ALEXIS FITZJEAN Ó COBHTHAIGH
Avocat au Barreau de Paris
5, rue Daunou - 75002 PARIS
Tél. 01.53.63.33.10 - Fax 01.45.48.90.09
afoc@afocavocat.eu

CONSEIL D'ÉTAT

SECTION DU CONTENTIEUX

OBSERVATIONS COMPLÉMENTAIRES

POUR : **1/ La Quadrature du Net**
2/ French Data Network
3/ La Fédération des fournisseurs d'accès à Internet associatifs
4/ Igwan.net

CONTRE : **1/ Le Premier ministre**
2/ Ministre de l'intérieur
3/ Ministre des armées

Sur :

1. la requête n° 393.099 demandant l'annulation de la décision implicite de rejet de la demande d'abrogation de l'article R. 10-13 du code des postes et des communications électroniques et du décret n° 2011-219 du 25 février 2011 ;
2. la requête n° 394.922 demandant l'annulation du décret 2015-1185 du 28 septembre 2015 relatif à la désignation des services spécialisés de renseignement ;
3. la requête n° 394.925 demandant l'annulation du décret 2015-1211 du 1er octobre 2015 relatif au contentieux sur les techniques de renseignement ;
4. la requête n° 397.844 demandant l'annulation du décret 2015-1639 du 11 décembre 2015 relatif à la désignation des services autres que les services spécialisés ;
5. la requête n° 397.851 demandant l'annulation du décret 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement.

Table des matières

FAITS

1. Le 6 mai 2015, La Quadrature du Net, French Data Network et la Fédération des fournisseurs d'accès à Internet associatifs ont demandé au gouvernement d'abroger l'article R. 10-13 du CPCE et le décret n°2011-219 comme étant contraires à la Charte des droits fondamentaux de l'Union européenne (Charte de l'UE) et à la directive 2002/58/CE de l'Union européenne (directive 2002/58). Le 6 juillet 2015, tacitement, le Gouvernement a refusé de les abroger.

2. Le 1er septembre 2015, ces trois associations ont demandé au Conseil d'État d'annuler pour excès de pouvoir la décision implicite de rejet résultant du silence gardé par le Premier ministre sur leurs demandes.

3. Le 30 novembre 2015, ces trois associations ont aussi demandé au Conseil d'État d'annuler pour excès de pouvoir le décret n° 2015-1185 du 28 septembre 2015 portant désignation des services spécialisés de renseignement et le décret n° 2015-1211 du 1er octobre 2015 relatif au contentieux de la mise en oeuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État.

4. Le 11 mars 2016, ces trois associations ont demandé au Conseil d'État d'annuler pour excès de pouvoir le décret n° 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement.

5. Ce même 11 mars 2016, l'association Igwan.net a demandé au Conseil d'Etat d'annuler pour excès de pouvoir le décret n° 2015-1639 du 11 décembre 2015 relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques de renseignement.

6. Le 27 juillet 2018, sur l'ensemble de ces affaires, le Conseil d'État a décidé de transmettre à la Cour de justice de l'Union européenne cinq questions préjudicielles.

7. Le 6 octobre 2020, dans les affaires C-511/18, C-512/18 et C-520/18, le Cour a rendu en grande chambre un arrêt pour répondre à ces questions.

8. Le 21 janvier 2021, le Premier Ministre a produit un mémoire en défense devant le Conseil d'État tendant en substance à priver d'effet l'arrêt de la Cour de justice.

DISCUSSION

1 Applicabilité du droit de l'Union

En conclusion, l'applicabilité du droit de l'Union et les conséquences qu'en donne la Cour de justice dans la présente affaire ne sauraient être écartées de façon légitime. Surtout, tel que la partie suivante le démontre, une décision aussi illégitime ne serait pas même justifiée en opportunité : si la CJUE a invalidé le régime de conservation généralisé des données, c'est notamment car il est bien peu utile en pratique.

2 Conservation généralisée des données de connexion

9. L'article R. 10-13 du code des postes et des communications électronique et le décret n° 2011-219 du 25 février 2011 imposent un régime de conservation généralisée de données aux fournisseurs d'accès à Internet et aux hébergeurs de contenus.

10. En répondant aux questions préjudicielles posées par les requérantes dans son arrêt rendu le 6 octobre 2020, la CJUE a démontré l'illégalité manifeste de ce régime de conservation imposée par le droit français aux opérateurs (I) ainsi qu'aux hébergeurs (II).

2.1 Conservation imposée aux opérateurs

La conservation imposée aux opérateurs ne respecte pas le droit de l'Union européenne en ce qu'elle repose sur des finalités de collecte trop larges (A), n'est

encadrée par aucune garantie suffisante (B), ni ne fait l'objet d'un contrôle effectif (C).

2.1.1 Finalités excessives

Le droit français prévoit un régime de conservation généralisée pour des finalités dépassant largement celles conformes à la Charte.

11. En droit, les articles 7, 8 et 52 de la Charte, interprétés par la CJUE, exige que toute mesure de surveillance réponde « à des **critères objectifs**, établissant un rapport entre les données à conserver et l'objectif poursuivi » (Tele2, § 110). Ces conditions doivent « s'avérer, en pratique, de nature à délimiter effectivement l'ampleur de la mesure et, par suite, le public concerné » (Tele2, § 110).

12. Ainsi, la Cour a pu considérer qu'une réglementation nationale prévoyant la conservation généralisée et indifférenciée des données de connexion, en vue de lutter contre la criminalité grave, « excède les limites du strict nécessaire et ne saurait être considérée comme étant justifiée dans une société démocratique » (Tele2,point 107).

13. Cette solution est reprise par la Cour dans son arrêt de réponse au Conseil d'État : une conservation des données de connexion ne peut être mis en oeuvre par les opérateurs de communications électroniques sur l'ensemble des leurs utilisateurs que si « il existe des circonstances suffisamment concrètes permettant de considérer que l'État membre concerné fait face à une **menace grave** [...] pour la sécurité nationale qui s'avère **réelle et actuelle ou prévisible** » (LQDN, § 137), étant entendu que de telles menaces « se distinguent, par leur nature et leur particulière gravité, du risque général de survenance de tensions ou de troubles, même graves, à la sécurité publique » (idem, § 136).

14. La Cour insiste : « eu égard à la gravité de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte résultant d'une telle mesure de conservation généralisée et indifférenciée des données, il importe d'assurer que le recours à celle-ci soit effectivement limité aux situations dans lesquelles il existe une menace grave pour la sécurité nationale » (idem, § 139). Cette exigence ne

connaît qu'un relâchement unique : la conservation « des seules adresses IP attribuées à la source d'une connexion » qui, elle et elle seule, est permise pour lutter contre la criminalité grave en plus des atteintes à la sécurité nationale (idem, §§ 155 et 156).

15. En l'espèce, l'article L34-1, III, du CPCE définit les finalités qui permettent au gouvernement d'imposer une obligation de conservation généralisée aux opérateurs de communication électronique :

- la recherche, la poursuite et la constatation des infractions pénal en général ;
- "un manquement à l'obligation définie à l'article L. 336-3 du code de la propriété intellectuelle", c'est à dire pour la lutte par la Haute autorité pour la diffusion des œuvres et la protection des droits sur internet (HADOPI) contre les personnes échouant à sécuriser leur accès à Internet qui a permis le partage d'une œuvre protégé par le droit d'auteur ;
- "les besoins de la prévention des atteintes aux systèmes de traitement automatisé de données prévues et réprimées par les articles 323-1 à 323-3-1 du code pénal".

