N°s 459724, 459726, 468361, 469712
Société Free, Free Mobile et Scaleway, M. M... et M. T...

10ème et 9ème chambres réunies

Séance du 19 juin 2023
Décision du 30 juin 2023

CONCLUSIONS

M. Laurent DOMINGO, Rapporteur public

Tirant les conséquences de la décision rendue par l'Assemblée du contentieux le 21 avril 2021 dans les affaires French Data Network et autres (n°s 393099, 424717, 424718, 394922, 397844, 397851, A)[1], le législateur (loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement, art. 17) a réorganisé le cadre juridique de la conservation des données dites de connexion, que ce soit pour les opérateurs de communications électroniques relevant de l'article 34-1 du code des postes et communications électroniques ou pour les fournisseurs d'accès à internet et les hébergeurs de contenus relevant de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

Il en résulte dorénavant que les opérateurs, fournisseurs et hébergeurs doivent conserver :

- Pour les besoins des procédures pénales, de la prévention des menaces contre la sécurité publique et de la sauvegarde de la sécurité nationale, d'une part, les informations relatives à l'identité civile de l'utilisateur, et, d'autre part, les autres informations fournies par l'utilisateur lors de la souscription d'un contrat ou de la création d'un compte ainsi que les informations relatives au paiement ;

- Pour les besoins de la lutte contre la criminalité et la délinquance grave, de la prévention des menaces graves contre la sécurité publique et de la sauvegarde de la sécurité nationale, les données techniques permettant d'identifier la source de la connexion ou celles relatives aux équipements terminaux utilisés ;

- Pour la seule sauvegarde de la sécurité nationale, d'autres données de trafic et des données de localisation, pour une durée d'un an, lorsque le Premier ministre constate, par décret, une menace grave, actuelle ou prévisible contre la sécurité nationale ;

[1] RFDA 2021 p. 421, concl. Lallet, AJDA 2021 n° 21, p. 1194 chron Malverti et Beaufils.

- Enfin, les autorités disposant d'un accès aux données peuvent prononcer une injonction de conservation rapide afin d'accéder aux données conservées, à des fins de prévention et de répression de la criminalité, de la délinquance grave et des autres manquements graves aux règles dont elles ont la charge d'assurer le respect.

Pour l'application de ces dispositions législatives, ont été pris :

- Deux décrets du 20 octobre 2021 (n° 2021-1361[2] et n° 2021-1362[3]) relatif aux catégories de données conservées. Ils sont attaqués par les sociétés Free, Free Mobile et Scaleway.

- Un autre décret (n° 2021-1363) du 20 octobre 2021 portant injonction, au regard de la menace grave et actuelle contre la sécurité nationale, de conservation pour une durée d'un an de certaines catégories de données de connexion. Etonnement, il n'a pas fait l'objet d'un recours. Lui a cependant succédé un décret n° 2022-1327 du 17 octobre 2022 portant injonction, au regard de la menace grave et actuelle contre la sécurité nationale, de conservation pour une durée d'un an de certaines catégories de données de connexion, qui, lui, est contesté par les sociétés Free et Free Mobile et par M. M... et M. T...[4].

N°s 459724, 459726

Commençons par les catégories de données conservées, soit les deux premiers décrets du 20 octobre 2021.

A. Sont tout d'abord soulevés des moyens relatifs au contreseing de ces décrets (article 22 de la Constitution). Ces décrets du Premier ministre ont été contresignés par le ministre de l'économie et celui des outre-mer.

