COUR DE JUSTICE
DE
L'UNION EUROPÉENNE

Affaires C-511/18 et C-512/18
sur renvois préjudiciels du Conseil d'État (FRANCE)

ENTRE
French Data Network ; La Quadrature du Net ; Fédération des fournisseurs d'accès à Internet associatifs ; Igwan.net
Parties requérantes

ET
Privacy International ; Center for Democracy and Technology
Parties intervenantes

CONTRE
Premier ministre ; Garde des Sceaux, ministre de la Justice ; Ministre de l'Intérieur ; Ministre des Armées
Parties défenderesses

OBSERVATIONS POUR PRIVACY INTERNATIONAL

Soumises le 26 novembre 2018 par :

Hugo ROY | Avocat à la Cour
1 rue Paul Baudry, 75008 Paris
Barreau de Paris

avocat@hugoroy.eu
Tél. +33 7 61 61 90 46

Table des matières

1 L'organisation non-gouvernementale britannique à but non-lucratif Privacy International (ci-après « la partie intervenante ») est intervenue en février 2016 devant le Conseil d'État, avec l'organisation américaine à but non-lucratif Center for Democracy and Technology, au soutien de la requête d'associations françaises demandant l'annulation du refus implicite du Gouvernement français d'abroger les dispositions règlementaires issues, notamment, du décret n° 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques, adopté neuf jours après la directive 2006/24[1]. Ce faisant, la partie intervenante entendait s'inscrire dans la continuité de l'arrêt *Digital Rights*[2] de la grande chambre de la Cour, déclarant invalide la directive 2006/24 précitée.

2 La partie intervenante entend faire valoir par les présentes observations que les motifs retenus par la grande chambre de la Cour dans l'arrêt *Digital Rights* précité, dans l'arrêt *Schrems*[3], ainsi que dans l'arrêt *Tele2/Watson*[4], doivent être appliqués dans les présentes affaires jointes, pour les raisons qui suivent.

3 **En premier lieu,** cette solution s'impose en droit, en raison de l'absence de tout changement de circonstance significatif depuis le 21 décembre 2016, date de l'arrêt *Tele2/Watson*. Les besoins liés à la lutte contre la criminalité et à la sauvegarde de la sécurité nationale dans le contexte d'une réelle menace terroriste, ne sont pas nouveaux et n'ont pas changé d'échelle depuis le 21 décembre 2016.

4 De même, le cadre juridique applicable reste substantiellement identique s'agissant des dispositions du droit de l'Union sur lesquelles la grande chambre de la Cour s'est fondée. En effet, ni la directive 2002/58[5], ni la Charte des droits fondamentaux de l'Union européenne (la « Charte ») n'ont fait l'objet d'une quelconque modification depuis décembre 2016. Si le droit de l'Union européenne en matière de protection des données à caractère personnel a évolué, avec l'abrogation de la directive 95/46[6] ; l'entrée en application du règlement 2016/679[7] (le « RGPD ») assure désormais un niveau de protection cohérent, élevé et

1. Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE
2. CJUE, g^de^ ch., 8 avr. 2014, *Digital Rights Ireland et autres*, C-293/12, C-594/12
3. CJUE, g^de^ ch., 6 oct. 2015, *Schrems*, C-362/14
4. CJUE, g^de^ ch., 21 déc. 2016, *Tele2 Sverige, Watson et autres*, C-203/15, C-698/15
5. 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)
6. Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
7. Règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

équivalent dans tous les États membres. En particulier, le droit au recours effectif en cas de violation des droits à la protection des données à caractère personnel prévu à l'article 22 de la directive 95/46 est maintenant prévu à l'article 79 du RGPD. Enfin, le droit de l'Union consacre effectivement depuis mai 2018, le principe de « minimisation des données » tant au titre du RGPD (articles 5(1)(c), 25 et 89 notamment) qu'au titre de la directive 2016/680 [8] (articles 4(1)(c) et 20). Plus généralement, le niveau de protection des données personnelles exigé dans l'Union est plus élevé aujourd'hui qu'en 2016.

5 **En second lieu,** cette solution est nécessaire pour garantir le respect des droits et libertés fondamentaux et, en particulier, le droit au respect de la vie privée et le droit à la protection des données personnelles. Eu égard au développement d'Internet et des services de communications électroniques et à l'importance prise par leur utilisation dans la vie privée et familiale de chacun, dans l'exercice de la liberté d'expression, ainsi que dans la participation à la vie démocratique, les garanties nécessaires pour assurer la confidentialité des communications électroniques doivent être considérées comme fondamentales dans une société démocratique.

6 Or, tel que l'a relevé l'avocat général Øe dans ses conclusions présentées le 19 juillet 2016 dans les affaires jointes *Tele2* et *Watson* (C-203/15 et C-698/15), « *les risques liés à l'accès aux données relatives aux communications (ou « métadonnées ») peuvent être équivalents, voire supérieurs à ceux résultant de l'accès au contenu de ces communications* » ; « *les « métadonnées » permettent un catalogage presque instantané d'une population dans son entièreté* » (point 259). Comme l'a déjà relevé la grande chambre de la Cour, « *[p]rises dans leur ensemble, ces données sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci* » (arrêt *Tele2/Watson*, point 99 et arrêt *Digital Rights*, point 27). Il en résulte qu'une obligation généralisée et indifférenciée de données de connexion constitue une ingérence particulièrement grave et d'une vaste ampleur, incompatible avec le respect de la Charte (voir, notamment, arrêt *Tele2/Watson*, point 100 et arrêt *Digital Rights*, point 37).