16. Ces finalités sont particulièrement larges et ne répondent à aucun critère objectif permettant de limiter l'étendue de l'ingérence dans les droits fondamentaux consacrés par la Charte. De plus, aucune de ces finalités ne répond à un objectif de défense de la sécurité nationale tel que visé par la Cour dans son arrêt du 6 octobre 2020.

17. Par ailleurs, l'article 6, 8, II, de la LCEN prévoit que les fournisseurs d'accès à Internet « détiennent et conservent les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires », sans que cette obligation ne soit limitée par la moindre finalité. Le décret 2011-219 qui applique cette disposition n'apporte lui non-plus aucune précision quant à la finalité poursuivie.

18. **En conclusion**, les dispositions attaquées permettent la conservation des données de connexions de l'ensemble de la population pour des finalités absentes ou contraires aux articles 7, 8 et 52 de la Charte et doivent être annulés de ce seul fait.

2.1.2 Défaut de nécessité

19. Dans son mémoire en défense, le Premier Ministre invite le Conseil d'État à ignorer l'arrêt de la CJUE afin d'instaurer une conservation généralisée et constante des données de connexion. Il tente de justifier une demande aussi radicale par la nécessité opérationnelle qu'aurait cette conservation pour les activités de l'État. Pourtant, pour démontrer cette nécessité, il se contente d'une succession d'affirmations abstraites et hypothétiques, non-fondées sur des faits, et dont l'essentiel peut être démontré comme étant fausses ou obsolètes.

20. **En premier lieu**, le gouvernement prétend que « seule une telle conservation donne aux services de renseignement et d'investigations judiciaires une capacité d'analyse rétrospective de données de connexion afférentes aux communications passées par une personne ». Il précise que « l'accès au données de trafic et de localisation des communications qu'une personne a passées au cours des mois précédents permet de dresser un portrait précis de son réseau relationnel comme de ses déplacements. Or cet accès n'est disponible qu'à la condition que ces données n'aient pas été détruites par les opérateurs qui ont dû les traiter pour acheminer les communications ».

21. Il est faux de prétendre que seule l'accès aux données traités par les opérateurs permet d'analyser rétrospectivement les communications.

22. Il est de plus en plus répandu que la police accède au données enregistrées sur le téléphone des personnes mises en cause. Une fois saisies, ces données suffisent largement pour analyser rétrospectivement les communications sur plusieurs semaines ou mois. Si, en théorie, l'accès à ces données est conditionné au fait que la personne ne les a pas supprimé de son téléphone avant d'être saisi, en pratique, supprimer ses données efficacement et à une fréquence suffisante est une opération technique complexe et peu accessible. Sur le terrain, ce risque de suppression des données est suffisamment marginal pour convaincre l'État d'investir de plus en plus de ressources dans des appareils de collecte.

23. Dans un entretien de 2019, la cheffe du pôle central d'analyse des traces technologiques de la police nationale expliquait, au sujet de l'outil fourni par la société Cellebrite : « avec ce kiosque qui sera installé dans les commissariats de pre-

mier niveau, il suffira de brancher le téléphone et toutes les données seront extraites pendant la garde à vue : SMS, photos géolocalisées… [...] L'an prochain, cent nouvelles machines seront installées en Île-de-France et dans le Sud. En tout, cinq cents machines doivent être installées d'ici 2024, pour un coût de quatre millions d'euros. Nous l'avons déjà testé lors du G7, pour traiter les téléphones des personnes gardées à vue, et les retours ont été très positifs » (Reporterre, 21 novembre 2019, « Nous avons visité Milipol, le salon de la répression »). En tout, l'État a conclut deux marchés publics pour déployer et maintenir ces kiosques, pour un coût total de 7 millions d'euros (Streetpress, 20 janvier 2020, « Bientôt dans presque tous les commissariats, un logiciel pour fouiller dans vos portables »).

24. Ainsi, les services d'investigation judiciaire, comme ceux de renseignement, peuvent d'ores et déjà se passer entièrement et de plus en plus facilement des données conservées par des opérateurs afin d'analyser rétrospectivement les communications d'une personne.

25. **En deuxième lieu**, il est tout aussi faux de prétendre qu'il faudrait contraindre les opérateurs pour que ceux-ci conservent des données exploitables par l'administration.

Au contraire, plus les années passent et plus les usages d'Internet évoluent vers une plus grande diversité de données de communication disponibles. Les utilisateurs ont recours à de plus en plus des services différents (messageries instantanées, email, réseaux sociaux) qui collectent et conservent volontairement des données pour leurs propres besoins, notamment techniques. Ainsi, entre 2017 et 2019, la proportion de la population française qui « échange des messages via des applications » est passée de 43 % et 62 % et celle qui « téléphone via des applications » de 31 % à 51 % (ARCEP, Baromêtre du numérique de 2019). La multiplication du nombre d'intermédiaires auprès de qui l'administration peut obtenir des données de connexion diminue mécaniquement la nécessité de s'assurer que ceux-ci conservent le plus longtemps possibles les données qu'ils exploitent.

26. Ainsi, les services d'investigation judiciaire, comme ceux de renseignement, ont de moins en moins besoin de contraindre les intermédiaires pour que ceux-ci conservent des données de communication utiles à leurs enquêtes.

27. **En troisième lieu**, le Premier Ministre présente comme étant toujours d'actualité une appréciation que le Conseil d'État avait donnée dans sa décision de juillet 2018, selon laquelle la conservation généralisée présentait « une utilité sans équivalence par rapport » aux autres techniques de renseignement.

28. Pourtant, la situation a largement évolué depuis 2018, tel que le constate la CNCTR deux années plus tard, en juin 2020, dans son 4ème rapport d'activité. Elle détaille que le nombre de demandes d'accès aux données de connexion a baissé de 20 % au cours des deux dernières années observées (passant de 48 000 à 40 000) tandis que les autres techniques de renseignement continuent de croître à des taux importants (de 8 800 à 12 500 pour les interceptions, de 3 700 à 7 600 pour la géolocalisation et de 9 300 à 13 700 pour les « autres techniques »).

29. Ici encore, les faits montrent que l'obligation de conservation généralisée est de moins en moins utile au fur et à mesure que les années passent, les services de renseignement diversifiant les types de techniques auxquelles ils recourent.

30. **En conclusion**, la demande radicale du Premier Ministre n'est soutenue en opportunité que par des affirmations abstraites qui ne résistent pas à la confrontation des faits. La conservation généralisée et constante des données de connexion est beaucoup moins utile qu'il ne voudrait le présenter. C'est précisément car cette conservation n'est pas strictement nécessaire aux activités de l'État que la Cour de justice s'est permise de l'interdire.

2.1.3 Garanties insuffisantes

Régime généralisé

31. Dans son arrêt du 6 octobre 2020, la Cour de justice impose un cadre précis concernant la possibilité pour les États membres de recourir à la conservation des données de connexion, qu'il convient de confronter aux mesures permises par le droit français.