Les sociétés requérantes soutiennent que le premier aurait également dû être contresigné par le Garde des sceaux, au motif que les tarifs correspondant à la fourniture des données conservées sont fixés par un arrêté du ministre de l'économie, des finances et de l'industrie et du garde des sceaux. Toutefois, le renvoi par l'article R. 213-1 du code de procédure pénale à cet arrêté interministériel existait déjà auparavant, l'arrêté en question figurant à l'article A. 43-9 du code de procédure pénale. Vous pourrez considérer que dans la mesure où le décret attaqué ne fait que modifier les catégories de données conservées selon la finalité poursuivie et qu'il ne modifie l'article R. 213-1 du code de procédure pénale que pour des raisons de coordination, il n'appelait pas une mesure d'exécution différente de celle déjà prévue par le

[2] Relatif aux catégories de données conservées par les opérateurs de communications électroniques, pris en application de l'article L. 34-1 du code des postes et des communications électroniques.
[3] Relatif à la conservation des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne, pris en application du II de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.
[4] En référé v. JRCE, 26 octobre 2022, M. M… et autre, n°468364 (L. 521-1) ; JRCE, 28 octobre 2022, Association Via La voie du peuple, n°468489 (L. 521-2).

texte en vigueur, si bien que le contreseing du garde des sceaux n'était donc pas requis pour ce décret modificatif.

Les sociétés soutiennent que le deuxième décret aurait dû être contresigné par les ministres de la défense, de l'intérieur, de la justice et des douanes, car ils peuvent présenter des demandes d'autorisation de recours aux techniques de recueil de renseignements de l'article L. 821-1 du code de la sécurité intérieure permettant notamment d'avoir un accès aux données de connexion. Mais accéder aux données de connexion, ce n'est pas une mesure d'exécution du décret relatif à la conservation de ces données. Le moyen est inopérant.

B. Sont ensuite soulevés des moyens d'incompétence négative, au motif notamment que le décret n°2021-1362 n'aurait pas épuisé sa compétence, faute de comporter des dispositions relatives aux modalités de conservation, alors que l'article 6 de la LCEN renvoi à un DCE pour définir les données conservées, la durée de conservation et (ce que ne fait pas le CPCE) les modalités de cette conservation. Toutefois, aucune disposition ni aucun principe n'impose au pouvoir réglementaire d'épuiser, par un seul décret, la compétence qu'il tient de dispositions législatives (27 octobre 2008, Fédération départementale des associations agréées de la pêche et de protection du milieu aquatique de l'Orne, n°307546, Rec. p. 364). Tout au plus s'agirait-il d'une question d'inapplicabilité de la loi en l'absence des dispositions réglementaires nécessaires, mais ce n'est, en tout état de cause, pas le cas en l'espèce.

Le moyen d'incompétence négative est également développé sur le terrain de la précision suffisante des termes employés, mais, à ce stade, le moyen n'est pas assorti de précisions suffisantes, faute d'indiquer quelle donnée serait insuffisamment précise et pour quelles raisons. Il ne l'est qu'avec l'examen des données auquel il convient maintenant de procéder.

C. Pour les sociétés requérantes, les données listées dans les décrets attaqués méconnaitraient le droit dérivé de l'Union européenne (directive e-privacy et RGPD) et le droit au respect de la vie privée (Charte des DF de l'UE et article 8 ConvEDH). Il leur est notamment reproché, faute d'être trop largement définies, de ne pas être limitées à celles strictement nécessaires à la finalité envisagée.

1ère liste, les données d'identité (conservées 5 ans pour les besoins des procédures pénales, de la prévention des menaces contre la sécurité publique et de la sauvegarde de la sécurité nationale), soit :

1°) Les nom et prénom, la date et le lieu de naissance pour une personne physique ou la raison sociale, ainsi que les nom, prénom, date et lieu de naissance de la personne agissant en son nom, lorsque le compte est ouvert au nom d'une personne morale.

Les sociétés requérantes soutiennent qu'elles ne collectent pas toujours la date et le lieu de naissance dès lors que ce ne sont pas des informations nécessaires à leurs services. Mais, et vous pourrez faire la même réponse à chaque fois que cet argument est avancé, les décrets en litige n'ont pas pour effet d'obliger un opérateur, un fournisseur ou un hébergeur à collecter

plus de données qu'elles ne le font, mais seulement de conserver les données qu'ils collectent et dans la limite où ils les collectent[5]. Nous n'avons au demeurant pas vraiment de doutes sur le fait qu'en pratique, ils collectent effectivement la plupart des données envisagées par les décrets en litige.

