Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de justice et police DFJP

Office fédéral de la justice OFJ
Représentation de la Suisse devant la CourEDH, le CAT, le CEDAW, le CERD et le CRC

P.P. CH-3003 Berne

OFJ; bj-std

POST CH AG

Madame
Olga Chernishova
Greffière de section adjointe
Cour européenne des Droits de l'Homme
Conseil de l'Europe
F-67075 Strasbourg Cedex

Numéro du dossier : 311.2-3306/6
Votre référence : CEDH-LF4.liG OBS IMSI CHB DAR/CPR/ssc
Notre référence : F.2022/8 bj-std
Berne, le 10 mars 2023

Requête n°47351/18 – Glättli et autres c. Suisse
Observations du Gouvernement suisse sur la recevabilité et le fond

Madame la Greffière de section adjointe,

Par lettre du 18 novembre 2022, vous nous avez informé que la requête citée en objet est pendante devant la Cour européenne des droits de l'homme (ci-après : la Cour). Vous nous avez invités à présenter, par écrit, un exposé des faits ainsi que nos observations sur la recevabilité et le bien-fondé de cette requête dans un délai échéant le 13 mars 2023.

Nous sommes invités à répondre aux questions suivantes :

1. *Y a-t-il eu ingérence dans le droit des requérants au respect de leur vie privée et/ou de leur correspondance, au sens de l'article 8 § 1 de la Convention ?*

   Dans l'affirmative, l'ingérence dans l'exercice de ce droit était-elle prévue par la loi, poursuivait-elle un but légitime et était-elle nécessaire, au sens de l'article 8 § 2 ?

2. *Y a-t-il eu ingérence dans le droit à la liberté d'expression des requérants, au sens de l'article 10 § 1 de la Convention ?*

   Dans l'affirmative, cette ingérence était-elle prévue par la loi, poursuivait-elle un but légitime et était-elle nécessaire, au sens de l'article 10 § 2 ?

3. *Y a-t-il eu ingérence dans le droit à la liberté de réunion pacifique des requérants, au sens de l'article 11 § 1 de la Convention ?*

   Dans l'affirmative, cette ingérence était-elle prévue par la loi, poursuivait-elle un but

Office fédéral de la justice OFJ
Adrian Scheidegger
Bundesrain 20
3003 Berne
Tél. +41 58 462 47 90
Adrian.Scheidegger@bj.admin.ch
www.ofj.admin.ch

légitime et était-elle nécessaire, au sens de l'article 11 § 2 ?

4. *Les requérants avaient-ils à leur disposition, comme l'exige l'article 13 de la Convention, un recours interne effectif au travers duquel ils auraient pu formuler leurs griefs de méconnaissance de la Convention ?*

Dans le délai imparti par la Cour, le Gouvernement suisse se prononce comme suit :

I. Exposé des faits

1. Le Gouvernement se réfère à l'état des faits établi par le Tribunal administratif fédéral (TAF) dans son arrêt du 9 novembre 2016 et par le Tribunal fédéral (TF) dans son arrêt du 2 mars 2018. Il se réfère également aux faits tels qu'exposés dans l'Objet de l'affaire publié par le Greffe de la Cour le 28 novembre 2022 et tels qu'exposés par les requérants sous la rubrique « Prozessgeschichte » de leur requête du 27 septembre 2018.

2. Dans la mesure où l'état des faits, ainsi que le « complément à l'état des faits » présentés par les auteurs présentent et critiquent le cadre légal applicable au cas d'espèce, le Gouvernement prendra position sur ces éléments dans le cadre de ses observations ci-après, ch. 3ss.

II. Objet du litige

3. Il convient, en premier lieu, de rappeler et souligner quel est l'objet du présent litige :

4. Dans sa décision du 30 juin 2014, le Service Surveillance de la correspondance par poste et télécommunication (ci-après : Service SCPT ou « le Service ») n'est pas entré en matière sur la demande des requérants d'ordonner aux fournisseurs de services de télécommunication (ci-après : « FST ») de ne pas lui transmettre, ou de ne pas transmettre à d'autres autorités ou tribunaux, les données relatives au trafic et à la facturation les concernant, faute d'intérêt actuel digne de protection au sens de l'art. 48 al. 1 let. c de la Loi fédérale sur la procédure administrative du 20 décembre 1968 (PA ; RS 172.021) (en relation avec l'art. 6 PA). En effet, le droit en matière de surveillance de la correspondance par poste et télécommunication prévoit une séparation des aspects de droit administratif et de procédure pénale. La Loi fédérale sur la surveillance de la correspondance par poste et télécommunication du 6 octobre 2000 (état le 16 juillet 2012) (ci-après : aLSCPT) et le Code de procédure pénale suisse du 5 octobre 2007 (état le 1er octobre 2016) (Code de procédure pénale, CPP) ont des destinataires différents et poursuivent des objectifs différents. Alors que le CPP régit la poursuite et le jugement, par les autorités pénales de la Confédération et des cantons, des infractions prévues par le droit fédéral (art. 1, al. 1, CPP) et se concentre sur la personne inculpée, la aLSCPT assure la mise en œuvre technique et organisationnelle d'une surveillance autorisée par la procédure pénale. La aLSCPT s'adresse aux fournisseurs de services de télécommunication et règle les tâches du Service. Elle détermine comment les FST peuvent être tenus de coopérer dans le cadre d'une telle surveillance, alors que la base légale de la surveillance elle-même se trouve dans le CPP. Conformément à la séparation des aspects de droit administratif et de procédure pénale de la surveillance, la compétence matérielle et le pouvoir d'examen du ministère public, respectivement du tribunal des mesures de contrainte, qui autorise la surveillance, et du Service diffèrent également. Le ministère public ordonne la surveillance lorsque les conditions de procédure pénale des articles 269 ss CPP (cf. ci-après, ch. 19) sont remplies. Cette décision est vérifiée (ultérieurement) par le tribunal des mesures de contrainte (art. 274 al. 2 CPP ; cf. ci-après, ch. 21). Le prévenu peut recourir contre l'ordre de surveillance,

après communication de la surveillance par le ministère public (art. 279 al. 3 CPP, cf. ci-après, ch. 25). Du point de vue de la procédure pénale, le Service ne vérifie plus que formellement si la surveillance concerne une infraction pouvant faire l'objet d'une telle mesure en vertu du droit applicable et qu'elle a été ordonnée par l'autorité compétente (art. 13, al. 1, let. a, aLSCPT ; cf. ci-après, ch. 15). La voie de la procédure administrative est ouverte (aux fournisseurs ou aux personnes tenues de collaborer) contre les décisions du Service (art. 32 de l'Ordonnance sur la surveillance de la correspondance par poste et télécommunication du 31 octobre 2001, état le 1er janvier 2012, ci-après : aOSCPT). La transmission de données secondaires enregistrées concerne donc les aspects de la surveillance de la correspondance par télécommunication relevant de la procédure pénale. Les données secondaires ne pouvaient dès lors n'être transmises aux autorités que sur la base d'un ordre de surveillance. En l'absence d'ordre de surveillance, il n'y avait pas en l'espèce d'intérêt digne de protection suffisamment actuel pour statuer sur la demande des requérants d'ordonner aux FST de ne pas transmettre au Service ou à d'autres autorités ou tribunaux les données relatives au trafic et à la facturation les concernant. Pour cette raison, le Service LSCPT n'était pas compétent matériellement pour statuer sur cette demande des requérants (cf. arrêt du TAF du 9 novembre 2016, consid. 8.1ss).

5. Dans son arrêt du 9 novembre 2016, le TAF a donc, à juste titre, limité l'examen à la question formelle du bien-fondé de la décision de non-entrée en matière sur cette demande des requérants. Le TAF a confirmé, après un examen minutieux (cf. en détail, arrêt du TAF du 9 novembre 2016, consid. 7.2 et consid. 8.2 ss.), que le Service n'était pas compétent pour statuer sur la demande des requérants d'ordonner aux FST de ne pas transmettre au Service ou à d'autres autorités ou tribunaux les données relatives au trafic et à la facturation les concernant. Le Gouvernement relève que si le TAF avait admis le recours des requérants sur ce point, la seule conséquence en aurait été que le Service aurait dû statuer sur le fond, après que la cause lui ait été renvoyée (cf. arrêt du TAF du 9 novembre 2016, consid. 8.4).

6. Dès lors, il appartenait uniquement au TF d'examiner si cette appréciation était correcte. Dans son arrêt du 2 mars 2018 (consid. 2.2.), le TF a constaté que les requérants se sont contentés, dans leur recours devant lui, d'affirmer que le TAF aurait dû examiner leur demande sur le fond, respectivement renvoyer la cause à cet effet au Service, sans se pencher sur les considérants du TAF relatifs à cette question. Le TF a dès lors constaté, à juste titre, que les requérants n'ont pas satisfait aux exigences de motivation sur ce point et qu'il n'y avait pas lieu d'entrer en matière sur ce grief.

7. Il s'ensuit, comme l'a constaté le TF dans son arrêt du 2 mars 2018 (consid. 2.2.), qu'était uniquement objet du litige devant lui, la question de savoir si *l'enregistrement et la conservation* des données secondaires liées aux télécommunications des requérants étaient conformes à la Constitution et à la Convention. Seul l'aspect administratif du double droit de la surveillance de la correspondance par poste et télécommunication était donc concerné L'accès aux données secondaires des requérants par les autorités de poursuite pénale à des fins de surveillance, qui est réglé dans le CPP, n'était pas objet de la procédure devant le TF.

8. Comme l'a précisé le TF dans son arrêt du 2 mars 2018 (consid. 2 et les références) n'étaient dès lors pas objet de la procédure nationale, notamment les griefs selon lesquels :

- les conditions pour ordonner une surveillance (rétroactive) et les types de surveillance eux-mêmes ne sont pas formulés dans la loi ou ne le sont pas de manière suffisamment précise ;

- l'approbation ultérieure de la surveillance par le tribunal des mesures de contrainte n'offre pas une protection suffisante ;

- l'utilisation de données conservées à des fins de surveillance - en particulier dans le domaine des délits commis sur Internet - ne se limite en principe pas aux cas de criminalité grave, va au-delà de ce qui est nécessaire et peut également concerner des tiers ;

- il n'existe pas de base légale suffisante pour les surveillances des ressources d'adressage étrangères (« Kopfschaltungen ») et les recherches par champ d'antennes (recherches par quadrillage) ;

- il est contraire au principe selon lequel les mesures de contrainte présupposent des soupçons suffisants, alors que seule l'exploitation des données par champ d'antennes enregistrées en fonde de tels ;

- la protection des sources journalistiques garantie dans la procédure pénale est insuffisante ;

- la surveillance secrète des informateurs d'un journaliste, dont ce dernier n'est pas informé, viole son droit à un recours effectif ;

- les interdictions d'exploitation prévues dans le CPP n'offrent pas une protection suffisante ;

- le service de renseignement peut accéder aux données de surveillance même en l'absence de soupçons concrets.

9. Ces questions font l'objet d'autres arrêts du TF et peuvent, dans un cas d'espèce, être soumises au TF par un recours en matière pénale (cf. arrêt du TF du 2 mars 2018, consid. 2).

10. Le TF n'a donc abordé la question des droits d'accès que dans la mesure où cela était nécessaire pour examiner la proportionnalité de l'enregistrement et de la conservation systématique des données secondaires, mis en cause par les requérants.

III. Droit et pratique internes

A. Droit interne pertinent

11. Au vu des nombreuses dispositions pertinentes en l'espèce, le Gouvernement ne reproduira ci-après (ch. 15ss) que les dispositions du droit interne les plus importantes pour le traitement du cas d'espèce. Les autres dispositions applicables seront exposées dans le cadre de ses observations relatives au respect des articles 8, 10,11 et 13 de la Convention (ch. 44ss).

12. Le 1er mars 2018, est entrée en vigueur l'actuelle Loi fédérale sur la surveillance de la correspondance par poste et télécommunication du 18 mars 2016 (LSCPT ; RS

780.1). Cette loi a également modifié ou introduit diverses dispositions du Code de procédure pénale suisse du 5 octobre 2007 (CPP ; RS 312) et de la Loi fédérale sur le renseignement du 25 septembre 2015 (LRens ; RS 121). L'arrêt du TF date du 2 mars 2018, mais, comme l'a expressément retenu le TF dans son arrêt, selon l'art. 45 al. 2 LSCPT, les recours contre les décisions du Service sont traités selon le droit applicable en première instance (cf. arrêt du TF du 2 mars 2018, consid. 1.3). Est dès lors applicable en l'espèce le droit applicable devant le TAF, qui a rendu son arrêt le 9 novembre 2016, soit la Loi fédérale sur la surveillance de la correspondance par poste et télécommunication du 6 octobre 2000 (état le 16 juillet 2012) (ci-après : aLSCPT), l'Ordonnance sur la surveillance de la correspondance par poste et télécommunication du 31 octobre 2001 (version en vigueur jusqu'au 28 février 2018, état le 1er janvier 2012, ci-après : aOSCPT), ainsi que le CPP, état le 1er octobre 2016 [ci-après : aCPP]. Pour les autres dispositions légales applicables, cf. ci-après, ch. 44ss.

13. Dans l'arrêt *Ekimdzhiev c. Bulgarie* du 11 janvier 2022 (req. n° 70078/12, §§292 s. et les références), la Cour a retenu que dans des affaires, où les requérants se plaignent dans l'abstrait d'un système de surveillance secrète plutôt que de cas spécifiques de cette surveillance, les lois et pratiques nationales pertinentes doivent être examinées dans l'état où elles se trouvent lorsque la Cour examine la recevabilité de la requête plutôt que dans celui où elles se trouvaient au moment de son introduction.

14. Sont dès lors pertinents en l'espèce, le droit applicable devant le TAF, soit le 9 novembre 2016, ainsi que le droit actuellement en vigueur, que le Gouvernement exposera dans le cadre de ses observations relatives au respect des articles 8, 10,11 et 13 de la Convention (ch. 44ss) et auquel il renverra au moyen de liens hypertextes, afin de ne pas surcharger la présente partie relative au droit interne pertinent.

1. Loi fédérale sur la surveillance de la correspondance par poste et télécommunication du 6 octobre 2000 (état le 16 juillet 2012 ; ci-après : aLSCPT)

15. *Art. 1 Champ d'application*

[1] La présente loi s'applique à la surveillance de la correspondance par poste et télécommunication qui est ordonnée et mise en œuvre :
a. dans le cadre d'une procédure pénale fédérale ou cantonale ;
b. lors de l'exécution d'une demande d'entraide conforme à la loi du 20 mars 1981 sur l'entraide pénale internationale ;
c. dans le cadre de la recherche et du sauvetage de personnes disparues.
[2] Elle s'applique à tous les organismes étatiques, aux organismes soumis à concession ou à l'obligation d'annoncer qui fournissent des services postaux ou de télécommunication ainsi qu'aux fournisseurs d'accès à Internet.
[3] Les renseignements sur les services de paiement soumis à la loi du 30 avril 1997 sur la poste sont régis par les dispositions fédérales et cantonales sur l'obligation de témoigner et sur l'obligation de renseigner les autorités.
[4] Les exploitants de réseaux de télécommunication internes et de centraux domestiques sont tenus de tolérer une surveillance.

16. *Art. 3*

[1] En dehors d'une procédure pénale, une surveillance de la correspondance limitée à l'identification des usagers et aux données relatives au trafic en vue de retrouver une personne disparue peut être ordonnée. Des données relatives à des tiers non impliqués peuvent, dans ce contexte, aussi être consultées.

17. *Art. 13 Tâches du service*

[1] En cas de surveillance de la correspondance par télécommunication, le service remplit les tâches suivantes :
a. il vérifie que la surveillance concerne une infraction pouvant faire l'objet d'une telle mesure en vertu du droit applicable et qu'elle a été ordonnée par l'autorité compétente ; si l'ordre de surveillance est clairement erroné ou qu'il n'est pas motivé, le service prend contact avec l'autorité qui a autorisé la surveillance avant de transmettre des informations à l'autorité qui a ordonné la surveillance ;
b. il ordonne aux fournisseurs de services de télécommunication de prendre les mesures nécessaires à la mise en œuvre de la surveillance ;
c. il reçoit les communications de la personne surveillée qui ont été déviées par les fournisseurs de services de télécommunication ; il les enregistre et transmet les supports de données et les documents à l'autorité qui a ordonné la surveillance ;
d. il veille à l'installation du branchement direct mais il n'enregistre pas les communications ainsi surveillées ;
e. il reçoit des fournisseurs de services de télécommunication les données permettant l'identification des usagers ainsi que les données relatives au trafic et à la facturation et il les transmet à l'autorité qui a ordonné la surveillance ;
f. il met en œuvre les mesures visant à protéger le secret professionnel qui ont été ordonnées par l'autorité qui a autorisé la surveillance.
g. il vérifie que la surveillance ne s'étend pas au-delà de la durée autorisée et y met fin à l'expiration du délai si aucune demande de prolongation n'a été déposée ;
h. il communique immédiatement la levée de la surveillance à l'autorité qui l'a autorisée ;
i. il conserve l'ordre de surveillance durant une année après la levée de celle-ci ;
j. il tient une statistique des surveillances ;
k. il suit l'évolution technique dans le domaine des télécommunications.
[2] Sur demande, le service peut également être chargé des tâches suivantes :
a. enregistrer les communications surveillées par branchement direct ;
b. transcrire l'enregistrement des communications ;
c. traduire les transcriptions rédigées dans une langue étrangère ;
d. trier les communications enregistrées ;
e. fournir des conseils techniques en matière de surveillance de la correspondance par télécommunication aux autorités et aux fournisseurs de services de télécommunication.
[3] Le Conseil fédéral fixe les modalités d'application.

