N° 393099 – French Data Network et autres
N°s 394922-397851 – La Quadrature du Net et autres
N° 397844 – Association Igwan.net
N° 424717 – Société Free Mobile
N° 424718 – Société Free

Assemblée

Séance du 16 avril 2021
Lecture du 21 avril 2021

CONCLUSIONS

M. Alexandre LALLET, 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 XIème 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 A. N. est retrouvé près de Chambéry. N. L., déjà mis en examen pour l'enlèvement de la petite M…, avoue le meurtre, 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[1],

[1] Selon les chiffres communiqués par le Gouvernement, 1,8 millions 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

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'Etat 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 quels 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,

---

Internet qui ne sont pas connectés à cette plateforme).

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[2] 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 Etats 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[3], 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[4], afin d'introduire dans le code des postes et des communications électroniques – le CPCE - un article L. 32-3-1, devenu L. 34-1[5], 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 :

---

[2] 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.
[3] CJCE, 18 janvier 2001, *Commission c/ France*, C-151/00. Le défaut de transposition portait notamment sur l'article 7 relatif à l'obligation d'effacement ou d'anonymisation des données de trafic et de localisation.
[4] Loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne.
[5] Article 10 de la loi n° 2004-669 du 9 juillet 2004.

- 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[6] 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[7] 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* »[8]. 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[9]. 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.

---

[6] 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'article L. 34-2 du même code.

[7] 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. Bruno Le Roux, enregistré le 24 octobre 2001, n° 3352.

[8] V. le 2° de l'article L. 39-3 du même code. Le 1. du VI de l'article 6 de la LCEN prévoit quant à lui une peine d'un an d'emprisonnement et de 250 000 euros d'amende en cas de non conservation des éléments d'information visés au II de cet article.

[9] 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., n° 2001-457 DC du 27 décembre 2001, cons. 6 à 9, 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., n° 2015-478 QPC du 24 juillet 2015, cons. 11 à 14, jugeant que les « données de connexion » accessibles aux services de renseignement sont suffisamment définies par l'article L. 34-1).

Ce dispositif s'est ajouté à celui, issu d'une loi de 2000[10], 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[11] à l'Autorité de la concurrence[12], en passant par les douaniers[13], l'Autorité des marchés financiers (AMF)[14], la HADOPI[15], l'Agence nationale de la sécurité des systèmes d'informations (ANSSI)[16] ou l'inspection du travail[17].

Les **services de renseignement** n'ont pas été en reste, à partir de 2006, pour les seuls besoins de la prévention du terrorisme[18], puis plus largement, à partir de la loi de programmation militaire de 2013 et de la loi dite « renseignement » de 2015[19], 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 ;

---

[10] V. l'article 1er de la loi n° 2000-719 du 1er août 2000 qui a introduit un article 43-9 dans la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication.
[11] Art. L. 96 G du livre des procédures fiscales, qui s'est substitué à l'article L. 83 du même livre.
[12] Art. L. 450-3-3 du code de commerce, issu de l'article 212 de la loi n° 2019-486 du 22 mai 2019 (dite loi Pacte).
[13] Art. 65 *quinquies* du code des douanes.
[14] Art. L. 621-10-2 du code monétaire et financier.
[15] Haute autorité pour la diffusion des œuvres et la protection des droits sur internet : art. 14 de la loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet.
[16] Art. 24 de la loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.
[17] 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.
[18] Art. L. 34-1-1 du code des postes et des communications électroniques, issu de l'article 6 de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant diverses dispositions relatives à la sécurité et aux contrôles frontaliers.
[19] Loi n° 2015-912 du 24 juillet 2015 relative au renseignement

- **L'accès <u>en temps réel</u> aux données de connexion conservées ou traitées[20] 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 œuvre 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 œuvre 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'Etat 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°s 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*[21].

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

[20] Il s'agit des informations énumérées au 2° du I de l'article R. 851-5 du code de la sécurité intérieure. 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.
[21] CE, Ass., 19 juillet 2019, n° 424216-424217, au Rec.

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 10ème et 9ème 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 (CE, 10 décembre 2012, *Ministre du budget, des comptes publics et de la fonction publique c/ Sté Rhodia*, n° 317074, aux T.). 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[22].

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 en constitue sa base légale** (CE, 13 juin 2016, *C... et M...*, n° 372721, aux T.)[23]. Nous vous proposons de consacrer dans cette formation solennelle cette **transposition du raisonnement d'opérance de l'exception d'illégalité[24] 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[25].

---

[22] Vous avez notamment entrepris de cantonner la portée des décisions avant dire droit dans votre décision d'Assemblée du 27 mars 2015, *CNCCFP*, n° 382083, au Rec.

[23] V. aussi CE, 20 octobre 2016, *CIMADE et autres*, n° 395105 ; CE, 28 novembre 2016, *CIMADE et autres*, n° 394114

[24] CE, Section, 11 juillet 2011, *Société d'équipement du département de Maine-et-Loire (Sodemel) et a.*, n° 320735-320854, au Rec.

[25] 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

A 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[26]. Ce faisant, il se borne à mettre en œuvre l'article L. 811-2 de ce code qui définit les missions générales de ces entités et renvoie à un décret en Conseil d'Etat 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 de 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'Etat 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

---

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 (cf. CE, Section, 10 novembre 2010, *Commune de Palavas-les-Flots et communes de Lattes*, n° 31449-314580, au Rec. ; CE, Ass., 31 mai 2016, *G…-G…*, n° 396848, au Rec.) 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 œuvre d'une loi inconventionnelle sous tel ou tel aspect (V. par exemple : CE, 7 juin 2006, *Association Aides et autres*, n° 285576, au Rec. : annulation d'un décret en tant qu'il met en œuvre des dispositions législatives pour une catégorie de personnes. V. aussi CE, 6 avril 2007, *Comité Harkis et Vérité*, n° 282390, aux T. ; CE, 16 juin 2008, *La Cimade*, n° 300636-300637, au Rec.) 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 œuvre afin de garantir le respect des engagements de la France au stade de son application pratique.

[26] A l'exclusion de la direction du renseignement militaire et de Tracfin.

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 en 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 œuvre 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[27].

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[28].

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

[27] 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.

[28] 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.

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 œuvre des traitements algorithmiques[29], de même que des dispositions qui précisent les modalités opérationnelles de mise en œuvre 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 œuvre l'ensemble des techniques de renseignement[30], des compensations financières dues aux opérateurs[31], des modalités de saisine du Conseil d'Etat par la CNCTR[32] ou de la cryptologie[33].

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[34].