32. **En droit**, en plus de la condition tenant à la présence d'une menace grave pour la sécurité nationale mentionnée ci-dessus, la conservation préventive des don-

nées de l'ensemble des utilisateurs des moyens de communications électroniques ne peut être initiée que par une injonction spécifique des autorités aux opérateurs, celle-ci devant en outre être temporellement limitée au strict nécessaire (§138 LQDN).

33. Ensuite, la Cour ajoute que seuls les cas où une menace grave à la sécurité nationale persisterait permettent de renouveler l'injonction sans que la durée de chaque injonction ne dépasse un laps de temps prévisible (LQDN, même paragraphe).

34. La Cour conclut de façon limpide que de façon générale « cette conservation ne saurait présenter un caractère systématique ».

35. **En l'espèce**, les article L34-1 et R. 10 13 du CPCE prévoient un régime de conservation généralisée et illimité dans le temps des données de connexion de l'ensemble des utilisateurs de moyens de communications électronique en France, applicables systématiquement, en toutes circonstances et en tous lieux.

36. Ainsi, il apparaît clairement que les règles et limitations du régime français ne sont pas circonscrites à une période temporelle, ni à un contexte de menace grave à la sécurité nationale susceptible de fonder une injonction prise par le pouvoir administratif ou le législateur. Au contraire, la conservation de données de connexion peut être mise en oeuvre pour tout motif, et sur toute personne peu importe qu'il existe ou non un indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain avec une menace grave à la sécurité nationale telle qu'envisagée par la Cour. Ce régime impose donc la conservation des données de connexion de la quasi-totalité de la population française sans être soumise à une exigence de nécessité.

37. **En conclusion**, les règles et limitations des régimes français sont largement insuffisantes et incompatibles avec les exigences de stricte nécessité que le respect de la Charte demande. Les dispositions attaqués mettent en oeuvre un régime généralisé de conservation préventive des données de connexion sans garanties suffisantes telles que prévues par les articles 7, 8 et 52 de la Charte et doivent être annulés de ce seul fait.

Conservation des adresses IP

38. Dans son arrêt, la Cour de justice apporte des précisions sur la collecte des adresses IP de l'ensemble des personnes physiques susceptible d'être mise ne oeuvre par les pouvoirs publics. La Cour impose ainsi qu'une telle conservation réponde à des garanties spécifiquement et précisément limitées, à savoir que cette possibilité soit utilisée uniquement pour attribuer ces adresses « à la source d'une connexion ». De plus, la conservation doit être limitée au strict respect des conditions matérielles et procédurales devant régir l'utilisation de ces données.(§155)

39. Pour la Cour de justice, « seule la lutte contre la criminalité grave et la prévention des menaces graves contre la sécurité publique sont de nature, à l'instar de la sauvegarde de la sécurité nationale », à justifier une telle ingérence (§156).

40. Outre la finalité pouvant justifier une telle collecte, la Cour insiste sur le fait que « la durée de conservation ne saurait excéder celle qui est strictement nécessaire au regard de l'objectif poursuivi » et qu'une « mesure de cette nature doit prévoir des conditions et des garanties strictes quant à l'exploitation de ces données, notamment par un traçage, à l'égard des communications et des activités effectuées en ligne par les personnes concernées » (§156).

41. **En l'espèce**, le CPCE prévoit la collecte généralisée des adresses IP de l'ensemble de la population, pour une durée minimum d'une année, pour la recherche de toutes infractions pénales, même banales. En outre, le droit français ne prévoit aucune aucune garantie permettant d'éviter tout abus dans l'exploitation de ces données par les autorités publiques, qui peuvent ainsi utiliser ces données dans le cadre d'enquêtes qui ne se rapporte ni à la sauvegarde de la sécurité nationale, ni à la lutte contre la criminalité grave ni encore à la prévention des menaces graves contre la sécurité publique. Comme cela est démontré ci-après, aucun contrôle n'existe concernant l'utilisation ultérieure des données de connexion collectées dans le cadre du régime de l'article L34-1 du CPCE.

42. Une telle absence de garantie et d'encadrement implique nécessairement que ce régime de conservation des adresses IP est contraire à la protection accordée par la Charte, et doit être annulé de ce seul fait.

2.1.4 Défaut de contrôle effectif

En matière de surveillance administrative, le droit français opère une distinction claire entre le recueil des données de connexion et leur utilisation ultérieure. Aucun de ces deux types de traitement n'est soumis à des garanties suffisantes ou à un contrôle effectif.

43. L'article 8, paragraphe 3, de la Charte prévoit que « le respect [des règles sur la protection des données] est soumis au contrôle d'une autorité indépendante ». En matière de données de connexion, cela implique que « il est essentiel que l'accès des autorités nationales compétentes aux données conservées soit, en principe, sauf cas d'urgence dûment justifié, 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 » (Tele2, § 120).

44. En l'espèce, aucun contrôle par une juridiction ou une autorité administrative indépendante n'est organisé dans le système français. Tout au plus les articles L. 821-1 et L. 851-1 du code de la sécurité intérieure donnent-ils à la Commission nationale de contrôle des techniquesde renseignement (CNCTR) un pouvoir d'avis lorsque les services de renseignement souhaitent accéder aux données de connexion

==> reprendre passage Arthur dans l'autre mémoire sur le controle effectif

2.2 Conservation imposée aux hébergeurs

45. En France, l'article 6 de la LCEN lu en combinaison avec le décret n°2011-219 du 25 février 2011 impose une conservation des données de connexion aux fournisseurs d'accès à des services de communication au public en ligne et aux fournisseurs de services d'hébergement de contenus.

46. Dans son arrêt du 6 octobre 2020, la Cour de justice tranche la question de la légalité d'une telle obligation de conservation des données de connexion au regard du droit de l'Union européenne.

47. La question préjudicielle soumise à la Cour et objet de l'arrêt du 6 octobre porte sur la conservation des données incluant « notamment, les données relatives à l'identité civile des personnes ayant fait usage de ces services, tels que leurs nom, prénom, leurs adresses postales associées, leurs adresses de courrier électronique ou de compte associées, leurs mots de passe et, lorsque la souscription du contrat ou du compte est payante, le type de paiement utilisé, la référence du paiement, le montant ainsi que la date et l'heure de la transaction" ainsi que "les identifiants des abonnés, des connexions et des équipements terminaux utilisés, les identifiants attribués aux contenus, les dates et heures de début et de fin des connexions et des opérations ainsi que les types de protocoles utilisés pour la connexion au service et pour le transfert des contenus ».(§195 et 196).

48. Ces données constituant à la fois des données à caractère personnel couvert par les règles du règlement 2016/679 (le "RGPD") et des données de connexion dont le régime est prévu parla directive 2002/58, la Cour en déduit que l'obligation de conservation des données par les fournisseurs d'accès à des services de communication au public en ligne et les fournisseurs de services d'hébergement visés par l'article 6 de la LCEN doit être régie soit par l'un ou l'autre de ces deux textes, lus à la lumière articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte. Plus précisément, ce sont les articles prévoyant des limitations aux droits conférés par le RGPD et la directive 2002/58, au titre notamment de la sécurité nationale, qui sont mobilisés dans le raisonnement de la Cour afin de déterminer si la conservation de données peut être considérée comme conforme au droit de l'Union (§202).