18. *Art. 15 Obligations des fournisseurs de services de télécommunication*

[1] A la demande du service, les fournisseurs de services de télécommunication sont tenus de lui transmettre les communications de la personne surveillée ainsi que les données permettant d'identifier les usagers et celles relatives au trafic et à la facturation. Ils sont également tenus de fournir les informations nécessaires à la mise en œuvre de la surveillance.

[3] Ils sont tenus de conserver durant six mois les données permettant l'identification des usagers ainsi que les données relatives au trafic et à la facturation.

2. Code de procédure pénale suisse du 5 octobre 2007 (état le 1er octobre 2016 ; ci-après : aCPP)

19. *Art. 269 Conditions*

[1] Le ministère public peut ordonner la surveillance de la correspondance par poste et télécommunication aux conditions suivantes :
a. de graves soupçons laissent présumer que l'une des infractions visées à l'al. 2 a été commise;
b. cette mesure se justifie au regard de la gravité de l'infraction ;
c. les mesures prises jusqu'alors dans le cadre de l'instruction sont restées sans succès ou les recherches n'auraient aucune chance d'aboutir ou seraient excessivement difficiles en l'absence de surveillance.

20. *Art. 273 Données relatives au trafic et à la facturation et identification des usagers*

[1] Lorsque de graves soupçons laissent présumer qu'un crime, un délit ou une contravention au sens de l'art. 179septies CP a été commis et que les conditions visées à l'art. 269, al. 1, let. b et c, sont remplies, le ministère public peut exiger que lui soient fournies:
a. les données indiquant quand et avec quelles personnes ou quels raccordements la personne surveillée a été ou est en liaison par poste ou télécommunication ;
b. les données relatives au trafic et à la facturation.
[2] L'ordre de surveillance est soumis à l'autorisation du tribunal des mesures de contrainte.
[3] Les données mentionnées à l'al. 1 peuvent être demandées avec effet rétroactif sur une période de six mois au plus, indépendamment de la durée de la surveillance.

21. *Art. 274 Procédure d'autorisation*

[1] Le ministère public transmet dans les 24 heures à compter du moment où la surveillance a été ordonnée ou les renseignements fournis, les documents suivants au tribunal des mesures de contrainte :
a. l'ordre de surveillance ;
b. un exposé des motifs ainsi que les pièces du dossier qui sont déterminantes pour l'autorisation de surveillance.
[2] Le tribunal des mesures de contrainte statue dans les cinq jours à compter du moment où la surveillance a été ordonnée ou les renseignements fournis, en indiquant brièvement les motifs de sa décision. Il peut autoriser la surveillance à titre provisoire, assortir l'autorisation de conditions ou encore demander que le dossier soit complété ou que d'autres éclaircissements soient apportés.
[3] Le tribunal des mesures de contrainte communique immédiatement sa décision au ministère public et au service chargé de la surveillance de la correspondance par poste et télécommunication au sens de l'art. 2 de la loi fédérale du 6 octobre 2000 sur la surveillance de la correspondance par poste et télécommunication.
[4] L'autorisation indique expressément :
a. si des mesures visant à sauvegarder le secret professionnel doivent être prises ;
b. si des branchements directs peuvent être effectués.
[5] Le tribunal des mesures de contrainte octroie l'autorisation pour trois mois au plus. L'autorisation ne peut être prolongée que pour des périodes n'excédant pas trois mois. Si la prolongation de la surveillance est nécessaire, le ministère public la demande avant l'expiration du délai en en indiquant les motifs.

22. *Art. 275 Levée de la surveillance*

[1] Le ministère public lève immédiatement la surveillance dans les cas suivants :
a. les conditions requises pour son application ne sont plus remplies ;
b. l'autorisation ou sa prolongation a été refusée.
[2] Dans le cas visé à l'al. 1, let. a, le ministère public communique la levée de la surveillance au tribunal des mesures de contrainte.

23. *Art. 276 Informations non nécessaires à la procédure*

[1] Les documents et enregistrements collectés lors d'une surveillance dûment autorisée qui ne sont pas nécessaires à la procédure doivent être conservés séparément et détruits immédiatement après la clôture de la procédure.

24. *Art. 277 Informations recueillies lors d'une surveillance non autorisée*

[1] Les documents et enregistrements collectés lors d'une surveillance non autorisée doivent être immédiatement détruits. Les envois postaux doivent être immédiatement remis à leurs destinataires.
[2] Les informations recueillies lors de la surveillance ne peuvent être exploitées.

25. *Art. 279 Communication*

[1] Au plus tard lors de la clôture de la procédure préliminaire, le ministère public communique au prévenu ainsi qu'au tiers qui ont fait l'objet d'une surveillance au sens de l'art. 270, let. b, les motifs, le mode et la durée de la surveillance.
[2] Avec l'accord du tribunal des mesures de contrainte, il est possible de différer la communication ou d'y renoncer aux conditions suivantes :
a. les informations recueillies ne sont pas utilisées à des fins probatoires ;
b. cela est indispensable pour protéger des intérêts publics ou privés prépondérants.
[3] Les personnes dont le raccordement de télécommunication ou l'adresse postale ont été surveillés ou celles qui ont utilisé le même raccordement ou la même adresse postale peuvent interjeter recours conformément aux art. 393 à 397. Le délai de recours commence à courir dès la réception de la communication.

3. Loi fédérale sur la protection des données du 19 juin 1992 (LPD)

26. *Art. 8 Droit d'accès*

[1] Toute personne peut demander au maître d'un fichier si des données la concernant sont traitées.
[2] Le maître du fichier doit lui communiquer :
a. toutes les données la concernant qui sont contenues dans le fichier, y compris les informations disponibles sur l'origine des données ;
b. le but et éventuellement la base juridique du traitement, les catégories de données personnelles traitées, de participants au fichier et de destinataires des données.
[3] Le maître du fichier peut communiquer à la personne concernée des données sur sa santé par l'intermédiaire d'un médecin qu'elle a désigné.
[4] Le maître du fichier qui fait traiter des données par un tiers demeure tenu de fournir les renseignements demandés. Cette obligation incombe toutefois au tiers, s'il ne révèle pas l'identité du maître du fichier ou si ce dernier n'a pas de domicile en Suisse.
[6] Nul ne peut renoncer par avance au droit d'accès.

27. *Art. 9 Restriction du droit d'accès*

[1] Le maître du fichier peut refuser ou restreindre la communication des renseignements demandés, voire en différer l'octroi, dans la mesure où :
a. une loi au sens formel le prévoit ;
b. les intérêts prépondérants d'un tiers l'exigent.
[2] Un organe fédéral peut en outre refuser ou restreindre la communication des renseignements demandés, voire en différer l'octroi, dans la mesure où :
a. un intérêt public prépondérant, en particulier la sûreté intérieure ou extérieure de la Confédération, l'exige ;
b. la communication des renseignements risque de compromettre une instruction pénale ou une autre procédure d'instruction.
[3] Dès que le motif justifiant le refus, la restriction ou l'ajournement disparaît, l'organe fédéral est tenu de communiquer les renseignements demandés, pour autant que cela ne s'avère pas impossible ou ne nécessite pas un travail disproportionné.
[4] Un maître de fichier privé peut en outre refuser ou restreindre la communication des renseignements demandés ou en différer l'octroi, dans la mesure où ses intérêts prépondérants l'exigent et à condition qu'il ne communique pas les données personnelles à un tiers.
[5] Le maître du fichier doit indiquer le motif pour lequel il refuse de fournir, restreint ou ajourne les renseignements.

28. *Art. 25 Prétentions et procédure*

[1] Quiconque a un intérêt légitime peut exiger de l'organe fédéral responsable qu'il :
a. s'abstienne de procéder à un traitement illicite ;
b. supprime les effets d'un traitement illicite ;
c. constate le caractère illicite du traitement.
[2] Si ni l'exactitude, ni l'inexactitude d'une donnée personnelle ne peut être prouvée, l'organe fédéral doit ajouter à la donnée la mention de son caractère litigieux.
[3] Le demandeur peut en particulier demander que l'organe fédéral :

a. rectifie les données personnelles, les détruise ou en empêche la communication à des tiers ;
b. publie ou communique à des tiers sa décision, notamment celle de rectifier ou de détruire des données personnelles, d'en interdire la communication ou d'en mentionner le caractère litigieux.
[4] La procédure est régie par la loi fédérale du 20 décembre 1968 sur la procédure administrative. Toutefois, les exceptions prévues aux art. 2 et 3 de cette loi ne sont pas applicables.

29. *Art. 27 Surveillance des organes fédéraux*

[1] Le préposé surveille l'application par les organes fédéraux de la présente loi et des autres dispositions fédérales relatives à la protection des données. Aucune surveillance ne peut être exercée sur le Conseil fédéral.
[2] Le préposé établit les faits d'office ou à la demande de tiers.
[3] Aux fins d'établir les faits, il peut exiger la production de pièces, demander des renseignements et se faire présenter des traitements. Les organes fédéraux sont tenus de collaborer à l'établissement des faits. Le droit de refuser de témoigner au sens prévu à l'art. 16 de la loi fédérale du 20 décembre 1968 sur la procédure administrative s'applique par analogie.
[4] S'il apparaît que des prescriptions sur la protection des données ont été violées, le préposé recommande à l'organe fédéral responsable de modifier ou de cesser le traitement. Il informe le département compétent ou la Chancellerie fédérale de sa recommandation.
[5] Si une recommandation est rejetée ou n'est pas suivie, il peut porter l'affaire pour décision auprès du département ou de la Chancellerie fédérale. La décision sera communiquée aux personnes concernées.
[6] Le préposé a qualité pour recourir contre la décision visée à l'al. 5 et contre celle de l'autorité de recours.

4. Ordonnance sur la surveillance de la correspondance par poste et télécommunication du 31 octobre 2001 (état le 1er janvier 2012, ci-après : aOSCPT)

30. *Art. 9 Protection et sécurité des données*

[1] La sécurité des données traitées par le service est régie par les dispositions de l'ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données et par les dispositions relatives à la sécurité des technologies de l'information et de la communication de l'ordonnance du 26 septembre 2003 sur l'informatique dans l'administration fédérale.
[2] Les fournisseurs de services postaux ou de télécommunication se conforment aux instructions du service pour les questions de sécurité des données relatives à la transmission des données provenant d'une surveillance. Ils sont responsables de la sécurité des données jusqu'au point de transmission des données au service.

31. *Art. 10 Destruction des données*

[1] Le service détruit les données relatives à une surveillance après les avoir transmises aux autorités mentionnées à l'art. 8, al. 3 ou 4, mais au plus tard trois mois après la levée de la surveillance.
[2] Il détruit les données figurant dans le système de suivi des affaires une année après la levée de la surveillance.

32. *Section 4 Surveillance des services téléphoniques*

33. *Art. 15 Ordre de surveillance*

[1] L'ordre de surveillance transmis au service doit contenir les indications suivantes :
a. le nom de l'autorité qui a ordonné la surveillance ;
b. le nom de l'autorité de poursuite pénale à laquelle les résultats de la surveillance sont destinés ;
c. pour autant que ces informations soient connues : les noms, adresses et professions des suspects et des autres personnes qui doivent, le cas échéant, être également surveillées ;
d. dans le cas de personnes tenues au secret professionnel au sens de l'art. 271, al. 1, CPP : une mention indiquant cette particularité ;

e. l'infraction que la surveillance doit permettre de révéler ;
f. si possible, le nom du fournisseur de services de télécommunication ;
g. les types de surveillance ordonnés ;
h. les ressources d'adressage connues ;
i. si nécessaire, les demandes relatives :
1. à l'autorisation d'effectuer un branchement direct,
2. à l'autorisation générale de surveiller plusieurs raccordements sans qu'il soit nécessaire de demander à chaque fois une nouvelle autorisation (art. 272, al. 2 et 3, CPP) ; et
3. à des mesures supplémentaires de protection de la personnalité ;
j. le début et la fin de la surveillance ;
k. les tâches demandées au service en vertu de l'art. 13, al. 2, LSCPT.
[2] Si l'exécution de certains types de surveillance l'exige, le département peut prévoir que l'ordre de surveillance transmis au service contienne des indications techniques supplémentaires.

34. *Art. 16 Types de surveillance (en temps réel et rétroactive)*

Les types de surveillance suivants peuvent être ordonnés :
d. la transmission des données suivantes, si la communication a été établie (surveillance rétroactive) :
1. les ressources d'adressage disponibles (numéros d'appel des communications entrantes et sortantes, pour autant qu'ils soient connus du fournisseur de services de télécommunication),
2. les paramètres de communication de l'équipement terminal de la téléphonie mobile et les paramètres pour l'identification de l'usager (comme le numéro IMSI et le numéro IMEI),
3. pour la téléphonie mobile : l'identification cellulaire (Cell-ID), la position et la direction d'émission de l'antenne de téléphonie mobile avec laquelle l'équipement terminal de la personne surveillée est reliée au moment de la communication,
4. la date, l'heure et la durée de la correspondance ;
e. la recherche par champ d'antennes : recherche rétroactive de toutes les communications effectuées par téléphonie mobile à un endroit précis et durant un laps de temps déterminé si une communication a été établie.

35. *Art. 16b Mesures de surveillance en rapport avec l'étranger*

[1] Les mesures de surveillance selon l'art. 16, let. a, c, ch. 1, 2, 3 et 5, et let. d, ch. 1, 2 et 4, peuvent avoir pour cible toute ressource d'adressage, indépendamment de la position de l'équipement terminal, de l'indicatif national et de l'appartenance de réseau.
[2] Les mesures de surveillance selon l'art. 16, let. a, b, c, ch. 4, et let. d, ch. 3, et selon l'art. 16a peuvent également avoir pour cible une ressource d'adressage étrangère se trouvant dans le réseau d'un fournisseur de services de télécommunication suisse.

36. *Section 6 Surveillance de l'Internet*

37. *Art. 23 Ordre de surveillance*

L'ordre de surveillance transmis au service doit contenir les indications suivantes :
a. le nom de l'autorité qui a ordonné la surveillance ;
b. le nom de l'autorité de poursuite pénale à laquelle les résultats de la surveillance sont destinés ;
c. pour autant que ces informations soient connues : les noms, adresses et professions des suspects et des autres personnes qui doivent, le cas échéant, être également surveillées ;
d. dans le cas de personnes tenues au secret professionnel au sens de l'art. 271, al. 1, CPP : une mention indiquant cette particularité ;
e. l'infraction que la surveillance doit permettre de révéler ;
f. le nom du fournisseur d'accès à Internet, si celui-ci est connu ;
g. les types de surveillance ordonnés ainsi que :
1. les ressources d'adressage connues (par exemple adresse e-mail, case postale électronique, équipement de courrier électronique, adresse IP, nom d'utilisateur, adresse MAC, numéro E.164, numéro IMSI, numéro IMEI),
2. les données connues utilisées pour la procédure d'identification (login),
3. l'autorisation d'effectuer un branchement direct,
4. les demandes de mesures pour protéger les utilisateurs non concernés ;
h. le début et la fin de la surveillance ;

i. les tâches demandées au service en vertu de l'art. 13, al. 2, LSCPT.

38. *Art. 24 Accès Internet et applications pouvant faire l'objet d'une surveillance*

[1] Les accès
éo). Internet suivants peuvent faire l'objet d'une surveillance :
a. accès via un serveur d'accès distant par ligne commutée ;
b. accès à large bande (par exemple xDSL, modem câble) ;
c. accès par réseau mobile à commutation de paquets (par exemple GPRS, LTE) ;
d. accès Internet sans fil (par exemple Wi-Fi, Wimax, WLL) ;
e. autres accès de couche OSI 2 au réseau (par exemple Ethernet par accès FTTH) ;
f. autres accès de couche OSI 3 au réseau (par exemple accès IP à large bande).
[2] Les applications suivantes peuvent faire l'objet d'une surveillance :
a. services de messagerie synchrones et asynchrones (par exemple messagerie instantanée, e-mails) ;
b. services de télécommunication fondés sur des médias numériques (par exemple VoIP, transmission audio et vid

5. Ordonnance relative à la loi fédérale sur la protection des données du 14 juin 1993 (état le 16 octobre 2012 ; ci-après : OLPD)

39. *Section 4 Mesures techniques et organisationnelles*

40. *Art. 8 Mesures générales*

[1] La personne privée qui traite des données personnelles ou qui met à disposition un réseau télématique assure la confidentialité, la disponibilité et l'intégrité des données afin de garantir de manière appropriée la protection des données. Elle protège les systèmes notamment contre les risques de :
a. destruction accidentelle ou non autorisée ;
b. perte accidentelle ;
c. erreurs techniques ;
d. falsification, vol ou utilisation illicite ;
e. modification, copie, accès ou autre traitement non autorisés.
[2] Les mesures techniques et organisationnelles sont appropriées. Elles tiennent compte en particulier des critères suivants :
a. but du traitement de données ;
b. nature et étendue du traitement de données ;
c. évaluation des risques potentiels pour les personnes concernées ;
d. développement technique.
[3] Ces mesures font l'objet d'un réexamen périodique.