En résumé, le litige dont vous êtes saisi 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[35], 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. Evidemment, toutes sont directement intéressées, en pratique, par le sort que vous réserverez au vivier de données dans lequel elles peuvent aujourd'hui puiser.

---

[29] 2° du I de l'article R. 851-5 CSI.
[30] 2nd alinéa de l'article L. 821-1 du CSI.
[31] Art. L. 871-7 du CSI.
[32] Art. L. 833-8 du CSI.
[33] Articles L. 871-1 et suivants du CSI.
[34] La primauté du droit de l'Union ne met pas en échec l'autorité de la chose jugée, en principe (V. notamment : CJUE, 3 septembre 2009, *Amministrazione dell'Economia e delle Finanze*, C-2/08).
[35] V. respectivement, pour l'enquête de flagrance, l'enquête préliminaire et l'instruction, les articles 60-2 (1er alinéa), 77-1-2 et 99-4 de ce code.

*

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.

A l'origine, l'Etat 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[36], ont été très largement reprises par la directive dite *e-privacy* du 12 juillet 2002[37]. 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'Etat et les activités de l'Etat dans des domaines relevant du droit pénal. Par ailleurs, le paragraphe 1 de son article 15, éclairé par son considérant 11, permet aux Etats 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[38] 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.

---

[36] V. les arrêts C-151/00, C-211/02 et C-350/02.

[37] 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).

[38] CEDH, 4 décembre 2008, *M... c/ Royaume-Uni*, n° 30562/04 et 30566/04, § 67.

La seule ombre au tableau gouvernemental résultait d'un arrêt *Digital Rights Ireland* du 8 avril 2014[39]. 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 Etats 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[40] et de vos 10ème et 9ème chambre réunies, dans leur décision inédite du 12 février 2016, *Association French Data Network et autres* (n° 388134), 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[41] ; *La Quadrature du Net et autres* du 6 octobre 2020[42], 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*[43], du même jour, au Royaume-Uni ; et, enfin, *H.K c/ Prokuratuur*, en Estonie, rendu le 2 mars dernier[44]. 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 Etats membres peuvent prendre à des fins de sécurités nationale et

---

[39] CJUE, 8 avril 2014, *Digital Rights Ireland Ltd contre Minister for Communications, Marine and Natural Resources e.a. et Kärntner Landesregierung e.a., C*-293/12 et C-594/12
[40] V. notamment la chronique de jurisprudence de la CJUE à l'AJDA 2021, p. 387.
[41] C-207/16.
[42] C-511/18, C-512/18 et C-520/18.
[43] C-623/17.
[44] C-746/18.

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[45]. 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[46] : l'Etat 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[47]. On peut penser que cette exclusion couvrirait les activités d'opérateurs d'Etat 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[48]. Ces derniers relèvent en revanche du RGPD. Et elle

[45] Sont en outre exclues, comme vous avez pris sur vous de le juger en 2018, à juste titre, les opérations réalisées par l'Etat qui n'impliquent aucun traitement de la part des opérateurs et qui ne présentent donc pas la moindre adhérence avec la directive *e-privacy*.

[46] L'Etat est en réalité un « destinataire » des données, selon la terminologie consacrée.

[47] 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) par la différence de rédaction de la directive e-privacy, qui n'exclut que les « activités » de l'Etat, 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.

[48] Au point 205 de son arrêt du 6 octobre 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 points 35 et 38 de son arrêt Google du 13 juin 2019 (C-193/18). 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'article 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

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[49]. 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

---

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'article L. 33-1 du CPCE (V. son avis n° 2010-0764 du 6 juillet 2010). Il faut probablement comprendre le « dès lors » figurant au point 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, *Skype Communications SARL*, C-142/18). Sous cette réserve, nous pensons que le premier et le troisième alinéa du II de l'article 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 défini par le IV de l'article 1er de la LCEN (auquel renvoie le 23° de l'article 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'article 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. Didier Mathus, n° 2238, 8 mars 2000). L'état du droit doit toutefois évoluer. L'article 2 de la directive 2018/1972 du Parlement européen et du Conseil du 11 décembre 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 décembre 2020 les services de « *communications interpersonnelles* » dans les services de communications électroniques. La France tarde à la transposer.

[49] En raison de l'effet potentiellement dissuasif des mesures étatiques sur l'utilisation des moyens de communication.

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'Etat, 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* »[50].

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 10ème 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[51]. 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 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 euros d'amende.

Pas plus que ses avocats généraux[52], 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,

---

[50] Pt 119.

[51] 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…

[52] 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. W… 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*

depuis 20 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 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 ses 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 euros d'amende[53].

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**, « quoiqu'il en coûte », en quelque sorte[54] ;

- **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.

---

informatiques ». A 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.

[53] Art. 226-18 du code pénal.

[54] Cette logique irrigue largement le droit positif depuis quelques années maintenant comme en atteste, par exemple, 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, qu'elles ont pris toutes les mesures de conformité permettant d'éviter qu'une infraction soit commise en leur sein.

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.

A 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'Etat, il est celui d'être protégé contre l'Etat 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[55]. 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[56].

Ce cadre de raisonnement général la conduit à rédiger un chapitre alternatif des codes de procédure pénale et de sécurité intérieure des Etats 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[57], 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.

---

[55] Pt 122
[56] Pt 111
[57] V. sur ce point l'arrêt *Ministerio fiscal*.

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[58]. 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 :

[58] Il ressort des éléments fournis par le Gouvernement que, conformément à la doctrine de la CNCTR (délibération n° 1/2016 du 14 janvier 2016) qui analyse les URL comme des données mixtes (de connexion et de contenu), seul le protocole (http par exemple) et le nom de domaine (youtube.com) peut être connu, et non le chemin d'accès (par exemple, celui de la vidéo visionnée sur *Youtube*). Un projet de loi est en cours d'élaboration pour permettre de mettre en œuvre des traitements algorithmiques sur les URL complètes.

- 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[59], ratifiée ou approuvée par la quasi-totalité des Etats membres, dont la France[60]. 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* »[61].

---

[59] 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).

[60] 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.

[61] La convention de Budapest fait obligation aux Etats 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'article 14 de la

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[62] ;

- 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.

A 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 Etats 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 Etats 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[63]. Mais elle assortit cette faculté de trois conditions :

---

convention que la conservation rapide peut permettre la collecte des preuves électroniques de toute infraction pénale (et non pas seulement les infractions commises au moyen d'un système informatique ou relevant de la cybercriminalité au sens des articles 2 à 11 de la convention).

[62] V. l'article 21.

[63] Naturellement, en-dehors des périodes couvertes par cette injonction spécifique, la sauvegarde de la sécurité

- 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* » [64] ;

- 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[65] ;

- 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 »[66]. 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'Etat d'accéder

---

nationale peut tout à fait justifier, *a fortiori*, la conservation ciblée ou rapide des données dans les conditions que nous avons décrites précédemment.