---

8. Directive 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil

7 **En troisième lieu,** la solution inverse ouvrirait la possibilité à des dérogations nationales de nature à neutraliser ou fragmenter le niveau de protection des données personnelles cohérent, élevé et équivalent dans tous les États membres, ainsi qu'à affaiblir le plein effet de la Charte. La solution inverse contribuerait donc à une remise en cause de l'espace de liberté, de sécurité et de justice sans frontières intérieures que l'Union offre à ses citoyens au titre de l'article 3, paragraphe 2, du Traité sur l'Union européenne.

8 Ainsi qu'il le sera démontré, après un exposé concernant le cadre juridique litigieux dans l'affaire au principal ayant pour objet d'apporter à la Cour des précisions sur les enjeux de la présente affaire (section 1) ; la conservation des données de communications électroniques imposée aux fournisseurs ne saurait être généralisée et indifférenciée (section 2 page 9), et le recueil de telles données par les autorités doit être strictement encadré, ainsi que soumis à une décision préalable d'une juridiction ou d'une autorité indépendante (section 3 page 13), et être assorti d'une information à destination des personnes concernées dès le moment où la communication de cette information n'est plus susceptible de compromettre les enquêtes menées par ces autorités (section 4 page 15).

1. Précisions sur le cadre juridique litigieux

9 S'agissant des premières questions des affaires C-511/18 et C-512/18, le cadre juridique litigieux est comparable à celui de l'affaire *Tele2 Sverige* (C-203/15), en ce qu'il porte sur la question de la transposition de la directive 2006/24.

10 Le cadre juridique litigieux s'est construit dans la foulée du 11 septembre 2001 avec l'adoption de la loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne. Il s'est, depuis, étendu et complexifié.

11 Sans revenir sur le cadre juridique litigieux dans son intégralité, exposé par la décision de renvoi, la partie intervenante souhaite apporter les précisions qui suivent, afin d'éclairer la Cour sur les enjeux des premières questions des affaires jointes, ainsi que des deuxième et troisième questions de l'affaire C-511/18.

1.1. **La conservation des données en cause n'est pas limitée à la lutte contre le terrorisme et à sa prévention.**

12 Les mesures nationales en cause dans les affaires au principal ne sont aucunement limitées à des finalités de sauvegarde de la sécurité nationale. Ces mesures poursuivent en effet des finalités bien plus larges. La conservation des données de connexion en droit français est notamment prévue pour les besoins de la recherche, de la constatation et de la poursuite

des infractions pénales (sans limitation à la criminalité grave). De plus, le droit français connaît depuis 2001 une extension continue des possibilités d'accès aux données ainsi conservées, pour des finalités et activités diverses. À titre d'exemple, l'article L. 621-10 du code monétaire et financier permet la communication de ces données aux enquêteurs et contrôleurs de l'Autorité des marchés financiers [9]. Enfin, les finalités poursuivies pour l'accès à ces données par les autorités administratives au titre du livre VIII du code de la sécurité intérieure ont trait « *à la défense et à la promotion des intérêts fondamentaux de la Nation* » listés à l'article L. 811-3 du code de la sécurité intérieure, lesquels comprennent, notamment, la prévention d'atteintes à la paix publique [10], la défense et la promotion des intérêts économiques, industriels et scientifiques majeurs de la France [11], ainsi que la prévention de la criminalité et de la délinquance organisées [12].

1.2. **La difficulté sérieuse d'interprétation posée par le cadre litigieux dépasse le champ des questions transmises.**

13 S'agissant de la deuxième question de l'affaire C-511/18, la juridiction de renvoi vise les « mesures de recueil en temps réel des données relatives au trafic et à la localisation d'individus déterminés ». La partie intervenante observe que la juridiction de renvoi a exclu une part importante du cadre juridique litigieux dans l'affaire au principal.

14 En effet, la question dont la Cour a été saisie se rapporte principalement à l'article L. 851-2 du code de la sécurité intérieure. Cet article prévoit un recueil en temps réel de données de connexion, notamment sur les réseaux de communications électroniques, visant certaines personnes en lien avec une menace [13].

15 La juridiction de renvoi n'a donc pas saisi la Cour d'une question se rapportant à l'article L. 851-3 du même code. Cet article prévoit à son paragraphe I, qu'« *il peut être imposé aux*

9. Cette disposition, jugée anticonstitutionnelle, demeure cependant en vigueur jusqu'au 31 décembre 2018. Cf. Conseil constit., 21 juill. 2017, *Droit de communication aux enquêteurs de l'AMF des données de connexion*, 2017-646/647 QPC

10. Le texte vise les « violences collectives de nature à porter gravement atteinte à la paix publique » au sens des articles 431-1 à 431-10 du code pénal et comprend notamment le délit défini à l'article 431-9 du code pénal qui consiste à « *avoir organisé une manifestation sur la voie publique n'ayant pas fait l'objet d'une déclaration préalable dans les conditions fixées par la loi* ». Puni de six mois d'emprisonnement, il ne peut être considéré comme relevant de la criminalité grave (Conseil constit., 23 juill. 2015, *Loi renseignement*, 2015-713 DC, considérant 10).

11. Ces intérêts sont compris dans les intérêts fondamentaux de la nation au sens de l'article 410-1 du code pénal, d'après l'interprétation des dispositions de l'article L. 811-3 du code de la sécurité intérieure par le Conseil constitutionnel (ibid.).