41. *Art. 9 Mesures particulières*

[1] Le maître du fichier prend, en particulier lors de traitements automatisés de données personnelles, des mesures techniques et organisationnelles propres à réaliser notamment les objectifs suivants :
a. contrôle des installations à l'entrée : les personnes non autorisées n'ont pas accès aux locaux et aux installations utilisées pour le traitement de données personnelles ;
b. contrôle des supports de données personnelles : les personnes non autorisées ne peuvent pas lire, copier, modifier ou éloigner des supports de données ;
c. contrôle du transport : les personnes non autorisées ne peuvent pas lire, copier, modifier ou effacer des données personnelles lors de leur communication ou lors du transport de supports de données ;
d. contrôle de communication : les destinataires auxquels des données personnelles sont communiquées à l'aide d'installations de transmission peuvent être identifiés ;
e. contrôle de mémoire : les personnes non autorisées ne peuvent ni introduire de données personnelles dans la mémoire ni prendre connaissance des données mémorisées, les modifier ou les effacer ;
f. contrôle d'utilisation : les personnes non autorisées ne peuvent pas utiliser les systèmes de traitement automatisé de données personnelles au moyen d'installations de transmission ;

g. contrôle d'accès : les personnes autorisées ont accès uniquement aux données personnelles dont elles ont besoin pour accomplir leurs tâches ;
h. contrôle de l'introduction : l'identité des personnes introduisant des données personnelles dans le système, ainsi que les données introduites et le moment de leur introduction peuvent être vérifiés a posteriori.
[2] Les fichiers doivent être organisés de manière à permettre à la personne concernée d'exercer ses droits d'accès et de rectification.

42. *Art. 10 Journalisation*

[1] Le maître du fichier journalise les traitements automatisés de données sensibles ou de profils de la personnalité lorsque les mesures préventives ne suffisent pas à garantir la protection des données. Une journalisation est notamment nécessaire, lorsque, sans cette mesure, il ne serait pas possible de vérifier a posteriori que les données ont été traitées conformément aux finalités pour lesquelles elles ont été collectées ou communiquées. Le préposé peut recommander la journalisation pour d'autres traitements.
[2] Les procès-verbaux de journalisation sont conservés durant une année et sous une forme répondant aux exigences de la révision. Ils sont accessibles aux seuls organes ou personnes chargés de vérifier l'application des dispositions de protection des données personnelles, et ils ne sont utilisés qu'à cette fin.

B. Pratique interne pertinente

43. Le Gouvernement exposera la pratique interne pertinente dans le cadre de ses observations relatives au respect des articles 8, 10,11 et 13 de la Convention (ch. 44ss).

IV. Respect de l'art. 8 de la Convention

A. Griefs des requérants

44. Les requérants soulèvent de nombreux griefs devant la Cour. Le Gouvernement rappelle toutefois l'objet du présent litige, cf. ci-avant, ch. 3ss.

B. Jurisprudence de la Cour

45. Depuis l'arrêt du TF du 2 mars 2018, la Cour a développé sa jurisprudence concernant les systèmes de surveillance de masse. Le Gouvernement renvoie en particulier aux arrêts *Ekimdzhiev*, précité, qui concerne le stockage systématique des données secondaires de télécommunication par les fournisseurs de services de télécommunication, ainsi qu'aux arrêts *Big Brother Watch and Others c. Royaume-Uni* du 25 mai 2021 (Grande Chambre ; req. no 58170/13) et *Centrum för Rättvisa c. Suède* du 25 mai 2021 (req. no 35252/08).

46. Dans l'arrêt *Ekimdzhiev*, précité, la Cour a considéré que la conservation des données de communication par les fournisseurs de services de communication et leur accès par les autorités dans des cas individuels doivent être assortis, *mutatis mutandis*, des mêmes garanties que la surveillance secrète (§ 394s.). A ce sujet, le Gouvernement renvoie à l'arrêt *Big Brother Watch* (précité, §§ 348ss), dans lequel la Cour a retenu en ce qui concerne l'approche à adopter dans les affaires relatives à l'interception en masse, qu'il est impératif que lorsqu'un État met en œuvre un tel système, le droit interne contienne des règles détaillées prévoyant les circonstances dans lesquelles les autorités peuvent avoir recours à de telles mesures. Le cadre juridique devrait, en particulier, énoncer avec suffisamment de clarté les motifs pour lesquels une interception en masse pourrait être autorisée et les circonstances dans lesquelles les communications d'un individu pourraient être interceptées. La Cour a considéré qu'afin de réduire autant que possible le risque d'abus du pouvoir d'interception en masse, le processus doit être encadré

par des « garanties de bout en bout », c'est-à-dire qu'au niveau national, la nécessité et la proportionnalité des mesures prises devraient être appréciées à chaque étape du processus, que les activités d'interception en masse devraient être soumises à l'autorisation d'une autorité indépendante dès le départ – dès la définition de l'objet et de l'étendue de l'opération – et que les opérations devraient faire l'objet d'une supervision et d'un contrôle indépendant opéré *a posteriori*. Pour déterminer si l'État défendeur a agi dans les limites de sa marge d'appréciation, la Cour, en examinant conjointement les critères selon lesquels la mesure doit être « prévue par la loi » et « nécessaire », conformément à l'approche établie dans ce domaine, recherche si le cadre juridique national définit clairement (1) les motifs pour lesquels l'interception en masse peut être autorisée ; (2) les circonstances dans lesquelles les communications d'un individu peuvent être interceptées ; (3) la procédure d'octroi d'une autorisation ; (4) les procédures à suivre pour la sélection, l'examen et l'utilisation des éléments interceptés ; (5) les précautions à prendre pour la communication de ces éléments à d'autres parties ; (6) les limites posées à la durée de l'interception et de la conservation des éléments interceptés, et les circonstances dans lesquelles ces éléments doivent être effacés ou détruits ; (7) les procédures et modalités de supervision, par une autorité indépendante, du respect des garanties énoncées ci-dessus, et les pouvoirs de cette autorité en cas de manquement et (8) les procédures de contrôle indépendant *a posteriori* du respect des garanties et les pouvoirs conférés à l'organe compétent pour traiter les cas de manquement. La Cour a considéré également que, compte tenu de la nature différente des données de communication associées et des différentes façons dont elles sont utilisées par les services de renseignement, à condition que les garanties énoncées ci-dessus soient en place, il n'est pas nécessaire que les dispositions juridiques régissant le traitement des données de communication associées soient identiques en tous points à celles régissant le traitement du contenu des communications (cf. arrêt *Big Brother Watch*, précité, §§ 348ss).

C. Ingérence dans le droit des requérants au respect de leur vie privée et/ou de leur correspondance

47. Dans l'arrêt *Ekimdzhiev*, précité, la Cour a rappelé que le simple fait de stocker des données relatives à la vie privée d'une personne, indépendamment de la question de savoir si les autorités ont ensuite accès aux données conservées, constitue une ingérence dans le droit de cette personne au respect de sa " vie privée ". Il en va ainsi par exemple des données relatives aux abonnés, au trafic et à la localisation (§ 372 et les références). Cette conservation constitue également une ingérence dans le droit des requérants au respect de leur correspondance (§ 372 et les références).

48. Le Gouvernement rappelle que l'accès aux données n'est pas objet de la présente procédure (cf. ci-avant, ch. 3ss).

49. Dans l'arrêt *Big Brother Watch*, précité, (§§325ss), la Cour a jugé que l'interception en masse est un processus graduel dans lequel l'intensité de l'ingérence dans l'exercice des droits protégés par l'article 8 augmente au fur et à mesure que le processus avance. Sous réserve du fait que les régimes d'interception en masse ne sont pas forcément tous conçus exactement sur le même modèle, que les différentes étapes du processus ne sont pas nécessairement distinctes et ne répondent pas toujours à un ordre chronologique strict, la Cour a considéré néanmoins que les étapes du processus d'interception en masse qu'il convient d'examiner peuvent être décrites comme suit :

(a) interception et rétention initiale des communications et des données de communication associées (c'est-à-dire des données de trafic qui se rapportent aux communications interceptées). Au cours de cette étape, les services de renseignement interceptent en masse des communications électroniques (ou des « paquets » de communications électroniques). Ces communications sont celles d'un grand nombre de personnes, dont la plupart ne présentent absolument aucun intérêt pour les services de renseignement. Certaines communications peu susceptibles de présenter un intérêt pour le renseignement peuvent être éliminées à ce stade.

(b) application de sélecteurs spécifiques aux communications retenues et aux données de communication associées. La recherche initiale, qui est en grande partie automatisée, intervient lors de cette étape : différents types de sélecteurs, y compris des « sélecteurs forts » (tels qu'une adresse de courrier électronique) et/ou des requêtes complexes, sont appliqués aux paquets de communications retenus et aux données de communication associées. À ce stade, il est possible que le processus commence à cibler des individus par l'utilisation de sélecteurs forts.

(c) examen par des analystes des communications sélectionnées et des données de communication associées. Lors de cette étape, les éléments interceptés sont examinés pour la première fois par un analyste.

(d) rétention subséquente des données et utilisation du « produit final », notamment partage de ces données avec des tiers. Cette étape est celle où les services de renseignement utilisent concrètement les éléments interceptés. Les éléments retenus peuvent alors être inclus dans un rapport de renseignement, communiqués à d'autres services de renseignement du pays, ou même transmis à des services de renseignement étrangers.

50. La Cour a considéré que l'article 8 s'applique à chacune des étapes décrites ci-dessus. Si l'interception suivie de l'élimination immédiate d'une partie des communications ne constitue pas une ingérence particulièrement importante, l'intensité de l'ingérence dans l'exercice des droits protégés par l'article 8 augmente au fur et à mesure que le processus d'interception en masse avance. À cet égard, la Cour a clairement dit que le simple fait de conserver des données relatives à la vie privée d'un individu s'analyse en une ingérence au sens de l'article 8, et que la nécessité de disposer de garanties se fait d'autant plus sentir lorsqu'il s'agit de protéger les données à caractère personnel soumises à un traitement automatique. Le fait que les données retenues soient conservées sous une forme codée intelligible uniquement à l'aide de l'informatique et ne pouvant être interprétée que par un nombre restreint de personnes ne saurait avoir d'incidence sur cette conclusion. En définitive, c'est à la fin du processus, lorsque des informations relatives à une personne en particulier sont analysées ou que le contenu de communications est examiné par un analyste, que la présence de garanties est plus que jamais nécessaire. Ainsi, l'intensité de l'atteinte au droit au respect de la vie privée augmente au fur et à mesure que le processus franchit les différentes étapes.

51. Dans son arrêt du 2 mars 2018, le TF a admis l'existence d'une ingérence aux droits protégés par l'article 8 CEDH, en particulier le droit à l'autodétermination en matière d'information et à la protection de la vie privée (consid. 4.2). Il est toutefois parti du principe (contrairement au TAF) que le simple enregistrement et la conservation des données secondaires de télécommunication ne constituaient pas encore une

ingérence grave qui, dans la pratique, nécessitait une réglementation claire et explicite dans une loi au sens formel : certes, de grandes quantités de données sont saisies et un grand nombre de personnes sont concernées, mais les autorités n'ont pas d'accès direct aux données enregistrées chez les fournisseurs de télécommunications ; en outre il s'agit de données secondaires et non du contenu des communications ; celles-ci ne sont ni triées ni reliées entre elles au niveau de l'enregistrement et de la conservation chez les différents fournisseurs de télécommunications, raison pour laquelle aucun profil sensible ne peut être établi. Seul l'accès des autorités de poursuite pénale aux données enregistrées (réglé dans le CPP) permet leur exploitation et leur mise en relation et constitue donc une atteinte grave. Le Gouvernement soutient cette appréciation, au regard de la jurisprudence de la Cour (cf. ci-avant, ch. 49), constatant qu'en l'occurrence le processus litigieux se déroule dans la première étape (étape a).

52. Toutefois, comme l'a également expressément constaté le TF (cf. consid. 5.5 in fine), même si la Cour devait arriver à la conclusion que la conservation des données secondaires pendant six mois constitue déjà une ingérence grave, cela ne changerait rien au résultat, car une ingérence grave serait également justifiée en vertu de l'art. 8 § 2 CEDH (cf. ci-après, ch. 54ss).

53. Une ingérence dans les droits garantis par l'article 8 de la Convention ne peut se justifier au regard du paragraphe 2 de cet article que si elle est prévue par la loi, vise un ou plusieurs des buts légitimes énumérés dans ce paragraphe et est nécessaire, dans une société démocratique, pour atteindre ce ou ces buts (cf. arrêt *Big Brother Watch*, précité, §332).

D. Prévue par la loi

54. Les termes « prévue par la loi » signifient que la mesure litigieuse doit avoir une base en droit interne. La loi doit être accessible à la personne concernée et prévisible quant à ses effets. Dans les affaires où la législation autorisant la surveillance secrète est contestée devant la Cour, la question de la légalité de l'ingérence est étroitement liée à celle de savoir s'il a été satisfait au critère de la « nécessité », raison pour laquelle la Cour doit vérifier en même temps que la mesure était « prévue par la loi » et qu'elle était « nécessaire ». La « qualité de la loi » en ce sens implique que le droit national doit non seulement être accessible et prévisible dans son application, mais aussi garantir que les mesures de surveillance secrète soient appliquées uniquement lorsqu'elles sont « nécessaires dans une société démocratique », notamment en offrant des garanties et des garde-fous suffisants et effectifs contre les abus. Au fil de sa jurisprudence relative à l'interception de communications dans le cadre d'enquêtes pénales, la Cour a déterminé que pour prévenir les abus de pouvoir, la loi doit au minimum énoncer les éléments suivants : i) la nature des infractions susceptibles de donner lieu à un mandat d'interception ; ii) la définition des catégories de personnes dont les communications sont susceptibles d'être interceptées ; iii) la limite à la durée d'exécution de la mesure ; iv) la procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies ; v) les précautions à prendre pour la communication des données à d'autres parties ; et vi) les circonstances dans lesquelles les données interceptées peuvent ou doivent être effacées ou détruites. Elle a confirmé que ces mêmes garanties minimales, au nombre de six, s'appliquaient aussi dans les cas où l'interception était faite pour des raisons de sécurité nationale ; toutefois, pour déterminer si la loi litigieuse était contraire à l'article 8, elle a tenu compte également des éléments suivants : les modalités du contrôle de l'application de mesures de surveillance secrète, l'existence éventuelle d'un mécanisme

de notification et les recours prévus en droit interne (cf. arrêt *Big Brother Watch*, précité, §§332ss).

55. Le TF pose des exigences similaires (cf. arrêt du TF du 2 mars 2018, consid. 6.1. et les références) : le principe de légalité selon l'art. 36 al. 1 de la Constitution (Cst.) exige, dans l'intérêt de la sécurité du droit et de l'application uniforme du droit, une précision suffisante et appropriée des règles de droit à appliquer. Celles-ci doivent être formulées de manière suffisamment précise pour permettre aux sujets de droit d'orienter leur comportement et de connaître les conséquences d'un comportement déterminé avec un degré de certitude correspondant aux circonstances. L'exigence de précision des normes juridiques ne doit pas être comprise de manière absolue. Le législateur ne peut pas renoncer à utiliser des notions générales et plus ou moins vagues, dont l'interprétation et l'application doivent être laissées à la pratique. Le degré de précision requis ne peut pas être fixé de manière abstraite. Il dépend entre autres de la diversité des faits à considérer, de leur complexité et de la décision appropriée qui n'est possible que lors de la concrétisation dans le cas particulier.

56. Comme devant les juridictions nationales, les requérants font valoir qu'il ne ressort pas de la loi mais seulement d'ordonnances et de lignes directrices quelles sont les données qui doivent être enregistrées par les fournisseurs de services de télécommunication et comment elles peuvent être utilisées. Ils font valoir également que les règlementations techniques et complexes ne permettent pas aux particuliers de savoir quelles données les concernant sont enregistrées et comment elles sont utilisées. Ils estiment dès lors que la base légale n'est pas suffisante pour la conservation des données secondaires. Le Gouvernement rappelle qu'étant donné que l'accès aux données secondaires des requérants par les autorités de poursuite pénale à des fins de surveillance n'était pas objet de la procédure devant le TF, ne sont dès lors pas objet de la présente procédure les griefs selon lesquels les conditions pour ordonner une surveillance (rétroactive) et les types de surveillance eux-mêmes ne sont pas formulés dans la loi ou ne le sont pas de manière suffisamment précise ou encore qu'il n'existe pas de base légale suffisante pour les surveillances des ressources d'adressage étrangères (« Kopfschaltungen ») et les recherches par champ d'antennes (recherches par quadrillage) (cf. ci-avant, ch. 7).

57. L'ingérence était prévue par l'art. 15, al. 3 aLSCPT (cf. ci-avant, ch. 18). Il en ressort que les fournisseurs de services de télécommunication sont tenus de conserver durant six mois les données permettant l'identification des usagers ainsi que les données relatives au trafic et à la facturation. Cette loi au sens formel était publiée dans le RS et accessible au public.

