entre autres, des responsabilités internationales particulières assumées par cet Etat membre, des conflits ou des menaces auxquels il est confronté, ou encore du contexte géopolitique dans lequel cet Etat évolue.

15. Elle a cependant estimé qu'il ne découlait pas du respect dû par l'Union aux fonctions essentielles de l'Etat que les décisions des Etats membres relatives à l'organisation de leurs forces armées échapperaient au champ d'application du droit de l'Union. Elle a déduit de son interprétation de l'article 4, paragraphe 2, du traité sur l'Union européenne que ne sauraient relever du champ d'application de la directive du 4 novembre 2003 les activités des militaires intervenant dans le cadre d'une opération militaire, de leur formation initiale, d'un entraînement opérationnel, ainsi que celles qui présentent un lien d'interdépendance avec des opérations militaires et pour lesquelles l'application de la directive se ferait au détriment du bon accomplissement de ces opérations. Elle a également rappelé que les activités qui ne se prêtent pas à un système de rotation des effectifs, eu égard aux hautes qualifications des militaires en question ou à leurs tâches extrêmement sensibles, ainsi que celles qui sont exécutées dans le cadre d'événements exceptionnels, ne sauraient se voir appliquer les règles de la directive.

16. En dépit de la portée que la Cour de justice a ainsi conférée aux stipulations de l'article 4, paragraphe 2, du traité sur l'Union européenne en ce qui concerne l'application du droit de l'Union dans les forces armées et malgré les exclusions qu'elle en a déduites, les exigences constitutionnelles mentionnées au point 13, qui s'appliquent à des domaines relevant exclusivement ou essentiellement de la compétence des Etats membres en vertu des traités constitutifs de l'Union, ne sauraient être regardées comme bénéficiant, en droit de l'Union, d'une protection équivalente à celle que garantit la Constitution.

17. Il résulte de ce qui est dit aux points 3 et 7 à 16 qu'il incombe d'abord au juge administratif, saisi de conclusions dirigées contre le rejet d'une demande tendant à la transposition d'une directive susceptible de limiter la disponibilité des forces armées, de vérifier si les militaires concernés ne sont pas exclus du champ de cette directive en raison de leurs activités. S'ils en sont exclus, il rejette les conclusions dont il est saisi. Dans l'hypothèse inverse, il lui revient de vérifier si le droit national est compatible avec les objectifs de la directive. A supposer, enfin, qu'il constate l'incompatibilité du droit national avec ces objectifs et qu'il soit saisi d'un moyen en défense en ce sens, il lui appartient de s'assurer que l'application du droit de l'Union ne conduirait pas à ce que les limites fixées à la disponibilité des forces armées privent de garanties effectives l'exigence constitutionnelle de nécessaire libre disposition de la force armée, aux fins d'assurer la sauvegarde des intérêts fondamentaux de la Nation, et, le cas échéant, d'écarter le moyen tiré de la méconnaissance du droit de l'Union dont le requérant l'a saisi.

Sur la requête :

S'agissant du champ d'application de la directive du 4 novembre 2003 :

18. Aux termes du paragraphe 3 de l'article 1er de la directive du 4 novembre 2003 : " La présente directive s'applique à tous les secteurs d'activités, privés ou publics, au sens de l'article 2 de la directive 89/391/CEE, sans préjudice des articles 14, 17, 18 et 19 de la présente directive. (...) ". Aux termes de l'article 2 de la directive du 12 juin 1989, cette directive " s'applique à tous les secteurs d'activités, privés ou publics (...) ". Toutefois, elle n'est pas applicable " lorsque des particularités inhérentes à certaines activités spécifiques dans la fonction publique, par exemple dans les forces armées ou la police, ou à certaines activités spécifiques dans les services de protection civile s'y opposent de manière contraignante ".

19. La directive du 4 novembre 2003 renvoie à la directive du 12 juin 1989 pour la définition de son champ d'application matériel. Le choix de leurs auteurs a été, d'une part, de donner une dimension extrêmement large à ce champ qui couvre tous les secteurs d'activités, privés ou publics, d'autre part, de prendre en compte la nature de l'activité exercée et non le statut assigné par la loi nationale à telle ou telle catégorie de travailleurs. Et ce n'est, selon les termes mêmes de l'article 2 de la directive du 12 juin 1989, que lorsque des particularités

inhérentes à certaines activités spécifiques, par exemple susceptibles d'être exercées par les membres des forces armées, s'y opposent de manière contraignante que les activités en cause sont exclues des prévisions de cette directive.

20. La Cour de justice de l'Union européenne a ainsi jugé, dans son arrêt du 15 juillet 2021, que les militaires n'étaient pas exclus du champ d'application de cette directive du fait de cette seule qualité. Comme il a été dit au point 14, elle a toutefois estimé que les règles de temps de travail de la directive ne pouvaient être interprétées d'une telle manière qu'elles empêcheraient les forces armées d'accomplir leurs missions, afin de ne pas porter atteinte à la préservation de l'intégrité territoriale et la sauvegarde de la sécurité nationale par les Etats. Elle en a déduit que ne sauraient relever du champ d'application de la directive du 4 novembre 2003 les activités des militaires mentionnées au point 15 de la présente décision.

21. Aux termes de l'article L. 3211-1 du code de la défense : " Les forces armées comprennent : / 1° L'armée de terre, la marine nationale et l'armée de l'air et de l'espace (...) / 2° La gendarmerie nationale ; / 3° Les services de soutien et les organismes interarmées. (...) ". Selon l'article L. 3211-3 de ce code : " La gendarmerie nationale est une force armée instituée pour veiller à l'exécution des lois. / Sans préjudice des dispositions de l'article L. 421-1 du code de la sécurité intérieure, elle participe à la défense de la patrie et des intérêts supérieurs de la Nation, notamment au contrôle et à la sécurité des armements nucléaires. / L'ensemble de ses missions militaires s'exécute sur toute l'étendue du territoire national, ainsi qu'en haute mer à bord des navires battant pavillon français. Hors de ces cas, elles s'exécutent en application des engagements internationaux de la France, ainsi que dans les armées. ". L'article L. 421-1 du code de la sécurité intérieure, dont le premier alinéa définit la gendarmerie nationale dans des termes identiques à celui de l'article L. 3211-3 du code de la défense, cité ci-dessus, dispose en ses alinéas suivants que : " La police judiciaire constitue l'une de ses missions essentielles. / La gendarmerie nationale est destinée à assurer la sécurité publique et l'ordre public, particulièrement dans les zones rurales et périurbaines, ainsi que sur les voies de communication. / Elle contribue à la mission de renseignement et d'information des autorités publiques, à la lutte contre le terrorisme, ainsi qu'à la protection des populations. / (...) ". Les articles L. 3225-1 et L. 421-2 de ces mêmes codes prévoient que la gendarmerie exerce des missions militaires, pour lesquelles elle est placée sous l'autorité du ministre de la défense, des missions civiles, sous l'autorité du ministre de l'intérieur, ainsi que des missions judiciaires. Enfin, selon l'article R. 3225-6 du code de la défense : " Les formations de gendarmerie départementale remplissent dans leur ressort l'ensemble des missions dévolues à la gendarmerie nationale. (...). "

22. Il résulte de ces dispositions que les formations de gendarmerie départementale sont susceptibles de remplir des missions civiles et militaires. Il ne ressort pas des pièces du dossier que les militaires de la gendarmerie départementale, qui constitue une composante des forces armées, exercent dans leur ensemble des activités relevant d'une des exclusions au champ d'application de la directive du 4 novembre 2003 mentionnées au point 15, les ministres soutenant d'ailleurs que seule une partie " très minoritaire " des effectifs exerce de telles activités.