12. Cette finalité fait référence aux incriminations pénales énumérées à l'article 706-73 du code de procédure pénale et aux délits punis par l'article 414 du code des douanes commis en bande organisée (ibid.).

13. « *une personne préalablement identifiée susceptible d'être en lien avec une menace [ou] une ou plusieurs personnes appartenant à l'entourage de la personne concernée par l'autorisation [qui] sont susceptibles de fournir des informations* » (L. 851-2, paragraphe I)

opérateurs [de communications électroniques] [...] la mise en œuvre sur leurs réseaux de traitements automatisés destinés, en fonction de paramètres précisés dans l'autorisation, à détecter des connexions susceptibles de révéler une menace terroriste ». Cet article prévoit donc des traitements : (i) en temps réel, (ii) utilisant des données de connexion (y compris des données à caractère personnel), (iii) notamment sur les réseaux de communications électroniques. Cet article, L. 851-3, a donc un objet qui se rapproche et qui est complémentaire de celui de l'article L. 851-2. Or, l'article L. 851-3 porte sur l'ensemble d'un réseau et donc, sur l'ensemble de ses utilisateurs, sans aucune limitation dans sa portée matérielle ou quant aux individus affectés.

16 L'article L. 851-3 soulève, de même que l'article L. 851-2 si ce n'est plus, une difficulté sérieuse d'interprétation quant à sa conformité au droit de l'Union. La juridiction de renvoi a pourtant décidé de ne pas demander à la Cour si la mise en œuvre de tels traitements automatisés, directement sur les infrastructures des fournisseurs, selon des paramètres techniques déterminés par l'État, est justifiée et limitée au stricte nécessaire au regard des exigences de la Charte. Cette exclusion est d'autant plus surprenante que le rapporteur public du Conseil d'État avait justement invité la juridiction de renvoi à inclure cet article dans le champ de ses questions préjudicielles (cf. conclusions du rapporteur public, page 13, troisième et quatrième paragraphes [annexe n° **A.1**]).

17 La partie intervenante souligne l'opportunité qui se présente à la Cour de rappeler les garanties appropriées et le champ d'application de celles-ci, en matière de traitements de données affectant la confidentialité des communications électroniques.

1.3. **Les garanties procédurales du cadre juridique litigieux sont insuffisantes pour compenser l'absence de notification aux personnes concernées.**

18 S'agissant de la troisième question de l'affaire C-511/18, la juridiction de renvoi vise les « garanties procédurales existantes » autour du recueil des données de connexion. La partie intervenante appelle en particulier l'attention de la Cour sur les points suivants.

19 **Premièrement**, aucun mécanisme destiné à compenser effectivement et suffisamment l'absence de toute notification *a posteriori* n'est prévu. Les articles L. 833-4 et L. 841-1 du code de la sécurité intérieure prévoient que toute personne peut saisir la Commission nationale de contrôle des techniques de renseignement (CNCTR) ou le Conseil d'État dans le but de « *vérifier qu'aucune technique de renseignement n'est irrégulièrement mise en œuvre à son égard* ». Toutefois, ce mécanisme ne saurait passer pour « *une possibilité satisfaisante de demander et d'obtenir auprès des autorités des informations*

sur les interceptions » au sens de la jurisprudence de la Cour européenne des droits de l'homme (Cour EDH, g^de^ ch., 4 déc. 2015, *Zakharov c. Russie*, n° 47143/06, § 298).

20 En effet, à aucun moment la CNCTR ne fournit d'informations significatives à la personne concernée. Dans le meilleur des cas, en application des articles L. 773-6 et L. 773-7 du code de justice administrative, la décision du Conseil d'État n'informe le requérant que de l'existence ou de l'inexistence d'une illégalité dans la mise en œuvre d'une technique de renseignement, sans donner un droit d'accès à un quelconque élément de fait utile pour l'exercice du recours effectif de la personne concernée, ni aucun détail sur les données recueillies.

21 **Deuxièmement,** dans le cadre des procédures *a posteriori*, le secret de la défense nationale fait bien souvent obstacle au débat contradictoire devant le Conseil d'État. En effet, l'article R. 773-24, alinéa 1^er^, du code de justice administrative dispose que « *[d]ans les cas où les débats sont susceptibles de porter sur des informations protégées par le secret de la défense nationale, ou de confirmer ou infirmer la mise en œuvre d'une technique de renseignement à l'égard du requérant, ou de révéler des éléments contenus dans le traitement de données, ou si le requérant figure ou non dans le traitement, le requérant est invité à présenter ses observations avant les conclusions du rapporteur public et, après les avoir formulées, à se retirer. [. . .]* » Cette exclusion est d'autant plus problématique que l'ensemble des politiques publiques concourt à la sécurité nationale d'après l'article L. 1111-1, alinéa 2, du code de la défense. De plus, d'après l'arrêté du 30 novembre 2011 portant approbation de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale, « *la protection du secret concerne tous les domaines d'activité relevant de la défense et de la sécurité nationale : politique, militaire, diplomatique, scientifique, économique, industriel* ».

22 En application des articles 413-9 du code pénal et R. 2311-6 du code de la défense, sont considérés comme présentant un caractère de secret de la défense nationale tous éléments qui ont fait l'objet d'une mesure de classification, décidée comme telle par les autorités administratives et ministérielles elles-mêmes. Toute procédure de déclassification, en application de l'article L. 2312-4 du code de la défense, fait intervenir la Commission consultative du secret de la défense nationale (CCSDN), mais les avis rendus par celle-ci ne s'imposent pas aux autorités administratives.