58. Le TAF a examiné la question de la base légale dans son arrêt du 9 novembre 2016 (consid. 10.6.2ss et les références). Il a constaté que les termes "identification des usagers" et "données relatives au trafic et à la facturation" sont de nature technique et, pour cette raison, restent indéterminés. Toutefois, compte tenu de la complexité de l'objet de la réglementation, à savoir la surveillance de la correspondance par télécommunication, cela n'est pas fondamentalement critiquable, d'autant plus que la disposition régit une mesure administrative et oblige les fournisseurs de services de télécommunication privés et non les requérants. Il a constaté que le législateur ne peut pas renoncer, dans ce domaine, à utiliser des notions générales et plus ou moins vagues, dont l'interprétation et l'application doivent être laissées à la pratique. Il a retenu également qu'il ne faut pas se baser uniquement sur le texte de la disposition concernée. Il faut au contraire mesurer l'exigence de précision, eu égard à la description de la mesure contestée, à l'objectif et au but de l'objet de la réglementation et il faut s'interroger sur

la signification que revêt la disposition dans le contexte d'autres dispositions. Il convient donc d'examiner tout d'abord le libellé de l'art. 15, al. 3 LSCPT. Selon l'usage courant, les « données permettant l'identification des usagers » sont toutes les indications nécessaires pour déterminer ou constater les raccordements et (donc) les abonnés participant à une télécommunication (cf. https://www.duden.de/ pour le mot "identifizieren" ["identifier"]). Il s'agit par exemple des numéros d'appel et, dans la mesure où sont utilisées Internet ou d'autres formes de communication sans fil et mobiles, d'autres éléments tels que les adresses internet Protocol (adresses IP) et les numéros d'appareils permettant d'identifier les raccordements participants et donc les abonnés. Cela inclut également l'historique IP, c'est-à-dire les données sur le trafic Internet d'une personne, comme par exemple quand elle a surfé sur Internet et quel a été son trafic de courrier électronique. En outre, ce sont les adresses IP des raccordements participant à une communication qui sont enregistrées et conservées, et pas seulement celles de l'origine de la communication. S'y ajoutent les « données relatives au trafic et à la facturation ». Selon l'usage courant, il s'agit d'informations sur la communication, respectivement le trafic de télécommunication des requérants qui sont enregistrées par les fournisseurs, notamment en vue de la facturation, c'est-à-dire l'heure et la durée d'une communication. Les fournisseurs sont donc tenus de stocker et de conserver les informations relatives aux communications des requérants. Il a relevé qu'une restriction importante concernant ce que les fournisseurs doivent stocker et conserver conformément à l'art. 15, al. 3 aLSCPT, résulte du contexte avec l'art. 15 al. 1 aLSCPT (cf. ch. 18), disposition qui fait la distinction entre le contenu de la correspondance par télécommunication ("communications de la personne surveillée") et les informations liées à la correspondance par télécommunication ou données secondaires ("données permettant d'identifier les usagers et celles relatives au trafic et à la facturation"). La disposition de l'article 15, alinéa 3 de la LSCPT ne permet donc pas de stocker et de conserver le contenu des communications. Ce qui reste, ce sont les données secondaires de la communication, c'est-à-dire les données qui permettent de savoir avec qui les requérants ont communiqué, quand et pendant combien de temps. La séparation entre la surveillance du contenu de la correspondance par télécommunication et la collecte (rétroactive) de ses données secondaires découle également du CPP, qui fait la distinction entre la surveillance de la correspondance par télécommunication (art. 269 aCPP ; ci-avant, ch. 19) et les renseignements sur les données relatives au trafic et à la facturation ainsi que sur l'identification des abonnés (art. 273 aCPP ; cf. ci-avant, ch. 20). Comme l'a constaté le TAF, la aLSCPT définissait elle-même, en tous les cas dans les grandes lignes, le but, les organes impliqués et l'étendue du traitement des données. Certes, les termes utilisés étaient moins précis, mais les grandes lignes de la réglementation étaient clairement reconnaissables. L'art. 15, al. 3, de la aLSCPT, décrit et limite l'obligation de manière suffisamment précise, tant du point de vue matériel que temporel, compte tenu de l'objet de la réglementation. Il était dès lors prévisible pour les requérants, sur la base de cette disposition, que les fournisseurs conservent durant six mois les données permettant l'identification des usagers ainsi que les données relatives au trafic et à la facturation, soit les données secondaires de leurs communications - en les distinguant du contenu des communications. Ils étaient et sont donc en mesure de prévoir avec suffisamment de certitude l'enregistrement et la conservation de données secondaires comme conséquence de l'utilisation de services de communication. Pour cela, il n'était pas nécessaire de savoir en détail quelles sont les données (techniques) qui sont enregistrées, dans la mesure où, comme en l'espèce, l'étendue du traitement des données découle dans les grandes lignes de la loi elle-même. D'autre part, comme l'a constaté le TAF, il n'apparaît pas que les fournisseurs aient enregistré et transmis des données qui ne sont pas couvertes par l'art. 15 al. 3 aLSCPT. Il a précisé que les dispositions des art. 16 let. d (ch. 34) et 24 let. d aOSCPT (ch. 38) ne vont pas au-

delà de l'art. 15 al. 3 aLSCPT en ce qui concerne les données dont la transmission peut être ordonnée. Cela vaut - sous la notion de données relatives au trafic - également pour les données (techniques) telles que l'emplacement et la direction principale du faisceau de l'antenne à laquelle le terminal est connecté au moment de la communication. Le TAF s'est référé également aux matériaux relatifs à la révision totale de la LSCPT. Dans cette nouvelle loi, la mention des données relatives au trafic et à la facturation et des « données permettant l'identification des usagers » est supprimée et remplacée par la notion de "données secondaires" (cf. art. 26 al. 5 LSCPT). Comme l'a constaté le TAF, ce toutefois sans que le contenu matériel de la notion ne change. L'actuelle LSCPT définit en outre la notion de données secondaires à l'art. 8 let. b LSCPT, soit « les données indiquant avec qui, quand, combien de temps et d'où la personne surveillée a été ou est en communication ainsi que les caractéristiques techniques de la communication considérée ». Le TAF a dès lors interprété les notions de « données permettant l'identification des usagers » ainsi que de « données relatives au trafic et à la facturation » à la lumière du projet de nouvel art. 8, let. b LSCPT. Il a conclu que le reproche d'une précision insuffisante de l'art. 15, al. 3, LSCPT s'avère donc infondé (consid. 10.7). Le TAF a constaté que la aLSCPT définissait elle-même, du moins dans les grandes lignes, le but, les organes impliqués et l'étendue du traitement des données. Les termes utilisés étaient certes moins précis, mais les grandes lignes de la réglementation étaient clairement reconnaissables. L'obligation prévue à l'art. 15, al. 3 aLSCPT est ainsi décrite et limitée de manière suffisamment précise, tant du point de vue matériel que temporel, compte tenu de l'objet de la réglementation ; aucune interprétation essentielle n'est laissée aux autorités chargées de l'application de la loi (cf. arrêt du TAF du 9 novembre 2016, consid. 10.6.3 et les références). Le TF s'est rallié à ces conclusions. Il a noté que les requérants eux-mêmes s'appuient sur la définition des données secondaires de la correspondance par télécommunication prévue à l'art. 8 let. b de la nouvelle LSCPT, qui correspond matériellement à la définition en vigueur au moment de son arrêt. Il est donc évident pour tout utilisateur de services de télécommunication ou participant à des télécommunications que les données secondaires liées à ses communications sont enregistrées et conservées pendant six mois par les fournisseurs, en particulier même en l'absence de soupçon concret d'infraction. Il a souligné que l'on ne voit pas quelles indications plus précises la loi aurait dû contenir. Il a constaté, s'appuyant sur la jurisprudence de la Cour, qu'une liste détaillée de toutes les données secondaires à saisir ne serait pas appropriée compte tenu de la situation et de la complexité qui en découle. Une telle énumération serait très technique et probablement peu compréhensible pour un profane. Le TF a donc estimé, comme le TAF, que pour qu'il y ait une base légale suffisante, il faut que l'étendue et le but de l'enregistrement et de la conservation des données secondaires des télécommunications soient fixés dans les grandes lignes dans la loi. Par conséquent, l'art. 15, al. 3 LSCPT constitue une base légale suffisante pour l'enregistrement et la conservation des données secondaires de la correspondance par télécommunication (cf. arrêt du TF du 2 mars 2018, consid. 6.2s. et les références).

59. Actuellement, la base légale pour la conservation des données par les FST est l'art. 26 al. 5 LSCPT, qui prévoit que « Les fournisseurs de services de télécommunication conservent les données secondaires de télécommunication durant six mois » (cf. ég. art. 273 al. 1 et 3 CPP). L'art. 8 lit. b LSCPT définit les données secondaires qui sont enregistrées et conservées. L'art. 31 LSCPT prévoit en outre que le Conseil fédéral précise les renseignements que les fournisseurs de services de télécommunication doivent livrer et les types de surveillance qu'ils doivent exécuter. Il détermine pour chaque type de renseignement et de surveillance les données qui doivent être livrées. Cette délégation est due au fait qu'il s'agit en l'espèce de détails techniques soumis à des changements rapides. Partant, les données à enregistrer sont définies au niveau de

lois au sens formel, à savoir le CPP et la LSCPT. La formulation choisie au niveau de la définition des données est claire et compréhensible pour tout non-spécialiste. Le fait que les données soient techniquement spécifiées par une ordonnance n'invalide pas que l'exigence d'une définition au niveau d'une loi au sens formel soit respectée (cf. Hansjakob, Überwachungsrecht der Schweiz, N 1716, "*La question pertinente pour les droits fondamentaux est celle de savoir si une surveillance peut être effectuée est cette question doit être réglée dans le CPP (art. 273 CPP). La question de savoir comment les fournisseurs de services de télécommunication (FST) doivent mettre en œuvre les surveillances est en revanche moins délicate pour les droits de la personne concernée, de sorte que les détails peuvent être réglés au niveau de l'ordonnance*").

60. Dans la mesure où les requérants affirment (requête, état des faits, ch. 6) que des données relatives au contenu des télécommunications sont stockées dans le cadre de l'enregistrement de données secondaires, cette affirmation n'est pas correcte. Ce type de données n'est enregistré que dans le cadre de surveillances en temps réel.

61. Partant, les données à enregistrer sont définies au niveau de lois au sens formel, à savoir le CPP et la LSCPT. La formulation choisie au niveau de la définition des données est claire et compréhensible pour tout non-spécialiste. Le fait que les données soient techniquement spécifiées par une ordonnance (cf. ci-après, ch. 78ss) n'invalide pas que l'exigence d'une définition au niveau d'une loi au sens formel soit respectée.

62. La législation pertinente, que ce soit le droit applicable à la présente cause, soit l'art. 15, al. 3 aLSCPT (cf. ci-avant, ch. 18) ou la législation actuellement en vigueur, soit l'art. 26 al. 5 LSCPT et l'art. 273 al. 1 et 3 CPP), ainsi que l'art. 8 lit. b LSCPT, satisfait ainsi aux exigences de la Convention. Comme il sera exposé ci-après, sous l'examen de la nécessité de l'ingérence (ch. 65ss), la législation pertinente satisfait en outre à l'exigence de qualité de la loi découlant de la Convention, telle qu'elle est appliquée en pratique (cf. *a contrario* arrêt *Ekimdzhiev*, précité).

E. But légitime

63. L'art. 15 al. 3 LSCPT a pour but de conserver des données secondaires pour d'éventuelles procédures pénales futures, pour l'exécution de demandes d'entraide judiciaire, pour la recherche et le sauvetage de personnes disparues ainsi que pour la recherche d'informations par les services de renseignement (cf. art. 1 al. 1 aLSCPT). Comme l'a retenu le TF (cf. arrêt du 2 mars 2018, consid. 7 et les références), en ce sens, ces mesures ne servent pas seulement la sécurité et l'ordre publics (cf. ég. arrêt *Big Brother Watch*, précité,§§338s.), mais protègent également les droits et libertés d'autrui (voir les arrêts *Peruzzo et Martens c. Allemagne* du 4 juin 2013 [no 7841/08 et 57900/12] § 40 ; *Uzun c. Allemagne* du 2 septembre 2010 [no 35623/05] § 77), ainsi que la santé publique.

64. La collecte et la conservation des données en question sont nécessaires à l'exécution d'obligations positives découlant de nombreux articles de la Convention (entre autres de l'article 8 lui-même, voir par exemple *K.U. c. Finlande*, du 2 décembre 2008, req. no 2872/02, § 49, où la Cour a déclaré que l'article 8 impose à l'État l'obligation de garantir que les fournisseurs d'accès à Internet divulguent l'identité des personnes impliquées dans la diffusion de matériel indécent et offensant, une obligation qui ne peut être remplie sans une conservation générale des données relatives aux utilisateurs d'Internet).

F. Nécessité

65. Pour ce qui est de la question de savoir si une ingérence était « nécessaire dans une société démocratique » à la réalisation d'un but légitime, la Cour a reconnu que les autorités nationales disposent d'une ample marge d'appréciation pour choisir les moyens de sauvegarder au mieux la sécurité nationale. Cette marge d'appréciation va toutefois de pair avec un contrôle européen portant à la fois sur la loi et sur les décisions qui l'appliquent. La Cour doit se convaincre de l'existence de garanties adéquates et effectives contre les abus car un système de surveillance secrète destiné à protéger la sécurité nationale (ou tout autre intérêt national essentiel) risque de saper, voire de détruire, les processus démocratiques sous couvert de les défendre. L'appréciation de cette question est fonction de toutes les circonstances de la cause, telles que par exemple la nature, la portée et la durée des mesures pouvant être prises, les raisons requises pour les ordonner, les autorités compétentes pour les permettre, les exécuter et les contrôler, et le type de recours fourni par le droit interne. La Cour doit rechercher si les procédures de supervision de la décision et de la mise en œuvre de mesures restrictives sont de nature à circonscrire « l'ingérence » à ce qui est « nécessaire dans une société démocratique » (cf. arrêt *Big Brother Watch*, précité, 338s et les références).

66. Le TAF a exposé le droit interne pertinent au considérant 7.2 s. (et les références) de son arrêt du 9 novembre 2016. La surveillance de la correspondance par poste et télécommunication a d'abord été réglée de manière exhaustive dans l'aLSCPT. Avec l'adoption du CPP, les dispositions de procédure pénale ont été pour l'essentiel transférées dans ce code (cf. art. 269 ss CPP), tandis que l'exécution proprement dite de la surveillance de la correspondance par poste et télécommunication, c'est-à-dire les aspects techniques et organisationnels, continuaient à être réglée dans l'aLSCPT. L'aLSCPT fixe pour l'essentiel les obligations des fournisseurs de services postaux et de télécommunication et règle les tâches du service chargé de la surveillance de de la correspondance par poste et télécommunication (service SCPT) (art. 1, al. 2 et art. 2, al. 1 aLSCPT). Les art. 13 (Tâches du service) et art. 15 (Obligations des fournisseurs de services de télécommunication) aLSCPT règlent les tâches du Service SCPT, ainsi que les obligations des FST en matière de surveillance de la correspondance par télécommunication.

1. *Nature des données enregistrées et conservées*

67. Les requérants font valoir se sentir influencés dans leur comportement du fait que leurs données secondaires sont conservées par les FST et du fait que ces données pourraient être utilisées à des fins de surveillance.

68. Le Gouvernement rappelle que les informations enregistrées et conservées sont des données secondaires et non le contenu de la télécommunication. Les données secondaires ne sont pas directement disponibles dans leur intégralité pour les services publics compétents. Elles sont enregistrées par les différents FST et restent dans leur sphère d'influence pendant la durée de conservation, sans être examinées ou mises en relation avec d'autres données. Les autorités n'ont pas accès aux données enregistrées auprès des FST. Lesdites données ne sont ni visionnées ni reliées entre elles au niveau de l'enregistrement et de la conservation auprès des FST, raison pour laquelle aucun profil ne peut être établi à ce stade. Dans la mesure ou les requérants sous-entendent la possibilité d'établir des profils de surf sur internet par le biais des données secondaires enregistrées (ch. 8 état des faits de la requête), le Gouvernement précise que la

surveillance des télécommunications en Suisse n'a pas le grand public pour objet. Elle est uniquement utilisée à l'égard de personnes faisant l'objet de soupçons aggravés d'avoir commis une ou des infractions graves. Donc les données secondaires ne sauraient être utilisées aux fins d'établir des profils aléatoires.

69. La possibilité d'associer des données secondaires, éventuellement en combinaison avec d'autres données, n'existe qu'au niveau de la surveillance (rétroactive) des télécommunications, qui, en l'espèce, se situe en dehors de l'objet du litige (cf. ci-avant, ch. 6). Seul l'accès des autorités de poursuite pénale aux données stockées (réglé par le CPP) permet leur exploitation et leur mise en relation (ATF 1C_598/2016 consid. 5.3-5.5). Cet accès est soumis aux conditions strictes détaillées ci-dessous, ch. 94ss.