2°) La ou les adresses postales associées.

Les sociétés requérantes arguent de ce que ces adresses postales ne sont ni certifiées ni vérifiées. Mais c'est indifférent à leur conservation, comme ça l'est de leur collecte et des autres traitements dont elles peuvent faire l'objet. En outre, la notion « d'adresse postale associée » n'est pas floue (c'est celle associée à l'identité du 1°).

3°) La ou les adresses de courrier électronique de l'utilisateur et du ou des comptes associés le cas échéant.

Même réponse : la circonstance que les courriers électroniques soient enregistrés sur une base purement déclarative ne fait pas obstacle à leur conservation et les termes employés ne sont pas flous.

4°) Le ou les numéros de téléphone.

Il n'y a pas d'hésitation à avoir : il s'agit du ou des numéros du client, qu'il s'agisse d'une personne physique ou d'une personne morale.

De manière plus générale sur cette première liste, si la CNIL avait exprimé sa préférence pour qu'une seule donnée soit collectée lorsque c'est possible (adresse, numéro de téléphone, courrier électronique), vous pourrez juger que, compte-tenu des finalités poursuivies, la collecte de plusieurs données d'une même catégorie demeure justifiée dès lors que l'une des deux données, déclarées par l'utilisateur, peut ne pas correspondre à l'activité de l'utilisateur et qu'il n'est pas possible de savoir à l'avance laquelle.

2ème liste, les autres informations fournies par l'utilisateur lors de la souscription d'un contrat ou de la création d'un compte (conservées 1 an pour les mêmes finalités).

1°) L'identifiant utilisé.

Les sociétés requérantes se bornent à réitérer une remarque formulée par la CNIL sur le manque de précision de cet item, mais sans tenir compte de ce que la demande de la Commission a été satisfaite car l'identifiant utilisé se rapporte nécessairement, puisque c'est l'objet de cette liste, à l'information fournie lors de la création du compte.

[5] Ce que l'article R. 10-12 du code des postes et des communications électroniques prévoit expressément pour les données de trafic et de localisation.

2°) Le ou les pseudonymes utilisés.

Les sociétés expliquent qu'elles n'offrent pas la possibilité de recourir à un pseudonyme lors de la souscription d'un contrat. Dans ce cas, il n'y a pas d'obligation de conserver une donnée qui n'existe pas et n'est donc pas collectée.

3°) Les données destinées à permettre à l'utilisateur de vérifier son mot de passe ou de le modifier, le cas échéant par l'intermédiaire d'un double système d'identification de l'utilisateur, dans leur dernière version mise à jour.

Sur ce point, et c'était une demande de la CNIL, les données en cause ne sont, contrairement à ce que soutiennent les requêtes, que celles permettant à l'utilisateur lui-même, et non à l'opérateur, de vérifier et modifier le mot de passe. En outre, cette disposition n'implique aucunement la conservation des mots de passe et des données d'authentification des utilisateurs.

3ème liste, les informations relatives au paiement (conservées 1 an pour les mêmes finalités), qui recouvrent le type de paiement utilisé, la référence du paiement, le montant et la date, l'heure et le lieu en cas de transaction physique.

Conserver des données relatives aux paiements est justifié au regard de la finalité poursuivie et la question de savoir si le montant doit être TTC ou HT n'est pas un sujet. Mais, deux questions méritent plus d'attention :

En premier lieu, la durée de conservation. Les textes sont construits différemment, les recours aussi.

L'article 6 de la LCEN se réfère à l'article 34-1 du CPCE, mais il renvoie à un décret en Conseil d'Etat, pris après avis de la CNIL, pour la définition des données à conserver et la détermination de la durée et des modalités de leur conservation. Le décret attaqué a défini les données et déterminé la durée de leur conservation. Mais dans leur recours contre ce décret, les sociétés ne formulent pas de critiques contre cette durée.