23 Il en résulte que l'administration peut elle-même, et sans contrôle effectif et indépendant, exclure totalement certaines informations du débat contradictoire en les plaçant sous le sceau du secret de la défense nationale. Enfin, et corrélativement, les dispositions des articles L. 773-1 à L. 773-8 du code de justice administrative ont méconnu les exigences du droit à un recours effectif faute d'avoir prévu un ensemble de mesures susceptibles de

contrebalancer efficacement l'accès privilégié à un ensemble de documents protégés par le secret de la défense nationale dont dispose l'administration.

24 **Troisièmement,** en matière de surveillance dite internationale, aucune voie de recours devant le Conseil d'État n'est ouverte aux personnes concernées. La surveillance internationale couvre de manière large « *la surveillance des communications qui sont émises ou reçues à l'étranger* ». Elle est exclusivement régie par un régime spécial et, à de nombreux égard, dérogatoire (articles L. 854-1 à L. 854-9 du code de la sécurité intérieure). Dès lors, l'accès à un juge est totalement ineffectif (pour une illustration, voir l'affaire de la députée du Parlement européen Sophie in't Veld (Conseil d'État, form. spé., 20 juin 2018, *In't Veld*, n^{os} 404012 et 404013)).

25 Il résulte de ce qui précède, selon la partie intervenante, qu'il importe de mettre en évidence les garanties nécessaires sans lesquelles les traitements de données de connexion réalisés sans le consentement des personnes concernées et interférant avec la confidentialité des communications, ne peuvent être considérés conformes au droit de l'Union et, en particulier, au respect de la Charte.

2. Premières questions des affaires C-511/18 et C-512/18

26 Il est demandé à la Cour de déterminer si l'ingérence causée par une mesure nationale prévoyant une obligation de conservation généralisée et indifférenciée, imposée aux fournisseurs de services de communications électroniques, peut être regardée comme justifiée, compte-tenu de la responsabilité qui incombe aux seuls États membres de sauvegarder la sécurité nationale. Les deux premières questions renvoient ainsi, implicitement, à l'arrêt *Tele2/Watson* de la grande chambre. Bien que cet arrêt porte en particulier sur la lutte contre la criminalité, sa motivation s'applique *mutatis mutandis* en matière de sauvegarde de la sécurité nationale, dans le contexte de réelles menaces terroristes.

27 La partie intervenante observe, à titre liminaire, que le cadre juridique de la conservation des données de connexion est loin de respecter les exigences et les garanties posées par la grande chambre en la matière (arrêt *Tele2/Watson*, points 108 à 111). L'obligation de conservation n'est aucunement ciblée quant aux données sur lesquelles elle porte à titre préventif. Cette obligation s'applique systématiquement, quelles que soient les circonstances. Elle concerne donc, directement, l'ensemble des abonnés et utilisateurs sans distinction ni limitation objective en lien avec l'objectif poursuivi. Le cadre juridique ne prévoit pas non plus les garanties nécessaires pour protéger contre les risques d'abus.

28 La question posée porte spécifiquement sur la poursuite d'objectifs tenant à la sauvegarde de la sécurité nationale, pris dans le contexte du risque terroriste (bien que le cadre litigieux n'y soit nullement limité, cf. section 1.1 page 5). Pour autant, ni la poursuite de ces finalités, ni ce contexte, ne sont de nature à soustraire les mesures en cause du champ d'application du droit de l'Union. Ils ne doivent pas, non plus, appeler une analyse différente de celle opérée par la grande chambre dans l'arrêt *Tele2/Watson*.

2.1. **La Charte est pleinement applicable aux traitements en cause.**

29 Les premières questions précisent que la sauvegarde de la sécurité nationale relève de la seule responsabilité des États membres. Pour autant, des mesures nationales affectant une activité soumise au droit de l'Union ne peuvent être considérées comme totalement soustraites au champ d'application du droit de l'Union. Même si ces dérogations nationales poursuivent des finalités tenant à la sécurité nationale, elles doivent être adéquates, limitées au strict nécessaire et proportionnées.

30 L'Union dispose d'un cadre juridique solide pour la régulation du secteur des communications électroniques, régissant l'activité des fournisseurs de services de communications électroniques, ainsi que l'utilisation de ces services. C'est dans ce contexte que la directive 2002/58 s'inscrit, avec l'objectif prévu à son article premier d'« *assurer un niveau équivalent de protection des droits et libertés fondamentaux, et en particulier du droit à la vie privée et à la confidentialité* » dans ce secteur. L'article 3 précise que cette directive « *s'applique au traitement des données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux de communications publics dans la Communauté* ». La directive 2002/58 doit donc être regardée comme régissant les activités des fournisseurs de services de communications électroniques (arrêt *Tele2/Watson* point 70).

31 Les obligations de conservation de données imposées aux fournisseurs dont il est question dans les affaires au principal et sur lesquelles portent les premières questions relèvent de l'activité des fournisseurs de services de communications électroniques et, partant, du champ d'application de la directive 2002/58 (voir, par analogie, arrêt *Tele2/Watson*, point 75). Comme l'a déjà précisé la Cour, ce champ d'application concerne aussi les mesures prises pour la sécurité nationale visées par l'article 15, paragraphe 1 (ibid. points 71 à 73).

32 Si des limitations aux droits et obligations prévus par le droit de l'Union sont permises par celui-ci, pour la poursuite d'objectifs tenant, en particulier, à la sauvegarde de la sécurité nationale (voir, par exemple, article 15 précité, ou article 23 du RGPD) ; c'est à la condition

que de telles limitations soient adéquates, strictement nécessaires et proportionnées, au sens de la Charte.