70. Le Gouvernement relève que dans le complément à l'état des faits de leurs requêtes, les requérants mélangent surveillance rétroactive, surveillance en temps réel, demandes de renseignements, données contractuelles etc. Ils citent sans trier tous les types de données liées. Il précise également que les données citées par les requérants au ch. 2.1 du complément à l'état des faits, sont des données saisies lors de la conclusion du contrat et non pas dans le cadre des données secondaires. De même, les données citées au ch. 2.2 sont pour la plupart des données relatives à des surveillances en temps réel. Quant aux allégations avancées au ch. 3.1, le Gouvernement précise qu'il n'y a pas de pratique relative aux données secondaire qui ne soit pas définie dans les dispositions légales. Quant aux allégations figurant ch. 3.2, il souligne que les recherches par champ d'antennes ont comme objectif d'identifier les ressources d'adressage de personnes soupçonnées d'infractions graves. Par exemple dans une série de braquages, les recoupements des recherches par champ d'antennes permettent d'identifier les ressources d'adressages communes aux évènements. Ce qui peut amener à identifier les auteurs. Au ch. 4 du complément à l'état des faits, le Gouvernement précise qu'il s'agit de questions générales de sécurité des données ne concernant pas la question de la licéité de l'enregistrement des données secondaires. Au ch. 6 du complément à l'état des faits, les requérants confondent surveillance en temps réel et surveillance rétroactive. Le contenu des télécommunications n'est pas stocké dans les données secondaires. La protection du secret professionnel est exécutée sous la direction d'un tribunal.

71. Dans l'arrêt *Big Brother Watch*, précité, (§§ 363s), la Cour a considéré que l'interception et la conservation des données de communication associées, ainsi que les recherches effectuées sur celles-ci, doivent être analysées au regard des mêmes garanties que celles applicables au contenu des communications. Cela étant, même si l'interception des données de communication associées est normalement autorisée en même temps que l'interception du contenu des communications, une fois qu'elles ont été obtenues, ces données peuvent faire l'objet d'un traitement différent par les services de renseignement. Compte tenu de la nature différente des données de communication associées et des différentes façons dont elles sont utilisées par les services de renseignement, la Cour est d'avis que, à condition que les garanties énoncées ci-dessus (ch. 46) soient en place, il n'est pas nécessaire que les dispositions juridiques régissant le traitement des données de communication associées soient identiques en tous points à celles régissant le traitement du contenu des communications.

2. Enregistrement et conservation systématiques des données secondaires

72. Comme devant les autorités nationales, les requérants mettent tout d'abord en doute l'utilité et l'effectivité de la collecte systématique des données secondaires par les FST. Ils reprochent aux autorités nationales de ne pas avoir examiné ces questions.

73. Dans sa jurisprudence, la Cour ne remet pas en cause le système d'enregistrement et de conservation systématiques des données secondaires, en soi. Ce système doit toutefois être entouré de garanties suffisantes (cf. arrêt *Ekimdzhiev*, précité, §§ 394ss).

74. Dans son arrêt du 2 mars 2018, le TF s'est longuement penché sur la question de savoir si l'enregistrement et la conservation systématiques des données secondaires de la correspondance par télécommunication étaient nécessaires pour atteindre les buts légitimes cités ci-avant, ch. 63s. Il a examiné en particulier s'il suffirait (comme l'ont fait valoir les requérants) de ne sauvegarder les données secondaires nécessaires qu'en cas de soupçon d'infraction (procédure dite de "quick-freeze"). Dans ce contexte, il s'est penché sur la jurisprudence de la Cour de Justice de l'Union Européenne et sur les critiques exprimées dans la doctrine. Il a retenu que, bien que ces arrêts ne soient pas sans importance pour l'appréciation du présent litige, ils ne sont pas contraignants pour la Suisse. Il a rappelé que l'essence de la conservation des données consiste précisément à conserver pendant un certain temps les données externes générées par les utilisateurs de services de télécommunication lors de leurs communications, sans savoir si elles seront ou non importantes pour une éventuelle enquête pénale future (cf. consid. 8.2.2 et les références ; cf. ég. arrêt du TAF du 9 novembre 2016, consid. 12.6 et les références). Le législateur fédéral suisse s'est expressément prononcé en faveur de ce système de stockage et de conservation exhaustif et sans motif des données secondaires de télécommunication et a confirmé cette décision dans le cadre de la révision de la LSCPT. Lors des débats parlementaires au Conseil national, l'introduction de la procédure de "quick freeze" comme mesure moins contraignante a été explicitement rejetée, au motif que cette dernière présente une utilité moindre que le système en vigueur et qu'elle n'est pas en mesure de produire les effets souhaités par le législateur. La procédure de "quick freeze" se rapprocherait plutôt d'une surveillance en temps réel. En tout état de cause, une surveillance rétroactive serait pratiquement impossible, puisque les données secondaires ne pourraient être mises à disposition qu'après l'apparition d'un fort soupçon. La possibilité de surveillance rétroactive créée et voulue par le législateur implique que les données (secondaires) sont enregistrées sans motif et conservées (pour une durée limitée). En effet, si la conservation des données secondaires n'était ordonnée qu'après la découverte d'un soupçon, les données pertinentes risqueraient d'être déjà effacées. De même, si moins de données étaient stockées, il se pourrait qu'une surveillance rétroactive ne puisse pas être effectuée, car il manquerait des données pour établir un lien. Pour une surveillance rétroactive, il est donc nécessaire de stocker autant que possible un grand nombre de données secondaires différentes. Le TF a considéré que cette décision était conforme à la Constitution et à la Convention (cf. arrêt du TF du 2 mars 2018, consid. 8.2.2 et les références ; cf. ég. arrêt du TAF du 9 novembre 2016, consid. 12.6 et les références).

75. Comme l'a retenu le TF, la collecte systématique des données secondaires par les FST est apte à atteindre l'objectif visé, comme le prouvent les exemples cités par les juridictions nationales (cf. en particulier consid. 12.5 de l'arrêt du TAF du 9 novembre 2016). Grâce à la conservation de données secondaires, les autorités de poursuite pénale disposent de possibilités supplémentaires pour élucider des infractions. En raison de la large diffusion et de l'utilisation des moyens de communication électroniques, ces mesures s'avèrent être un moyen utile pour les enquêtes pénales. Dans le cadre du contrôle des mesures de surveillance, le TF a affirmé à plusieurs reprises que le résultat d'une collecte rétroactive de données secondaires pouvait être essentiel pour l'élucidation et la qualification juridique de l'infraction faisant l'objet de l'enquête. Ainsi, selon la jurisprudence, la surveillance rétroactive peut être appropriée pour déterminer le motif de l'infraction et les circonstances exactes de l'infraction et des informations sur

la relation personnelle entre la victime et le prévenu ainsi que sur les réseaux de relations peuvent être rendues disponibles. Dans le cadre d'une enquête pénale pour vol en bande et par métier, dommages à la propriété et violation de domicile, les relevés de données marginales et les recoupements correspondants avaient notamment pour but de vérifier si les prévenus s'étaient entendus par téléphone entre eux ou avec d'autres personnes aux dates et sur les lieux d'autres infractions pertinentes. Dans un autre cas, la comparaison des données de bord de liaison devait servir à déterminer si plusieurs braquages avaient été exécutés, du moins en partie, par le même auteur. Il ne peut pas être contesté que l'enregistrement et la conservation de données secondaires et, partant, la surveillance rétroactive de la correspondance par télécommunication sont de nature à contribuer à l'élucidation d'infractions. Cela est d'autant plus vrai que la surveillance rétroactive permet d'obtenir des données non pas seulement après l'existence d'un soupçon fondé, mais déjà à un stade antérieur (cf. arrêt du TAF du 9 novembre 2016, consid. 12.5 et les références). En outre, l'enregistrement et la conservation des données marginales permettent une surveillance rétroactive différenciée en permettant aux autorités de poursuite pénale de surveiller un trafic de télécommunication donné à l'aide de différentes cibles, c'est-à-dire de différents paramètres techniques tels que le numéro d'appel d'un suspect ou le numéro d'un appareil utilisé par celui-ci. Comme l'ont constaté le TAF et le TF, le fait que l'Institut Max Planck ait conclu en 2011 que rien n'indiquait que l'enregistrement et la conservation des données secondaires pratiqués en Suisse depuis plusieurs années avaient systématiquement permis d'élucider davantage d'infractions ne change rien à cette conclusion (cf. consid. 12.5 de l'arrêt du TAF du 9 novembre 2016). Dans ce contexte, il faut également tenir compte du fait que la surveillance rétroactive des données secondaires peut servir non seulement à confondre un auteur et à empêcher de futures infractions, mais aussi à disculper une personne injustement soupçonnée. Comme l'a conclu le TF, grâce à la conservation de données secondaires, les autorités de poursuite pénale disposent de possibilités supplémentaires pour élucider des infractions (cf. arrêt du TF du 2 mars 2018, consid 8.1 et les références).

76. En outre, comme l'on constaté les juridictions nationales, en l'espèce, il n'apparaît pas que les données secondaires à enregistrer et à conserver dépassaient, d'un point de vue matériel, ce qui est nécessaire pour atteindre l'objectif visé (cf. arrêt du TF du 2 mars 2018, consid. 8.2.2 et les références ; cf. ég. arrêt du TAF du 9 novembre 2016, consid. 12.6 et les références).

3. Protection et sécurité des données

77. Le TF a examiné en détail si la saisie et la conservation systématiques des données litigieuses étaient accompagnées de garanties juridiques appropriées et efficaces afin de prévenir les abus et l'arbitraire (considérants 8.3.4 - 8.3.9). Il a répondu par l'affirmative en se fondant sur la jurisprudence (de l'époque) de la Cour relative à l'art. 8 en relation avec l'art. 13 CEDH. Ce faisant, il a tenu compte des réglementations pertinentes au niveau de la loi et de l'ordonnance (aLSCPT et aOSCPT), ainsi que des directives techniques, organisationnelles et administratives du Service SCPT (consid. 8.3.6) et du contrôle effectué par le Préposé fédéral à la protection des données et à la transparence (PFPDT).

78. Pour ce qui est de la protection et de la sécurité des données, l'art. 9 al. 1 aOSCPT (cf. ci-avant, ch. 30) renvoie notamment à l'aOLPD (cf. ch. 5). L'art. 9, al. 2, aOSCPT (cf. ci-avant, ch. 30) précisait en outre que « les fournisseurs de services postaux ou de télécommunication se conforment aux instructions du service pour les questions de sécurité des données relatives à la transmission des données provenant d'une

surveillance. Ils sont responsables de la sécurité des données jusqu'au point de transmission des données au service ». L'art. 33, al. 1bis aOSCPT disposait que « le Service SCPT règle dans des directives les détails techniques et administratifs relatifs à la mise en œuvre de chaque type de surveillance ». Les directives du 22 octobre 2015 réglant les aspects d'ordre organisationnel et administratif de la surveillance des télécommunications (OAR), ainsi que les directives techniques applicables à la surveillance des télécommunications (TR TS)[1] renvoyaient à la LPD (cf. ci-avant, ch. 3) pour la garantie de la sécurité des données par les fournisseurs de services de télécommunication et le Service. La LPD régit le traitement de données concernant des personnes physiques et morales effectué par des personnes privées ou des organes fédéraux (art. 2, al. 1, LPD). Selon l'art. 7 LPD (sécurité des données), « les données personnelles doivent être protégées contre tout traitement non autorisé par des mesures organisationnelles et techniques appropriées ». L'al. 2 prévoyait que « Le Conseil fédéral édicte des dispositions plus détaillées sur les exigences minimales en matière de sécurité des données » (cf. arrêt du TF du 2 mars 2018, consid. 8.3.5. et les références).

79. L'art. 16 let. d aOSCPT (cf. ci-avant, ch. 34), cite en outre les données pouvant être transmises si la communication a été établie (surveillance rétroactive). Pour internet, cf. art. 24b aOSCPT.

80. Selon l'art. 20 OLPD , « Les organes fédéraux responsables prennent, conformément aux art. 8 à 10, les mesures techniques et organisationnelles propres à protéger la personnalité et les droits fondamentaux des personnes dont les données sont traitées » (première phrase). Selon les explications pertinentes et non contestées du TAF, cette disposition s'applique également aux FST, d'autant plus qu'ils ont été chargés de tâches publiques de la Confédération lors de l'enregistrement et de la conservation de données secondaires de la correspondance par télécommunication (art. 3 let. h LPD ; cf. consid. 12.7.3 de l'arrêt du TAF du 9 novembre 2016 ; arrêt du TF du 2 mars 2018, consid. 8.3.5. et les références).

81. Les articles 8 à 10 OLPD (cf. ci-avant, ch. 40ss) détaillent les mesures techniques et organisationnelles que doivent prendre la personne privée qui traite des données personnelles ou qui met à disposition un réseau télématique ainsi que le maître du fichier. Quiconque traite des données personnelles ou exploite un réseau de communication de données doit, selon l'art. 8 al. 1 OLPD (cf. ch. 41), quiconque traite des données personnelles ou qui met à disposition un réseau télématique assure la confidentialité, la disponibilité et l'intégrité des données afin de garantir de manière appropriée la protection des données. Elle protège les systèmes notamment contre les risques de destruction accidentelle ou non autorisée ; perte accidentelle ; erreurs techniques ; falsification, vol ou utilisation illicite ; modification, copie, accès ou autre traitement non autorisés. Les mesures techniques et organisationnelles doivent être appropriées lors d'une évaluation globale tenant compte du but, du type et de l'ampleur du traitement des données, des risques estimables pour les personnes concernées et de l'état de la technique. De telles mesures doivent notamment empêcher, dans le cas de fichiers et de systèmes d'information automatisés, que des données soient traitées de manière illicite.

82. A cet effet, l'art. 9, al. 1 OLPD (cf. ci-avant, ch. 41) définit différents objectifs qui doivent être mis en œuvre dans le respect du principe de proportionnalité. En font notamment partie les contrôles des supports de données, du transport, de la communication, du stockage, des utilisateurs et de l'accès. Parmi les mesures de protection techniques ou

[1] Directives publiées qu'en anglais.

organisationnelles, on peut citer les restrictions d'accès, les filtres (comme les pare-feu), le cryptage des données, les configurations de système sûres, les logiciels de protection contre les virus informatiques, les attaques ou l'espionnage, la formation du personnel, les contrôles et la journalisation.

83. Comme l'a également souligné le TF, dans la mesure où les requérants critiquent le fait qu'il ne suffit pas d'invoquer des dispositions générales et abstraites pour garantir la sécurité des données, ils ne peuvent pas être suivis. Les directives susmentionnées (ch. 78) énuméraient des mesures importantes qui garantissaient un traitement sûr des données. Ainsi, la communication d'informations dans le sens d'un contrôle du transport et de la communication ne devait être effectuée que par du personnel préalablement authentifié et de manière cryptée (directive OAR, ch. 11.1 et directive TR TS, ch. 14.1). En outre, seules les personnes autorisées à utiliser le système de consultation des informations relatives aux abonnés aux services de télécommunication et disposant d'une identification d'utilisateur avaient accès à ce système. Ces personnes devaient se faire enregistrer au préalable auprès du service SCPT et étaient soumises par ce dernier à un contrôle (Directive technique et administrative du 30 novembre 2004 à l'intention des fournisseurs de services de télécommunication concernant le système d'information des centres d'appel, ch. 10). Ainsi, les objectifs de contrôle de la mémoire, des utilisateurs et de l'accès aux fichiers automatisés étaient respectés. En outre, les FST, tout comme le Service, devaient protéger leurs systèmes contre tout accès non autorisé et les personnes impliquées devaient respecter la confidentialité des informations dans le cadre de leurs activités (directive OAR, ch. 11.3 s. ou directive TR TS, ch. 14.3 s.). Elles s'exposaient à des sanctions pénales en cas de violation du secret professionnel (art. 35 LPD), tout comme en cas de violation du secret des télécommunications (art. 43 de la loi sur les télécommunications [LTC ; RS 784.10]) par la communication de données enregistrées à des tiers (art. 321ter CP). Comme l'a constaté le TF, l'effet dissuasif qui en découlait contribuait ainsi à la protection contre les traitements abusifs de données, bien qu'un comportement illicite d'individus - comme la vente ou la disparition de données critiquées par les requérants - ne puisse jamais être totalement exclu. En outre, les requérants n'ont pas fait valoir et rien n'indiquait que des pirates informatiques ou des autorités étrangères aient voulu accéder à leurs données ou que les fournisseurs de services de télécommunication les aient rendues accessibles à des tiers non autorisés (cf. arrêt du TF du 2 mars 2018, consid. 8.3.6. et les références).

84. Comme l'a également constaté le TF, le fait que ni les directives susmentionnées, ni les FST n'informent de manière complète et détaillée sur les mesures techniques et organisationnelles n'est pas critiquable, d'autant plus que leur divulgation pourrait nuire considérablement aux objectifs de sécurité poursuivis.

85. En outre, le traitement des données est soumis au contrôle du PFPDT, qui « exerce ses fonctions de manière indépendante et sans recevoir ni solliciter d'instructions de la part d'une autorité ou d'un tiers » (art. 26, al. 3 LPD). En vertu de l'art. 27 LPD, « Le préposé surveille l'application par les organes fédéraux de la présente loi et des autres dispositions fédérales relatives à la protection des données » (al. 1). « Aux fins d'établir les faits, il peut exiger la production de pièces, demander des renseignements et se faire présenter des traitements » (al. 3, 1re phrase). Dans ce contexte, le PFPDT dispose également de compétences étendues pour vérifier la sécurité des données dans le domaine de l'enregistrement et de la conservation des données secondaires des télécommunications par les FST ou de la transmission de ces informations au Service en cas d'ordre de surveillance. On peut s'attendre à ce qu'il exerce effectivement ces droits dans le cadre de son activité de surveillance, qu'il peut engager de sa propre initiative

ou à la demande de tiers, et qu'il découvre dans cette mesure des irrégularités. « S'il apparaît que des prescriptions sur la protection des données ont été violées, le préposé recommande à l'organe fédéral responsable de modifier ou de cesser le traitement. Il informe le département compétent ou la Chancellerie fédérale de sa recommandation » (al. 4). « Si une recommandation est rejetée ou n'est pas suivie, il peut porter l'affaire pour décision auprès du département ou de la Chancellerie fédérale. La décision sera communiquée aux personnes concernées (al. 5). Le PFPDT a qualité pour recourir contre la décision visée à l'al. 5 et contre celle de l'autorité de recours (al. 6) (cf. ég. arrêt du TF du 2 mars 2018, consid. 8.3.6. et les références).