[64] Pt. 138

[65] 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 article 15, paragraphe 1 (voir, en ce sens, arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 167)* ».

[66] V. aussi l'arrêt *H.K c/ Prokuratuur*, pt. 31.

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 »[67] ;

- 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[68]. 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[69] ;

- 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[70].

*

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 *Télé2*[71]. Il est peu dire que la Cour a suscité la sidération et la consternation parmi les

[67] Arrêt *H.K c/ Prokuratuur*.
[68] 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.
[69] 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.
[70] Pt. 121 de l'arrêt *Télé2* et pt. 190 de l'arrêt *LQDN et autres* pour ce qui concerne l'accès en temps réel.

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.

5.1. A 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[72]. La première à l'avoir effectivement utilisé est la Cour constitutionnelle tchèque dans son arrêt *H*... de 2012[73]. Elle a été suivie dans ses travaux pratiques par les Danois en 2016[74] 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 portant sur le programme PSPP 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

---

[71] Rapport d'information de la mission d'information commune sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement, n° 3069, enregistré le 10 juin 2020, présenté par M. Guillaume Larrivé, président, et MM. Kervran et Mis, rapporteurs.

[72] 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, p. 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* ».

[73] Cour constit. tchèque, 31 janvier 2012, Régime de pensions slovaque, Pl. ÚS 5/12, commenté par A. Levade dans la revue Constitutions, 2012, p. 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.

[74] Højesteret, 6 décembre 2016, aff. 15/2014, *Dansk Industri (DI), agissant pour Ajos / Succession R*...

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 Etats 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 Etats 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 Etats 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[75]. 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* »[76].

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[77], 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[78], 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 érigé en organe de contrôle de son activité, pour lui reprocher

[75] Arrêt *Honeywell* du 6 juillet 2010, 2 BvR 2661/06 ; et arrêt *OMT* du 21 juin 2016, 2 BvR 2728/13.
[76] Pt. 118.
[77] *L'autorité du droit de l'Union européenne : le point de vue des juridictions constitutionnelles et suprêmes*, discours prononcé le 19 octobre 2017 au Congrès du 25ème anniversaire de l'Académie de droit européen (ERA) à Trèves.
[78] CJUE, 4 octobre 2018, *Commission c/ France*, C-416/17.

d'avoir mal fait son travail. Nous ne vous inviterons pas à emprunter cette voie[79], ce que le Conseil constitutionnel n'a, pour sa part, jamais fait[80].

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 œuvre 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[81] définit la participation de la République à l'Union européenne comme un choix libre d'exercer certaines de ses compétences avec les autres Etats 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 posée 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

---

[79] 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, p.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, p. 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.

[80] 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'article 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* ».

[81] Nous ne croyons pas possible, en revanche, de mobiliser le principe de subsidiarité, auquel l'article 88-6 confère une valeur constitutionnelle, et qui renvoie au principe énoncé à l'article 5 du Traité sur l'Union européenne, qui 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'article 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, avril 2019).

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[82]. 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[83], que pour le Conseil constitutionnel, en interprétant l'article 62 de la Constitution[84], 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[85]. 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*[86]. C'est encore vous qui, abandonnant votre jurisprudence *ONIC*[87], 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 (CE, Ass., 11 décembre 2006, *Société De Groot En Slot Allium BV et a.*, n° 234560, au Rec.). 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

[82] Cette force obligatoire n'est formellement affirmée qu'à l'article 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 novembre 2012, *G… et al. c/ S…*, C-456/11, pt. 40 ; CJCE, 1er juin 2006, *P & O European Ferries SA et a.*, C-442/03 P et C-471/03 P, pt 44).

[83] Rappelons au passage que vous avez constamment reconnu cette autorité de la chose jugée aux jugements judiciaires statuant incompétemment (CE, 19 décembre 1924, *Compagnie des phosphates de Constantine*, Rec. ; CE, Ass., 16 mars 1945, *D…*, Rec. p. 93).

[84] 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, Section, 22 juin 2007, *L…*, n° 288206, au Rec.).

[85] CE, Assemblée, 30 juillet 2014, *V…*, n° 358564, au Rec.

[86] CE, 1er octobre 2015, *Société Melitta France et autres*, n° 373018-373022-373023, aux T.

[87] CE, Section, 26 juillet 1985, *Office national interprofessionnel des céréales*, n° 42204, au Rec.

Cour, dans la logique de sa propre jurisprudence[88]. 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* »[89].

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[90].

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[91].

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

---

[88] CJCE, 13 décembre 1990, *B…*, C-42/90, pt. 6 ; CJCE, 24 octobre 2002, *H…*, C-121/00, pt. 21. V. sur la question : F. Dieu, *Le Conseil d'Etat face à l'autorité des interprétations données par la CJCE dans le cadre d'un renvoi préjudiciel : une position délicate*, RTD Eur. 2007, p. 473.

[89] AJDA 2007, p. 136.

[90] Etant 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.

[91] En l'occurrence, par exemple, 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 paragraphe 2 de l'article 4 du traité sur l'Union européenne lui fait obligation de respecter « *l'identité nationale* » des Etats 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 octobre 2004, *Omega Spielhallen*, C-36/02, dans lequel elle autorise les Etats 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 décembre 2010, *S…-W…*, C-208/09, pt. 92-94.

respect nécessaire de ce droit, notamment des libertés de circulation et d'établissement[92]. 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.

5.2. 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[93]. 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[94]**. 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[95], 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

[92] CJCE, 11 novembre 1981, *C...*, C-203/80 ; CJCE, 4 juin 1992, *D...*, C-13/91 et C-113/91 ; CJUE, 4 juin 2013, *ZZ*, C-300/11, pt. 38 ; CJUE, 20 mars 2018, *Commission/Autriche*, C-187/16, pts. 75 et 76 ; CJUE, 2 avril 2020, *Commission/Pologne, Hongrie et République tchèque*, C-715/17, C-718/17 et C-719/17, EU:C:2020:257, points 143 et 170

[93] V. en dernier lieu : CE, Ass., 19 juillet 2019, *Association des américains accidentels*, n° 424216-424217, au Rec.

[94] Cons. const., n° 2018-765 DC du 12 juin 2018, cons. 2 et 3 ; n° 2019-810 QPC du 25 octobre 2019, cons. 7

[95] TC, 17 octobre 2011, n° 3828-3829, au Rec.

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[96], toute disposition contraire (CE, Section, 23 mars 2012, *Fédération SUD Santé Sociaux*, n° 331805, au Rec.)[97], et même tout engagement international contraire, à tout le moins à un règlement européen (CE, Ass., 19 juillet 2019, *Association des Américains accidentels*, n° 424216-424217, au Rec.)[98].