33 En effet, l'applicabilité du droit de l'Union implique celle de la Charte (CJUE, g^de ch., 26 févr. 2013, *Åklagaren*, C-617/10, point 21). Dès lors, il ne saurait exister de cas de figure qui relèvent ainsi du droit de l'Union sans que les droits fondamentaux garantis par la Charte trouvent à s'appliquer. Ainsi, la Charte s'applique y compris à des situations relevant par ailleurs de question de sécurité nationale.

34 Par conséquent, le droit de l'Union et en particulier l'article 15, paragraphe 1, de la directive 2002/58 lu à la lumière de la Charte, est pleinement applicable aux obligations de conservation de données imposées aux fournisseurs telles que prévues par les mesures nationales des affaires au principal.

2.2. **Le caractère généralisé et indifférencié de la conservation est incompatible avec une société démocratique.**

35 L'ingérence que comporte une obligation de conservation généralisée et indifférenciée dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte est d'une vaste ampleur et doit être considérée comme particulièrement grave (voir, notamment, arrêt *Tele2/Watson*, point 100 et arrêt *Digital Rights*, point 37).

36 Eu égard à la gravité de cette ingérence, seules des finalités suffisamment graves peuvent être invoquées conformément à la Charte, telles que la criminalité grave (arrêt *Tele2/Watson*, point 102). La sauvegarde de la sécurité nationale, prise dans le contexte de réelles menaces terroristes et en lien avec la lutte contre celles-ci, peut indéniablement être considérée comme suffisamment grave. La partie intervenante invite toutefois la Cour à considérer de manière restrictive la portée de la notion de sauvegarde de la sécurité nationale, conformément au droit international. La Cour européenne des droits de l'homme considère que le périmètre de cette notion ne doit pas être laissé à l'entière discrétion des États (voir, par exemple, arrêt *Zakharov* précité, paragraphe 248).

37 Toutefois, comme l'a déjà jugé la grande chambre en décembre 2016, si l'efficacité de la lutte contre le terrorisme peut dépendre dans une large mesure de l'utilisation des techniques modernes d'enquête, un tel objectif d'intérêt général, pour fondamental qu'il soit, ne saurait à lui seul justifier qu'une réglementation nationale prévoyant la conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation soit considérée comme nécessaire aux fins de ladite lutte (arrêt *Tele2/Watson*, point 103 et, par analogie, en ce qui concerne la directive 2006/24, arrêt *Digital Rights*, point 51). Il ne suffit pas qu'une telle mesure soit considérée comme appropriée au regard

des objectifs poursuivis, pour qu'elle soit conforme à l'article 15, paragraphe 1, lu à la lumière de la Charte. Encore faut-il, en effet, qu'elle soit limitée au strict nécessaire et, enfin, proportionnée.

38 Or, une obligation de conservation généralisée et indifférenciée couvre de manière généralisée tous les abonnés et utilisateurs, sans aucune différenciation, limitation ou exception en fonction de l'objectif poursuivi. Elle concerne de manière globale l'ensemble des personnes faisant usage de services de communications électroniques. Eu égard au développement d'Internet et des services de communications électroniques et à l'importance prise par leur utilisation dans la vie privée et familiale de chacun, dans l'exercice de la liberté d'expression, ainsi que dans la participation à la vie démocratique, une telle mesure affecte la quasi-totalité de la population au sein de l'État membre concerné. Elle s'applique même directement à des personnes pour lesquelles il n'existe aucun indice laissant croire légitimement qu'il existe un quelconque lien avec les objectifs de sauvegarde de la sécurité nationale ou de menace terroriste (voir, par analogie, arrêt *Tele2/Watson* point 105 et, en ce qui concerne la directive 2006/24, arrêt *Digital Rights*, point 57).

39 Sauf à considérer que n'importe quelle personne soit suspectée d'être potentiellement une menace pour la sécurité de l'État — un état de suspicion généralisée incompatible avec une société démocratique — une obligation de conservation généralisée et indifférenciée excède donc, par nature, les limites du strict nécessaire.

40 À cet égard, dans l'arrêt *Zakharov* précité, la grande chambre de la Cour européenne des droits de l'homme considère que cette exigence s'impose également en matière de sécurité nationale et que l'autorité compétente pour l'autorisation de l'interception « *doit être à même de vérifier l'existence d'un soupçon raisonnable à l'égard de la personne concernée, en particulier de rechercher s'il existe des indices permettant de la soupçonner de projeter, de commettre ou d'avoir commis des actes délictueux ou d'autres actes susceptibles de donner lieu à des mesures de surveillance secrète, comme par exemple des actes mettant en péril la sécurité nationale* » (paragraphe 260).

41 Au surplus, une telle obligation ne prévoit aucune exception pour les personnes soumises au secret professionnel (voir, par analogie, arrêt *Tele2/Watson* point 105 et, en ce qui concerne la directive 2006/24, arrêt *Digital Rights*, point 58).

42 Pour toutes ces raisons, une obligation de conservation généralisée et indifférenciée ne saurait donc être considérée comme limitée au strict nécessaire, contrairement à ce qu'exige le respect de la Charte.

3. Deuxième question de l'affaire C-511/18

43 Il est demandé à la Cour de déterminer si l'ingérence causée par une mesure nationale prévoyant un recueil en temps réel de données relatives au trafic et à la localisation d'individus déterminés, affectant les droits et obligations des fournisseurs de services de communications électroniques, peut être regardée comme justifiée alors même qu'elle n'impose pas une obligation spécifique de conservation de leurs données.