S'agissant de l'organisation du temps de service des militaires de la gendarmerie départementale :

23. L'organisation générale du temps de service des militaires de la gendarmerie départementale, ainsi qu'elle est notamment fixée par l'instruction du 8 juin 2016, comprend, en premier lieu, des temps d'activité, durant lesquels ces militaires sont directement employés pour les besoins du service. En deuxième lieu, les gendarmes peuvent également être placés sous astreinte, durant laquelle ils peuvent, selon les cas, être mobilisés immédiatement ou sous un délai qui est, en principe, de deux heures. Enfin, la réglementation applicable leur garantit des droits à repos, dont certains ne sont pas exclusifs d'une astreinte.

24. Ainsi qu'il a été dit aux points 21 et 22, la gendarmerie départementale exerce des missions civiles et militaires. Elle concourt notamment aux missions de défense opérationnelle du territoire, prévues à l'article R*. 1421-1 du code de la défense, pour assurer le maintien de la liberté et de la continuité d'action du Gouvernement, ainsi que la sauvegarde des organes essentiels à la défense de la Nation. Conformément au 2° de cet article, la gendarmerie départementale contribue en effet à " assurer au sol la couverture générale du territoire " en présence d'une menace extérieure. Afin de permettre le bon accomplissement de l'ensemble de ses missions civiles et militaires, l'état militaire implique des sujétions particulières. Il en découle, s'agissant de chaque militaire, selon l'article L. 4111-1 du code de la défense, que l'" esprit de sacrifice, pouvant aller jusqu'au sacrifice suprême " constitue l'une des obligations inhérentes à l'état militaire. Cet état exige en outre, en vertu des mêmes dispositions, que le militaire fasse preuve de " disponibilité " en toute circonstance, et l'article L. 4121-5 de ce code prévoit que " Les militaires peuvent être appelés à servir en tout temps et en tout lieu ". La disponibilité constitue ainsi l'un des devoirs de tout militaire de la gendarmerie. Il y a dès lors lieu, pour

apprécier l'organisation du temps de service des gendarmes, de prendre en compte les particularités de leur état et les sujétions qu'ils ont ainsi acceptées, leurs missions n'étant pas exercées dans des conditions similaires à celles d'autres travailleurs qui ne relèvent pas du statut militaire.

25. C'est au regard de ces principes et de ces missions qu'il convient ainsi, d'abord, de se prononcer sur la qualification des astreintes des militaires de la gendarmerie départementale, avant d'examiner les garanties législatives et réglementaires en matière de repos et, enfin, de vérifier, au regard des réponses aux deux questions précédentes, si l'organisation de la gendarmerie départementale assure le respect des objectifs de l'article 6 de la directive du 4 novembre 2003.

En ce qui concerne les astreintes :

26. Aux termes de l'article 2 de la directive du 4 novembre 2003 : " Aux fins de la présente directive, on entend par : / 1. " temps de travail " : toute période durant laquelle le travailleur est au travail, à la disposition de l'employeur et dans l'exercice de son activité ou de ses fonctions, conformément aux législations et/ou pratiques nationales ; / 2. " période de repos " : toute période qui n'est pas du temps de travail ; (...) ".

27. Par son arrêt du 9 mars 2021, RJ c/ Stadt Offenbach am Main (C-580/19), ainsi qu'aux points 93 à 95 de son arrêt précité du 15 juillet 2021, la Cour de justice de l'Union européenne a jugé que les périodes d'astreinte effectuées sur des lieux de travail qui ne se confondent pas avec le domicile du travailleur devaient normalement être qualifiées, dans leur intégralité, de temps de travail, dès lors que le travailleur doit alors rester éloigné de son environnement social et familial et bénéficie d'une faible latitude pour gérer le temps pendant lequel ses services ne sont pas sollicités. S'agissant des autres périodes d'astreinte, la Cour a jugé qu'elles étaient également susceptibles d'être qualifiées de temps de travail selon qu'elles permettent ou non au travailleur de gérer librement son temps pendant ses périodes d'astreinte et de consacrer ce temps à ses propres intérêts. Elle a dit pour droit, aux points 48 à 53 de son arrêt du 9 mars 2021, qu'une telle qualification devait faire l'objet d'une appréciation au cas par cas, prenant en compte, premièrement, le temps de réaction laissé au travailleur, deuxièmement, les contraintes et facilités accordées au travailleur pendant cette période et, troisièmement, la fréquence moyenne des prestations effectives normalement réalisées par ce travailleur.

28. L'instruction du 8 juin 2016 dispose, en ses points 1.2 et 1.3, que les militaires de la gendarmerie, lorsqu'ils ne sont pas employés pour les besoins du service, peuvent être placés soit dans la position d'activité dite de la " ressource immédiatement employable ", c'est-à-dire sous astreinte immédiate, soit dans celle de la " ressource complémentaire ", c'est-à-dire en astreinte sous délai, laquelle permet de les rappeler dans un créneau de temps qui est en principe de deux heures. L'organisation ainsi instituée a pour objet de garantir le bon accomplissement des missions spécifiques de la gendarmerie, dans le cadre de son organisation militaire, qui lui permet notamment d'assurer sa réactivité en toute circonstance ainsi que le maillage complet du territoire par des unités polyvalentes et de faible effectif.

29. En premier lieu, eu égard au délai maximal, en principe de deux heures, laissé aux militaires placés en astreinte sous délai pour rejoindre leur unité, le temps passé dans cette position ne saurait, en tout état de cause, être regardé comme relevant du temps de travail au sens de la directive du 4 novembre 2003.

30. En second lieu, si les militaires placés sous astreinte immédiate sont susceptibles d'être appelés à tout instant par le commandant de leur unité, ainsi qu'il résulte de l'annexe II de l'instruction du 8 juin 2016, il ne s'ensuit pas, pour autant, que ces périodes doivent nécessairement être prises en compte pour apprécier le respect de l'objectif fixé par l'article 6 de la directive du 4 novembre 2003, lorsque ces militaires ne sont pas effectivement mobilisés.

