Conseil d'État

N° 433539
ECLI:FR:CECHR:2026:433539.20260430
Inédit au recueil Lebon

10ème - 9ème chambres réunies

M. Stéphane Eustache, rapporteur
FITZJEAN O COBHTHAIGH, avocats

Lecture du jeudi 30 avril 2026

REPUBLIQUE FRANCAISE

AU NOM DU PEUPLE FRANCAIS

Vu la procédure suivante :

Par une décision avant dire droit du 5 juillet 2021, le Conseil d'Etat statuant au contentieux a, d'une part, rejeté les conclusions de la ministre de la culture tendant à ce qu'il soit donné acte du désistement d'office des associations La Quadrature du Net, French Data Network, Franciliens.net et Fédération des fournisseurs d'accès à internet associatifs, d'autre part, écarté les moyens tirés d'un défaut de motivation, d'un défaut de base légale, de la méconnaissance du règlement (UE) 2016/679 du 27 avril 2016 et du droit à un recours effectif, dirigés contre la décision implicite par laquelle le Premier ministre a rejeté la demande de ces associations tendant à abroger le décret n° 2010-236 du 5 mars 2010, enfin, sursis à statuer sur les conclusions tendant à l'annulation pour excès de pouvoir de cette décision implicite, jusqu'à ce que la Cour de justice de l'Union européenne se soit prononcée sur les questions préjudicielles suivantes :

1°) Les données d'identité civile correspondant à une adresse IP sont-elles au nombre des données relatives au trafic ou de localisation soumises, en principe, à l'obligation d'un contrôle préalable par une juridiction ou une entité administrative indépendante dotée d'un pouvoir contraignant '

2°) S'il est répondu par l'affirmative à la première question, et eu égard à la faible sensibilité des données relatives à l'identité civile des utilisateurs, y compris leurs coordonnées, la directive du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, lue à la lumière de la Charte des droits fondamentaux de l'Union européenne, doit-elle être interprétée comme s'opposant à une réglementation nationale prévoyant le recueil de ces données correspondant à l'adresse IP des utilisateurs par une autorité administrative, sans contrôle préalable par une juridiction ou une entité administrative indépendante dotée d'un pouvoir contraignant '

3°) S'il est répondu par l'affirmative à la deuxième question, et eu égard à la faible sensibilité des données relatives à l'identité civile, à la circonstance que seules ces données peuvent être recueillies, pour les seuls besoins de la prévention de manquements à des obligations définies de façon précise, limitative et restrictive par le droit national, et à la circonstance qu'un contrôle systématique de l'accès aux données de chaque utilisateur par une juridiction ou une entité administrative tierce dotée d'un pouvoir contraignant serait de nature à compromettre l'accomplissement de la mission de service public confiée à l'autorité administrative elle-même indépendante qui procède à ce recueil, la directive fait-elle obstacle à ce que ce contrôle soit effectué selon des modalités adaptées, tel qu'un contrôle automatisé, le cas échéant sous la supervision d'un service interne à l'organisme présentant des garanties d'indépendance et d'impartialité à l'égard des agents chargés de procéder à ce recueil '

Par un arrêt du 30 avril 2024 (C-470/21), la Cour de justice de l'Union européenne a répondu aux questions préjudicielles du Conseil d'Etat.

Vu les autres pièces du dossier ;

Vu :
- la Charte des droits fondamentaux de l'Union européenne ;
- le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 ;
- la directive 2001/29/CE du Parlement européen et du Conseil du 22 mai 2001 ;
- la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 ;
- la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 ;
- le code pénal ;
- le code des postes et des communications électroniques ;
- le code de la propriété intellectuelle ;
- le code des relations entre le public et l'administration ;
- loi n° 86-1067 du 30 septembre 1986 ;

- le décret n° 2010-236 du 5 mars 2010 ;
- l'arrêt de la Cour de justice de l'Union européenne du 30 avril 2024 (C-470/21) ;
- le code de justice administrative ;

Après avoir entendu en séance publique :

- le rapport de M. Stéphane Eustache, maître des requêtes,

- les conclusions de Mme Charline Nicolas, rapporteure publique ;

Considérant ce qui suit :

1. Les associations La Quadrature du Net, French Data Network, Franciliens.net et Fédération des fournisseurs d'accès à internet associatifs ont demandé au Conseil d'Etat d'annuler pour excès de pouvoir la décision implicite par laquelle le Premier ministre a rejeté leur demande tendant à l'abrogation du décret du 5 mars 2010 relatif au traitement automatisé de données à caractère personnel autorisé par l'article L. 331-23 du code de la propriété intellectuelle dénommé " Système de gestion des mesures pour la protection des oeuvres sur internet ". Par une décision avant dire droit du 5 juillet 2021, le Conseil d'Etat statuant au contentieux a sursis à statuer sur ces conclusions jusqu'à ce que la Cour de justice de l'Union européenne se soit prononcée sur les questions qu'il lui a renvoyées à titre préjudiciel. Par un arrêt C-470/21 du 30 avril 2024, la Cour de justice de l'Union européenne a répondu à ces questions.