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[99], avec de rares tempéraments[100], avec pour conséquence l'injonction expressément faite au juge national de laisser inappliquée une disposition constitutionnelle contraire au droit

---

[96] Cette expression est curieuse car le moyen tiré de la contrariété au droit de l'Union n'est pas d'ordre public (CE, 11 janvier 1991, *SA Morgane*, n° 90995, au Rec. ; CE, 28 juillet 1993, *B… et autres*, n° 118717, au Rec.).

[97] 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, Section, 3 décembre 1999, *Association ornithologique et mammalogique de Saône-et-Loire et Rassemblement des opposants à la chasse*, n° 164789;165122, au Rec.).

[98] 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'article 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 Julien Boucher dans ses conclusions sur la décision *K…* : 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.

[99] 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 décembre 1970, *Internationale Handelsgesellschaft*, aff. 11/70, ; CJCE, 5 mars 1996, *Commission c/ Luxembourg*, aff. C-473/93). « *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 septembre 2010, *Winner Wetten GmbH*, aff. C-409/06).

[100] 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 novembre 1995, *Atlanta*, n° C-465/93), 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, *K…*, n° C-234/04, réaffirmée par CJUE, 3 septembre 2009, *Amministrazione dell'Economia e delle Finanze*, C-2/08 ; cette solution a seulement été écartée en matière de compatibilité des aides d'Etat au traité : CJUE, 18 juillet 2007, Lucchini, C-119/05), 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, 5 décembre 2017, *MAS, MB*, C-105/14, 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, p. 563). D'une certaine manière, l'absence d'engagement de la responsabilité de l'Etat 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 septembre 2003, *K…*, C-224/01 ; CE, 18 juin 2008, *G…*, n° 295831, au Rec.).

de l'Union[101]. 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[102], n'est plus vrai dans l'ordre interne, où, comme l'ont rappelé vos décisions *S... et L...* et *SNIP*[103], **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[104].

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[105], c'est cette dernière qui doit être regardée comme la disposition réellement en débat[106]. C'est **l'original qui se cache derrière la copie**. Un peu comme s'il

---

[101] V. pour une telle injonction : CJCE, 22 mai 2003, *Connect Austria*, aff. C-462/99.

[102] Sous réserve des modestes tempéraments que la cour elle-même y apportés (V. *infra*).

[103] CE, Assemblée, 30 octobre 1998, *S... et L... et autres*, n° 200286-200287, au Rec. ; CE, 3 décembre 2001, *Syndicat national de l'industrie pharmaceutique et autres*, n° 226514, au Rec. La Cour de cassation a repris la logique de l'arrêt *S... et L...*, tout en semblant réserver le cas de l'Union européenne (Cass. Ass. Plén, 2 juin 2000, *F...*, Bull Ass. Plén, n° 4, p. 7).

[104] Const. Const., n° 2012-653 DC du 9 août 2012.

[105] Ce qui ne peut être le cas que si cette norme est inconditionnelle.

[106] 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 octobre 2017, *Syndicat éducation populaire – UNSA*, n° 403855, aux T. dans la ligne de CE, Assemblée, 19 mai 1983, *Club sportif et familial de la Fève et autre*, n°s 23127-23181-23182, au Rec.), de la confrontation entre deux engagements internationaux, qui se résout conformément au mode d'emploi issu de votre décision d'Assemblée *K...* du 23 décembre 2011 (n° 303678, au Rec.), 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. A 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

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[107]. 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**[108] - autrement dit lorsqu'une norme constitutionnelle[109] n'a

---

rappelée par Julien Boucher dans ses conclusions sur l'affaire *K…* (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*). Echappe 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.

[107] La jurisprudence rendue à propos de l'article 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.

[108] Initialement, la clause de sauvegarde était limitée aux « *dispositions expresses contraires de la Constitution* » (décision n° 2004-496 DC du 10 juin 2004, cons. 7). Mais il ressort du commentaire autorisé de cette décision que cette notion renvoyait à une norme constitutionnelle écrite propre à la Constitution française (JE Schoettl, *Le nouveau régime juridique de la communication en ligne devant le Conseil constitutionnel*, Les Petites Affiches, 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.

pas d'homologue européenne, le Conseil constitutionnel s'assure de son respect par la loi donc, en réalité, par la directive[110]. 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[111].

Concrètement, cela signifie que **le Conseil constitutionnel s'autorise à laisser inappliqué le droit de l'Union, dans des cas résiduels[112] et qu'il n'a d'ailleurs jamais illustrés[113]**. 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 »[114]. Cette soupape, disons-le, n'est pas l'instrument d'un repli

---

[109] 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.

[110] Cons. const. n° 2006-540 DC du 27 juillet 2006, cons. 17 à 20 ; n° 2010-79 QPC du 17 décembre 2010. 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., n° 2004-496 DC, 10 juin 2004). De même, le Conseil constitutionnel, saisi au titre de l'article 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).

[111] C'est ce qui explique d'ailleurs que le Conseil constitutionnel n'ait pas estimé nécessaire une révision de la Constitution préalablement à la ratification de feu le traité établissant une Constitution pour l'Europe.

[112] Le commentaire aux cahiers de la décision du 19 novembre 2004 indique que la « *porte constitutionnelle* » a été ouverte aux « *neuf dixièmes* » à la réception immédiate du droit communautaire dans l'ordre juridique interne.

[113] L'Assemblée générale du Conseil d'Etat 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 »).

[114] 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 énumérés au troisième alinéa de l'article 79 de la même Loi fondamentale et auxquels 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'Etat social et démocratique de droit établi par la Constitution nationale (déclaration n° 1/2004 du 13 décembre 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 constitutionnelle, 18 décembre 1973, n° 183 ; 22 octobre 2014, n° 238, concernant l'affaire

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'Etat 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[115].

Vous vous êtes directement inspiré de cette jurisprudence constitutionnelle pour bâtir, il y a près de quinze ans maintenant, la « clause de sauvegarde *Arcelor* »[116].

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. A 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[117]. 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[118]. **Vous**

Taricco qui a finalement conduit la Cour de justice à adapter sa jurisprudence : CJUE, 8 septembre 2015, aff. C-105/14). Le Conseil d'Etat grec a quant à lui affirmer la supériorité de la Constitution sur le droit de l'Union (CE n° 3242/2004 du 16 novembre 2004). A 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'Etat au transport* [2014] UKSC 3).

[115] V. pour cette présentation l'intéressant article de Jean-Paul Jacqué, *La Cour de justice de l'Union européenne et la théorie des contre limites*, http://www.droit-union-europeenne.be/432984946.