86. Comme l'a constaté le TF, en l'absence d'indices ou d'indications contraires, on peut partir du principe, que les dispositions pertinentes en matière de protection des données pour un traitement sûr des informations personnelles ont été respectées dans le cas des requérants.

87. Cela vaut en particulier également pour la *délocalisation (partielle) du traitement des données à l'étranger*. Conformément aux explications du TAF dans son arrêt du 9 novembre 2016 (cf. consid. 12.7.3), « le mandant doit notamment s'assurer que le tiers garantit la sécurité des données » (art. 10a al. 2 LPD). En effet, l'organe fédéral qui fait traiter des données personnelles par des tiers reste responsable de la protection des données (cf. art. 16, al. 1 LPD et art. 22, al. 2, aOLPD). Si le tiers n'est pas soumis à la LPD, l'organe responsable veille à ce que d'autres dispositions légales assurent une protection équivalente ou, à défaut, garantit une telle protection par des clauses contractuelles (art. 22, al. 3, aOLPD). En cas de transfert d'une partie du traitement des données à un tiers à l'étranger - par exemple dans le cadre d'une externalisation informatique - il convient en outre de respecter l'art. 6 LPD. Selon l'alinéa 1 de cet article, « Aucune donnée personnelle ne peut être communiquée à l'étranger si la personnalité des personnes concernées devait s'en trouver gravement menacée, notamment du fait de l'absence d'une législation assurant un niveau de protection adéquate ». La liste des Etats établie par le PFPDT permet de déterminer si tel est le cas (art. 31, al. 1, let. d, LPD en relation avec l'art. 7, al. 2, LPD) (cf. ég. arrêt du TF du 2 mars 2018, consid. 8.3.6. et les références).

88. Outre les mesures de protection susmentionnées, les requérants disposent de garanties procédurales pour se protéger contre des traitements de données inappropriés :

89. Il s'agit en premier lieu du *droit d'accès* prévu à l'article 8 LPD (cf. ci-avant, ch. 26). Dans ce sens, le droit d'accès selon l'art. 8 LPD sert à la mise en œuvre de la protection de la personnalité en permettant aux personnes concernées de contrôler les données traitées à leur sujet dans un fichier, dans le but de vérifier et, le cas échéant, d'imposer le respect des principes et dispositions de la protection des données. L'art. 9 LPD (cf. ci-avant, ch. 27) énumère différents motifs de restriction du droit d'accès. Selon son alinéa 1, lettre a, le maître d'un fichier peut refuser, restreindre ou différer l'accès si une loi au sens formel le prévoit. Les fournisseurs de services de télécommunication ont invoqué cette exception pour refuser de communiquer aux requérants les données secondaires en cause dans le litige. Le TF a constaté qu'en l'espèce, ces droits garantissent une protection efficace des droits fondamentaux, d'autant plus qu'ils ouvrent la possibilité d'imposer, le cas échéant, un enregistrement et une conservation licites des données secondaires de télécommunication par les FST, y compris par voie judiciaire. Les requérants peuvent invoquer le droit d'accès en matière de protection des données selon l'art. 8 LPD pour obtenir toutes les informations qui se rapportent à leur personne ou qui

peuvent leur être attribuées (cf. arrêt du TF du 2 mars 2018, consid. 8.3.7. et les références).

90. En font également partie les droits selon l'art. 25 al. 1 LPD (cf. ci-avant, ch. 28). Selon cette disposition, on peut exiger de l'organe fédéral responsable, en présence d'un intérêt digne de protection, qu'il s'abstienne de traiter des données personnelles de manière illicite, qu'il élimine les conséquences d'un traitement illicite ou qu'il constate le caractère illicite du traitement. L'art. 25, al. 3, let. a LPD (cf. ci-avant, ch. 28) confère au requérant le droit de demander que l'organe fédéral rectifie les données personnelles, les détruise ou en empêche la communication à des tiers (cf. en outre l'art. 5, al. 2 LPD). Pour cela, il faut que les données ne puissent pas ou plus du tout être traitées par l'organe fédéral responsable. C'est notamment le cas lorsque le traitement des données n'est pas (ou plus) nécessaire à l'accomplissement de la tâche publique ou que des données collectées légalement sont conservées trop longtemps. Les personnes concernées ont la possibilité d'intenter une action en justice contre les décisions relatives à ces droits en matière de protection des données (cf. art. 33, al. 1, LPD), ce qui leur permet de faire examiner l'affaire par un tribunal indépendant (cf. arrêt du TF du 2 mars 2018, consid. 8.3.7. et les références).

91. L'art. 15 al. 3 aLSCPT (ci-avant, ch. 18) prévoyait une durée de conservation de six mois. Il en va de même du droit actuellement en vigueur (cf. l'art. 26 al. 5 LSCPT et l'art. 273 al. 1 et 3 CPP). Les données secondaires de télécommunication enregistrées devaient (et doivent) donc être effacées (irrévocablement) par les FST à l'expiration de ce délai, à moins que des motifs justificatifs particuliers n'imposent une conservation plus longue. Les FST ont d'ailleurs expressément confirmé dans la présente procédure qu'ils effacent les données marginales de la correspondance par télécommunication enregistrées après six mois (cf. arrêt du TF du 2 mars 2018, consid. 8.3.8. et les références).

92. Actuellement, toute la réglementation relative à la surveillance des télécommunications est définie au moyen de lois et d'ordonnances. Il n'y a pas de pratique relative aux données secondaire qui ne soit pas définie dans les dispositions légales. Le Service SCPT est responsable de la sécurité du système de traitement des données (art. 12 LSCPT). L'ordonnance sur le système de traitement pour la surveillance de la correspondance par poste et télécommunication du 15 novembre 2017 (OST-SCPT ; RS 780.12), prévoit aux art. 10ss des mesures pour la protection et la sécurité des données. L'art. 10 al. 1 OST-SCPT prévoit que le Service SCPT s'assure en particulier des points suivants par des mesures techniques et organisationnelles :

    - la protection des accès et contre les modifications: par une authentification sûre des personnes et des services habilités et une description détaillée de leurs droits respectifs de lecture et d'écriture (let. a);

    - le contrôle du transport: par une transmission sécurisée des données du système de traitement (let. b);

    - Le contrôle des accès et des modifications : par la journalisation de tous les accès à des données et de toutes les modifications de données et par des contrôles réguliers par sondage pour détecter des irrégularités (let. c).

    Il s'assure également des mesures à prendre en cas de dérangement (art. 11 OST-SCPT) et de la destruction des données (art. 14 OST-SCPT). Seules les personnes définies et autorisées par l'ordre de surveillance peuvent obtenir accès aux données

de surveillance (arts. 9 LSCPT et 8 OST-SCPT). L'obligation de garder le secret est prévu par l'art. 6 OSCPT.

93. C'est à juste titre que les tribunaux nationaux ont dès lors constaté que les dispositions de la législation sur la protection des données offrent une protection suffisante contre les traitements de données non autorisés et les détournements de finalité. Comme l'a constaté le TF, les requérants n'ont ni prétendu ni démontré qu'il y aurait eu en l'espèce un traitement non autorisé de leurs données ou un use de ces données non conformes à leur finalité (cf. arrêt du TF du 2 mars 2018, consid. 8.3.6. et les références).

4. Accès aux données conservées

94. Comme il a été dit (ch. 4ss), la question des droits d'accès n'est pas objet du présent litige et n'est dès lors examiné que dans la mesure où cela était nécessaire pour examiner la proportionnalité de la conservation systématique des données pendant six mois prévue par l'art. 15 al. 3 aLSCPT (ci-avant, ch. 18).

95. Les données secondaires peuvent certes être enregistrées sans motif, mais ne peuvent être transmises aux autorités de poursuite pénale que lorsque de graves soupçons laissent présumer qu'un crime, un délit ou une contravention au sens de l'art. 179septies CP a été commis (art. 273, al. 1 aCPP, cf. ci-avant, ch. 20) et que les conditions visées à l'art. 269, al. 1, let. b et c a CPP (cf. ci-avant, ch. 19), sont remplies, soit que cette mesure se justifie au regard de la gravité de l'infraction et que les mesures prises jusqu'alors dans le cadre de l'instruction sont restées sans succès ou les recherches n'auraient aucune chance d'aboutir ou seraient excessivement difficiles en l'absence de surveillance (principe de proportionnalité) (cf. également arrêt du TAF du 9 novembre 2016, consid. 12.7 et les références ; cf. *a contrario* arrêt *Ekimdzhiev*, précité, § 406). En vertu du principe de proportionnalité (art. 197 al. 1 let. c et d et 269 al. 1 let. b aCPP), la mesure de surveillance doit être adéquate et poursuivre un intérêt public; elle doit ainsi être susceptible d'obtenir des résultats concrets. La mesure de surveillance doit avoir un lien matériel direct avec l'infraction faisant l'objet de l'enquête. Les circonstances d'espèce sont dès lors déterminantes pour examiner la gravité de l'infraction ; à cet égard, il n'est pas en soi suffisant que celle-ci figure dans le catalogue de l'art. 269 al. 2 aCPP. La surveillance est ainsi admissible si, objectivement et subjectivement, elle se justifie au regard de la nature du bien juridiquement protégé atteint par l'acte punissable, la mise en danger de ce dernier, la gravité de la lésion, le mode opératoire utilisé, l'énergie criminelle déployée et/ou les mobiles de l'auteur (ATF 141 IV 459 consid. 4.1 p. 461 s.; 142 IV 289 consid . 2.3 p. 295 s.). Enfin, une surveillance ne peut être autorisée que si elle respecte le principe de subsidiarité (art. 269 al. 1 let. c aCPP). Celui-ci présuppose notamment que l'autorité examine d'abord si une autre mesure moins incisive peut atteindre le résultat recherché (*ultima ratio*: ATF 141 IV 459 consid. 4.1 p. 462; 142 IV 289 consid . 2.3 p. 296). Les griefs des requérants selon lesquels le CPP permet l'utilisation des données secondaires de télécommunication par les autorités étatiques même dans le cadre d'infractions de gravité légère (requêtes, ch. 3) ne sont dès lors pas fondés : en vertu des arts. 273 al 1 et 269 al. 1 lit b aCPP, une mesure de surveillance rétroactive doit être justifiée au regard de la gravité de l'infraction. Ainsi, une telle mesure n'est pas fondée et ne sera dès lors pas autorisée aux fins de poursuivre une infraction de moindre gravité. Il résulte donc de ce qui précède, que la simple réalisation d'un crime, d'un délit ou de la contravention prévue à l'art. 179 septies aCPP ne suffit pas pour justifier la mise en œuvre d'une surveillance rétroactive. Il faut que ces infractions aient également des conséquences graves.

96. La protection du secret professionnel est garantie par le tri des informations qui n'ont pas de rapport avec l'objet de l'enquête ni avec le motif pour lequel la personne concernée est soumise à surveillance, tri qui doit être exécuté sous la direction d'un tribunal. Ce tri est opéré de telle sorte que les autorités de poursuite pénale n'aient connaissance d'aucun secret professionnel (art. 271 al. 1 aCPP).

97. Comme la surveillance du contenu des communications (art. 272 al. 1 aCPP), les mesures prises en vertu de l'art. 273 aCPP nécessitent l'autorisation du tribunal des mesures de contrainte (art. 273 al. 2 aCPP ; cf. ci-avant, ch. 20). Ce tribunal doit statuer dans un délai de cinq jours à compter de l'ordonnance de surveillance ou de communication de renseignements, en motivant brièvement sa décision (art. 274 al. 2 aCPP ; cf. ci-avant, ch. 21 ; cf. ég. arrêt *Ekimdzhiev*, précité, § 405, dans lequel la Cour a estimé que "*the provision of reasons, even if succinct, is the only way of ensuring that the judge examining an access application has properly reviewed the application and the materials which support it, and has truly directed his or her mind to the questions whether accessing the communications data at issue would be a justified and proportionate interference with the Article 8 rights of the person(s) whose data is being accessed, and any person(s) likely to be collaterally affected by that*"). Le tribunal des mesures de contrainte statue sur la base de la requête du ministère public motivée et étayée par les pièces essentielles de la procédure (art. 274 al. 1 aCPP ; cf. ci-avant, ch. 21 ; cf. *a contrario* arrêt *Ekimdzhiev*, précité, § 401ss). Dans l'ATF 142 IV 289 (en particulier consid. 2.2.2 et 2.2.3), le TF a rappelé que pour effectuer ce contrôle, le tribunal des mesures de contrainte se fondera en particulier sur la demande du ministère public, l'ordre de surveillance de ce dernier, un exposé des motifs et les actes déterminants du dossier (cf. art. 274 al. 1 let. a et b CPP ; cf. ci-avant, ch. 21). La requête contiendra notamment une - courte - description de l'état de fait, l'indication de l'infraction poursuivie et des circonstances fondant les graves soupçons. Elle exposera de plus les démarches entreprises au cours de l'enquête, en particulier celles restées sans succès. Quant aux actes déterminants que doit fournir le ministère public au tribunal des mesures de contrainte, il peut s'agir de pièces à conviction au sens de l'art. 192 CPP. La doctrine mentionne aussi des rapports de police et/ou des notes du ministère public, voire même des éléments recueillis au cours des premières 24 heures de surveillance. L'établissement des graves soupçons peut aussi se fonder sur les déclarations de témoins, de parties (art. 104 CPP), d'autres participants (art. 105 CPP), ainsi que de collaborateurs des autorités pénales (consid. 2.2.2 et les références). Il a retenu qu'il ne faut cependant pas perdre de vue que les déclarations de parties ou de témoins peuvent manquer d'objectivité. Dès lors, la seule affirmation - notamment d'une partie - sans indication de source ou sans avoir le caractère spécifique de témoignage n'est en principe pas suffisante. Il en va de même de simples spéculations, de rumeurs ou de suppositions générales. Une appréciation plus nuancée est envisageable s'agissant des éléments relevés par la police dans ses rapports. En effet, il arrive que ceux-ci ne puissent pas être davantage étayés, notamment afin de protéger, provisoirement ou durablement, l'identité de certains informateurs ; l'utilisation de telles informations n'en est pas pour autant exclue si celles-ci semblent objectivement plausibles au vu des circonstances entourant l'enquête (cf. consid. 2.2.3 et les références). Dès lors, contrairement à ce qui était le cas dans l'arrêt *Ekimdzhiev*, (précité, § 309 en lien avec §§312-317), la procédure d'autorisation présente les garanties nécessaires. Le "third factor" (§317 de l'arrêt précité) n'est pas donné en Suisse.

98. L'ordre du ministère public doit être déposé auprès du Service et doit - dans la mesure où il concerne la surveillance de la correspondance par télécommunication - contenir les indications prévues à l'art. 15 aOSCPT (cf. ch. 32), respectivement à l'art. 23

aOSCPT. Dans ce contexte, l'autorisation doit notamment se prononcer sur la nécessité de prendre des mesures pour protéger les secrets professionnels (art. 274, al. 4, let. a, aCPP ; cf. ci-avant, ch. 21).

99. En principe, le ministère public communique aux personnes surveillées, au plus tard à la fin de la procédure préliminaire, le motif, le type et la durée de la surveillance (art. 279 al. 1 aCPP, cf. ci-avant, ch. 25). Une communication formelle est nécessaire. Avec l'accord du tribunal des mesures de contrainte, il est possible de différer la communication ou d'y renoncer aux conditions suivantes : a. les informations recueillies ne sont pas utilisées à des fins probatoires ; b. cela est indispensable pour protéger des intérêts publics ou privés prépondérants (art. 279 al. 2 aCPP, cf. ch. 25). Les personnes dont le raccordement de télécommunication ou l'adresse postale ont été surveillés ou celles qui ont utilisé le même raccordement ou la même adresse postale peuvent interjeter recours conformément aux art. 393 à 397 aCPP (art. 279 al. 3 aCPP, cf. ch. 25).

100. Lorsqu'une surveillance du service de télécommunication est ordonnée, le Service vérifie notamment si la surveillance concerne une infraction pouvant être surveillée en vertu du droit applicable et si elle a été ordonnée par l'autorité compétente (art. 13 al. 1 let. a aLSCPT ; cf. ci-avant, ch. 15). Il ordonne aux fournisseurs de prendre les mesures nécessaires à la surveillance (art. 13 al. 1 let. b aLSCPT, cf. ci-avant, ch. 15) et reçoit les données secondaires qu'ils transmettent avant de les transmettre à l'autorité qui a ordonné la surveillance (art. 13 let. e aLSCPT, cf. ci-avant, ch. 15 et art. 8 al. 3 OSCPT). Il met en œuvre les mesures prises par l'autorité d'approbation pour protéger les secrets professionnels et conserve l'ordre de surveillance pendant un an après la cessation de la mesure (art. 13 al. 1 let. f et i aLSCPT, cf. ci-avant, ch. 15) (cf. arrêt du TF du 2 mars 2018, consid. 8.3.2 et les références).