49. En premier lieu, la Cour distingue, parmi les acteurs concernés en droit français par cette obligation, ceux fournissant des services pouvant être couverts par la directive 2002/58 "dès lors qu'ils consistent entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques" (§204 et 205). Tel est le cas des fournisseurs "d'accès à des services de communication au public en ligne" visés par la LCEN, qui peuvent être considérés comme relevant de la qualification de "services de communication électronique" au sens de la directive 2002/58.

50. La Cour assimile alors ces services à ceux des fournisseurs "au public de services de communications électroniques" visés par l'article L34-1 du CPCE. Ayant déjà répondu sur la légalité de la conservation de données de connexion par ces opérateurs aux premières questions dans les affaires C-511/18 et C-512/18 ainsi

qu'aux première et deuxième questions dans l'affaire C-520/18, la Cour considère que l'ensemble des constations et appréciations faites dans le cadre de ces réponses s'applique à ce premier type de services visés par l'article 6 de la LCEN.

51. Dès lors, les mêmes conclusions doivent être tirés concernant l'illégalité du régime généralisé et illimité de conservations des données de connexion, aussi bien au regard de l'absence de proportionnalité (voir §§ ci dessus fixme) que de l'absence de garanties suffisantes concernant sa mise en oeuvre (voir §§ ci dessus fixme). Un tel régime imposé aux fournisseurs "d'accès à des services de communication au public en ligne" est, déjà, contraire au droit de l'UE.

52. En second lieu, la Cour se penche sur la légalité de la conservation des données par les acteurs ne relevant pas de la qualification de "services de communication électronique" au sens de la directive 2002/58 et dont la collecte imposée de données doit être appréciée au regard des dispositions du RGPD. En effet, puisqu'une telle collecte de données constitue un traitement de données personnelles couvert par le RGPD, la protection accordée par ce texte ne peut être limitée que par les cas prévus à l'article 23, §1 du RGPD et dans le respect des conditions prévues à l'article 23,§2 de ce même texte.

53. Cet article 23,§2 prévoit que toute mesure limitant la portée des droits protégés par le RGPD doit contenir des " dispositions spécifiques relatives, au moins, le cas échéant :

- a) aux finalités du traitement ou des catégories de traitement ;
- b) aux catégories de données à caractère personnel ;
- c) à l'étendue des limitations introduites ;
- d) aux garanties destinées à prévenir les abus ou l'accès ou le transfert illicites ;
- e) à la détermination du responsable du traitement ou des catégories de responsables du traitement ;
- f) aux durées de conservation et aux garanties applicables, en tenant compte de la nature, de la portée et des finalités du traitement ou des catégories de traitement ;
- g) aux risques pour les droits et libertés des personnes concernées ; et
- h) au droit des personnes concernées d'être informées de la limitation, à moins que cela risque de nuire à la finalité de la limitation."

54. La Cour de justice explique en conséquence que tout traitement de données personnelles mis en oeuvre en application des dérogations prévues par l'article 23 du RGPD ne peut "porter atteinte au respect de la vie privée, en méconnaissance de l'article 7 de la Charte, tout comme aux autres garanties prévues par celle-ci". La Cour précise qu' "en particulier, à l'instar de ce qui vaut pour l'article 15, paragraphe 1, de la directive 2002/58, le pouvoir que confère l'article 23, paragraphe 1, du règlement 2016/679 aux États membres ne saurait être exercé que dans le respect de l'exigence de proportionnalité, selon laquelle les dérogations à la protection des données à caractère personnel et les limitations de celles-ci doivent s'opérer dans les limites du strict nécessaire" (§210).

55. Ainsi, la Cour en conclut que le droit de l'Union européenne doit être interprété "en ce sens qu'il s'oppose à une réglementation nationale imposant aux fournisseurs d'accès à des services de communication au public en ligne et aux fournisseurs de services d'hébergement la conservation généralisée et indifférenciée, notamment, des données à caractère personnel afférentes à ces services."

56. Un tel constat par la Cour signifie que l'application du RGPD empêche toute conservation généralisée de données de connexion, dès lors qu'une telle conservation ne respecte ni les dispositions de l'article 23 du RGPD ni la protection accordée par la Charte.

57. En l'occurence, l'article 6, II, de la LCEN qui prévoit la mise en oeuvre d'un traitement de données personnelles par la conservation des données « de nature à permettre l'identification de quiconque a contribué à la création » de contenu d'un service de communication au public en ligne, ne respecte pas les critères de proportionnalité et de limitation au strict nécessaire prévus par le RGPD et la Charte.

58. En application du raisonnement tenu par la Cour, le caractère généralisé de la collecte de données imposée aux services d'hébergement, ainsi que l'absence de toute garantie encadrant la collecte et l'exploitation de ces données, doivent être considérés comme incompatibles avec les exigences du droit de l'Union européenne.

59. Les dispositions de l'article 6 de la LCEN lues en combinaison avec le décret n°2011-219 du 25 février 2011 doivent donc être annulées.

3 Collecte de renseignements

3.1 Finalités poursuivies

60. Le droit français permet de surveiller la population pour des finalités dépassant largement celles conformes à la Charte des droits fondamentaux de l'Union européenne (ci-après « la Charte »).

61. **En droit**, les articles 7, 8 et 52 de la Charte, interprétés par la Cour de justice de l'Union, exige que toute mesure de surveillance réponde « *à des **critères objectifs**, établissant un rapport entre les données à conserver et l'objectif poursuivi* » (*cf.* CJUE, 21 décembre 2016, *Tele2 Sverige*, aff. C-203/15, § 110).

62. Surtout, la Cour exige que les mesures de surveillance (au-delà des démarches les plus triviales telles que le traitement de l'état civil) soient **limitées à la « *lutte contre la criminalité grave* » et à la défense de la « *sécurité nationale* »** (*cf.* CJUE, *Tele2 Sverige*, préc., § 102 ; CJUE, 6 octobre 2020, *La Quadrature du Net e.a.*, aff. C-511/18, §§ 137, 146, 156, 163 et 177).

63. **En l'espèce**, les décrets attaqués ont été pris pour l'application du livre VIII du code de la sécurité intérieure (CSI), dont l'essentielle des mesures de surveillance peuvent être réalisées pour l'une des nombreuses finalités listées à son article L. 811-3, telles que :

— la défense des « *intérêts majeurs de la **politique étrangère*** », ces intérêts étant définis par le Gouvernement ;

— « *l'exécution des **engagement européens et internationaux** de la France* », notamment l'application des normes de l'Union européenne sur l'agriculture, la pêche, les transports, l'emploi, la culture ou le tourisme ainsi que les accords internationaux tels que l'accord de Paris de 2015 sur le climat ou la Convention de Genève de 1931 sur le droit de timbre en matière de chèque ;

— la défense des « ***intérêts économiques, industriels** et scientifiques de la France* », qui permet l'espionnage industriel et scientifique ;

— les prévention des « *violences collectives de nature à porter gravement atteinte à la paix publique* », couvrant notamment la lutte contre les **manifes-**

tations, même non violentes, n'ayant pas été déclarées ou ayant fait l'objet d'une déclaration incomplète (voir la décision DC 2015-713 du Conseil constitutionnel français qui, à son considérant 10, renvoie aux articles 431-1 à 431-10 du code pénal pour définir cette finalité, notamment celle prévue à l'article 431-9 du code pénal) ;

— « *la prévention de la criminalité et de la délinquance organisée* », notamment la lutte contre l'acquisition illicite de **stupéfiants**, même par un individu seul qui n'agit pas en groupe (voir la décision DC 2015-713 du Conseil constitutionnel qui renvoie aux infractions listées à l'article 706-73 du code de procédure pénale pour définir cette finalité, notamment celle prévue à l'article 222-37 du code pénal).