[116] CE, Assemblée, 8 février 2007, *Société Arcelor Atlantique et Lorraine et autres*, n° 287110, au Rec. 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'Etat 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 septembre 2015, *Société Notrefamille.com*, n° 389806, aux T.).

[117] Vous avez par la suite réitéré ce mode d'emploi, en abandonnant au passage, très logiquement, la référence à l'article 55 de la Constitution : CE, 7 février 2020, *Confédération paysanne et autres*, n° 388649, au Rec.

[118] V. *a contrario* : CE, 8 juillet 2020, *Association de défense des ressources marines et Fédération nationale de*

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[119] **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[120]. Au-delà de « l'identité nominale », vous vous assurez d'une « équivalence réelle »[121] : 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 »[122].

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

---

la plaisance et des pêches en mer, n° 428271-428276-429018-429469, aux T. Cette décision juge aussi logiquement que, lorsque le décret intervient dans le cadre de la marge d'appréciation de l'Etat, et non pour la transposition de stipulations ou dispositions inconditionnelles, le contrôle de constitutionnalité du décret s'effectue normalement.

[119] Vous n'êtes pas allé, en revanche, jusqu'à consacrer la méthodologie de l'avis de l'Assemblée générale du Conseil d'Etat du 26 septembre 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.

[120] V. à propos du respect de la vie privée : n° 2004-499 DC du 29 juillet 2004, cons. 7 et 8 ; pour le principe d'égalité et la liberté d'entreprendre (n° 2018-768 DC du 26 juillet 2018, cons. 12 et 38 à 40).

[121] 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.

[122] 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 Etats membres une certaine marge de manœuvre dans sa mise en œuvre, elle considère qu'un Etat membre ne peut appliquer des standards nationaux de protection des droits fondamentaux dans la mise en œuvre 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 février 2013, *A…-F…*, C-617/10, pt 29 et *M…*, C-399/11, pts 55 et s. ; V. aussi CJUE, 24 septembre 2019, *Google*, C-507/17, pt. 72).

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'il n'aurait pu faire, dans ce second cas, que par la voie d'une QPC[123]. 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'Etat 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[124], ce qui poserait un problème de loi-écran, mais bien celle de la directive e-privacy et du RGPD. Vous êtes donc convié à opérer le même contrôle de constitutionnalité adapté que dans l'affaire *Arcelor*.

Vous pourriez être gêné, 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. A

[123] L'écran législatif joue aussi lorsque le décret se borne à tirer les conséquences nécessaires de la loi (CE, 6 décembre 2012, *Société Air Algérie*, n° 347870-347871, au Rec.). 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'Etat 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.

[124] On imagine d'ailleurs assez mal l'Etat 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.

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 (CE, Ass., 9 juillet 2010, *Fédération nationale de la libre pensée*, n° 327663 et autres, au Rec.[125]). 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[126].

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[127] ;

---

[125] V. aussi CE, Ass., 23 décembre 2011, *K...*, n° 303678, au Rec. 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, p. 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. A notre avis, le seul argument recevable est celui qui tire de la Constitution, notamment de son article 54, la volonté du constituant de ne pas investir le juge administratif de la mission de contrôler la conformité des traités à la Constitution.

[126] Dans son article de référence sur le Conseil d'Etat et l'interprétation de la loi (RFDA 2002, p. 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.

[127] On se gardera toutefois de donner trop de portée à cet argument : en allant jusqu'au bout de cette logique, il

- 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[128], 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[129]. A 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 15 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

---

faudrait aussi considérer que l'obligation de respecter les traités, qui découle du principe *Pacta sunt servanda* issu du 14ème alinéa du Préambule de 1946, et la supériorité de leur autorité sur celle des lois, conférée par l'article 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*…

[128] L'article 15 de la directive e-privacy se borne à ouvrir une faculté de dérogation aux Etats-membres.

[129] 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'article 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'article 88-1 n'est pas au nombre des droits et libertés que la Constitution garantit (Cons. const., n° 2010-79 QPC du 17 décembre 2010). 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.

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[130].

La configuration de l'espèce appelle en conséquence la mise en œuvre 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 œuvre 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.

---

[130] En tout état de cause, nous pensons 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 conformes 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.

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[131]. 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[132]. 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[133].

---

[131] BVerfG, 7 juin 2000, *Solange III*, 2 BvL 1/97, RTDE, 2001, p. 155.

[132] 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.

[133] Nous pensons que vous disposez d'une certaine marge d'interprétation des arrêts préjudiciels. L'article 104 du règlement de procédure de la Cour de justice exclut, dans sa relation avec les juridictions de renvoi, l'application de l'article 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 paragraphe 2 de l'article 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.

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[134]. C'est tout le sens de la vénérable jurisprudence *SA Morgane* en matière d'inconventionnalité de la loi : alors même qu'est en cause l'applicabilité au litige de la loi, 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[135]. 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* ». A 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[136]. 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* »[137]. Nous ne voyons pas bien en quoi

---

[134] V. aussi, à propos de la subdélégation illégale du pouvoir réglementaire : CE, 17 novembre 2010, *Société Arthus Consulting*, n° 320827, aux T.

[135] Il l'est par exception, s'agissant de l'incompétence du pouvoir réglementaire intervenant dans le domaine de la loi.

[136] 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.

[137] 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*

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 Etats membres en tant que parties aux traités.

*

5.3. 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[138], 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[139], et l'objectif de recherche des auteurs d'infractions[140], notamment pénales.

5.3.1. 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[141], 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[142]. Les exemples sont multiples, tant dans la jurisprudence du Conseil

---

conformément à l'article 14 du traité ».

[138] Cons. const., n° 2011-192 QPC du 10 novembre 2011, cons. 20 ; n° 2016-738 DC du 10 novembre 2016, cons. 20 à 23.

[139] Cons. const., n° 2020-805 DC du 7 août 2020.

[140] Cons. const., n° 2004-492 DC Du 2 mars 2004.

[141] V. parmi d'innombrables exemples : Cons. const., n° 2011-631 DC, 9 juin 2011, cons. 78 ; n° 2014-420/421 QPC, cons. 9.