L'article 34-1 du CPCE comporte lui les catégories de données, les finalités poursuivies et aussi les durées de conservation. S'il renvoie également à un DCE, ce n'est cependant que pour fixer la liste des données et les modalités de compensation des coûts. Mais il n'y a pas de renvoi à la durée de conservation, puisque cette question est réglée directement par la loi. Ce qui explique que le décret pris au titre de l'article 34-1 du CPCE, à la différence de celui pris au titre de l'article 6 de la LCEN, ne comporte pas de durées de conservation.

Les sociétés requérantes contestent cependant ces durées, en dirigeant, logiquement, leur moyen contre l'article 34-1 du CPCE, à travers une exception d'inconventionnalité.

Toutefois, la contrariété d'une disposition législative aux stipulations d'un traité international ne peut être utilement invoquée à l'appui de conclusions dirigées contre un acte réglementaire que si ce dernier a été pris pour son application ou si elle en constitue la base légale (Ass., 21 avril 2021, préc ; 13 juin 2016, C..., n°372721, B - Rec. T. pp. 615-902). Or, le décret attaqué, en ce qui concerne les durées de conservation, n'est pas pris pour l'application de l'article 34-1, ni cet article 34-1 ne peut constituer la base légale du décret, car il n'y a pas besoin de décret pour fixer les durées de conservation[6]. Le moyen, dans la seule requête où il est soulevé, est donc inopérant.

En second lieu, est également discuté la date, l'heure et le lieu en cas de transaction physique. Contrairement à ce que soutiennent les requêtes, on ne peut, juridiquement, voir dans le lieu de la transaction physique une donnée de localisation, car la donnée de localisation est définie (en droit de l'UE v. l'article 2 de la directive e-privacy, en droit interne v. le VI de l'article 34-1 du CPCE) comme celle indiquant la position géographique de l'équipement terminal d'un utilisateur. Or, en l'espèce, la donnée conservée ne renseigne que sur le lieu d'un paiement, qu'il soit réalisé par l'utilisateur ou non, en possession de son équipement terminal ou non. La conservation de cette donnée pour des finalités comprenant les besoins des procédures pénales, de la prévention des menaces contre la sécurité publique est donc possible.

En outre, le Premier ministre justifie la nécessité de cette donnée pour les besoins du renseignement (nombre de transactions dans un même lieu) et des enquêtes sur le terrain (interrogation des vendeurs dans le lieu du paiement, exploitation de la video surveillance notamment). Vous pourrez écarter cette deuxième contestation en matière de paiements.

4ème liste, les données techniques permettant d'identifier la source de la connexion ou celles relatives aux équipements terminaux utilisés (conservées 1 an pour les besoins de la lutte contre la criminalité et la délinquance grave, de la prévention des menaces graves contre la sécurité publique et de la sauvegarde de la sécurité nationale).

Ne fait véritablement l'objet d'une critique que l'adresse IP attribuée à la source de la connexion et le port associé. Mais elle s'écarte : à la lecture du texte, l'adresse IP vise tout à la fois l'adresse IP publique et l'adresse IP privée et ces deux données sont pareillement justifiées au regard de la finalité poursuivie En effet, comme l'explique le Premier ministre en défense, l'adresse IP publique, celle visible sur le réseau public de communication, peut correspondre à plusieurs terminaux de communications électroniques connectés à un réseau interne. Connaitre l'adresse IP privée permet d'identifier le terminal à l'origine de la communication (la même justification s'appliquant à l'adresse MAC). Les sociétés requérantes vous expliquent que, techniquement, ce n'est pas toujours nécessaire et que

[6] Données traitées et durées de conservation de ces données sont, au regard du principe général de proportionnalité des traitements de données, liées (pour un tel lien, v. par ex. 30 décembre 2009, Société Expérian, n° 306173, Rec. p. 535), mais il s'agit bien de questions dissociables et divisibles, la durée pouvant être annulée seule (par ex. 30 décembre 2009, SOS Racisme et GISTI et autres, n°s 312051, 313760, A).

d'ailleurs leurs services ne fonctionnent pas comme ça, mais c'est sans incidence sur la légalité des dispositions contestées.