64. Nombre de ces finalités sont particulièrement larges ou laissées à l'appréciation discrétionnaire de l'administration, ne répondant à **aucun critère objectif** permettant de délimiter effectivement l'ampleur des mesures de surveillance. Il en va notamment de la défense des « *intérêts majeurs de la politique étrangère* », de « *l'exécution des engagements européens et internationaux* » ou de la défense des « *intérêts économiques, industriels et scientifiques* » de la France.

65. D'autres finalités concernent la lutte contre des infractions qui ne relèvent pas de la criminalité grave. Il en va notamment de la lutte contre les manifestations non déclarées ou l'acquisition de stupéfiants à titre individuel. De même, aucune des finalités évoqués ci-avant ne relève de la défense de la sécurité nationale.

66. **En conclusion**, les décrets attaqués ont été pris pour l'application de dispositions législatives autorisant la surveillance de la population pour des finalités contraires aux articles 7, 8 et 52 de la Charte et doivent être annulés de ce seul fait.

3.2 Techniques de collecte

67. La Cour de justice de l'Union européenne apporte des précisions quant à l'encadrement de certaines techniques de surveillance permises par le CSI.

3.2.1 Accès aux données de connexion

68. Dans son arrêt de réponse au Conseil d'État, la Cour de justice a précisé le cadre de la conservation et d'accès aux données de connexion.

69. **En droit**, les articles 7, 8 et 52 de la Charte, interprétés par la Cour, prévoient que les opérateurs de communications électroniques ne peuvent être contraints de conserver les données de connexion de l'ensemble des leurs utilisateurs que s'« *il existe des circonstances suffisamment concrètes permettant de considérer que l'État membre concerné fait face à une* ***menace grave*** [...] *pour la sécurité nationale qui s'avère* ***réelle et actuelle ou prévisible*** » (CJUE, 6 octobre 2020, *La Quadrature du Net e.a.*, préc., § 137), étant entendu que de telles menaces « *se distinguent, par leur nature et leur particulière gravité, du risque général de survenance de tensions ou de troubles, même graves, à la sécurité publique* » (même arrêt, § 136).

70. La Cour insiste : « *eu égard à la gravité de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte résultant d'une telle mesure de conservation généralisée et indifférenciée des données, il importe d'assurer que le recours à celle-ci soit effectivement limité aux situations dans lesquelles il existe une menace grave pour la sécurité nationale* » (même arrêt, § 139). Cette exigence ne connaît qu'un relâchement unique : la conservation « *des seules adresses IP attribuées à la source d'une connexion* » qui, elle et elle seule, est permise pour lutter contre la criminalité grave en plus des atteintes à la sécurité nationale (même arrêt, §§ 155 et 156).

71. Par ailleurs, la conservation des données de connexion doit résulter d'une « *injonction* [...] ***temporellement limitée*** *au strict nécessaire* » et qui « *ne saurait présenter un caractère systématique* » (même arrêt, § 138).

72. Enfin, les conditions autorisant une mesure de conservation des données de connexion déterminent **les conditions qui permettront ensuite l'accès** à ces données, la Cour expliquant concrètement qu'« *un accès à de telles données à des fins de poursuite et de sanction d'une infraction pénale ordinaire ne saurait en aucun cas être accordé lorsque leur conservation a été justifiée par l'objectif de lutte contre la criminalité grave ou, a fortiori, de sauvegarde de la sécurité nationale* »

(même arrêt, § 166).

73. **En l'espèce**, les décrets attaqués ont notamment été pris pour l'application de l'article L. 851-1 du CSI, qui autorise le recueil par l'administration des données de connexion conservées en application des articles L. 34-1 du code des postes et des communications électroniques (CPCE) ainsi que du II de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (dite « LCEN »).

74. Le CPCE et la LCEN imposent un régime de conservation généralisée de données de connexion qui, allant bien au-delà des seules adresses IP, n'est **en rien conditionné à la survenance d'une menace pour la sécurité nationale** mais, au contraire, s'applique de façon systématique, sans limitation de durée ou de circonstance. L'article L. 851-1 du CSI organise ainsi l'accès à des données conservée en violation de la Charte.

75. Même dans l'hypothèse où le régime de conservation du CPCE et de la LCEN serait limité à la survenance d'une menace pour la sécurité nationale, le régime d'accès défini par l'article L. 851-1 autorise l'ensemble des finalités listées à l'article L. 811-3 du CSI, dépassant largement la seule sécurité nationale et dépassant même la lutte contre la criminalité grave.

76. **En conclusion**, les décrets attaqués ont été pris pour l'application de dispositions législatives autorisant l'administration à accéder à une large diversité de données de connexion conservées de façon généralisée pour d'autres finalités que la défense de la sécurité nationale, en violation des articles 7, 8 et 52 de la Charte, et doivent être annulés de ce seul fait.

3.2.2 Accès en temps réel

77. Dans son arrêt de réponse au Conseil d'État, la Cour reconnaît explicitement que les articles L. 851-2 et L. 851-4 du CSI sont contraires à la Charte sur plusieurs points.

78. **En droit**, les articles 7, 8, 11 et 52 de la Charte, interprétés par la Cour, pré-

voient que « *le recueil en temps réel des données relatives au trafic et des données de localisation* [...] *ne saurait être mise en œuvre, compte tenu de son caractère particulièrement intrusif, qu'à l'égard des personnes pour lesquelles il existe une raison valable de soupçonner qu'elles sont* ***impliquées d'une manière ou d'une autre dans des activités de terrorisme*** » (CJUE, 6 octobre 2020, *La Quadrature du Net e.a.*, préc., § 188). La Cour précise : « *quant aux données des* ***personnes ne relevant pas de cette catégorie****, elles peuvent seulement faire l'objet d'un accès en temps différé* » (même arrêt, § 188).

79. Enfin, lorsque la mesure peut être réalisée, la Cour prévoit qu'« *il est essentiel que la mise en œuvre de la mesure autorisant le recueil en temps réel soit soumise à un* ***contrôle préalable*** *effectué soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un* ***effet contraignant*** » (même arrêt, § 189).

80. **En l'espèce**, l'article L. 851-4 du CSI autorise l'accès en temps réel au données de localisation pour l'ensemble des finalités prévues à l'article L. 811-3 du même code, qui ne sont **en rien limitées à la lutte contre le terrorisme**.