31. En effet, premièrement, les officiers et sous-officiers de la gendarmerie sont tenus d'occuper un logement en caserne, comme le prévoit l'article L. 4145-2 du code de la défense et ses textes d'application. Cette obligation de logement en caserne est directement liée à l'obligation de disponibilité mentionnée au point 24. En contrepartie, le logement des gendarmes leur est concédé par nécessité absolue de service et de manière gratuite, conformément à l'article R. 2124-67 du code général de la propriété des personnes publiques. Il résulte par ailleurs du point 3.1.1.1 de l'instruction du 13 décembre 2018 que ce logement est situé sur le lieu de travail ou, à défaut, à proximité immédiate.

32. Il ressort des écritures des ministres, non contestées sur ce point, que les officiers et sous-officiers de la gendarmerie, dans le cadre fixé par l'annexe II de l'instruction du 8 juin 2016, effectuent leur période d'astreinte à leur résidence. La circonstance que le logement concédé gratuitement aux gendarmes est situé sur le lieu de

travail ou à son immédiate proximité permet aux militaires concernés d'y disposer librement de leur temps lorsqu'ils ne sont pas mobilisés, ce dans leur environnement social et familial, tout en rejoignant rapidement leur lieu d'emploi en cas de besoin. La facilité qui est ainsi accordée aux gendarmes permet de réduire l'impact objectif des périodes d'astreinte immédiate sur les militaires concernés, alors même que le délai de mobilisation qui leur est imposé serait très bref.

33. Deuxièmement, il résulte du deuxième alinéa du I de l'instruction du 8 juin 2016 que les responsables hiérarchiques engagent en priorité, en cas de nécessité opérationnelle, les militaires de la " ressource employée ", c'est-à-dire des militaires déjà en service, et qu'ils ne recourent aux gendarmes placés sous astreinte immédiate que dans un deuxième temps, lorsque les ressources sont insuffisantes. Cet ordre de priorité est de nature à limiter la fréquence des sollicitations et, par suite, les temps d'activité effectifs des militaires concernés.

34. Il résulte de ce qui précède que, contrairement à ce que soutient M. Q..., eu égard à l'ensemble des contraintes et facilités accordées aux militaires de la gendarmerie placés sous astreinte immédiate, compte tenu de ce que les règles d'emploi fixées par l'instruction du 8 juin 2016 prévoient qu'ils ne soient mobilisés que dans un deuxième temps, en cas de nécessité opérationnelle, et dans le cadre de l'équilibre entre les sujétions et les compensations propres à l'état militaire, ces périodes d'astreinte immédiate ne sauraient être regardées, dès lors qu'elles sont effectuées à domicile, comme constituant en totalité du temps de travail, seules les périodes de mobilisation effective des gendarmes concernés devant recevoir cette qualification. Dès lors, eu égard à ce qui a été dit au point 29, il n'y a pas lieu de prendre en compte les astreintes des militaires de la gendarmerie départementale pour apprécier le respect de l'objectif de l'article 6 de la directive du 4 novembre 2003.

En ce qui concerne les droits à repos prévus par les dispositions applicables à la gendarmerie départementale :

35. En premier lieu, la circulaire du 4 novembre 2013 dispose que chaque militaire a droit à deux jours de repos par semaine, qui couvrent une période de quarante-huit heures consécutives ou deux périodes de vingt-quatre heures chacune. Il résulte du point 1.3 de cette circulaire que le repos hebdomadaire est octroyé au cours de la semaine qui y ouvre droit, sauf nécessité absolue de service.

36. En deuxième lieu, l'instruction du 8 juin 2016 prévoit, en son point 2.1, que les militaires de la gendarmerie départementale bénéficient d'une période de repos physiologique journalier de onze heures consécutives par période d'activité de vingt-quatre heures, soit cinquante-cinq heures par semaine. En son point 2.2, elle prévoit l'octroi d'un repos physiologique compensateur dans le cas où le repos physiologique journalier a été réduit, qui est accordé soit sous la forme d'une période de repos de onze heures, accordée dès la fin du dernier service effectué, soit par report des heures non attribuées dans un délai maximal de quatorze jours. Si elle prévoit en son point 2.3 que les repos physiologiques peuvent ne pas être accordés dans des cas exceptionnels, pour des raisons opérationnelles objectives définies au regard de plusieurs conditions cumulatives, pour des services particuliers ou pour atteindre des objectifs opérationnels de formation, il résulte de ce qui a été dit au point 15 sur les exclusions du champ de la directive du 4 novembre 2003 que ces activités ne relèvent pas de celui-ci en tout état de cause.

37. Il résulte également des dispositions des points 1.2, 1.3 et 2.1 de cette même instruction que les militaires de la gendarmerie départementale sont susceptibles, durant leurs onze heures de repos physiologiques, d'être placés en astreinte immédiate ou sous délai. Toutefois, d'une part, l'instruction du 8 juin 2016 permet d'assurer, lorsque le militaire est effectivement engagé durant une période d'astreinte, que celui-ci bénéficie de son droit au repos, soit sous la forme d'un repos physiologique journalier octroyé après son dernier service, soit par le report, dans un délai rapproché, des heures de repos non consommées. D'autre part, ainsi qu'il a été dit au point 34, il n'y a pas lieu de prendre en compte les astreintes des militaires de la gendarmerie départementale pour apprécier le respect de l'objectif fixé par l'article 6 de la directive du 4 novembre 2003, lorsqu'ils ne sont pas effectivement mobilisés.

38. En troisième lieu, la circulaire du 16 mars 2021 prévoit que les militaires de la gendarmerie départementale disposent de deux " quartiers libres " par semaine, lesquels constituent, selon le point 1.1 de cette circulaire, des périodes durant lesquelles les gendarmes ne sont soumis à aucune obligation de service et bénéficient de leur liberté de mouvement. Un quartier libre peut être accordé pour une période de six, cinq ou quatorze heures selon qu'il est fixé le matin, l'après-midi ou la nuit, en vertu du point 1.2 de cette circulaire. Ainsi que le précise le deuxième alinéa du point 2.1.2 de cette circulaire, chaque militaire bénéficie par principe de deux quartiers libres nocturnes. Il résulte par ailleurs du dernier alinéa de ce même point que, lorsque le minimum de deux quartiers libres nocturnes ne peut être octroyé en raison de circonstances particulières, le commandant d'unité peut alors accorder vingt-quatre heures consécutives de quartiers libres.

39. Chacun des deux quartiers libres nocturnes hebdomadaires étant plus long de trois heures que les droits à repos ouverts au titre du seul titre repos physiologique journalier, les dispositions de la circulaire du 16 mars 2021 garantissent un temps de repos supplémentaire minimal d'au moins six heures par semaine aux militaires de la gendarmerie départementale.

40. Il résulte des textes à caractère réglementaire analysés aux points 35 à 39 qu'un militaire affecté à la gendarmerie départementale bénéficie d'un temps de repos hebdomadaire garanti de cent-neuf heures. Il s'en déduit que la durée pendant laquelle ce militaire ne bénéficie pas d'un tel repos garanti n'excède pas cinquante-neuf heures par semaine.