Pour les autres données, comprenant le numéro d'identifiant de l'utilisateur, l'identifiant de la connexion, le numéro d'identification du terminal, le numéro de téléphone à l'origine de la communication ou encore les types de protocoles utilisés, la réponse est évidente : si elles ne sont pas disponibles, il n'y a pas matière à conservation. Et précisons en outre qu'il n'y a pas de doute à avoir : il s'agit bien uniquement des données de la source, ie à l'origine de la communication, aucunement celle du destinataire.

5ème et dernière liste, les catégories de données conservées un an en vertu d'un décret du PM lorsqu'est constatée une menace grave, actuelle ou prévisible contre la sécurité nationale.

Ces données sont : 1°) Les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication, 2°) Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs, 3°) Les données techniques permettant d'identifier le ou les destinataires de la communication, 4°) Pour les opérations effectuées à l'aide de téléphones mobiles, les données permettant d'identifier la localisation de la communication.

Pour l'essentiel, les sociétés requérantes se plaignent du caractère imprécis de ces catégories et de la quantité de données à conserver, par ex. les listes d'adresse IP, mais il s'agit d'une critique de principe qui n'est pas assortie de précisions.

Il est cependant une donnée qui fait l'objet d'une critique plus particulière, c'est celle qui porte sur les services complémentaires. Ces services ne sont pas détaillés, alors qu'ils sont très divers (blocage d'appels, renvoi d'appels, mode conférence, duplication de carte SIM, etc.). Le PM le reconnaît mais il vous explique que la liste de ces services diffère d'un opérateur à un autre, et qu'au demeurant elle varie dans le temps. Cependant, il vous indique aussi que l'identification des services complémentaires nécessaires pour les enquêtes fait l'objet d'un dialogue entre l'Etat et les opérateurs. D'où l'on devine que des précisions peuvent être utilement apportées à cette catégorie. Elles le peuvent, à tout le moins, en ce qui concerne la nature des services complémentaires en cause, pour la circonscrire à ceux qui permettent de fournir des informations sur l'identification de l'origine et des destinataires d'une communication. En outre, ainsi que le soutiennent les sociétés requérantes, il n'est pas précisé quelles sont les données afférentes à ces services complémentaires qui doivent être conservées, telles que la date et l'heure de souscription ou d'utilisation du service en question ou d'autres données encore.

Cette catégorie de données est ainsi entachée d'imprécision sur le champ de la conservation qui est exigée. Ce qui, au regard du principe de proportionnalité des données et de respect de la vie privée, l'entache d'illégalité.

D. Les sociétés Free, Free Mobile et Scaleway soulèvent, pour terminer sur ces deux premières requêtes, trois autres moyens.

Le premier porte sur les règles d'accès à ces données, mais ce n'est aucunement l'objet des décrets en litige. Il est donc inopérant.

Le deuxième prend appui sur l'article 39-3 du CPCE qui pénalise (un an d'emprisonnement et de 75 000 euros d'amende) le fait de ne pas procéder à la conservation des données techniques dans les conditions où cette conservation est exigée par la loi et il réitère le grief tiré de l'imprécision des catégories de données en litige : il doit y être répondu de la même manière.

Le troisième porte sur le principe de sécurité juridique et l'absence de report de l'entrée en vigueur dans le temps (le gouvernement ayant au contraire décidé d'une entrée en vigueur immédiate avec la publication au JO, manifestement pour tenir le délai de 6 mois de la décision d'Assemblée). Cependant, en terme de données, les catégories prévues dans les deux décrets du 21 octobre 2021 ne diffèrent pas fondamentalement de celles que les opérateurs, fournisseurs et hébergeurs devaient auparavant conserver, c'est d'avantage l'architecture d'ensemble (finalité et durée) qui a été revue, et il n'est pas établi que, techniquement, les services soumis à l'obligation de conservation auraient été pris au dépourvu, d'autant que le gouvernement avait procédé, au mois de septembre, à une consultation publique.

Dans ces affaires, nous concluons donc à l'annulation du 2° du V de l'article 3 du décret n° 2021-1361 du 20 octobre 2021 et au rejet du surplus des conclusions.