Sur le cadre juridique de l'Union européenne :

2. En vertu de l'article 2 de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), constituent des " données relatives au trafic " " toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation " et des " données de localisation " " toutes les données traitées dans un réseau de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public ". Aux termes du paragraphe 1 de l'article 5 de cette directive : " Les États membres garantissent, par la législation nationale, la confidentialité des communications effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles au public, ainsi que la confidentialité des données relatives au trafic y afférentes. En particulier, ils interdisent à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés sauf lorsque cette personne y est légalement autorisée, conformément à l'article 15, paragraphe 1. Le présent paragraphe n'empêche pas le stockage technique nécessaire à l'acheminement d'une communication, sans préjudice du principe de confidentialité ". Aux termes de l'article 6 de cette directive : " 1. Les données relatives au trafic concernant les abonnés et les utilisateurs traitées et stockées par le fournisseur d'un réseau public de communications ou d'un service de communications électroniques accessibles au public doivent être effacées ou rendues anonymes lorsqu'elles ne sont plus nécessaires à la transmission d'une communication sans préjudice des paragraphes 2, 3 et 5, du présent article ainsi que de l'article 15, paragraphe 1. / 2. Les données relatives au trafic qui sont nécessaires pour établir les factures des abonnés et les paiements pour interconnexion peuvent être traitées. Un tel traitement n'est autorisé que jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement. / 3. Afin de commercialiser ses services de communications électroniques ou de fournir des services à valeur ajoutée, le fournisseur d'un service de communications électroniques accessible au public peut traiter les données visées au paragraphe 1 dans la mesure et pour la durée nécessaires à la fourniture ou à la commercialisation de ces services, pour autant que l'abonné ou l'utilisateur que concernent ces données ait donné son consentement (...) ".

3. Aux termes du paragraphe 1. de l'article 15 de la même directive : " Les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale - c'est-à-dire la sûreté de l'État - la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/ 46/CE. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe. Toutes les mesures visées dans le présent paragraphe sont prises dans le respect des principes généraux du droit communautaire, y compris ceux visés à l'article 6, paragraphes 1 et 2, du traité sur l'Union européenne ".

En ce qui concerne la conservation de données à caractère personnel par les fournisseurs de services de communications électroniques :

4. Il résulte des dispositions citées aux points 2 et 3, telles qu'interprétées par la Cour de justice de l'Union européenne dans son arrêt du 30 avril 2024, qu'un Etat membre peut imposer aux fournisseurs de services de communications électroniques, au titre du paragraphe 1 de l'article 15 de la directive du 12 juillet 2002, d'assurer la conservation généralisée et

indifférenciée des adresses IP de leurs utilisateurs pour les besoins de la lutte contre les infractions pénales en général, lorsqu'il est effectivement exclu que cette conservation puisse engendrer des ingérences graves dans la vie privée des personnes concernées en raison de la possibilité de tirer des conclusions précises sur celles-ci au moyen, notamment, d'une mise en relation de ces adresses IP avec un ensemble de données de trafic ou de localisation qui auraient été également conservées par les fournisseurs.

5. Afin de prévenir une telle ingérence, il appartient à l'Etat membre de prévoir, dans sa législation, des règles claires et précises qui garantissent une séparation effectivement étanche des données conservées par les fournisseurs de services de communications électroniques. Ces règles doivent imposer que chaque catégorie de données, y compris les données relatives à l'identité civile et les adresses IP, soit conservée de manière pleinement séparée des autres catégories de données conservées, que cette séparation étanche soit effectivement assurée par une dispositif informatique sécurisé et fiable, que la mise en relation des adresses IP avec l'identité civile de la personne concernée soit réalisée par un procédé technique performant ne remettant pas en cause l'efficacité de la séparation étanche de ces catégories de données, enfin, que la fiabilité de cette conservation fasse l'objet d'un contrôle régulier par une autorité publique autre que celle qui cherche à obtenir l'accès aux données conservées par les fournisseurs de services de communications électroniques.