[142] Comme l'indique P. de Montalivet dans son article consacré aux objectifs de valeur constitutionnelle publié

constitutionnel[143] que dans la vôtre, à propos par exemple de l'objectif d'intelligibilité de la norme[144]. Même si les objectifs liés à la sécurité n'en offrent pas d'illustration explicite, à notre connaissance[145], la même logique doit prévaloir. Le Conseil constitutionnel a du reste qualifié la sauvegarde de l'ordre public d' « *exigence constitutionnelle* »[146] et jugé qu'elle « *implique notamment que soit assurée la protection des personnes* »[147]. 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[148]. 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 (V. précisément à propos de l'accès administratif aux données de connexion par les services de renseignement : n° 2015-713 DC du 23 juillet 2015, cons. 51 à 53, 55 et 56)[149]. 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[150]. Il y a bien

---

aux Cahiers du Conseil constitutionnel n° 20 de juin 2006, « l*e 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 ».*

[143] Il en va ainsi, par exemple, de l'objectif de pluralisme des quotidiens d'information politique et générale (n° 86-210 DC du 29 juillet 1986) ou de l'objectif d'accessibilité et d'intelligibilité de la loi (n° 2005-530 DC du 29 décembre 2005).

[144] V. par exemple : CE, Ass., 24 mars 2006, *Société KPMG et Société Ernst & Young Audit et autres*, n° 288460-288465-288474-288485, au Rec.). 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.

[145] 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 février 2005, *Association pour la transparence et la moralité des marchés publics*, n° 264712, 265248, 265281 et 265343, au Rec.).

[146] V. par exemple la décision du Conseil constitutionnel n°2011-631 DC du 9 juin 2011, cons. 64.

[147] Cons. const., n° 91-294 DC du 25 juillet 1991, cons. 17

[148] Cons. const. 22 janvier 1990, n° 89-269 DC. Dans sa décision n° 86-217 DC du 18 septembre 1986 (cons. 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.

[149] A propos de la saisie de données informatiques : Cons. const., n° 2016-600 QPC, 2 décembre 2016, cons. 7 à 13 ; ou encore : n° 2010-605 DC, 12 mai 2010, cons. 25 ; n° 2010-55 QPC, 18 octobre 2010, cons. 6 ; n° 2003-467 du 13 mars 2003, cons. 27.

[150] CE, Assemblée, 27 octobre 1995, *Commune de Morsang-sur-Orge*, n° 136727, au Rec.

longtemps[151] que vous contrôlez, sans texte exprès, la légalité des refus d'édicter des mesures de police nécessaires à la préservation de l'ordre public[152] 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[153].

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* »[154]. Il a même pu juger que, sans l'ordre public, « *l'exercice des libertés ne saurait être assuré* »[155]. Car à travers eux, c'est tout le corpus des droits fondamentaux qui est en jeu[156]. 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[157], moyens non seulement financiers – comme le prévoit explicitement l'article 13 de la Déclaration - mais aussi juridiques et opérationnels.

---

[151] 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, n° 2, p. 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'article 99 du 5 avril 1884.

[152] CE, 8 juillet 1992, *Ville de Chevreuse*, n° 80775, au Rec.

[153] CE, 28 novembre 2003, *Commune de Moissy-Cramayel*, n° 238349, au Rec.

[154] Cons. const., n° 2016-738 DC du 10 novembre 2016. On trouve aussi dans de nombreuses décisions une référence à la « protection » de principes et de droits de valeur constitutionnelle (V. par ex. : n° 2012-652 DC du 22 mars 2012).

[155] Cons. const., 25 janvier 1985, n° 85-187 DC.

[156] 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 ».*

[157] 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., n°2011-625 DC du 15 mars 2011, cons. 18 ; n° 2017-637 QPC du 16 juin 2017, cons. 4 et 5).

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[158], 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[159], vous avez aussi le droit à la sécurité matérielle[160], notamment à la sécurité sociale[161], et dans une certaine mesure à la sécurité juridique[162], mais le « *droit fondamental* » à la sécurité n'est proclamé, modestement, que par l'article L. 111-1 du code de la sécurité intérieure[163]. Vous n'y voyez donc pas une liberté fondamentale qu'il vous appartiendrait de protéger en référé-liberté[164]. 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[165].

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[166]. 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.

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

---

158 V. A. Vidal-Naquet, *La sécurité en droit constitutionnel : non-dit ou non-être ?*, https://halshs.archives-ouvertes.fr/halshs-02112622/document.

159 Art. 1er de la Charte de l'environnement.

160 11ème alinéa du Préambule de 1946.

161 Le droit à la protection sociale est garanti par la Constitution (Cons. const., n° 86-225 DC, 23 janvier 1987, cons. 16 et 17).

162 Art. 16 de la Déclaration de 1789 tel qu'interprété par la décision n° 2010-2 QPC du 11 juin 2010 (cons. 21 à 23). Les tables analytiques évoquent directement la sécurité juridique.

163 Qui codifie l'article 1er de la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité. Y est aussi affirmé le devoir de l'Etat 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.

164 JRCE, 20 juillet 2001, *Commune de Mandelieu-la-Napoule*, n° 236196, au Rec.

165 Cons. const., 17 octobre 2014, n° 2014-422 QPC. 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'article L. 111-1 du code de la sécurité intérieure édité par Dalloz, citant l'exemple du Portugal).

166 Cons. const., n° 2017-632 QPC, 2 juin 2017, cons. 4 et 6.

Il faut rendre cette justice à la Cour de Luxembourg : alors qu'initialement, elle ne voyait dans la lutte contre le terrorisme[167] et la criminalité grave[168] 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[169], son arrêt du 6 octobre 2020 énonce, en s'inspirant explicitement de la jurisprudence de la Cour européenne des droits de l'homme[170], que le droit au respect de la vie privée et familiale peut créer dans le chef des Etats certaines **obligations positives** d'agir pour lutter efficacement contre les infractions qui la menacent, en particulier pour les mineurs et les autres personnes vulnérables[171].

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'Etat 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[172]. 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 »,

---

[167] CJUE, 3 septembre 2008, *K… et Al Barakaat International Foundation c/ Conseil et Commission*, C-402/05 P et C-415/05 P, pt. 363.

[168] CJUE, 23 novembre 2010, *T…*, C-145/09, pts 46-47.

[169] CJUE, gr. ch., 26 juillet 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*, point 149.

[170] A propos de l'article 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 décembre 2008, *K.U c/ Finlande*, n° 2872/02, pt. 45).

[171] Pt. 126

[172] Dans ses conclusions sur l'affaire *LQDN et autres*, l'avocat général Campos 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.

même si ce n'est pas le sujet du jour[173]. D'une part, parce que l'article 4 du TUE prévoit que la responsabilité de la sécurité nationale relève des seuls Etats membres. D'autre part, parce que ce même article se borne à prescrire à l'Union de **respecter** « *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* ». **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[174]. C'est le juge national, qui plus est lorsqu'il se nomme Conseil d'Etat, 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'Etat. Assumons le raccourci jusqu'au bout : s'il n'y a plus d'Etat, il n'y a plus d'Etat membre, donc il n'y a plus de construction européenne, non plus[175]. 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. Ils 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 elle-même 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.