En ce qui concerne le respect de l'objectif fixé par l'article 6 de la directive du 4 novembre 2003 relatif à la durée maximale du travail :

41. En premier lieu, les sujétions spécifiques que connaissent les militaires de la gendarmerie afin de garantir leur disponibilité font l'objet de compensations. Ils disposent, en particulier, de quarante-cinq jours de permissions par année civile de service, soit neuf semaines, en application de l'article R. 4138-19 du code de la défense. Par ailleurs, des autorisations spéciales d'absence sont accordées aux gendarmes afin de " concilier vie professionnelle et personnelle ", selon les termes de la circulaire du 10 juillet 2019, et ce dans le cadre de l'obligation de tout chef militaire de porter attention aux conditions de vie de ses subordonnés. Si aucun de ces dispositifs ne garantit, par lui-même, la réduction de la durée d'activité sur toute période de six mois, ils sont de nature, dans le cadre de l'équilibre spécifique des sujétions et des compensations qui caractérise l'état militaire, à diminuer le temps d'activité des militaires de la gendarmerie nationale.

42. En second lieu, il ressort des pièces du dossier, et notamment des écritures du requérant qui produit ses propres relevés d'activité, que le temps d'activité fait l'objet d'un décompte individuel dans la gendarmerie départementale. Il ressort également des pièces du dossier, notamment de la réponse faite par les ministres à la mesure d'instruction diligentée par la 7ème chambre de la section du contentieux, que le temps moyen d'activité hebdomadaire dans la gendarmerie départementale est en pratique, hors astreinte, de quarante heures environ, et que, sauf circonstances exceptionnelles, il ne dépasse pas quarante-huit heures.

43. Il résulte ainsi, d'une part, des garanties réglementaires rappelées au point 40, d'autre part, des éléments mentionnés au point 42, dont il doit être tenu compte eu égard aux spécificités propres à l'état militaire, et enfin de la circonstance que les astreintes des gendarmes ne sauraient être prises en compte pour apprécier le respect de l'objectif fixé par l'article 6 de la directive du 4 novembre 2003, que l'organisation de la gendarmerie départementale assure que le temps de travail, au sens de cette directive, des militaires qui y servent est effectivement inférieur à quarante-huit heures par semaine, le respect de cette durée étant vérifié sur une période pouvant aller jusqu'à six mois. Il est rappelé en outre que ni la réglementation nationale ni la directive du 4 novembre 2003 ne font obstacle à ce que cette durée hebdomadaire soit dépassée pour l'exercice des activités de la gendarmerie qui ne relèvent pas, en tout état de cause, du champ de cette directive, ainsi qu'il a été rappelé au point 15, en particulier en cas de circonstances exceptionnelles. Le requérant n'est, dès lors, pas fondé à soutenir que la décision qu'il attaque méconnaît l'obligation de transposition de l'article 6 de la directive du 4 novembre 2003.

44. Il résulte de ce qui précède, sans qu'il soit besoin de se prononcer sur le bien-fondé du moyen en défense tiré des exigences constitutionnelles, que la requête de M. Q... doit être rejetée, y compris ses conclusions à fin d'injonction.

D E C I D E :

Article 1er : La requête de M. Q... est rejetée.
Article 2 : La présente décision sera notifiée à M. G... Q..., à la ministre des armées et au ministre de l'intérieur.
Délibéré à l'issue de la séance du 10 décembre 2021 où siégeaient : M. Bruno Lasserre, vice-président, présidant ; M. Christophe Chantepy, président de la section du contentieux ; Mme Martine de Boisdeffre, M. Didier-Roland Tabuteau, Mme Sylvie Hubac, M. Edmond Honorat, Mme Catherine Bergeal, présidents de section ; M. Rémy Schwartz, Mme Christine Maugüé, présidents adjoints de la section du contentieux ; M. Patrick Gérard, président adjoint de la section de l'administration ; M. Guillaume Goulard, M. Pierre Collin, M. Nicolas Boulouis, Mme Maud Vialettes, M. Bertrand Dacosta, M. Olivier Japiot, présidents de chambre et M. Alexis Goin, auditeur-rapporteur.

Cass. crim. 12 juill. 2022, n°21-83710

M. [C] [L] [E] a formé un pourvoi contre l'arrêt de la chambre de l'instruction de la cour d'appel de Paris, 7e section, en date du 27 mai 2021, qui, dans l'information suivie contre lui, notamment, des chefs de meurtre et tentative, destruction de biens, en bande organisée, et association de malfaiteurs, a prononcé sur sa demande d'annulation de pièces de la procédure.

Par ordonnance en date du 23 septembre 2021, le président de la chambre criminelle a prescrit l'examen immédiat du pourvoi.

Un mémoire a été produit.

Sur le rapport de Mme Ménotti, conseiller, les observations de la SCP Célice, Texidor, Périer, avocat de M. [L] [E], et les conclusions de M. Desportes, premier avocat général, l'avocat du demandeur ayant eu la parole en dernier, après débats en l'audience publique du 19 mai 2022 où étaient présents M. Soulard, président, Mme Ménotti, conseiller rapporteur, M. Bonnal, M. de Larosière de Champfeu, Mme Leprieur, Mme Sudre, M. Maziau, Mme Issenjou, M. Turbeaux, Mme Labrousse, M. Seys, M. Dary, Mme Thomas, M. Laurent, conseillers de la chambre, Mme Barbé, M. Violeau, M. Mallard, Mme Guerrini, M. Michon, conseillers référendaires, M. Desportes, premier avocat général, et M. Maréville, greffier de chambre,

la chambre criminelle de la Cour de cassation, composée des président et conseillers précités, après en avoir délibéré conformément à la loi, a rendu le présent arrêt.

Faits et procédure

1. Il résulte de l'arrêt attaqué et des pièces de la procédure ce qui suit.

2. À la suite d'une fusillade intervenue le 24 août 2019 au cours de laquelle [D] [P] a été tué, diverses investigations ont été effectuées par les enquêteurs sous le régime de la flagrance, puis une information a été ouverte des chefs susvisés, le 6 septembre suivant.

3. Interpellé le 23 juin 2020, M. [C] [L] [E] a été mis en examen le 26 juin et placé en détention provisoire.

4. Le 28 décembre 2020, il a déposé une requête en nullité.

Examen des moyens

Sur le premier moyen

Enoncé du moyen

5. Le moyen critique l'arrêt attaqué en ce qu'il a rejeté la requête en annulation de pièces présentées par M. [L] [E], alors « que par mémoire distinct, il est sollicité le renvoi au Conseil constitutionnel d'une question prioritaire de constitutionnalité portant sur la conformité aux droits et libertés que la Constitution garantit, et en particulier au droit au respect de la vie privée garanti par l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789, de l'article L. 34-1 du code des postes et des communications électroniques ; que l'abrogation de ce texte, en vertu duquel ont été recueillies, conservées et exploitées les données concernant M. [L] [E], entraînera la cassation de l'arrêt. »

Réponse de la Cour

6. Si le Conseil constitutionnel a, dans sa décision n° 2021-976/977 QPC du 25 février 2022, déclaré contraires à la Constitution certaines dispositions de l'article L. 34-1 du code des postes et des communications électroniques en ce qu'elles portent une atteinte disproportionnée au droit au respect de la vie privée, il a précisé que les mesures en cause ne peuvent être contestées sur le fondement de cette inconstitutionnalité.