N°s 468361, 469712

Venons-en au décret par lequel le PM a fait injonction, au regard de la menace grave et actuelle contre la sécurité nationale, de conserver pour une durée d'un an certaines catégories de données de connexion, celles de la 5ème liste.

La Cour de justice (Gde Ch, 6 octobre 2020, La Quadrature du net et autres, C-511/18, C-512/18, C-520/18, § 134 et s.) a jugé que la sécurité nationale, qui reste de la seule responsabilité de chaque État membre, correspond à l'intérêt primordial de protéger les fonctions essentielles de l'État et les intérêts fondamentaux de la société et inclut la prévention et la répression d'activités de nature à déstabiliser gravement les structures constitutionnelles, politiques, économiques ou sociales fondamentales d'un pays, et en particulier à menacer directement la société, la population ou l'État en tant que tel, notamment des activités de terrorisme. Elle a admis que, dans ces situations, le droit de l'Union ne s'oppose pas, en principe, à une mesure législative qui autorise les autorités compétentes à enjoindre aux fournisseurs de services de communications électroniques de procéder à la conservation des données relatives au trafic et des données de localisation de l'ensemble des utilisateurs des moyens de communications électroniques pendant une période limitée, dès lors qu'il existe des circonstances suffisamment concrètes permettant de considérer que l'État membre concerné fait face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible. L'injonction doit, néanmoins, être temporellement limitée au strict

nécessaire, mais, en raison de la persistance d'une telle menace, elle peut être renouvelée, la durée de chaque injonction ne devant dépasser un laps de temps prévisible et devant être entourée de garanties strictes.

A. Pour contester le décret du 17 octobre 2022, les sociétés Free et Free Mobile soutiennent, en premier lieu, qu'il est insuffisamment motivé.

Elles invoquent pour ce faire l'article 41 de la Charte des droits fondamentaux de l'Union européenne, mais il ressort clairement du libellé de cette disposition que celle-ci ne s'adresse pas aux États membres, mais uniquement aux institutions, aux organes et aux organismes de l'Union (en ce sens, Gde Ch., 24 novembre 2020, Minister van Buitenlandse Zaken, C-225/19 et C-226/19 ; par ex. CE, 25 janvier 2023, Association réunion biodiversité, n°460440, B).

Elles se réfèrent aussi au principe général du droit de l'Union, lequel s'applique aux États membres lorsqu'ils mettent en œuvre ce droit (même arrêt du 24 novembre 2020). C'est le cas ici au regard de l'article 15 de la directive e-privacy (v. 21 déc. 2016, Télé2 Sverige AB, n° C-203/15 et C-698/15 ; 16 février 2023, HYA et autres c. Bulgarie, C-349/21, à propos de la motivation des autorisations d'écoutes téléphoniques).

En l'espèce, le décret attaqué, qui n'a pas à être motivé en vertu du droit interne, comporte des motifs de droit, le constat d'une menace grave et actuelle contre la sécurité nationale et la mention de ce qu'il vise à la sauvegarde de la sécurité nationale, ce qui est conforme à l'article 34-1 du CPCE, qui prévoit que l'injonction de conservation des données peut être prononcé par le Premier ministre pour des motifs tenant à la sauvegarde de la sécurité nationale et lorsqu'il constate qu'elle fait l'objet d'une menace grave, actuelle ou prévisible.

Au regard du principe général du droit de l'Union, vous pourrez admettre que cette motivation, bien que sommaire, est, dans les circonstances de l'espèce, suffisante. En effet, la motivation d'un acte dépend de sa nature, de son objet, de son contexte et de l'ensemble des règles juridiques régissant la matière concernée (v. pour les actes des institutions de l'Union, par ex. 22 novembre 2018, Swedish Match AB c. Secretary of State for Health, C-151/17).