44 La partie intervenante rappelle, à titre liminaire, que les mesures nationales en cause dans les affaires au principal qui portent sur les données que les fournisseurs de services de communications électroniques ont l'obligation de conserver, et qui sont prévues pour les seuls besoins de la prévention du terrorisme, ne sont pas toutes ciblées (cf. section 1.2 page 6). La partie intervenante appelle toutefois à considérer la complémentarité des mesures en cause dans les affaires au principal, compte-tenu, en particulier, du caractère généralisé et indifférencié de l'ingérence constituée par la mise en place directement sur les réseaux des fournisseurs, d'équipements et de traitements de détection, dont les modalités sont déterminées par les agences de renseignement de l'État.

3.1. **Le recueil des données doit respecter les exigences de la Charte.**

45 Une mesure nationale obligeant un fournisseur à permettre l'accès ou le recueil à des données relatives au trafic ou des données de localisation relève du champ d'application de la directive 2002/58, même si aucune mesure de conservation spécifique n'est imposée.

46 L'article 3 de la directive 2002/58 précise que cette directive « *s'applique au traitement des données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux de communications publics dans la Communauté* ».

47 Ainsi que l'a jugé la grande chambre, relève du champ d'application de cette directive une mesure affectant l'activité d'un fournisseur de services de communications électroniques, lorsqu'une telle activité implique nécessairement un traitement, par celui-ci, de données à caractère personnel (arrêt *Tele2/Watson*, point 75).

48 L'article 4 du RGPD définit un traitement comme « *toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que [...] l'extraction [...], la communication par transmission, la diffusion ou toute autre forme de mise à disposition* ».

49 Par conséquent, le recueil de données en temps réel impliquant, pour le fournisseur de services de communications électroniques, une forme de mise à disposition de données qu'il

traite dans le cadre de son activité, un tel recueil relève de l'article 15 lu en combinaison avec l'article 3 de la directive 2002/58 et doit être conforme aux exigences de la Charte.

50 Le fait que les mesures nationales en cause poursuivent un objectif tenant à la sauvegarde la sécurité nationale ne saurait soustraire ces mesures du respect de la Charte, dès lors qu'elles constituent des limitations aux droits et obligations prévus par le droit de l'Union (cf. point 32 page 11). Partant, les garanties matérielles et procédurales dégagées par la grande chambre dans sa jurisprudence doivent être respectées pour assurer que les dérogations nationales soient adéquates, limitées au strict nécessaire et proportionnées.

3.2. **Les garanties appropriées, matérielles et procédurales, doivent êtres respectées.**

51 Une mesure de recueil en temps réel des données relatives au trafic et à la localisation constitue une ingérence d'une particulière gravité dans le droit à la vie privée des personnes concernées. Elle peut, cependant, être justifiée par des finalités suffisamment sérieuses et proportionnées à la gravité de l'ingérence, à condition que des garanties appropriées soient apportées pour que ce traitement soit limité au strict nécessaire (voir, par analogie, arrêt *Tele2/Watson*, point 117). Ces garanties doivent notamment respecter des conditions à la fois d'ordre matériel et d'ordre procédural.

52 S'agissant des conditions matérielles, des limitations sur le périmètre des données doivent être apportées. En particulier, un traitement causant une ingérence d'une gravité telle que décrite ci-dessus, ne saurait porter sur des personnes pour lesquelles il n'existe aucun indice laissant croire légitimement qu'il existe un quelconque lien avec les objectifs légitimes poursuivis ou pour lesquelles il n'existe aucun élément objectif permettant de considérer que ces données pourraient, dans un cas concret, apporter une contribution effective aux intérêts vitaux de la sécurité nationale (voir, par analogie, arrêt *Tele2/Watson* points 105 et 119 et, en ce qui concerne la directive 2006/24, arrêt *Digital Rights*, point 57).

53 S'agissant des conditions procédurales, ainsi que la Cour l'a déjà jugé, « *il est essentiel que l'accès des autorités nationales compétentes aux données conservées soit, en principe, sauf cas d'urgence dûment justifiés, subordonné à un contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante, et que la* ***décision*** *de cette juridiction ou de cette entité intervienne à la suite d'une demande motivée de ces autorités présentée* » (arrêt *Tele2/Watson*, point 120 [souligné par la partie intervenante], voir aussi : arrêt *Digital Rights*, point 62).

54 À cet égard, l'autorisation de mise en œuvre d'un recueil en temps réel ne peut être considérée comme soumise à des conditions répondant aux garanties procédurales nécessaires décrites par la grande chambre, lorsque ces conditions ne comprennent qu'un simple *avis*

d'une autorité administrative indépendante, sans valeur contraignante, qui ne saurait constituer une « décision ».

55 La Cour européenne des droits de l'homme considère également qu'une autorisation indépendante et préalable est une garantie minimum pour protéger le droit à la vie privée, plus particulièrement encore dans le contexte d'une surveillance secrète (voir, par exemple, arrêt *Zakharov* précité, paragraphe 233 ; voir, également, Cour EDH, 12 janv. 2016, *Szabó c. Hongrie*, n° 37138/14, paragraphe 77).

4. Troisième question de l'affaire C-511/18

56 Il est demandé à la Cour, en substance, de déterminer si l'exigence d'information des personnes concernées, lorsqu'une telle information n'est plus susceptible de compromettre les enquêtes menées par les autorités compétentes, est indispensable pour assurer le caractère effectif du droit au recours, ou si d'autres garanties procédurales peuvent assurer effectivement un droit au recours en l'absence d'une telle information.