En ce qui concerne l'accès par une autorité publique nationale aux données relatives à l'identité civile :

6. Les dispositions citées aux points 2 et 3, telles qu'interprétées par l'arrêt du 30 avril 2024 de la Cour de justice de l'Union européenne, ne font pas obstacle à ce qu'une autorité publique nationale, chargée de la protection des droits d'auteur et des droits voisins contre des atteintes à ces droits commises sur Internet, puisse accéder, pour les besoins de la lutte contre les infractions pénales en général, aux données relatives à l'identité civile des abonnés de services de communications électroniques, correspondant à des adresses IP, à la seule fin d'identifier les personnes soupçonnées d'avoir commis de telles atteintes et de prendre, le cas échéant, des mesures à leur égard. Cependant, dès lors que la même autorité publique peut mettre en relation ces données d'identité, de manière itérative pour une même personne, avec des informations, même limitées, portant sur le contenu des oeuvres illégalement mises à disposition sur Internet, et être ainsi renseignée sur des aspects, y compris sensibles, de la vie privée des personnes en cause, un tel accès doit être encadré par la réglementation nationale.

7. A ce titre, en premier lieu, la Cour de justice de l'Union européenne dit pour droit qu'il doit être interdit aux agents disposant d'un tel accès, d'une part, de divulguer, sous quelque forme que ce soit, des informations sur le contenu des fichiers consultés par les personnes en cause, sauf à la seule fin de saisir le ministère public, d'autre part, de procéder à un traçage du parcours de navigation de ces personnes et, d'une manière générale, d'utiliser leurs adresses IP à des fins autres que celle d'identifier leurs titulaires en vue de l'adoption d'éventuelles mesures à leur encontre.

8. En deuxième lieu, la Cour de justice de l'Union européenne dit pour droit que, lorsque cette autorité publique a déjà mis en relation à deux reprises les données d'identité d'une même personne avec des informations relatives au contenu d'oeuvres illégalement mises à disposition sur Internet, elle ne peut procéder pour une troisième fois à cette mise en relation sans y avoir été autorisée par une juridiction ou une entité administrative indépendante. La Cour juge à ce titre, ainsi qu'il résulte des motifs et du dispositif de l'arrêt, qu'un tel contrôle, qui ne peut pas être entièrement automatisé, doit être effectué de manière préalable, sauf urgence dûment justifiée, par un organe disposant de toutes les attributions et présentant toutes les garanties nécessaires en vue d'assurer une conciliation des différents intérêts légitimes et droits en cause. Lorsqu'il est effectué par une entité administrative, celle-ci doit jouir d'un statut lui permettant d'agir de manière objective et impartiale, et avoir la qualité de tiers par rapport à l'autorité qui demande l'accès aux données.

9. Par ailleurs, il résulte des motifs de l'arrêt du 30 avril 2024 de la Cour de justice de l'Union européenne que, dans l'hypothèse où la personne concernée est soupçonnée d'avoir commis des faits relevant des infractions pénales en général, la juridiction ou l'entité administrative indépendante chargée d'effectuer le contrôle mentionné au point précédent doit refuser l'accès aux données relatives à l'identité civile, lorsqu'il permettrait à l'autorité publique qui l'a sollicité de tirer des conclusions précises sur la privée de cette personne. En revanche, un tel accès peut être autorisé lorsque les éléments portés à la connaissance de cette juridiction ou de cette entité administrative indépendante permettent de soupçonner que la personne concernée a commis des faits relevant de formes graves de criminalité.

10. En troisième lieu, la Cour de justice de l'Union européenne dit pour droit que le traitement de données à caractère personnel utilisé par l'autorité publique doit faire l'objet, à intervalles réguliers, d'un contrôle par un organisme indépendant, ayant la qualité de tiers par rapport à cette autorité publique, aux fins de vérifier l'intégrité du système, y compris les garanties effectives contre les risques d'accès et d'utilisation abusifs ou illicites des données, ainsi que son efficacité et sa fiabilité pour détecter d'éventuels manquements.