S'agissant d'une mesure réglementaire, qui intervient dans le cadre de la sauvegarde de la sécurité nationale, la motivation du décret peut se borner, comme en l'espèce, à indiquer la situation d'ensemble qui a conduit à son adoption et l'objectif qu'il poursuit, ce qui ne fait au demeurant pas obstacle au contrôle du juge dès lors que c'est à l'administration de justifier du bien-fondé des motifs qu'elle a retenus. Le moyen doit donc être écarté.

B. Il est, en deuxième lieu et troisième lieu, soutenu que le décret attaqué est illégal, par lui-même ou parce que l'article 34-1 du CPCE qui en constitue la base légale méconnaît le droit de l'Union, au motif qu'il n'est pas prévu de contrôle effectif de l'injonction, ni de contrôle périodique de sa proportionnalité. Ces moyens ne peuvent qu'être écartés.

La Cour de justice a admis la conservation généralisée des données pour préserver la sécurité nationale pendant un « laps de temps prévisible » et vous avez, dans la décision d'Assemblée, indiqué que ce laps de temps ne saurait raisonnablement excéder un an.

En vertu de l'article 34-1 du CPCE, la durée de conservation sur injonction est d'un an (le décret attaqué indique qu'il est valable un an) et il faut un nouveau décret, fondé sur la persistance de la menace à la sécurité nationale, pour que la conservation continue. Il existe donc bien un examen périodique de l'injonction de conserver les données, qui conduit à un réexamen de la nécessité et de la proportionnalité de cette conservation. En revanche, il ne résulte d'aucune exigence que, pendant ce délai d'un an, le gouvernement devrait procéder à ce réexamen à des échéances régulières de 3 ou 6 mois. En tout état de cause, il résulte des règles applicables que l'administration, d'office ou sur demande, est tenue d'abroger expressément un acte réglementaire illégal depuis son édiction ou en raison de circonstances de droit ou de fait postérieures (L. 243-2 CRPA).

La Cour de justice a en outre jugé qu'il est essentiel qu'une décision faisant injonction aux fournisseurs de services de communications électroniques de procéder à une conservation des données dans le but de préserver la sécurité nationale puisse faire l'objet d'un contrôle effectif soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant.

Pour les sociétés Free et Free Mobile, le législateur aurait dû organiser une procédure spécifique afin de prévoir un contrôle préalable par une autorité administrative indépendante. Mais ce n'est pas une exigence résultant du droit de l'Union. Le contrôle juridictionnel, en référé en cas d'urgence ou en excès de pouvoir avant la fin de l'injonction, constitue une voie de recours effective et suffisante.

C. Enfin, M. M... et M. T... soutiennent que le renouvellement de l'injonction de conservation des données n'est pas justifié par le caractère « grave et actuel » de la menace à la sécurité nationale.

Le gouvernement vous produit cependant un ensemble d'éléments factuels, consignés dans une note des services de renseignement, portant en particulier sur la menace terroriste, les risques d'ingérences étrangères et les cyberattaques.

Les requérants les contestent mais uniquement en ce qui concerne la menace terroriste et en se prévalant d'arguments qui ne servent pas leur cause. Ils font en effet valoir que les projets d'attaques terroristes et les arrestations qui y sont liées sont, en Europe comme en France, en constante diminution. Pour l'Europe, ils se fondent sur le rapport d'Europol « European Union : Terrorism situation and trend report 2022 », qui indique qu'en 2021, 15 attentats ou projets d'attentat ont été dénombrés au sein de l'Union européenne (contre 57 en 2020 et 55 en 2019). Et pour la France, ils reprennent les chiffres donnés par le gouvernement, faisant état de 4 projets d'attentats déjoués en 2021 et 3 en 2022. Mais si effectivement les chiffres ont diminué, ils indiquent cependant que la menace terroriste demeure une réalité.

Pour le surplus, notamment les ingérences étrangères et les cyberattaques, les requérants se bornent à opposer qu'il ne s'agit que de circonstances propres à un contexte géopolitique incertain. Ce qui ne remet pas cause, là aussi, la réalité des menaces pour la sécurité nationale sur lesquelles le gouvernement s'est fondé et qui justifie légalement le décret attaqué.

Nous concluons donc au rejet de ces deux autres requêtes.