7. Il s'ensuit que le moyen est devenu sans objet.
Sur les deuxième et troisième moyens

Enoncé des moyens

8. Le deuxième moyen critique l'arrêt attaqué en ce qu'il a rejeté la requête en annulation de pièces présentée par M. [L] [E], alors :

« 1°/ que viole l'article 15 de la directive 2002/58/CE du 12 juillet 2002 modifiée, 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 la juridiction qui retient à l'encontre d'une personne des éléments de preuve obtenus par un recueil et une conservation préventifs, généralisés et indifférenciés des données relatives au trafic et des données de localisation incompatibles avec le droit de l'Union, notamment parce que ce recueil et cette conservation ne sont ni ciblés ni soumis à l'autorisation et au contrôle d'une autorité indépendante ; qu'au cas d'espèce, M. [L] [E] faisait valoir, pour solliciter l'annulation des données de trafic et de localisation requises, obtenues et exploitées à son encontre, que ces données avaient été conservées de façon préventive, généralisée et indifférenciée en violation des textes précités ; qu'en ne répondant pas à ce moyen opérant, la chambre de l'instruction a violé l'article 593 du code de procédure pénale ;

2°/ que viole l'article 15 de la directive 2002/58/CE du 12 juillet 2002 modifiée, 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 la juridiction qui retient à l'encontre d'une personne des éléments de preuve obtenus par un recueil et une conservation préventifs, généralisés et indifférenciés des données relatives au trafic et des données de localisation incompatibles avec le droit de l'Union, notamment parce que ce recueil et cette conservation ne sont ni ciblés ni soumis à l'autorisation et au contrôle d'une autorité indépendante ; qu'au cas d'espèce, M. [L] [E] faisait valoir, pour solliciter l'annulation des données de trafic et de localisation requises, obtenues et exploitées à son encontre, que ces données avaient été conservées de façon préventive, généralisée et indifférenciée en violation des textes précités ; qu'en retenant, pour rejeter cette demande, que l'atteinte ainsi portée à la vie privée de M. [L] [E] était proportionnée à l'objectif poursuivi, la chambre de l'instruction a violé les articles 15 de la directive 2002/58/CE du 12 juillet 2002 modifiée, 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne. »

9. Le troisième moyen critique l'arrêt attaqué en ce qu'il a rejeté la requête en annulation de pièces présentée par M. [L] [E], alors « que viole le droit à la vie privée garanti par l'article 8 de la Convention européenne des droits de l'homme la juridiction qui retient à l'encontre d'une personne des éléments de preuve obtenus par un recueil et une conservation des données relatives au trafic et des données de localisation préventifs, généralisés, indifférenciés et échappant à toute autorisation ou contrôle d'une autorité indépendante ; qu'au cas d'espèce, M. [L] [E] faisait valoir, pour solliciter l'annulation des données de trafic et de localisation requises, obtenues et exploitées à son encontre, qu'en violation du texte précité ces données avaient été conservées de façon préventive, généralisée et indifférenciée, et que leur recueil ne faisait l'objet ni d'une autorisation en amont ni d'un contrôle en aval par une autorité indépendante ; qu'en retenant, pour rejeter cette demande ; qu'il en déduisait que l'atteinte ainsi portée à sa vie privée était disproportionnée à l'objectif poursuivi ; qu'en retenant, pour rejeter la requête, que l'ingérence dans la vie privée de M. [L] [E] résultant du recueil et de l'exploitation de ces données était proportionnée au but légitime de poursuite des infractions pénales, la chambre de l'instruction a violé l'article 8 précité. »

Réponse de la Cour

10. Les moyens sont réunis.

11. Afin de garantir l'effectivité de l'ensemble des dispositions du droit de l'Union européenne, le principe de primauté impose aux juridictions nationales d'interpréter, dans toute la mesure du possible, leur droit interne de manière conforme au droit de l'Union. A défaut de pouvoir procéder à une telle interprétation, le juge national a l'obligation d'assurer le plein effet des dispositions du droit de l'Union en laissant au besoin inappliquée, de sa propre autorité, toute disposition contraire de la législation nationale, même postérieure, sans qu'il [L] à demander ou à attendre l'élimination préalable de celle-ci par voie législative ou par tout autre procédé constitutionnel (CJCE, arrêt du 9 mars 1978, Simmenthal, 106/77).

12. Il convient, dès lors, d'examiner si, à la date des réquisitions litigieuses, la réglementation française sur la conservation et l'accès aux données de connexion était conforme au droit de l'Union.

Sur la régularité de la conservation

Sur les exigences du droit de l'Union en matière de conservation générale et indifférenciée des données de connexion

13. La Cour de justice de l'Union européenne (CJUE) a dit pour droit qu'il résulte de l'article 15, paragraphe 1, de 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, telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009, 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, que le droit de l'Union européenne s'oppose à une conservation généralisée et indifférenciée, à titre préventif, des données de trafic et de localisation aux fins de lutte contre la criminalité, quel que soit son degré de gravité. Seule est admise une conservation généralisée et indifférenciée de ces données, en cas de menace grave, réelle et actuelle ou prévisible pour la sécurité nationale, sur injonction faite aux fournisseurs de services de télécommunications électroniques, pouvant faire l'objet d'un contrôle effectif par une juridiction ou une autorité administrative indépendante, dont la décision est dotée d'un effet contraignant, chargée de vérifier l'existence d'une telle menace et le respect des conditions et garanties devant être prévues, injonction ne pouvant être émise que pour une période limitée au strict nécessaire, mais renouvelable en cas de persistance de la menace.

14. En revanche, le droit de l'Union ne s'oppose pas à des mesures législatives prévoyant, aux fins de lutte contre la criminalité grave :

- une conservation ciblée des données relatives au trafic et des données de localisation qui soit délimitée, sur la base d'éléments objectifs et non discriminatoires, en fonction de catégories de personnes concernées ou au moyen d'un critère géographique, pour une période temporellement limitée au strict nécessaire, mais renouvelable ;
- une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion, pour une période temporellement limitée au strict nécessaire ;
- une conservation généralisée et indifférenciée des données relatives à l'identité civile, aux comptes et aux paiements des utilisateurs de moyens de communications électroniques ;
- le recours à une injonction faite aux fournisseurs de services de communications électroniques, au moyen d'une décision de l'autorité compétente soumise à un contrôle juridictionnel effectif, de procéder, pour une durée déterminée, à la conservation rapide des données relatives au trafic et des données de localisation dont disposent ces fournisseurs de services, dès lors que ces mesures assurent, par des règles claires et précises, que la conservation des données en cause est subordonnée au respect des conditions matérielles et procédurales afférentes et que les personnes concernées disposent de garanties effectives contre les risques d'abus.