101. Comme l'a rappelé le TF, il ressort de ce qui précède que les autorités de poursuite pénale n'ont pas un accès direct et illimité aux données accessoires de télécommunication stockées et conservées par les fournisseurs de services de télécommunication. Au contraire, cet accès est soumis à des exigences strictes qui entraînent des restrictions importantes, notamment en ce qui concerne le cercle des personnes, le type et l'étendue des données, et qui contribuent, avec de nombreux mécanismes de protection, à limiter les possibilités d'appréciation et d'accès des autorités pénales (cf. arrêt du TF du 2 mars 2018, consid. 8.3.3. et les références).

102. Le droit actuellement en vigueur présente les mêmes garanties. Une mesure de surveillance rétroactive est soumise aux conditions cumulatives suivantes :

1) La personne concernée par la surveillance doit faire l'objet de graves soupçons (art. 273 al. 1 CPP). Selon la jurisprudence du TF, afin que les soupçons graves puissent être fondés, des éléments de preuves sont nécessaires permettant d'établir avec forte vraisemblance la réalisation des éléments constitutifs de l'infraction (ATF 1B_230/2013, consid. 5.1).

2) L'infraction reprochée doit être un crime, un délit ou la contravention prévue à l'art. 179 septies CPP et doit être de gravité importante (art. 273 al. 1 et 269 al. 1 lit b CPP).

3) La surveillance rétroactive doit être ordonnée par un ministère public (art. 269 ss. CPP).

4) La surveillance rétroactive doit respecter le principe de subsidiarité (arts. 273 al. 1 et 296 al. 1 lit b CPP). Il doit donc être établi que toutes les mesures moins invasives préalables soient restées sans succès ou qu'en l'absence d'une telle surveillance les recherches n'aient aucune chance d'aboutir. Une surveillance rétroactive est dès lors la dernière mesure de contrainte à mettre en œuvre.

5) La surveillance rétroactive doit faire l'objet d'une vérification formelle au niveau du Service SCPT (art. 16 LSCPT).

6) La surveillance rétroactive est soumise à l'autorisation d'un tribunal des mesures de contraintes (art. 272 al. 1 CPP) qui examine, dans chaque cas particulier, entre autres, la proportionnalité de la mesure.

7) La protection du secret professionnel (cf. ci-dessus, ch. 96) est précisée par l'obligation de détruire immédiatement les données écartées et l'interdiction de les exploiter (art. 271 CPP).

103. Le Service SCPT publie chaque année la statistique des mesures de surveillance. De par cette statistique, la transparence des activités du Service SCPT est garantie. La statistique contient également des indications sur le nombre de surveillances téléphoniques effectuées par le Service de renseignement de la Confédération (SRC) (cf. article Statistique de la surveillance des télécommunications : Moins de mesures de surveillance, plus de renseignements sur des raccordements de télécommunication).

104. Les requérants font valoir que les *mesures ordonnées par le Service de renseignements de la Confédération* (ci-après : SRC) ne font pas l'objet des mêmes garanties prévues dans le cadre de procédures pénales (cf. état de fait des requêtes, ch.12). L'art. 26 al. 1 let. a LRens prévoit que « Les mesures suivantes sont soumises à autorisation: faire surveiller la correspondance par poste et la correspondance par télécommunication et exiger les données secondaires issues de la correspondance par poste et télécommunication conformément à la LSCPT. L'al. 2 de cette disposition précise que ces mesures sont exécutées secrètement et à l'insu des personnes concernées. L'art. 27 souligne que le SRC peut ordonner des mesures de recherche soumises à autorisation lorsque les conditions suivantes sont réunies : a. il existe une menace concrète au sens de l'art. 19, al. 2, let. a à d, ou la sauvegarde d'autres intérêts nationaux importants au sens de l'art. 3 le requiert; b. la gravité de la menace le justifie; c. la recherche d'informations est restée vaine, n'aurait aucune chance d'aboutir ou serait excessivement difficile sans recours à une mesure soumise à autorisation. Avant de mettre en œuvre la mesure, le SRC doit obtenir l'autorisation du TAF et l'aval du chef du DDPS. S'il est nécessaire que d'autres services fédéraux ou cantonaux participent à la mise en œuvre d'une mesure, le SRC le leur ordonne par écrit dès qu'il dispose de l'autorisation du TAF et de l'aval du chef du DDPS. Ces services sont tenus de maintenir la mesure secrète. L'art. 29 prévoit la procédure d'autorisation de ces mesures. Lorsque le SRC envisage d'ordonner une mesure de recherche soumise à autorisation, il adresse au TAF une demande contenant les éléments énumérés à l'al. 1. Le président de la cour compétente du TAF statue en tant que juge unique dans les cinq jours ouvrables à compter de la réception de la demande du SRC en indiquant brièvement les motifs ; il peut confier cette tâche à un autre juge. Le président de la cour compétente du TAF n'autorise pas une mesure de recherche demandée lorsque celle-ci a déjà été autorisée sur la base d'une procédure pénale engagée à l'encontre des personnes visées à l'al. 1, let. b, et que l'enquête pénale présente un lien avec la menace concrète que la mesure de recherche du SRC doit éclaircir. Les tribunaux des mesures de contrainte

compétents et le service de surveillance de la correspondance par poste et télécommunication fournissent au TAF les renseignements dont il a besoin. Le président de la cour compétente du TAF peut demander l'audition d'un ou de plusieurs représentants du SRC avant de prendre sa décision. Il peut assortir l'autorisation de conditions, demander au SRC de compléter les pièces du dossier ou demander des compléments d'informations. Les mesures de recherche sont autorisées pour trois mois au plus. L'autorisation peut être prolongée à plusieurs reprises de trois mois au plus. Lorsqu'une prolongation s'avère nécessaire, le SRC présente au TAF une demande motivée au sens de l'al. 1 avant l'expiration de l'autorisation. Le président de la cour compétente du TAF établit un rapport d'activité annuel à l'intention de la Délégation des Commissions de gestion (DélCdG). L'art. 31 LRens prévoit la procédure en cas d'urgence : En cas d'urgence, le directeur du SRC peut ordonner la mise en œuvre immédiate de mesures de recherche. Il en informe sans délai le TAF et le chef du DDPS. Ce dernier peut mettre un terme immédiat à une mesure de recherche. Le directeur du SRC soumet la demande au président de la cour compétente du TAF dans les 24 heures et justifie l'urgence. Le président de la cour compétente du TAF communique sa décision au SRC dans les trois jours ouvrables. Une fois la mesure de recherche autorisée, le chef du DDPS décide s'il y a lieu de la poursuivre après avoir consulté le chef du DFAE et le chef du DFJP. L'art. 32 LRens (Fin de la mesure de recherche) prévoit que le SRC met immédiatement un terme à la mesure de recherche soumise à autorisation dans les cas suivants : a. le délai dans lequel elle devait être mise en œuvre a expiré ; b. les conditions pour la poursuite de la mesure ne sont plus remplies ; c. le TAF refuse de donner son autorisation ou le chef du DDPS refuse de donner son aval à la poursuite de la mesure. L'al. 2 prévoit que lorsque la mesure a été mise en œuvre en procédure d'urgence, le SRC s'assure dans les cas suivants que les données obtenues sont immédiatement détruites : a. le président de la cour compétente du TAF a refusé la demande ; b. le chef du DDPS a mis un terme immédiat à la mesure ou a refusé de donner son aval à la poursuite de la mesure. L'al. 3 prévoit que lorsque d'autres services participent à la mise en œuvre de la mesure, le SRC leur communique qu'elle doit prendre fin. Et l'al. 4 prévoit que le SRC communique au TAF et au chef du DDPS qu'il a mis un terme à la mesure de recherche. L'art. 33 LRens prévoit l'obligation d'informer les personnes surveillées : à la fin d'une opération de surveillance impliquant des mesures de recherche soumises à autorisation, le SRC informe la personne surveillée dans un délai d'un mois des motifs, du type et de la durée de la surveillance à laquelle elle a été soumise. Il peut différer l'information des personnes surveillées ou déroger à l'obligation de les informer dans les cas suivants: a. le report est nécessaire pour ne pas mettre en péril une mesure de recherche en cours ou ne pas entraver une procédure juridique en cours; b. le report est nécessaire à cause d'un autre intérêt public prépondérant pour préserver la sûreté intérieure ou extérieure ou à cause des relations que la Suisse entretient avec l'étranger; c. l'information pourrait mettre des tiers en grand danger; d. la personne concernée n'est pas atteignable. Le report de l'information des personnes surveillées ou la dérogation à l'obligation de les informer doivent être autorisés par le TAF et avalisés par le chef du DDPS selon la procédure d'autorisation visée à l'art. 29. Les mesures ordonnées par le SRC doivent recevoir l'aval de trois conseillers fédéraux (art. 30 LRens), à savoir de trois des sept membres du Conseil fédéral qui est l'autorité directoriale et exécutive suprême de la Confédération (art. 174 de la Constitution fédérale). En outre, elles doivent en vertu de l'art 27 al. 2 LRens être autorisées par le TAF. Même si la voie de recours à l'encontre des mesures de surveillance rétroactive ordonnées par le SRC n'est pas prévue par la loi, la responsabilité de trois conseillers fédéraux et du TAF est engagée. Ces garanties doivent être considérées comme suffisantes dans la mesure où les mesures ordonnées par le SRC relèvent de la sécurité nationale. Cela étant, il s'agit en l'espèce de mesures rares, comme le démontre la statistique publiée par le Service SCPT. Le SRC publie

également, dans son rapport annuel de situation, le nombre de mesures de surveillance autorisées par domaine et détaille le nombre de personnes concernées.

105. Les requérants sous-entendent la possibilité d'établir des profils de surf sur internet par le biais des données secondaires enregistrées (requêtes, ch. 8). Le Gouvernement précise que la surveillance des télécommunications en Suisse n'a pas le grand public pour objet. Elle est uniquement utilisée à l'égard de personnes faisant l'objet de soupçons aggravés d'avoir commis une ou des infractions graves. La mise en œuvre d'une surveillance rétroactive est soumise à des contraintes très strictes. Donc les données secondaires ne sauraient être utilisées aux fins d'établir des profils aléatoires.

106. Les requérants relèvent (requêtes, ch. 4) qu'en vertu de l'art. 14 al. 4 aLSCPT, les FST ont l'obligation de livrer tout renseignement susceptible d'identifier l'auteur d'une infraction commise par le biais d'internet. Le Gouvernement précise que la livraison des données prévues l'art. 14 al. 4 aLSCPT concernait les demandes de renseignements et non les surveillances rétroactives. Partant, la disposition indiquée n'est pas objet de la présente procédure.

107. En conclusion, l'accès aux données est soumis à un contrôle sévère tant au niveau du ministère public, que du tribunal de mesures de contraintes et du Service SCPT. Tous les accès sont sécurisés et journalisés. Dans l'ensemble, ce processus garantit effectivement que l'accès ne soit accordé que lorsque cela est véritablement nécessaire et de manière proportionnée dans chaque cas.

5. Délai de conservation des données

108. L'art. 15 al. 3 aLSCPT prévoit que les FST sont tenus de conserver durant six mois les données permettant l'identification des usagers ainsi que les données relatives au trafic et à la facturation (cf. ci-avant, ch. 18). L'art. 26 al. 5 de la LSCPT actuellement en vigueur prévoit également ce même délai. Lors de la révision de la LSCPT, le Conseil fédéral a souhaité porter le délai à 12 mois afin d'accroître l'efficacité des poursuites pénales, notamment dans le domaine de la lutte contre la pornographie enfantine, le crime organisé et le terrorisme. Dans son message du 27 février 2013, il a expliqué que l'expérience des autorités de poursuite pénale avait montré que le délai de six mois était trop court ; souvent, ce délai était déjà entièrement ou en grande partie écoulé lorsque l'autorité était en mesure d'ordonner une surveillance en raison de l'état d'avancement de la procédure. Cela peut notamment avoir pour conséquence de ne pas pouvoir donner suite à une demande d'entraide judiciaire internationale ou de ne pas pouvoir identifier une personne accusée ou, pire encore, une victime, par exemple un enfant sur lequel des actes pédophiles ont été commis. Le Parlement a néanmoins maintenu le délai de six mois (cf. arrêt du TF du 2 mars 2018, consid. 8.3.9. et les références).

109. Les requérants ne remettent pas en cause la durée de conservation des données secondaires en tant que tel.

110. Le TF a considéré également que le délai de conservation de 6 mois était proportionné (cf. arrêt du TF du 2 mars 2018, consid. 8.3.9 et les références). Il a estimé qu'en ce qui concerne la durée de conservation en tant que telle, il convient de noter que l'élucidation des infractions, à laquelle sert en premier lieu la conservation des données secondaires de télécommunication, en particulier dans le domaine de la lutte contre les infractions graves telles que le terrorisme ou le crime organisé, prend souvent beaucoup de temps. Il s'agit en outre souvent de procédures complexes et de grande envergure,

impliquant de nombreuses personnes. Dans ce contexte, la période de conservation de six mois, durant laquelle les autorités de poursuite pénale doivent prouver qu'elles satisfont aux exigences strictes pour ordonner une surveillance rétroactive, ne s'avère pas être d'une durée disproportionnée. Cela est d'autant plus vrai que, dans l'arrêt *Zakharov c. Russie* du 4 décembre 2015 (req. no 47143/06, § 255), la Cour a qualifié de raisonnable le délai de conservation de six mois prévu par le droit russe pour les données de surveillance (du contenu) des communications mobiles. Dans l'arrêt *Ekimdzhiev*, précité, (§ 305), la Cour n'a pas non plus remis en cause la loi bulgare qui oblige tous les fournisseurs de services de communication dans le pays à conserver ces données pour tous leurs utilisateurs pendant six mois.

6. Levée de la surveillance et destruction des données

111. L'art. 275 CPP (Levée de la surveillance), prévoit que le ministère public lève immédiatement la surveillance si les conditions requises pour son application ne sont plus remplies ou si l'autorisation ou sa prolongation a été refusée.

112. En vertu de l'art. 13 let. g et h aLSCPT, le Service vérifiait que la surveillance ne s'étende pas au-delà de la durée autorisée et y mette fin à l'expiration du délai si aucune demande de prolongation n'a été déposée et communique immédiatement la levée de la surveillance à l'autorité qui l'a autorisée (cf. ci-avant, ch. 15 ; actuellement art. 16 let. f LSCPT). L'art. 10 aOSCPT (Destruction des données) prévoyait en outre que le service détruit les données relatives à une surveillance après les avoir transmises aux autorités mentionnées à l'art. 8, al. 3 ou 4, mais au plus tard trois mois après la levée de la surveillance (al. 1). Il détruit les données figurant dans le système de suivi des affaires une année après la levée de la surveillance (al. 2) (cf. ci-avant, ch. 31).

113. Comme il a été dit, en vertu de l'art. 25 al. 3 let. a LPD, les personnes concernées peuvent en outre demander que l'organe fédéral détruise les données personnelles (cf. ci-avant, ch. 90).

114. L'art. 276 CPP prévoit en outre que les documents et enregistrements collectés lors d'une surveillance dûment autorisée qui ne sont pas nécessaires à la procédure doivent être conservés séparément et détruits immédiatement après la clôture de la procédure. De même, les documents et supports de données issus de surveillances non autorisées devaient être immédiatement détruits et ne pouvaient pas être utilisés (art. 277 CPP).

G. Conclusion

115. L'ingérence aux droits des requérants garantis par l'art. 8 CEDH ne peut être niée. Elle est toutefois justifiée par d'importants intérêts généraux à la protection de l'ordre public et de la sécurité publique. La conservation des données secondaires donne aux autorités de poursuite pénale des possibilités supplémentaires pour élucider les infractions. Le législateur suisse s'est expressément prononcé en faveur du système de conservation systématique des données secondaires de télécommunication, constatant que la procédure "quick-freeze" présente une utilité moindre que le système en vigueur et n'est pas en mesure de produire les effets souhaités par le législateur. L'ingérence repose également sur une base légale qui satisfait ainsi aux exigences de la Convention. Comme il a été démontré la conservation "à titre préventif" de données secondaires relatives aux télécommunications sont nécessaires pour atteindre ces objectifs dans une société démocratique. L'intensité de l'ingérence doit également être relativisée dans la mesure où les informations enregistrées et conservées sont des données secondaires qui ne

sont ni examinées ni reliées entre elles au niveau de l'enregistrement et de la conservation chez les différents fournisseurs de services de télécommunication. Ce n'est que l'accès des autorités de poursuite pénale aux données stockées qui permet leur exploitation et leur mise en relation. Or, l'accès aux données enregistrées est toutefois soumis à des conditions strictes et doit être autorisé par le tribunal des mesures de contrainte. La surveillance est contrôlée par le Service et peut être contestée ultérieurement par les personnes surveillées, qui doivent être informées au plus tard à la fin de la procédure préliminaire. La saisie et la conservation systématiques des données litigieuses s'accompagnent de garanties juridiques adéquates et efficaces afin d'éviter les abus et l'arbitraire. La période de conservation de 6 mois est également proportionnée.

116. Le droit des télécommunications et en particulier le droit de la protection des données prévoient des garanties suffisantes pour protéger contre les abus lors du traitement des données secondaires des télécommunications (cf. *a contrario* arrêt *Ekimdzhiev*, précité, §§ 419ss). Le grief de violation de l'article 8 CEDH s'avère donc infondé.