81. L'article L. 851-2 du CSI est, lui, limité à la lutte contre le terrorisme mais, s'il autorise l'accès en temps réel aux données de connexion des personnes « *préalablement identifiée susceptible d'être en lien avec une menace* », il autorise aussi un tel accès s'agissant de « l'*entourage* » de ces premières, quand bien même il n'existerait **aucune raison raison valable de soupçonner les membres de cet entourage** d'être impliqué d'une manière ou d'une autre dans des activités de terrorisme.

82. Enfin, si les mesures permises par les articles L. 851-2 et L. 851-4 du CSI sont, en principe, préalablement notifiée à la Commission nationale de contrôle des techniques de renseignement (CNCTR) afin que celle-ci puisse rendre un avis sur la légalité de ces mesures, cet avis est **dépourvu de tout effet contraignant**.

83. **En conclusion**, les décrets attaqués ont notamment été pris pour l'application des articles L. 851-2 et L. 851-4 du CSI, dont le champ, tant individuel que matériel, et la procédure d'autorisation sont contraires aux articles 7, 8, 11 et 52 de la Charte et doivent être annulés de ce seul fait.

3.2.3 Analyse automatisée

84. Dans son arrêt de réponse, la Cour exige que l'article L. 851-3 du CSI soit complété de conditions supplémentaires pour être conforme à la Charte.

85. **En droit**, les articles 7, 8 et 11 de la Charte, interprétés par la Cour, prévoient que « *l'ingérence particulièrement grave que constitue* » l'analyse automatisée et généralisée de données de connexion ne peut être autorisée « *que dans des situations dans lesquelles un État membre se trouve face à une* ***menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible*** » (CJUE, 6 octobre 2020, *La Quadrature du Net e.a.*, préc., § 177).

86. **En l'espèce**, la Cour a reconnu qu'il « *ressort de l'article L. 851-3 du CSI que l'analyse automatisée qu'il prévoit correspond, en substance, à un filtrage de la totalité des données relatives au trafic et des données de localisation conservées par les fournisseurs de services de communications électroniques* » (même arrêt, § 172), que cette « *analyse automatisée s'applique de manière globale à l'ensemble des personnes faisant usage des moyens de communications électroniques* » et que « *les données faisant l'objet de l'analyse automatisée sont susceptibles de révéler la nature des informations consultées en ligne* » (même arrêt, § 174).

87. L'article L. 851-3 du CSI prévoit que cette analyse peut être réalisée pour les « *besoins de la prévention du terrorisme* », sans limiter ces besoins à ceux caractérisés par une menace réelle et actuelle ou prévisible. Au contraire, en se référant à des « *besoins* » qui ne résultent d'aucun événement spécifique mais à un danger théorique diffus et constant, cette disposition **permet un renouvellement perpétuel** de la mesure.

88. Ce résultat a immédiatement été atteint en pratique : « l*e premier algorithme a donc été autorisé par le Premier ministre le 12 octobre 2017* [...] *Il est toujours en fonctionnement aujourd'hui* » (rapport du 8 juin 2020 de la commission des lois de l'assemblée nationale sur le projet de loi n° 3117). Le caractère perpétuel de la mesure s'explique par le fait que son objectif n'est pas de lutter contre une menace déjà identifiée mais, au contraire, de surveiller suffisamment de communications pour **ne pas « *risquer de passer à côté d'une menace réelle* »** (Rapport du Gouvernement du 30 juin 2020 sur l'application de l'article L. 853–1, p. 4., cité

dans le rapport de la commission des lois).

89. **En conclusion**, les décrets attaqués ont notamment été adoptés pour l'application de l'article L. 851-3 du CSI qui, en permettant une analyse automatisée et généralisée des communications en l'absence d'une menace réelle et actuelle ou prévisible contre la sécurité nationale, viole les articles 7, 8, 11 et 52 de la Charte et doivent être annulés de ce seul fait.

3.2.4 Surveillance internationale

90. La Cour n'a pas eu à se prononcer sur les articles L. 854-1 et suivants du CSI, mais ses conclusions sur les articles L. 851-1 et L. 851-3 s'appliquent *mutatis mutandis*.

91. **En droit**, les articles 7, 8, 11 et 52 de la Charte prévoient que « *l'ingérence particulièrement grave que comporte une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation* [...] *ainsi que l'ingérence particulièrement grave que constitue leur analyse automatisée ne peuvent satisfaire à l'exigence de proportionnalité que dans des situations dans lesquelles un État membre se trouve face à* ***une menace grave pour la sécurité nationale*** *qui s'avère réelle et actuelle ou prévisible* » (CJUE, 6 octobre 2020, *La Quadrature du Net e.a.*, préc., § 177).

92. De même, une « *réglementation permettant aux autorités publiques d'****accéder de manière généralisée au contenu de communications*** *électroniques doit être considérée comme portant atteinte au contenu essentiel du droit fondamental au respect de la vie privée, tel que garanti par l'article 7 de la Charte* » (CJUE, gr. ch., 6 octobre 2015, *Schrems*, aff. C-362/14, § 94).

93. **En l'espèce**, l'article L. 854-2 du CSI permet au Premier ministre de désigner des « *réseaux de communications électroniques sur lesquels il autorise l'interception des communications émises ou reçues à l'étranger* ». Ces interceptions et **la conservation des données qui en résulte se réalisent de façon généralisée et indifférenciée**, pouvant couvrir l'ensemble des communications émises ou reçues à l'étranger depuis les réseaux désignés.

94. Au fur et à mesure que les données sont accumulées, le Premier ministre peut « *délivrer une autorisation d'exploitation de communications* ». Il peut aussi « *autoriser l'exploitation non individualisée des données de connexion interceptées* » au moyen de « ***traitements automatisés*** ».

95. Les mesures d'interceptions, de conservation puis d'exploitation sont autorisées pour l'ensemble des finalités de l'article L. 811-3 du CSI, qui dépassent largement la seule lutte contre les menaces à la sécurité nationale.

96. **En conclusion**, les décrets attaqués ont notamment été adoptés pour l'application des articles L. 854-1 et suivants du CSI qui, en permettant des mesures d'interception, de conservation et d'exploitation généralisées et indifférenciées du contenu des communications et de leur données de connexion en l'absence de menace réelle et actuelle ou prévisible à la sécurité nationale, sont contraire aux articles 7, 8, 11 et 52 de la Charte et doivent être annulés de ce seul fait.

3.3 Personnes surveillées

97. Les précisions apportées par la Cour concernant la surveillance de l'entourage des personnes concernées par l'article L. 851-2 du CSI offrent un nouvel éclairage sur l'ensemble des autres mesures de surveillance qui, toutes, échouent à limiter leur champ personnel au strict nécessaire.

98. **En droit**, les articles 7, 8 et 52 de la Charte, interprétés par la Cour de justice, prévoient qu'« *un accès ne saurait, en principe, être accordé, en relation avec l'objectif de lutte contre la criminalité,* ***qu'aux données de personnes soupçonnées de projeter, de commettre ou d'avoir commis une infraction grave*** *ou encore d'être impliquées d'une manière ou d'une autre dans une telle infraction* » (CJUE, 21 décembre 2016, *Tele2 Sverige*, préc., § 119). Ce n'est que par exception que la Cour nuance : « *toutefois, dans des situations particulières, telles que celles dans lesquelles des intérêts vitaux de la sécurité nationale, de la défense ou de la sécurité publique sont menacés par des activités de terrorisme, l'accès aux données d'autres personnes pourrait également être accordé* » (même arrêt).