15. Cette conservation rapide a pour fondement l'article 16 de la Convention du Conseil de l'Europe sur la cyber-criminalité, signée à Budapest le 23 novembre 2001, les Etats membres pouvant prévoir dans leur législation qu'un accès aux données de trafic et de localisation peut avoir lieu à des fins de lutte contre la criminalité grave, en vue de l'élucidation d'une infraction déterminée, dans le respect des conditions matérielles et procédurales prévues en droit européen (CJUE, arrêt du 6 octobre 2020, La Quadrature du Net e.a., [4] e.a., C-511/18, C-512/18, C-520/18).

16. Selon la CJUE, la conservation rapide et l'accès aux données ainsi conservées peuvent porter sur les données stockées par les fournisseurs de services de communications électroniques sur la base des articles 5, 6 et 9 de la directive 2002/58/CE ou sur celle des mesures législatives prises en vertu de l'article 15, paragraphe 1 (CJUE, arrêt La Quadrature du net, précité, points 160 et 167).

17. Cette position a été maintenue dans l'arrêt Commissioner of An Garda Siochana du 5 avril 2022 (C-140/20, points 85 et 87), la Cour ayant seulement écarté, à nouveau, la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation aux fins de lutte contre la criminalité grave pour répondre à une objection du gouvernement danois (même arrêt, points 96 à 100).

18. La conservation rapide peut donc porter sur les données que détiennent les opérateurs de télécommunications électroniques, soit pour leurs besoins propres, soit au titre d'une obligation de conservation imposée aux fins de sauvegarde de la sécurité nationale.

19. L'interprétation qui exclurait du champ d'application de la conservation rapide les données conservées aux fins de sauvegarde de la sécurité nationale priverait d'effet utile sa finalité, qui est de permettre aux autorités

nationales, en matière de lutte contre la criminalité grave, d'accéder à des données qui n'ont pas été conservées dans ce but.

20. Par ailleurs, une telle mesure peut être étendue aux données relatives au trafic et aux données de localisation afférentes à des personnes autres que celles qui sont soupçonnées d'avoir projeté ou commis une infraction pénale grave, pour autant que ces données puissent, sur la base d'éléments objectifs et non discriminatoires, contribuer à l'élucidation d'une telle infraction, telles les données de la victime et celles de son entourage social ou professionnel (CJUE, arrêt Commissioner of An Garda Siochana, précité, point 88).

Sur la conservation généralisée et indifférenciée des données de connexion en droit français

21. L'article L. 34-1, III, du code des postes et des communications électroniques, dans sa version en vigueur à la date des faits, imposait aux opérateurs de services de télécommunications électroniques la conservation généralisée et indifférenciée, pour une durée maximale d'un an, des données de connexion énumérées à l'article R. 10-13 dudit code, pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales.

22. Ce dernier texte, dans sa version en vigueur à la date des faits, précisait que cette obligation de conservation, d'une durée d'un an, portait sur :
a) les informations permettant d'identifier l'utilisateur ;
b) les données relatives aux équipements terminaux de communication utilisés ;
c) les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ;
d) les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ;
e) les données permettant d'identifier le ou les destinataires de la communication.

23. Il prévoyait également que, pour les activités de téléphonie, l'opérateur devait conserver les données relatives au trafic et, en outre, celles permettant d'identifier l'origine et la localisation de la communication.

Sur la conformité du droit français au droit européen s'agissant de la conservation généralisée et indifférenciée des données de connexion

24. Il résulte des principes rappelés aux paragraphes 13 et 14 qu'il convient d'écarter les textes précités de droit interne en ce qu'ils imposaient aux opérateurs de services de télécommunications électroniques, aux fins de lutte contre la criminalité, la conservation généralisée et indifférenciée des données de connexion, à l'exception des données relatives à l'identité civile et aux informations relatives aux comptes et aux paiements, ainsi que, dans le cadre de la recherche et la répression de la criminalité grave, aux adresses IP.

25. En revanche, l'obligation de conservation des données de trafic et de localisation imposée aux opérateurs par l'article L. 34-1, III, du code précité, mis en oeuvre par l'article R. 10-13 dudit code, en ce qu'elle permet notamment la recherche, la constatation et la poursuite des atteintes aux intérêts fondamentaux de la Nation et des actes de terrorisme, infractions incriminées aux articles 410-1 à 422-7 du code pénal, est conforme au droit de l'Union, comme poursuivant l'objectif de sauvegarde de la sécurité nationale.

26. La durée de conservation de ces données, pour une année, apparaît strictement nécessaire aux besoins de la sauvegarde de la sécurité nationale.

27. Pour autant, les dispositions des articles précités du code des postes et des communications électroniques ne subordonnent pas le maintien de cette obligation de conservation à un réexamen périodique de l'existence d'une menace grave, réelle et actuelle ou prévisible pour la sécurité nationale.

28. Il s'ensuit que cette obligation de conservation ne vaut injonction au sens où l'entend la CJUE et cette conservation n'est régulière que si le juge saisi du contentieux constate, sous le contrôle de la Cour de cassation, l'existence d'une menace présentant les caractéristiques précitées.

29. A cet égard, même en tenant compte de l'exigence du droit de l'Union selon laquelle cette conservation ne saurait présenter un caractère systémique (CJUE, arrêt La Quadrature du Net, précité, point 138), il résulte notamment des pièces régulièrement produites par le procureur général près la Cour de cassation relatives aux attentats commis en France depuis décembre 1994, soit antérieurement à la date des faits, que la France se trouve exposée, en raison du terrorisme et de l'activité de groupes radicaux et extrémistes, à une menace grave et réelle, actuelle ou prévisible à la sécurité nationale.

30. Dès lors, l'obligation faite aux opérateurs de télécommunications électroniques de conserver de façon généralisée et indifférenciée aux fins de sauvegarde de la sécurité nationale les données de connexion énumérées à l'article R. 10-13 du code précité, qui ont fait l'objet des réquisitions litigieuses, était conforme au droit de l'Union.

31. Le Conseil d'Etat n'a d'ailleurs déclaré illégales les dispositions de cet article qu'en ce qu'elles imposaient aux opérateurs de communications électroniques, aux fournisseurs d'accès à internet et aux hébergeurs la conservation généralisée et indifférenciée des données de connexion, autres que les données relatives à l'identité civile, aux adresses IP et aux informations relatives aux comptes et aux paiements, aux fins de lutte contre la criminalité et de prévention des menaces à l'ordre public et ne prévoyaient pas un réexamen périodique de l'existence d'une menace grave, réelle et actuelle ou prévisible pour la sécurité nationale (CE, 21 avril 2021, French Data Network, n° 393099, point 58).

Sur la conservation rapide en droit français

32. Il convient ensuite de rechercher s'il existait, à la date des faits, une réglementation conforme au droit de l'Union permettant la conservation rapide des données de trafic et de localisation. Une telle réglementation doit notamment préciser la ou les finalités pour laquelle ou lesquelles une conservation rapide peut être ordonnée (CJUE, arrêt La Quadrature du Net, précité, point 132).