6.1. 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. A 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

[173] Cons. const., n° 2014-450 QPC du 27 février 2015, cons. 6.

[174] 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 article 52 devait s'interpréter à la lumière de l'obligation de respecter ces mêmes fonctions essentielles de l'Etat. 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.

[175] Y compris celle d'une Europe du renseignement que porte en germe le nouveau Collège du renseignement en Europe.

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.

6.2. 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 Etats 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 œuvre.

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[176] et les interceptions judiciaires[177], réputées toutefois plus intrusives que l'accès en temps différé aux données[178]. A 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 »[179].

Cela étant, on voit bien que le quantum 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 œuf comme d'un bœuf 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 euros dans le métro parisien peut être l'œuvre

[176] Art. 76 du CPP.
[177] Art. 60-4 et 100 du CPP.
[178] 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 *K*... du 18 mai 2010 et *R*... *Z*... du 4 décembre 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.
[179] 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…

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[180]. C'est précisément ce que prévoit le droit français :

- pour les enquêtes pénales, le 6ème 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[181]. Il n'y a là que la codification de la jurisprudence constante de la Chambre criminelle, notamment à l'aune de la convention européenne[182] ;

- 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 œuvre des techniques de renseignement, que le Conseil constitutionnel a expressément relevée dans sa décision sur la loi « renseignement » de 2015[183], en plaçant le contrôle de son respect entre les mains de la CNCTR[184] et du Conseil d'Etat.

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

---

[180] 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.

[181] L'article 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 œuvre par les enquêteurs et la proportionnalité des actes d'investigation au regard de la nature et de la gravité des faits.

[182] V. par exemple, à propos de la géolocalisation en temps réel : Cass. Crim., 6 janvier 2015, n° 14-84822, au Bull.

[183] Cons. const., n° 2015-713 DC du 23 juillet 2015, cons. 11.

[184] L'article L. 833-5 du CSI fait obligation à la CNCTR de vérifier que la mesure respecte l'article L. 801-1.

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*[185] et *H.K*[186], que la criminalité grave est une notion contingente et multi-factorielle, dont les contours doivent être laissés à la main des Etats membres, dans le cadre de leur compétence de principe en matière pénale[187], 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'Etat dans son rapport « *Internet et les réseaux numériques* » de 1998, en appelant de ses vœux 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[188].

---

[185] Pts 93 et s.
[186] Pts. 91 et s.
[187] Selon l'article 83 du TFUE, c'est seulement lorsque l'harmonisation du droit pénal est indispensable pour la mise en œuvre 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.
[188] Les opérateurs, de nombreuses associations et, dans un premier temps, la CNIL (délibération n° 03-056 du 9 décembre 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 novembre 2005). Dans l'avis qu'elle a rendu le 20 décembre 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.

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.

6.3. 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.

6.3.1. La directive *e-privacy* explicite la notion de « sécurité nationale » par celle de « sûreté de l'Etat ». 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°)[189], 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'Etat* ». On peut davantage hésiter pour les autres rubriques[190], en particulier la prévention des violences collectives de nature à porter gravement atteinte à la paix publique (c. du 5°)[191] et la prévention de la

[189] Ce triptyque est l'explicitation de la notion de « sécurité nationale » qui figurait dans la loi avant 2015 (article L. 241-2 du CSI, repris dans le projet de loi initial), mais dans une acception évidemment plus étroite que celle de la Cour de justice.

[190] C'est aussi le cas pour la prévention des actions tendant au maintien ou à la reconstitution de groupements dissous en application de l'article 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).

[191] 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).

criminalité et de la délinquance organisées (6°)[192], qui représentent à elles deux environ 1/3 des techniques de renseignement mises en œuvre.

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 œuvre. 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 Etats membres de définir leurs intérêts essentiels de sécurité nationale[193], 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 certain, 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 Ier 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[194].

---

[192] Cette notion renvoie aux incriminations pénales énumérées à l'article 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 juillet 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.

[193] Arrêt *Privacy international*, pt. 44.

[194] Articles L. 2339-14 à L. 2339-18.

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. A 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 Etats et visant des cibles sensibles, y compris des hôpitaux. Peut-être plus que tout autre Etat 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[195]. 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

[195] Ce chiffre est issu du rapport de la délégation parlementaire au renseignement de 2015. Depuis lors, les crédits alloués aux services ont sensiblement augmenté.

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[196], 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'Etat, comme un attentat terroriste. On la retrouve dans de nombreuses législations européennes, l'Italie ayant quant à elle opté pour une durée de 6 ans.

Il en résulte que, pour cette finalité, la seule illégalité dont sont entachés l'article R. 10-13 du 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.

6.3.2. 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 10ème 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'Etat, donc une garantie du respect des objectifs de valeur constitutionnelle invoqués.

---

[196] Art. L. 243-2 du code des relations entre le public et l'administration.

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**[197], 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 »[198]. 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 œuvre 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 produits 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

[197] 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 *B… c/ Allemagne* du 19 octobre 2016 (C-582/14), 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.

[198] 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 location.

plusieurs données qui peut offrir des certitudes, y compris en détectant l'existence de manœuvres 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 XXIème siècle avec des outils du XXIème siècle, pour satisfaire les exigences du corps social du XXIème siècle. On peut apprécier le charme désuet des interrogatoires de l'inspecteur Colombo ou du commissaire Mégret, 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[199].

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 Etats 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 Etats 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 Etats, dont l'Allemagne[200], la Finlande[201] et la Suède[202] ont entrepris de resserrer l'obligation de conservation, selon le cas, sur des

[199] SSMSI, *Insécurité et délinquance en 2019 : bilan statistique*, septembre 2020.
[200] 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…).
[201] 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.
[202] 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.

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 Etats 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 Etats-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[203]. 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** :

[203] 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, septembre 2020, p. 112).

- 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[204], 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[205]. 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 20 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'Etat 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

[204] Le Gouvernement évoque « quelques jours », pour le contrôle des fraudes.
[205] V. l'arrêté du 31 décembre 2013 relatif aux factures des services de communications électroniques et à l'information du consommateur sur la consommation au sein de son offre.

évident que l'ergonomie et la rapidité du recueil, comme l'exploitabilité des données fournies, sont des conditions essentielles de l'efficacité opérationnelle de services d'enquêtes 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.