V. Respect de l'article 10 de la Convention

A. Griefs des requérants

117. Les requérants font valoir, sous l'angle de l'art. 10 CEDH, que la conservation des données secondaires porte atteinte à leur liberté d'expression, d'opinion et d'information. Ils font valoir qu'ils ne peuvent pas utiliser les canaux de communication électroniques habituels sans être soumis à la surveillance de masse inopinée liée à la conservation des données. Cela leur donne le sentiment d'être surveillés en permanence et les conduit à limiter leur communication (« chiling effect »). Les requérants font également valoir que la conservation des données porte atteinte à la liberté des médias et à la protection des sources journalistiques. Ils estiment que, pour les mêmes raisons que celles exposées en relation avec l'article 8 CEDH, l'ingérence à l'article 10 CEDH n'est pas non plus justifiée.

118. Le Gouvernement rappelle en premier lieu que la protection des sources journalistiques dans la procédure pénale n'est pas objet de la présente procédure (cf. ci-avant, ch. 7). Il souligne également que seuls les requérants Hasler et Strebel sont journalistes et pourraient dès lors se prévaloir de cette protection.

B. A titre principal : absence d'ingérence

119. La question de l'existence d'une ingérence dans le droit à la liberté d'expression est intimement liée à celle d'un effet dissuasif sur l'exercice de ce droit. La Cour procède à un examen au cas par cas des situations qui peuvent avoir un impact limitatif sur la jouissance de la liberté d'expression. Elle considère en tout état de cause que de simples allégations selon lesquelles les mesures litigieuses auraient un « effet dissuasif », sans plus de précisions quant à la situation concrète dans laquelle un tel effet se serait produit, ne suffisent pas pour constituer une ingérence au sens de l'article 10 de la Convention. Les ingérences à la liberté d'expression peuvent prendre la forme d'une large variété de mesures qui se manifestent généralement dans le cadre d'une « formalité, condition, restriction ou sanction » […]. Pour répondre s'il y a eu ingérence il est nécessaire de préciser la portée de la mesure litigieuse en la replaçant dans le contexte des faits de la cause et de la législation pertinente […]. D'après la jurisprudence de la Cour, et à titre d'illustration, peuvent être considérés comme des formes d'ingérence dans l'exercice du droit à la liberté d'expression (cf. décision *Schweizerische Radio- und*

Fernsehgesellschaft et autres c. Suisse du 12 novembre 2019 ; req. no 68995/13, § 72) : une condamnation pénale ou à payer des dommages-intérêts ; le fait d'avoir été l'objet de poursuites, ou le risque d'être poursuivi ; une interdiction de publier ; la confiscation d'une publication ; la saisie, par l'administration pénitentiaire, de journaux et revues ; le refus d'octroyer une fréquence de diffusion ; une décision de justice empêchant une personne de recevoir des émissions transmises par des satellites de télécommunication ; l'interdiction d'une publicité ; une sanction disciplinaire ; une injonction de divulgation de sources journalistiques ; le refus d'autoriser à filmer dans un centre pénitentiaire ; le refus d'autoriser l'entrée dans un centre d'accueil pour demandeurs d'asile en vue de recueillir des témoignages ; l'arrestation et la détention de protestataires ; des avertissements écrits adressés par le parquet aux responsables d'une ONG ayant organisé des manifestations publiques ; le retrait d'une accréditation de recherche dans des archives utilisée par un journaliste ; la levée de l'immunité parlementaire d'un requérant par une modification constitutionnelle ; un avertissement émis par une autorité de régulation des médias à l'encontre d'une maison d'édition ; la révocation de la licence de radiodiffusion d'une chaîne de télévision (cf. Guide sur l'article 10 de la Convention européenne des droits de l'homme Liberté d'expression, préparé par le Greffe de la Cour, Mis à jour au 31 août 2022, §§ 57ss et les références).

120. Les requérants n'ont pas subi de conséquences directes du fait de la conservation de leurs données secondaires par les FST. Ils n'ont pas été empêchés de s'exprimer en l'espèce, ni n'ont subi de quelconque censure. La simple conservation des données secondaires de leurs communications pour une durée de six mois n'est pas comparable aux mesures considérées par la Cour comme ingérence à la liberté d'expression (cf. ci-avant, ch. 119).

121. Pour ce qui est de la crainte d'un effet dissuasif (« chilling effect »), qu'aurait la conservation de leurs données secondaires par les FST sur les requérants, il n'est pas non plus fondé. Les requérants font valoir avoir le sentiment d'être surveillés en permanence, ce qui les incite à adapter leur comportement à cette surveillance, sans autres précisions. Ils n'apportent aucun autre élément permettant de conclure qu'ils ont en effet subi un tel « chilling effect » (cf. décision *Hannes Tretter et autrs c. Autriche* du 29 septembre 2020, req. no 3599/10, § 75). Or, des « risques purement hypothétiques » pour les requérants de subir un effet dissuasif ne suffisent pas pour constituer une ingérence au sens de l'article 10 de la Convention (décision *Schweizerische Radio-und Fernsehgesellschaft c. Suisse*, précitée, § 72 et les références). Le Gouvernement rappelle que les données secondaires sont enregistrées par les différents FST et restent dans leur sphère d'influence pendant la durée de conservation, sans être examinées ou mises en relation avec d'autres données. Les autorités n'ont pas accès aux données enregistrées auprès des FST. Lesdites données ne sont ni visionnées ni reliées entre elles au niveau de l'enregistrement et de la conservation auprès des FST (cf. ci-avant, ch. 68).

122. Il s'ensuit que l'enregistrement et de la conservation de leurs données secondaires par les FST n'a pas constitué une « ingérence » dans l'exercice par les requérants de leur droit à la liberté d'expression.

123. Par conséquent, les griefs tirés de l'article 10 de la Convention sont manifestement mal fondés et la requête doit être déclarée irrecevable, en application de l'article 35 §§ 3 a) et 4 de la Convention (cf. décision *Schweizerische Radio-und Fernsehgesellschaft c. Suisse*, précitée, §§ 80ss).

C. A titre subsidiaire : justification de l'ingérence (art. 10 § 2 de la Convention)

124. Si la Cour devait admettre que l'enregistrement et la conservation de leurs données secondaires par les FST a constitué une « ingérence » dans l'exercice par les requérants de leur droit à la liberté d'expression, le Gouvernement estime que cette ingérence est justifiée (art. 10 § 2 CEDH) pour les motifs exposés ci-avant, sous l'examen du respect de l'art. 8 CEDH, ch. 54ss. Il ajoute en outre ce qui suit :

125. Pour ce qui est de la *protection des sources des journalistes*, le Gouvernement rappelle qu'elle n'est pas objet de la procédure et que seuls les requérants Strebel et Hasler sont journalistes (cf. ci-avant, ch. 118). Il relève que dans l'arrêt *Big Brother Watch*, précité, (§§442ss), la Cour a rappelé les principes généraux relatifs à la protection des sources des journalistes, ainsi qu'à l'article 10 dans le contexte de l'interception en masse (§ 446). Elle a estimé (§ 450 et les références) que l'examen de communications journalistiques ou de données de communication associées par un analyste pouvant conduire à l'identification d'une source, le droit interne doit impérativement comporter des garanties solides en ce qui concerne la conservation, l'examen, l'utilisation, la transmission à des tiers et la destruction de ces éléments confidentiels. En outre, lorsqu'il apparaît que des communications journalistiques ou des données de communication associées n'ayant pas été sélectionnées pour examen par l'utilisation délibérée d'un sélecteur ou d'un terme de recherche dont on sait qu'il est lié à un journaliste contiennent malgré tout des éléments journalistiques confidentiels, la prolongation de leur conservation et la poursuite de leur examen par un analyste ne devraient être possibles qu'à la condition d'être autorisées par un juge ou un autre organe décisionnel indépendant et impartial habilité à déterminer si ces mesures sont « justifiées par un impératif prépondérant d'intérêt public ».

126. Ces conditions sont remplies en l'espèce, cf. ci-avant, ch. 54ss. En outre, comme l'a rappelé le TF dans son arrêt, l'autorisation du tribunal des mesures de contrainte doit se prononcer sur la question de savoir si des mesures devaient être prises pour protéger les secrets professionnels (c'est-à-dire également la protection des sources journalistiques) (art. 274 al. 4 let. a CPP ; ci-avant, ch. 21 ; disposition toujours en vigueur actuellement, cf. art. 274 al. 4 let. a CPP). Ces mesures devaient (et doivent) être mises en œuvre par le Service SCPT (art. 13 al. 1 let. f aLSCPT ; cf. ci-avant, ch. 15 ; actuellement : art. 16 let. e LSCPT).

127. Il en va de même pour le grief selon lequel la protection des sources journalistiques serait vidée de sa substance, parce que le tribunal des mesures de contrainte ne doit décider de l'autorisation de la surveillance que 5 jours après l'ordre et que le ministère public peut déjà exploiter entre-temps les données secondaires qui lui ont été transmises. Le TF a rappelé que les documents et supports de données issus de surveillances non autorisées devaient être immédiatement détruits et que les informations obtenues grâce à ces surveillances ne pouvaient pas être exploitées (art. 277, al. 2, CPP , cf. ci-avant ch. 24; actuellement toujours en vigueur art. 277 al. 2 CPP). Par ailleurs, il convient de souligner que cette problématique peut également se poser dans le cadre de la surveillance en temps réel de la correspondance par télécommunication (c'est-à-dire indépendamment de la conservation des données), lorsque des données sont produites entre la mise en place de la surveillance et la décision d'autorisation et qu'elles peuvent être consultées en permanence par le Ministère public.

128. Pour ce qui est du « chilling effect » que font valoir les requérants, le Gouvernement renvoie à ses considérations ci-dessus, ch. 121.

129. L'enregistrement et la conservation des données secondaires des requérants par les FST sont dès prévus par la loi, poursuivent un but légitime et sont entourés de garanties suffisantes au regard de l'art 10 de la Convention. Il n'y a pas de violation de cette disposition en l'espèce (cf. *a contrario* arrêt *Big Brother Watch*, précité, (§§456ss).

VI. Respect de l'article 11 de la Convention

A. Griefs des requérants

130. Les requérants font valoir que la conservation des données porte également atteinte à leur liberté de se réunir pacifiquement avec d'autres personnes et d'échanger leurs opinions avec d'autres personnes. Ils ne peuvent pas utiliser les canaux de communication électroniques habituels couverts par la conservation des données dans le cadre de leur participation à des rassemblements pacifiques sans être soumis à la surveillance liée à la conservation des données. La conservation des données peut en outre être utilisée dans le but de déterminer qui a participé à une réunion et avec qui les participants présumés à la réunion ont communiqué. Cela donne aux requérants le sentiment d'être surveillé en permanence et les incite à adapter leur comportement à cette situation (« chilling effect »). Ils estiment que pour les mêmes raisons que celles exposées en relation avec l'article 8 CEDH, l'ingérence dans l'article 11 CEDH n'est pas non plus justifiée.

B. A titre principal : absence d'ingérence

131. D'après la jurisprudence de la Cour, et à titre d'illustration, sont considérées comme des formes d'ingérence dans l'exercice du droit à la liberté de réunion pacifique deux types de restrictions : 1) le premier englobe les conditions imposées à l'exercice du droit à la liberté de réunion, en particulier les règles relatives à la planification et à la conduite d'un rassemblement qui sont dictées par les procédures de notification et d'autorisation obligatoires. Les restrictions de ce type s'adressent essentiellement aux organisateurs des réunions. 2) Le second type de restrictions correspond aux mesures répressives, notamment de canalisation de la foule, de dispersion d'un rassemblement, d'arrestation des participants, et/ou aux sanctions ultérieures. Les restrictions de ce type visent essentiellement les personnes qui participent à des réunions, ont l'intention de le faire ou l'ont fait dans le passé (cf. Guide sur l'article 11 de la Convention européenne des droits de l'homme Liberté d'expression, préparé par le Greffe de la Cour, Mis à jour au 31 août 2022, § 51 et les références). Pour ce qui est de la liberté d'association, les ingérences se manifestent habituellement par un refus d'enregistrement ou par la dissolution d'une association, mais elles peuvent aussi revêtir d'autres formes empêchant une association de se livrer à ses activités (par exemple par des inspections ou des restrictions à leur financement) (cf. Guide sur l'article 11 de la Convention européenne des droits de l'homme Liberté d'expression, préparé par le Greffe de la Cour, Mis à jour au 31 août 2022, § 145 et les références).

132. Les requérants n'ont subi aucune conséquence directe sur leur droit à la liberté de réunion et d'association du fait de la conservation de leurs données secondaires par les FST. De plus, seules les données secondaires et non le contenu de leurs communications ont été enregistrées et conservées (cf. ci-avant, ch. 67ss). Et ces données n'ont pas été utilisées. La simple conservation des données secondaires de leurs communications pour une durée de six mois n'est pas comparable aux mesures considérées par la Cour comme ingérence à ce droit (cf. ci-avant, ch. 131).

133. Pour ce qui est de l'effet dissuasif sur l'exercice de ce droit que font valoir les requérants, le Gouvernement renvoie à ses considérations ci-avant, ch. 121, dans le cadre de l'art. 10 CEDH. De simples allégations selon lesquelles les mesures litigieuses auraient un « effet dissuasif », sans plus de précisions quant à la situation concrète dans laquelle un tel effet se serait produit, ne suffisent pas pour constituer une ingérence au sens de l'article 11 de la Convention. Or, les requérants n'apportent aucun autre élément permettant de conclure qu'ils ont en effet subi un tel effet dissuasif.

134. Il s'ensuit que la conservation de leurs données secondaires par les FST n'a pas constitué une « ingérence » dans l'exercice par les requérants de leur liberté de réunion et d'association.

135. Par conséquent, les griefs tirés de l'article 11 de la Convention sont manifestement mal fondés et la requête doit être déclarée irrecevable, en application de l'article 35 §§ 3 a) et 4 de la Convention (cf. décision *Schweizerische Radio-und Fernsehgesellschaft c. Suisse*, précitée, §§ 80ss).

136. Même si la Cour devait admettre que l'enregistrement et la conservation de leurs données secondaires par les FST a constitué une « ingérence » dans l'exercice par les requérants de leur liberté de réunion et d'association, cette ingérence est justifiée (art. 11 § 2 CEDH).

C. A titre subsidiaire : justification de l'ingérence (art. 11 § 2 de la Convention)

137. Une éventuelle ingérence à la liberté d'expression est justifiée, au sens de l'art. 11 § 2 de la Convention, pour les motifs exposés ci-avant, ch. 54ss, dans les observations relatives à l'art. 8 CEDH.

138. L'enregistrement et la conservation des données secondaires des requérants par les FST sont dès prévus par la loi, poursuivent un but légitime et sont entourés de garanties suffisantes au regard de l'art 11 de la Convention. Il n'y a pas de violation de cette disposition en l'espèce.

VII. Respect de l'article 13 de la Convention

139. La Cour nous pose la question de savoir si les requérants avaient à leur disposition, comme l'exige l'article 13 de la Convention, un recours interne effectif au travers duquel ils auraient pu formuler leurs griefs de méconnaissance de la Convention.

140. Tel est manifestement le cas en l'espèce : les requérants ont pu faire valoir la violation de leurs droits protégés par la Convention en relation avec la conservation de leurs données secondaires de télécommunication en déposant un recours auprès du TAF ainsi que du TF, ce qui satisfait aux exigences de l'article 13 CEDH.

141. L'accès des autorités de poursuite pénale aux données secondaires conservées n'était pas l'objet du litige, pour les motifs exposés ci-avant, ch. 3ss. A ce sujet, le Gouvernement rappelle toutefois que le ministère public communique aux personnes surveillées, au plus tard à la fin de la procédure préliminaire, le motif, le type et la durée de la surveillance (art. 279 al. 1 CPP, cf. ci-avant, ch. 25). Les personnes dont le raccordement de télécommunication ou l'adresse postale ont été surveillés ou celles qui ont utilisé le même raccordement ou la même adresse postale peuvent interjeter recours conformément aux art. 393 à 397 CPP (art. 279 al. 3 CPP ; cf. ci-avant, ch. 25), jusqu'au TF (art. 78 ss.

LTF). La surveillance peut donc être contestée ultérieurement. En outre, l'ordre de surveillance des télécommunications, y compris la surveillance rétroactive des données secondaires, nécessite l'autorisation du tribunal des mesures de contrainte (art. 274 CPP ; cf. ci-avant, ch. 21).

142. Il n'y a dès lors pas, en l'espèce, de violation de l'art. 13 de la Convention.

VIII. Conclusions

A la lumière des considérations qui précèdent, le Gouvernement suisse invite la Cour :

- à déclarer irrecevable la requête no 47351/18 introduite par Glättli et autres contre la Suisse pour défaut manifeste de fondement (art. 35 §§ 3 let. a et 4 CEDH), pour ce qui est des griefs relatifs aux art. 10 et 11 CEDH ;
- à constater qu'il n'y a pas eu, en l'espèce, violation des art. 8 et 13 CEDH.

Nous vous prions d'agréer, Madame la Greffière de section adjointe, nos salutations distinguées.

Office fédéral de la justice OFJ

Scheidegger Adrian VUTGEV
10.03.2023

Info: admin.ch/esignature | validator.ch

Adrian Scheidegger
Agent suppléant du Gouvernement suisse