99. **En l'espèce**, toutes les mesures de surveillance autorisées par le livre VIII

du CSI (à l'exception de la mesure prévue à l'article L. 851-2) peuvent être réalisées contre des personnes qui ne participent à aucune menace du moment que leur surveillance est susceptible de révéler des informations utiles à la poursuite de n'importe laquelle des finalités listées à l'article L.811-3 du même code. Cette situation est la règle : elle ne dépend d'aucune « *situation particulière* » ni d'aucune circonstance exceptionnelle liée au terrorisme ou à la sécurité nationale.

100. **En conclusion**, les décrets attaqués ont notamment été adoptés pour l'application de dispositions législatives qui, en autorisant la surveillance de personnes ne présentant aucune menace en l'absence de situation particulière ou de menace exceptionnelle à la sécurité nationale, sont contraires aux articles 7, 8 et 52 de la Charte et doivent être annulés de ce seul fait.

3.4 Personnes recourant aux techniques

101. **En droit**, est contraire à la Charte une mesure de surveillance qui « *ne prévoit aucun critère objectif permettant de limiter le nombre de personnes disposant de l'autorisation d'accès et d'utilisation ultérieure des données* » (CJUE, gr. ch., 8 avril 2014, *Digital Rights Ireland et autres*, aff. C-293/12, C-594/12, § 62). Cette limitation est indispensable dans la mesure où les risques de dérives et d'abus des mesures de surveillance ainsi que la difficulté du contrôle que peut en faire une autorité indépendante sont proportionnels au nombre de personnes pouvant les mettre en œuvre.

102. **En l'espèce**, l'article L. 811-4 du CSI prévoit que le gouvernement, de son propre chef, « *désigne les services, autres que les services spécialisés de renseignement, relevant des ministres de la défense, de l'intérieur et de la justice ainsi que des ministres chargés de l'économie, du budget ou des douanes, qui peuvent être autorisés à recourir aux techniques* » prévues par ce code. Ainsi, aucune loi n'empêche le gouvernement d'étendre autant qu'il le souhaite le nombre des agents de son administration pouvant mettre en œuvre les mesures de renseignement, sans se soucier d'augmenter les risques de dérive et les difficultés du contrôle indépendant.

103. Depuis 2015, le gouvernement a déjà pris un décret n° 2015-1639 du 11

décembre 2015 et un décret n° 2017-36 du 16 janvier 2017 pour étendre considérablement le nombre de ses services (et donc de ses agents) pouvant recourir aux mesures de renseignement. En donner ici la liste, même sommaire, ne répondrait pas à la brièveté attendue par la Cour (La Quadrature du Net avait recensé ces services en 2015 dans un document joint en Annexe I).

104. **En conclusion**, les décrets attaqués ont notamment été adopté pour l'application de l'article L. 811-4 du CSI qui, permettant au gouvernement d'augmenter indéfiniment le nombre de personnes pouvant accéder aux données, viole la Charte et doivent être annulés de ce seul fait.

3.5 Contrôle indépendant

105. **En droit**, l'article 8, § 3, de la Charte prévoit que « *le respect* [des règles sur la protection des données] *est soumis au contrôle d'une autorité indépendante* ». La Cour de justice en déduit que la mise en œuvre d'une mesure de surveillance par des autorités nationales doit être « *subordonné*[e] *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* » (CJUE, 21 décembre 2016, *Tele2 Sverige*, préc., § 120). Pour les mesures intrusives, la Cour exige que cette décision soit « *dotée d'un effet contraignant* » (CJUE, 6 octobre 2020, *La Quadrature du Net e.a.*, préc., § 189).

106. De plus, l'article 58 du règlement UE n° 2016/679 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 (ci-après « RGPD ») exige que l'autorité de contrôle puisse accéder à toutes les données personnelles traitées et ordonner qu'un traitement soit mis en conformité à la loi ou prenne fin. De même, l'article 47 de la directive UE n° 2016/680 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 (ci-après directive « police-justice ») prévoit que « *chaque autorité de contrôle dispose de pouvoirs d'enquête effectifs. Ces pouvoirs comprennent au moins celui d'obtenir du responsable du traitement ou du*

sous-traitant l'accès à toutes les données qui sont traitées et que « chaque autorité de contrôle dispose de pouvoirs effectifs en matière d'adoption de mesures correctrices ».

107. **En l'espèce**, le contrôle prévu par le CSI est défaillant, qu'il s'agisse du contrôle de la collecte ou de l'exploitation des données.

3.5.1 Contrôle de la collecte

108. L'article L. 821-2 du CSI prévoit que la demande de mise en œuvre d'une technique de renseignement est formulée par le ministre de la défense, de l'intérieur, de la justice ou de l'économie au Premier ministre. L'article L. 821-3 du même code prévoit que la CNCTR, qui est l'entité indépendante du gouvernement censée contrôler ces mesures, est uniquement notifiée de la demande d'autorisation adressée au Premier ministre. La CNCTR n'a aucun pouvoir pour s'y opposer. Elle peut uniquement indiquer au Premier ministre qu'elle considère que la technique demandée est illicite puis, si le Premier ministre autorise toutefois cette mesure, saisir le Conseil d'État pour s'y opposer. La saisine du Conseil d'État ne suspend pas la mise en œuvre de la mesure et la décision du Conseil d'État peut intervenir très tard, la loi n'imposant aucun délai fixe.

109. Ainsi, en pratique, aucune autorité indépendante n'a le pouvoir d'empêcher que des renseignements ne soient collectés en violation de la loi. Aucune « *demande motivée* » n'est jamais faite auprès de la CNCTR, qui est surtout spectatrice et ne peut prendre aucune décision contraignante. Au mieux, la CNCTR peut intervenir une fois que l'atteinte à la protection de ces données a été réalisée, pour demander au Conseil d'État la suppression d'informations qui ont déjà pu être exploitées illégalement. L'action de la CNCTR intervient systématiquement après la collecte des données : il ne s'agit pas d'un contrôle préalable.

110. **En conclusion**, les décrets attaqués ont été pris pour l'application de dispositions législatives qui, en autorisant des mesures de renseignement qui échappent toutes au contrôle préalable d'une autorité indépendante dont la décision est dotée d'un effet contraignant, sont contraires à la Charte et doivent être annulés de ce seul fait.

3.5.2 Contrôle de l'exploitation

111. Si le CSI prévoit que la CNCTR doit être tenue informée de la façon dont les renseignements sont collectés, il ne prévoit pas que la CNCTR soit tenue informée de la façon dont ces renseignement seront ensuite exploitées par l'administration. Ainsi, aucune autorité de contrôle indépendante n'a le pouvoir de veiller à ce que les informations obtenues en application du CSI, une fois transcrites et extraites, soient utilisées dans la limite de ce qui est strictement nécessaire.

112. **En conclusion**, les décrets attaqués ont été pris pour l'application de dispositions législatives qui, en autorisant la collecte de données personnelles dont l'exploitation échappe à tout contrôle indépendant, sont contraires à l'article 8 de la Charte et doivent être annulés de ce seul fait.