A 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 œuvre. 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'Etat 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 – A 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'Etat 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[206], l'exclusion pure et simple des traitements réalisés par les

[206] La Cour indique clairement, aux points 100 et 101 de son arrêt du 6 octobre 2020, que l'inclusion des

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[207]. 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

---

réquisitions de « sécurité » dans le champ de la directive *e-privacy* s'explique par sa rédaction, qui exclut les « activités » de l'Etat en matière régalienne, c'est-à-dire des traitements dont l'Etat est le responsable de traitement, et non les traitements imposés par l'Etat aux opérateurs et dont ces derniers sont responsables – ce qui est le cas de la conservation et de la communication des données. A 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, *Parlement/Conseil et Commission*, C-317/04 et C-318/04).

[207] En revanche, s'agissant de la lutte contre la criminalité grave, le projet de règlement prévoit seulement en ses articles 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.

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 manœuvre 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 œuvre, 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.

9.1. 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 <u>préalable</u>** 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 œuvre 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'Etat en vue de faire annuler l'autorisation et ordonner la destruction des renseignements irrégulièrement collectés[208]. 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 œuvre 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 œuvre 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.

[208] Art. L. 773-7 et R. 773-26 du code de justice administrative.

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'Etat 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[209], soit en prévoyant qu'en cas de passé-outre un avis défavorable, la technique ne peut être effectivement mise en œuvre 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[210].

9.2. 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.

---

[209] 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.

[210] 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 le JLD examine 2 à 2,5 millions de réquisitions par an…

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 œuvre 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.

9.3. 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* »[211]. Vos chambres réunies l'ont invitée à réexaminer ce point en tenant compte des possibilités de recours devant la formation spécialisée du Conseil d'Etat. 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[212].

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 œuvre pour le compte de l'Etat et intéressant la sûreté de l'Etat 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

[211] Pt. 121.

[212] Ce qui est d'ailleurs le cas sous l'empire de l'article 13 de la directive police-justice, transposé au II de l'article 107 de la loi du 6 janvier 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 constitue une mesure 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 paragraphe 4 de l'article 13 de la directive autorise même l'adoption de mesures pour placer des catégories entières de traitements dans ce régime dérogatoire.

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 œuvre à son égard et, si elle n'en est pas satisfaite, de saisir la formation spécialisée du Conseil d'Etat[213].

9.4. 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 œuvre 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 12. Ils sont régis par le titre IV de la loi du 6 janvier 1978, comme tous les traitements « *intéressant la sûreté de l'Etat et la défense* ». Le moyen est donc inopérant.

9.5. 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* ».

10.1. 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

[213] V. respectivement les articles L. 833-4 et L. 841-1 du CSI.

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[214] 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[215], 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[216] ;

- 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.

A 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 *S...* de vos 2ème et 7ème chambres réunies du 28 février 2020 (n° 433886, au Rec.) 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

[214] Dont la CNCTR indique dans son rapport 2019 qu'elle a renouvelé l'intérêt opérationnel de cette technique, jusque-là peu utilisée (p. 35).
[215] V. CE, 17 mai 2017, *La Quadrature du Net et autres*, n° 405792.
[216] Cons. const., n° 2017-648 QPC du 4 août 2017.

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[217] 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 saisi, 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[218], si vous souhaitiez éclairer les parties prenantes quant à la conformité au droit de l'Union de ce dispositif.

A 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[219]. 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. A 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[220]. 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.

---

[217] 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, Section, 1er juillet 2016, *Commune d'Emerainville et syndicat d'agglomération nouvelle de Marne-la-Vallée-Val-Maubuée*, n° 363047-363134, au Rec.). Cette solution pourrait être étendue en toutes matières, comme le proposait Vincent 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.

[218] V. par exemple : CE, 21 mars 2001, *M... E... E...*, n° 208541, au Rec.

[219] 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.

[220] 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.

10.2. L'effort de lecture est plus grand pour ce qui concerne la **géolocalisation en temps réel**[221].

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[222].

La Cour s'est manifestement méprise en indiquant que cette technique était limitée à la prévention du terrorisme en droit français[223], 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 œuvre de cette technique, qui ne cesse de monter en puissance[224], 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[225].

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,

---

[221] Curieusement, le II de l'article 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 article) que pour l'accès en temps réel aux données de connexion (art. L. 851-2 CSI) 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'article 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).

[222] Cette précision peut toutefois varier en fonction de l'environnement, notamment en milieu urbain.

[223] V. le point 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.

[224] Le rapport 2019 de la CNCTR fait état de 7601 demandes de géolocalisations en temps réel en 2019, contre 2426 en 2016, soit une augmentation de 213 % !

[225] V. pour une analyse (un peu ancienne) de droit comparé, l'étude d'impact du projet de loi relatif à la géolocalisation du 20 décembre 2013.

comme l'a expressément jugé la Cour européenne des droits de l'homme qui n'a jamais circonscrit son périmètre autorisé au terrorisme[226].

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 œuvre, 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.

*

XI – 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 précocément 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 œuvre 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

[226] CEDH, 2 septembre 2010, *U… c/ Allemagne*, n° 35623/05.

détruites sous 60 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[227] doit être limitée au strict nécessaire, comme l'injonction de conservation généralisée aux mêmes fins ;

- la mise en œuvre 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 œuvre 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'Etat 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.

[227] La Cour évoque par erreur la « durée de la conservation » au point 177.

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 œuvre 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.

XII – 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 œuvre 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 œuvre 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.

XIII - 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.

13.1. 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'Etat 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[228]. 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[229]. Cela étant, il n'est pas exclu que le juge judiciaire porte un autre regard sur la question[230] et nous vous invitons donc à ne pas vous aventurer sur ses terres.

---

[228] Seules les techniques mentionnées aux articles 20 (collecte en temps réel) et 21 (interception de données relatives au contenu) sont facultatives, et seulement à certaines conditions mentionnées au paragraphe 3 de l'article 14.

[229] 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.

[230] 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.

13.2. S'agissant des décrets, vous n'êtes pas contraint 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 (n° 370321, au Rec.).

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 *V...*[231]. 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 œuvre, sauf urgence dûment justifiée, sans que la Commission ait été mise à même de saisir la formation spécialisée du Conseil d'Etat – c'est-à-dire ait disposé d'un délai raisonnable pour ce faire[232] - 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'Etat, 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

[231] CE, Assemblée, 29 juin 2001, n° 213229, au Rec. V. aussi pour un régime supplétif faisant suite à une annulation « en tant que » (et non « en tant que ne pas ») : CE, 31 juillet 2019, *Association La Cimade et autres*, n° 428530-428564, au Rec.

[232] Celle-ci doit être communiquée « sans délai » à la commission (3ème alinéa de l'article L. 821-4 du CSI) et indiquer les motifs pour lesquels l'avis défavorable n'a pas été suivi (2ème alinéa).

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'Etat la somme de 3000 euros au profit de chaque association requérante et de 1500 euros 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 œuvre 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 attachés, 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.