57 La partie intervenante observe à titre liminaire que, le recueil des données de connexion constituant une limitation des droits des personnes concernées au titre de la directive 2002/58, la procédure entourant un tel recueil doit être conforme à la Charte et notamment au droit à un recours effectif. Une telle procédure, par son caractère secret et l'absence de notification, constitue également une limitation des droits des personnes concernées d'accéder à des informations sur les traitements qui les concernent, ainsi que des obligations de responsables de traitement au titre du RGPD. Elle doit, dès lors, être conforme à la Charte.

58 En premier lieu, l'information des personnes concernées, dès le moment où cette communication n'est plus susceptible de compromettre les enquêtes menées par les autorités compétentes, est regardée, par la grande chambre de la Cour de Justice, comme étant « *de fait, nécessaire* » pour permettre l'exercice des droits de la personne concernée et en particulier le droit au recours en cas de violation (arrêt *Tele2/Watson*, point 121).

59 Si le droit au recours effectif nécessite l'accès aux informations pertinentes, la justification de la sauvegarde de la sécurité nationale ne saurait faire obstacle à toute communication à la personne concernée.

60 Par analogie, si la protection juridictionnelle peut connaître des aménagements pour tenir compte des considérations légitimes de sûreté de l'État, les règles de procédure doivent néanmoins opérer une conciliation entre ces considérations d'une part, et la nécessité de garantir à suffisance au justiciable le respect de ses droits procéduraux, d'autre part. La

Cour impose, s'agissant des « *exigences auxquelles doit répondre le contrôle juridictionnel de l'existence et du bien-fondé des raisons invoquées par l'autorité nationale compétente au regard de la sûreté de l'État membre concerné, [...] qu'un juge soit chargé de vérifier si ces raisons s'opposent à la communication des motifs précis et complets sur lesquels est fondée la décision en cause ainsi que des éléments de preuve y afférents* » (CJUE, g^de^ ch., 4 juin 2013, *ZZ*, C-300/11, point 60). Partant, comme l'a déjà jugé la grande chambre de la Cour, « *il incombe à l'autorité nationale compétente d'apporter, conformément aux règles de procédure nationales, la preuve que la sûreté de l'État serait effectivement compromise par une communication à l'intéressé des motifs précis et complets qui constituent le fondement [de la décision mise en cause]. Il en découle qu'il n'existe pas de présomption en faveur de l'existence et du bien-fondé des raisons invoquées par une autorité nationale [... et que] le juge national compétent doit procéder à un examen indépendant de l'ensemble des éléments de droit et de fait invoqués par l'autorité nationale compétente et il doit apprécier, conformément aux règles de procédure nationales, si la sûreté de l'État s'oppose à une telle communication* » (arrêt *ZZ*, points 60 et 62). Des considérations équivalentes s'appliquent dans les présentes affaires, s'agissant d'opérer une conciliation équilibrée entre les nécessités de la sauvegarde de la sécurité nationale et le droit au recours effectif des personnes concernées.

61 En droit international, c'est sur l'État que pèse la charge de démontrer l'effectivité du recours, notamment pour les limitations apportées au droit de recours en lien avec le respect de la vie privée (Cour EDH, 3^e^ sect., 3 févr. 2015, *Pruteanu c. Roumanie*, n^o^ 30181/05).

62 En second lieu, cette information est généralement exigée en droit de l'Union en matière de protection des données personnelles, même si celle-ci peut être décalée dans le temps pour ne pas compromettre les objectifs du traitement concerné.

63 L'article 12 du RGPD exige des responsables de traitement qu'ils facilitent l'exercice des droits des personnes concernées. En application du principe de transparence, les personnes concernées doivent donc être informées, y compris lorsque les données sont obtenues auprès d'un tiers, en application de l'article 14. Ce délai peut ne pas s'appliquer lorsque ladite communication est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs du traitement. En de tels cas, la communication des informations doit être faite dès que cette communication n'est plus de nature à compromettre les objectifs du traitement. C'est l'interprétation que font les autorités de contrôle en la matière (sous l'égide de la directive 95/46). Dans son avis 1/2006 du 1^er^ février 2006, le Groupe de travail de l'article 29 considérait que, « *lorsqu'il y a un risque sérieux que cette notification compromette la capacité de la société d'enquêter efficacement sur les faits*

allégués ou de collecter les preuves nécessaires, l'information de la personne mise en cause peut être retardée aussi longtemps que ce risque existe. Cette exception à la règle de l'article 11 vise à sauvegarder les preuves en empêchant leur destruction ou leur modification par la personne mise en cause. Elle doit s'appliquer de manière restrictive, au cas par cas, et doit tenir compte des intérêts plus larges qui sont en jeu. » [annexe n° **A.2**]

64 Enfin, il serait pour le moins curieux que la conciliation retenue par le Parlement européen et le Conseil, pour les traitements des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, ne soit pas également équilibrée dans le contexte de traitements des données à caractère personnel par les autorités administratives à des fins de sauvegarde des intérêts fondamentaux de la nation.[14] En effet, à cet égard, l'article 12 de la directive 2016/680 prévoit « *des mesures raisonnables pour fournir toute information visée à l'article 13 [...] à la personne concernée d'une façon concise, compréhensible et aisément accessible, en des termes clairs et simples* ». L'article 13 de cette directive prévoit bien que des mesures législatives peuvent être adoptées « *visant à retarder ou limiter la fourniture des informations à la personne concernée [...] ou à ne pas fournir ces informations* », mais ces modalités peuvent uniquement s'appliquer « *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* ». Il importe, en tout état de cause, que cette exception reçoive une interprétation stricte et que la charge de la preuve de la nécessité de déroger à l'obligation d'information repose sur les autorités, afin de ne pas priver d'effet utile la règle posée par l'article 13, aux paragraphes 1 et 2.