33. A la date des faits, la communication des données de trafic ou de localisation conservées par les opérateurs de télécommunication pouvait faire l'objet de réquisitions lors d'une enquête de flagrance, en application des articles 60-1 et 60-2 du code de procédure pénale, par un officier de police judiciaire ou par un agent de police judiciaire agissant sous son contrôle, lors d'une enquête préliminaire, sur le fondement des articles 77-1-1 et 77-1-2 dudit code, sur autorisation du procureur de la République, enfin, en cas d'ouverture d'une information, en application des articles 99-3 et 99-4, de ce code, par un officier de police judiciaire autorisé par commission rogatoire du juge d'instruction. La régularité de ces opérations peut être contestée devant la chambre de l'instruction ou la juridiction de jugement, sous le contrôle de la Cour de cassation.

34. Ces dispositions, qui prévoyaient la communication immédiate des données de connexion aux autorités nationales compétentes, doivent être analysées comme valant injonction de conservation rapide, au sens de la Convention de Budapest. En effet, le rapport explicatif de celle-ci précise que l'injonction de conservation rapide peut résulter d'une injonction de produire.

35. En outre, aux termes du sixième alinéa du paragraphe III de l'article préliminaire du code de procédure pénale, les mesures portant atteinte à la vie privée d'une personne ne peuvent être prises, sur décision ou sous contrôle effectif de l'autorité judiciaire, que si elles sont, au regard des circonstances de l'espèce, nécessaires à la manifestation de la vérité et proportionnées à la gravité de l'infraction.

36. Il s'ensuit que les dispositions précitées combinées peuvent être interprétées de façon conforme au droit de l'Union comme permettant, pour la lutte contre la criminalité grave, en vue de l'élucidation d'une infraction déterminée, la conservation rapide des données de connexion stockées, même conservées aux fins de sauvegarde de la sécurité nationale.

37. Il appartient à la juridiction, lorsqu'elle est saisie d'un moyen en ce sens, de vérifier, d'une part, que les éléments de fait justifiant la nécessité d'une telle mesure d'investigation répondent à un critère de criminalité grave, dont l'appréciation relève du droit national, d'autre part, que la conservation rapide des données de trafic et de localisation et l'accès à celles-ci respectent les limites du strict nécessaire.

38. S'agissant de la gravité des faits, il appartient au juge de motiver sa décision au regard de la nature des agissements de la personne poursuivie, de l'importance du dommage qui en résulte, des circonstances de la commission des faits et de la durée de la peine encourue.

Sur l'accès aux données

Sur les exigences européennes en matière d'accès aux données

39. La CJUE a jugé (CJUE, arrêt du 2 mars 2021, H.K./Prokuratuur, C-746/18) que l'accès aux données de connexion ne peut être autorisé que :

- si ces données ont été conservées conformément aux exigences du droit européen ;
- s'il a eu lieu pour la finalité ayant justifié la conservation ou une finalité plus grave, sauf conservation rapide ;
- s'il est limité au strict nécessaire ;
- s'agissant des données de trafic et de localisation, s'il est circonscrit aux procédures visant à la lutte contre la criminalité grave ;
- et s'il est soumis au contrôle préalable d'une juridiction ou d'une entité administrative indépendante.

Sur l'exigence d'un contrôle préalable

40. Il résulte de la jurisprudence de la CJUE que l'article 15, paragraphe 1, de la directive 2002/58/CE, lu à la lumière des articles 7, 8 et 11, ainsi que de l'article 52, paragraphe 1, de la Charte des droits fondamentaux, s'oppose à une réglementation nationale donnant compétence au ministère public, qui dirige la procédure d'enquête et exerce, le cas échéant, l'action publique, pour autoriser l'accès d'une autorité publique aux données relatives au trafic et à la localisation (CJUE, arrêt H.K./Prokuratuur, précité). Elle juge également qu'un fonctionnaire de police ne constitue pas une juridiction et ne présente pas toutes les garanties d'indépendance et d'impartialité requises (CJUE, arrêt Commissioner of An Garda Siochana, précité).

41. En effet, la CJUE rappelle qu'il est essentiel que l'accès des autorités nationales compétentes aux données conservées soit subordonné à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante, susceptible d'assurer un juste équilibre entre, d'une part, les intérêts liés aux besoins de l'enquête dans le cadre de la lutte contre la criminalité grave, et, d'autre part, les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel.

42. Ainsi, les articles 60-1, 60-2, 77-1-1 et 77-1-2 du code de procédure pénale sont contraires au droit de l'Union uniquement en ce qu'ils ne prévoient pas un contrôle préalable par une juridiction ou une entité administrative indépendante.

43. En revanche, le juge d'instruction est habilité à contrôler l'accès aux données de connexion. En effet, d'une part, il n'est pas une partie à la procédure mais une juridiction qui statue notamment sur les demandes d'actes d'investigation formées par les parties, lesquelles disposent d'un recours en cas de refus ; d'autre part, il n'exerce pas l'action publique mais statue de façon impartiale sur le sort de celle-ci, mise en mouvement par le ministère public ou, le cas échéant, la partie civile.

Sur les conséquences de la méconnaissance des exigences du droit de l'Union européenne

44. La CJUE juge qu'il appartient à l'ordre juridique interne de chaque État membre, en vertu du principe d'autonomie procédurale, de régler les modalités procédurales des recours en justice destinés à assurer la sauvegarde des droits que les justiciables tirent du droit de l'Union, à condition toutefois qu'elles ne soient pas moins favorables que celles régissant des situations similaires soumises au droit interne - principe d'équivalence - et qu'elles ne rendent pas impossible en pratique ou excessivement difficile l'exercice des droits conférés par le droit de l'Union - principe d'effectivité - (CJUE, arrêt La Quadrature du Net, précité, point 223).

45. Le principe d'effectivité impose au juge pénal national d'écarter des informations et des éléments de preuve qui ont été obtenus au moyen d'une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation incompatible avec le droit de l'Union ou encore au moyen d'un accès à ces données en violation de ce droit, à l'occasion d'une procédure pénale ouverte à l'encontre de personnes soupçonnées d'actes de criminalité, si celles-ci ne sont pas en mesure de commenter efficacement ces informations et ces éléments de preuve, provenant d'un domaine échappant à la connaissance des juges et qui sont susceptibles d'influencer de manière prépondérante l'appréciation des faits (CJUE, arrêt La Quadrature du Net, précité, points 226 et 227).

46. A cet égard, il résulte des articles 156 et suivants du code de procédure pénale que toute personne mise en examen peut solliciter du juge d'instruction une expertise et, le cas échéant, une contre-expertise, sous le contrôle de la chambre de l'instruction, lorsque se pose une question d'ordre technique. Il en est de même devant la juridiction de jugement.

47. Il s'ensuit que la législation française offre ainsi à toute personne mise en examen ou poursuivie la possibilité de contester efficacement la pertinence des éléments de preuve résultant de l'exploitation des données de connexion.

48. Le principe d'équivalence commande que l'ensemble des règles de procédure nationales s'applique indifféremment aux recours fondés sur la violation du droit de l'Union et aux recours fondés sur la méconnaissance du droit interne ayant un objet et une cause semblables.