Sur le cadre juridique interne :

11. En vertu de l'article L. 336-3 du code de la propriété intellectuelle, le titulaire d'un accès à des services de communication au public en ligne a l'obligation de veiller à ce que cet accès ne fasse pas l'objet d'une utilisation à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'oeuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires de ces droits, lorsqu'elle est requise. Pour assurer le respect de cette obligation, l'Autorité de régulation de la communication audiovisuelle et numérique (ARCOM), agissant sur saisine des organismes de défense professionnelle régulièrement constitués, des organismes de gestion collective, du Centre national du cinéma et de l'image animée, ou sur la base d'informations transmises par le procureur de la République

ou d'un constat d'huissier établi à la demande d'un ayant droit, est chargée de mettre en oeuvre les mesures de protection des oeuvres et des objets, auxquels est attaché un droit d'auteur ou un droit voisin, définies aux articles L. 331-19 à L. 331-24 du même code, relevant de la procédure dite de " réponse graduée ".

12. Conformément à l'article L. 331-13 et au I de l'article L. 331-14 du code de la propriété intellectuelle, cette mission est réalisée par le membre de l'ARCOM désigné en application du IV de l'article 4 de la loi du 30 septembre 1986 relative à la liberté de communication, ainsi que par des agents publics assermentés devant l'autorité judiciaire et habilités par le président de l'ARCOM dans les conditions prévues aux articles R. 331-2 à R. 331-5 du même code. En vertu de l'article 8 de cette loi, ce membre et ces agents sont astreints au secret professionnel pour les faits, actes et renseignements dont ils ont pu avoir connaissance en raison de leurs fonctions, dans les conditions et sous les peines prévues aux articles 413-9 et 413-10 du code pénal.

13. Comme en dispose le premier alinéa de l'article L. 331-20 du code de la propriété intellectuelle, la procédure de réponse graduée consiste à adresser aux abonnés ayant commis des faits susceptibles de constituer un manquement à l'obligation définie à l'article L. 336-3 du même code, une recommandation leur rappelant le contenu de cette obligation, leur enjoignant de la respecter et les avertissant des sanctions encourues. En cas de renouvellement de tels faits dans un délai de six mois, le deuxième alinéa du même article L. 331-20 prévoit que l'autorité peut adresser une nouvelle recommandation comportant les mêmes informations que la précédente, mais assortie " d'une lettre remise contre signature ou de tout autre moyen propre à établir la preuve de la date de présentation de cette recommandation ". Si, dans l'année suivant cette seconde recommandation, de nouveaux manquements sont constatés, l'article R. 331-12 du même code dispose que l'autorité informe l'intéressé par lettre remise contre signature que ces faits sont susceptibles de poursuites. Le cas échéant, conformément à l'article R. 331-14 du même code, la décision du membre compétent de l'ARCOM, constatant que les faits sont susceptibles de constituer l'infraction de négligence caractérisée définie à l'article R. 335-5 ou les infractions de contrefaçon prévues aux articles L. 335-2, L. 335-3 et L. 335-4 du même code, est transmise au procureur de la République près le tribunal judiciaire compétent.

14. Pour les besoins de cette réponse graduée, l'article L. 331-23 du code de la propriété intellectuelle autorise l'ARCOM à mettre en oeuvre un traitement automatisé de données à caractère personnel dans les conditions définies par un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés. Comme en dispose le I de l'article 4 et l'annexe du décret litigieux du 5 mars 2010 relatif au traitement automatisé de données à caractère personnel autorisé par l'article L. 331-23 du code de la propriété intellectuelle dénommé "Système de gestion des mesures pour la protection des oeuvres sur internet", le membre et les agents compétents de l'ARCOM ont " directement accès ", d'une part, aux données à caractère personnel transmises par les personnes et autorités ayant saisi l'ARCOM et qui portent notamment sur l'" adresse IP " de la personne ayant commis les faits signalés, les " informations relatives aux oeuvres ou objets protégés concernés par les faits " et le " nom du fichier tel que présent sur le poste de l'abonné " et, d'autre part, aux données à caractère personnel obtenues auprès des opérateurs de communications électroniques, notamment les " nom de famille, prénoms " de l'abonné, ses " adresse postale et adresses électroniques ", ses " coordonnées téléphoniques " et l'" adresse de l'installation téléphonique ".