65 En troisième et dernier lieu, l'information de la personne concernée est considérée comme une garantie de l'effectivité du recours en droit international. Dans l'arrêt *Zakharov* précité, la grande chambre de la Cour européenne des droits de l'homme a rappelé au sujet des mesures de surveillance secrète que « *lorsque la surveillance a cessé, la question de la notification a posteriori de mesures de surveillance est indissolublement liée à celle de l'effectivité des recours judiciaires et donc à l'existence de garanties effectives contre les abus des pouvoirs de surveillance* » (§234). De fait, « *la personne concernée [par la surveillance] ne peut guère, en principe, contester rétrospectivement devant la justice la légalité des mesures prises à son insu, sauf si on l'avise de celles-ci (Cour EDH, Plén., 6 sept. 1978,* Klass c. All.*, n° 5029/71, §57, et Cour EDH, 3e sect., 29 juin 2006,* Weber c. All.*, n° 54934/00, §135) ou si — autre cas de figure —, soupçonnant que ses communications font*

14. Sur la portée de cette notion des intérêts fondamentaux de la nation et, notamment, sur son inclusion d'une partie du champ du droit pénal, voir notes de bas de page 10, 11 et 12 page 6.

ou ont fait l'objet d'interceptions, la personne a la faculté de saisir les tribunaux, ceux-ci étant compétents même si le sujet de l'interception n'a pas été informé de cette mesure (Cour EDH, 4^e^ sect., 18 mai 2010, Kennedy c. R-U*, n^o^ 26839/05, §167]).* » (Ibid.).

66 De même, le Commissaire aux droits de l'Homme du Conseil de l'Europe, dans un mémorandum du 17 mai 2016, se prononçait en faveur d'un système de notification des personnes soumises à une surveillance, dès le moment où cette surveillance n'est plus compromise (paragraphe 25 [annexe n° **A.3**]).

67 En conclusion, l'exigence de notifier des informations à la personne concernée, dès lors que cette notification ne compromet plus les enquêtes des autorités compétentes, répond d'une conciliation équilibrée entre la sauvegarde de la sécurité nationale et le droit au recours. Une telle exigence serait d'ailleurs cohérente avec le droit de l'Union en matière de protection des données à caractère personnel, lequel doit être équivalent dans tous les États membres depuis l'entrée en application du RGPD. Enfin, une telle exigence serait compatible avec le droit international.

Par ces motifs, la partie intervenante propose à la Cour les réponses suivantes :

Aux premières questions des affaires C-511/18 et C-512/18

L'article 15, paragraphe 1, de la Directive 2002/58, lu à la lumière de la Charte, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale prévoyant, aux fins d'assurer la sécurité, une conservation généralisée et indifférenciée de données de connexion de tous les abonnés et utilisateurs imposée aux fournisseurs, nonobstant les garanties et contrôles dont sont assortis le recueil et l'utilisation subséquentes de ces données et nonobstant le contexte marqué par des menaces graves et persistantes pour la sécurité nationale.

À la deuxième question de l'affaire C-511/18

L'article 15, paragraphe 1, de la Directive 2002/58, lu à la lumière de la Charte, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale régissant le recueil en temps réel des données relatives au trafic et à la localisation d'individus déterminés affectant les droits et obligations des fournisseurs d'un service de communications électroniques, sans limiter ce recueil à des finalités justifiant la gravité de l'ingérence causée par un tel recueil, et sans soumettre ce recueil à l'autorisation préalable d'une juridiction ou d'une autorité administrative indépendante dans une fonction quasi-juridictionnelle.

À la troisième question de l'affaire C-511/18

L'article 15 de la Directive 2002/58, lu à la lumière des articles 7, 8 et 47 de la Charte, et lu en combinaison avec l'article 22 de la Directive 95/46, l'article 79 du RGPD ou l'article 54 de la Directive 2016/680, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale régissant le recueil par des autorités nationales de données de connexion se rapportant à une ou plusieurs personnes, sans prévoir d'informer les personnes concernées dès le moment où cette communication n'est plus susceptible de compromettre les enquêtes menées par ces autorités.

HUGO ROY
AVOCAT AU BARREAU DE PARIS

Annexes

(A) — 1. Conclusions de M. Édouard Crépey, rapporteur public au Conseil d'État, de la séance du 11 juillet 2018 des 10e et 9e chambres réunies, des affaires nos 393099, 394924, 394922, 394925, 397844 et 397851, *French Data Network et autres* (réf. supra, point 16 page 7) ..... *p. 21-37*

2. Avis 1/2006 relatif à l'application des règles de l'UE en matière de protection des données aux mécanismes internes de dénonciation des dysfonctionnements dans les domaines de la comptabilité, des contrôles comptables internes, de l'audit, de la lutte contre la corruption et la criminalité bancaire et financière, adopté le 1er février 2006 par le groupe de travail « Article 29 » sur la protection des données (réf. supra, point 63 page 17) ..... *p. 38-57*

3. *Memorandum on surveillance and oversight mechanisms in the United Kingdom*, du 17 mai 2016, du Commissaire aux droits de l'homme, Conseil de l'Europe (réf. supra, point 66 page 18) ..... *p. 58-68*