49. Hors les cas de nullité d'ordre public, qui touchent à la bonne administration de la justice, la juridiction, saisie d'une requête ou d'une exception de nullité, doit d'abord rechercher si le requérant a intérêt à demander l'annulation de l'acte, puis, s'il a qualité pour la demander et, enfin, si l'irrégularité alléguée lui a causé un grief. Pour déterminer si le requérant a qualité pour agir en nullité, la juridiction doit examiner si la formalité substantielle ou prescrite à peine de nullité, dont la méconnaissance est alléguée, a pour objet de préserver un droit ou un intérêt qui lui est propre (Crim., 7 septembre 2021, pourvoi n° 21-80.642, publié au Bulletin).

50. Les exigences européennes en matière de conservation et d'accès aux données de connexion ont pour objet la protection du droit au respect de la vie privée, du droit à la protection des données à caractère personnel et du droit à la liberté d'expression (CJUE, arrêt La Quadrature du Net, précité), de sorte que leur méconnaissance n'affecte qu'un intérêt privé.

51. Il en est ainsi en particulier de l'exigence d'un contrôle préalable par une juridiction ou une entité administrative indépendante qui vise à garantir, en pratique, le plein respect des conditions d'accès aux données à caractère personnel, telles que précisées au paragraphe 39, et notamment que l'ingérence dans l'exercice des droits précités est limitée à ce qui est strictement nécessaire (CJUE, arrêt H.K./Prokuratuur précité, points 51 et 58 ; CJUE, arrêt Commissioner of An Garda Siochana précité, point 110).

52. Il s'ensuit qu'en application du principe d'équivalence, la personne mise en examen ou poursuivie n'est recevable à invoquer la violation de cette exigence en matière d'accès aux données de connexion que si elle prétend être titulaire ou utilisatrice de l'une des lignes identifiées ou si elle établit qu'il aurait été porté atteinte à sa vie privée, à l'occasion des investigations litigieuses (Crim., 6 février 2018, pourvoi n° 17-84.380, Bull. crim. 2018, n° 30).

53. Enfin, le juge pénal ne peut prononcer la nullité, en application des dispositions de l'article 802 du code de procédure pénale, que si l'irrégularité elle-même a occasionné un préjudice au requérant, lequel ne peut résulter de la seule mise en cause de celui-ci par l'acte critiqué (Crim., 7 septembre 2021, précité).

54. La Cour de cassation juge que l'irrégularité fait nécessairement grief au requérant, lorsque la méconnaissance de la règle a irrévocablement affecté les droits de celui-ci.

55. Tel est le cas lorsque l'acte attentatoire à la vie privée a été accompli par une autorité qui n'était pas compétente, à défaut d'y avoir été autorisée, conformément à la loi. Tel est également le cas lorsque l'acte n'a pas été motivé par l'autorité compétente pour l'ordonner alors qu'il devait l'être (Crim., 8 juillet 2015, pourvoi n° 15-81.731, Bull. crim. 2015, n° 174).

56. A défaut, il appartient au requérant de justifier d'une atteinte à ses intérêts. La Cour de cassation juge qu'il en est ainsi notamment lorsque l'acte attentatoire à la vie privée a été accompli par un agent compétent mais sans le contrôle d'un tiers alors que celui-ci était prévu par la loi (Crim., 7 décembre 2021, pourvoi n° 20-82.733, publié au Bulletin). C'est le cas du procureur de la République ou de l'officier de police judiciaire compétent en vertu du droit national pour accéder aux données de connexion, mais qui agit sans le contrôle préalable d'une juridiction ou d'une entité administrative indépendante.

57. Il se déduit des principes énoncés ci-dessus aux paragraphes 50 et 51 que cette absence de contrôle indépendant préalable ne peut faire grief au requérant que s'il établit l'existence d'une ingérence injustifiée dans sa vie privée et dans ses données à caractère personnel, de sorte que cet accès aurait dû être prohibé.

58. Il appartient, dès lors, à la chambre de l'instruction de s'assurer du respect des quatre premières conditions énoncées au paragraphe 39 et notamment de ce que, d'une part, l'accès a porté sur des données régulièrement conservées, d'autre part, la ou les catégories de données visées, ainsi que la durée pour laquelle l'accès à celles-ci a eu lieu, étaient, au regard des circonstances de l'espèce, limitées à ce qui était strictement justifié par les nécessités de l'enquête.

59. En l'espèce, pour rejeter la demande de nullité résultant des modalités de conservation et d'accès aux données de connexion concernant M. [L] [E], la chambre de l'instruction énonce que les lignes téléphoniques utilisées par

celui-ci ont été exploitées par les enquêteurs, suite à leur identification dans le cadre de l'exploitation du flux des bornes couvrant les lieux intéressant l'enquête, à savoir la scène de crime d'[Localité 2] au moment du meurtre, la scène de l'incendie du véhicule Mercedes des auteurs à [Localité 1] et le secteur du domicile de la victime, [D] [P], à [Localité 3], où était localisé de manière récurrente le véhicule utilisé par les tueurs.

60. Elle précise que l'obtention de ces données et leur exploitation ont permis de localiser l'intéressé à proximité des lieux où se trouvait [D] [P], d'en conclure qu'il surveillait ce dernier et de constater qu'il se trouvait encore aux abords de son domicile peu de temps avant son assassinat, de sorte qu'il a pu donner le signal du départ à un individu pour venir le rejoindre à cet endroit où la victime a été abattue peu de temps après.

61. Elle ajoute que M. [L] [E], mis en examen le 26 juin 2020, a eu accès à la procédure à partir de cette date et était donc, depuis lors, en mesure de commenter efficacement l'ensemble des éléments de la procédure qui caractérisait des indices graves ou concordants rendant vraisemblable son implication comme auteur ou complice des faits.

62. Elle conclut que l'ingérence alléguée dans la vie privée de M. [L] [E] du fait des réquisitions des enquêteurs aux opérateurs téléphoniques est prévue par la loi, qu'elle a eu un but légitime qui est celui de la recherche d'infractions pénales relevant de la criminalité grave, en l'espèce meurtre et tentative de meurtre en bande organisée, destruction par moyen dangereux en bande organisée, association de malfaiiteurs, recel en bande organisée, que cet objectif tendant à la recherche d'infractions pénales est nécessaire dans une société démocratique, et que cette ingérence apparaît proportionnée à la poursuite de l'objectif.

63. En l'état de ces motifs, dont il résulte que l'accès aux informations litigieuses a porté sur des données régulièrement conservées et qu'il a eu lieu en vue de la poursuite d'infractions relevant de la criminalité grave, dans des conditions limitant cet accès à ce qui était strictement justifié par les nécessités de l'enquête, la chambre de l'instruction n'a méconnu aucun des textes visés au moyen.

64. En conséquence, celui-ci doit être écarté.

65. Par ailleurs l'arrêt est régulier en la forme.

PAR CES MOTIFS, la Cour :

REJETTE le pourvoi.