3.5.3 Contrôle des transferts

113. De même, aucune autorité de contrôle indépendante n'est chargée de contrôler le transfert à d'autres États des renseignements collectés en application du CSI.

114. Réciproquement, l'article L. 833-2 du CSI prévoit que, si la CNCTR peut consulter les renseignements, transcriptions et extraits dont dispose l'administration, c'est « *à l'exclusion des éléments communiqués par des services étrangers ou par des organismes internationaux* ». L'administration française peut ainsi librement conserver et utiliser indéfiniment n'importe quelle information obtenue sur une personne sans être soumise à aucun contrôle, du moment que cette information lui a été transmise par un service étranger.

115. **En conclusion**, les décrets attaqués ont été pris pour l'application de dispositions législatives qui, en autorisant la collecte de données personnelles dont le partage avec des États étrangers échappe à tout contrôle indépendant, sont contraires à l'article 8 de la Charte et doivent être annulés de ce seul fait.

3.6 Recours effectif

3.6.1 Information préalable

116. **En droit**, l'article 47 de la Charte, interprété par la Cour de justice, exige que les autorités mettant en œuvre des mesures de surveillance « *en informent les personnes concernées, dans le cadre des procédures nationales applicables, pour autant que et dès le moment où cette communication n'est pas susceptible de compromettre les missions qui incombent à ces autorités* [...] *cette information est, de fait, nécessaire pour permettre à ces personnes d'exercer leurs droits* » (CJUE, 6 octobre 2020, *La Quadrature du Net e.a.*, préc., § 190). Cette exigence est reprise à l'article 13 de la directive « police-justice ».

117. **En l'espèce**, le CSI n'organise aucune information, à aucun moment, des personnes dont il autorise la mise sous surveillance.

118. **En conclusion**, les décrets attaqués ont été pris pour l'application de dispositions législatives qui, en autorisant des mesures de surveillance sans jamais prévoir que les personnes concernées en soient informées, sont contraires à la Charte et à la directive « police-justice » et doivent être annulés de ce seul fait.

3.6.2 Information en cours de litige

119. **En droit**, l'article 47 de la Charte, interprété par la Cour de justice, implique que « *ce serait violer le droit fondamental à un recours juridictionnel effectif que de fonder une décision juridictionnelle sur des faits et des documents dont les parties elles-mêmes, ou l'une d'entre elles, n'ont pas pu prendre connaissance et sur lesquels elles n'ont donc pas été en mesure de prendre position* » (CJUE, 4 juin 2013, *ZZ contre Secretary of State for the Home Department*, aff. C-300/11, § 56).

120. Ce n'est que par exception que la Cour de justice admet que, si une décision a été prise sur la base d'informations potentiellement secrètes, « *le juge compétent de l'État membre concerné doit avoir à sa disposition et mettre en œuvre des techniques et des règles de droit de procédure permettant de concilier, d'une part,*

les considérations légitimes de la sûreté de l'État quant à la nature et aux sources des renseignements ayant été pris en considération pour l'adoption d'une telle décision et, d'autre part, la nécessité de garantir à suffisance au justiciable le respect de ses droits procéduraux, tels que le droit d'être entendu ainsi que le principe du contradictoire » (même arrêt, § 57).

121. Pour cela, l'État doit prévoir « *un contrôle juridictionnel effectif* […] *de l'existence et du bien-fondé des raisons invoquées par l'autorité* [qui] *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* », et ce alors qu'« *il n'existe pas de présomption en faveur de l'existence et du bien-fondé de* [ce]*s raisons* » (même arrêt, §§ 58, 60 et 62).

122. **En l'espèce**, l'article L. 773-3 du code de justice administrative prévoit qu'en cas de recours contre une mesure de surveillance, « *les exigences de la contradiction* […] *sont adaptées à celles du secret de la défense nationale* ». Cette adaptation implique notamment que, « l*orsqu'est en cause le secret de la défense nationale* », les pièces produites par l'administration ne sont pas transmises au plaignant ni même à son conseil.

123. L'article 413-9 du code pénal définit les informations qui « *présentent un caractère de secret de la défense nationale* » comme celles « *qui ont fait l'objet de mesures de classification* ». Cette mesure est définie à l'article R. 2311-6 du code de la défense et relève entièrement du pouvoir discrétionnaire de l'administration : « *dans les conditions fixées par le Premier ministre, les informations et supports classifiés au niveau Secret-Défense ou Confidentiel-Défense, ainsi que les modalités d'organisation de leur protection, sont déterminés par chaque ministre pour les administrations et les organismes relevant de son département ministériel* ». Si les articles L. 2312-4, L. 2312-7 et L. 2312-8 du code de la défense prévoient une procédure de déclassification, celle-ci relève ici encore du pouvoir discrétionnaire de l'administration.

124. En résumé, l'administration peut, de son seul chef et sans possibilité pour le juge de s'y opposer, exclure du débat contradictoire des informations qui ont fondé la mesure de surveillance contestée.

125. **En conclusion**, les décrets attaqués ont notamment été pris pour l'application de l'article L. 773-3 du code de justice administrative qui, en permettant à l'administration d'exclure arbitrairement toute information du débat contradictoire sans que le juge ni le plaignant ne puisse s'y opposer, est contraires à l'article 47 de la Charte et doivent être annulés de ce seul fait.

3.6.3 Absence de voie de recours

126. **En droit**, l'article 47 de la Charte garantit un droit au recours effectif contre les mesures de surveillance. Ce droit est repris à l'article 54 de la directive « police-justice ».

127. **En l'espèce**, le Conseil constitutionnel a reconnu sans nuance que « *la personne faisant l'objet d'une mesure de surveillance internationale* [prévue à l'article L. 854-2 du CSI] *ne peut saisir un juge pour contester la régularité de cette mesure* » (Cons. const, 26 novembre 2015, n° 2015-722 DC, pt. 18). Il en va de même des mesures de collecte ou de transfert de renseignement auprès d'États étrangers, qui échappent à tout cadre juridique.

128. **En conclusion**, les décrets attaqués ont notamment été pris pour l'application de l'article L. 854-2 du CSI qui, en autorisant des mesures de renseignement qui ne peuvent être contestées en justice par les personnes concernées, est contraires à l'article 47 de la Charte et doivent être annulés de ce seul fait.

PAR CES MOTIFS, l'association La Quadrature du Net, exposante, conclut qu'il plaise au Conseil d'État de :

ANNULER les décisions attaquées, avec toutes conséquences de droit ;

ENJOINDRE au ministre de l'intérieur de supprimer l'ensemble des données collectées en application des décisions attaqués, sous astreinte de 1 024 euros par jour de retard, à compter de la notification de la décision à intervenir ;

METTRE À LA CHARGE de l'État une somme de 4 096 euros, en application de l'article L. 761-1 du code de justice administrative.

Fait à Paris, le 1er mars 2021

Alexis FITZJEAN Ó COBHTHAIGH
Avocat au Barreau de Paris

BORDEREAU DES PRODUCTIONS

Pièce n° 1 : Décret attaqué ;

Pièce n° 2 : Statuts de LQDN ;