Sur la légalité du refus d'abrogation attaqué :

15. Aux termes de l'article L. 243-2 du code des relations entre le public et l'administration : " L'administration est tenue d'abroger expressément un acte réglementaire illégal ou dépourvu d'objet, que cette situation existe depuis son édiction ou qu'elle résulte de circonstances de droit ou de fait postérieures, sauf à ce que l'illégalité ait cessé ". L'effet utile de l'annulation pour excès de pouvoir du refus d'abroger un acte réglementaire illégal réside dans l'obligation, que le juge peut prescrire d'office en vertu des dispositions de l'article L. 911-1 du code de justice administrative, pour l'autorité compétente, de procéder à l'abrogation de cet acte afin que cessent les atteintes illégales que son maintien en vigueur porte à l'ordre juridique. Il s'ensuit que, lorsqu'il est saisi de conclusions aux fins d'annulation du refus d'abroger un acte réglementaire, le juge de l'excès de pouvoir est conduit à apprécier la légalité de l'acte réglementaire dont l'abrogation a été demandée au regard des règles applicables à la date de sa décision.

16. En premier lieu, si la ministre de la culture soutient que les quatre principaux fournisseurs d'accès à Internet opérant sur le territoire français conservent les données relatives à l'identité civile des abonnés et à leur " trafic IP " dans des conditions respectant les exigences énoncées au point 5, aucune disposition légale n'impose une telle conservation, dans ces conditions, aux opérateurs de communications électroniques, s'agissant des besoins de la lutte contre les infractions pénales en général. Par suite, les requérantes sont fondées à soutenir que le décret du 5 mars 2010 est entaché d'illégalité en tant qu'il ne limite pas les données enregistrées dans le traitement à celles qui ont été conservées par les opérateurs de communications électroniques dans des conditions satisfaisant aux exigences, rappelées au point 5, du droit de l'Union européenne. Elles sont, par suite, fondées à soutenir que le refus d'abroger le décret du 5 mars 2010 est, dans cette mesure, entaché d'illégalité.

17. En deuxième lieu, s'il est constant que le membre et les agents compétents de l'ARCOM mettent en oeuvre, conformément aux dispositions citées au point 12, la procédure de réponse graduée dans le respect des exigences de confidentialité et de protection de la vie privée énoncées au point 7, aucune disposition n'impose à ces personnes de solliciter l'autorisation d'une juridiction ou d'une entité administrative indépendante, dans les conditions prévues au point 8, pour accéder aux données d'identité d'une personne qui, bien qu'ayant fait l'objet de deux recommandations en application de l'article L. 331-20 du code de la propriété intellectuelle, a commis pour la troisième fois des faits susceptibles de constituer un manquement à l'obligation prévue à l'article L. 336-3 du même code. Or, ainsi que le dit pour droit la Cour de

justice de l'Union européenne, un tel accès est susceptible à ce stade de la procédure de réponse graduée de révéler des informations, le cas échéant sensibles, sur des aspects de la vie privée de la personne concernée et doit, par suite, être préalablement autorisé par une juridiction, ou par une entité administrative indépendante de l'ARCOM, agissant de manière objective et impartiale.

18. Il s'ensuit que les requérantes sont fondées à soutenir que les dispositions du I de l'article 4 du décret du 5 mars 2010, en tant qu'elles autorisent le membre et les agents de l'ARCOM mentionnés au point 12 à accéder, une troisième fois pour une même personne, aux données d'identité conservées dans le traitement sans que cet accès soit subordonné à l'autorisation d'une juridiction ou d'une entité administrative indépendante, méconnaissent les exigences qui découlent du droit de l'Union européenne. Elles sont, par suite, fondées à soutenir que le refus d'abroger le décret du 5 mars 2010 est, dans cette mesure, entaché d'illégalité.

19. Il résulte de tout ce qui précède que la décision attaquée doit être annulée en tant qu'elle refuse d'annuler le décret litigieux dans la seule mesure où, d'une part, pour les besoins de la lutte contre les infractions pénales en général, il ne limite pas les données enregistrées dans le traitement qu'il instaure à celles qui ont été conservées par les opérateurs de communications électroniques dans des conditions satisfaisant aux exigences, rappelées au point 5, du droit de l'Union européenne et où, d'autre part, les dispositions du I de son article 4 autorisent le membre et les agents de l'ARCOM mentionnés au point 12 à accéder directement aux données d'identité d'une personne qui, bien qu'ayant fait l'objet de deux recommandations en application de l'article L. 331-20 du code de la propriété intellectuelle, a commis pour la troisième fois des faits susceptibles de constituer un manquement à l'obligation prévue à l'article L. 336-3 du même code.

Sur les effets de l'annulation prononcée :

20. En premier lieu, si la ministre de la culture soutient que l'édiction et la mise en oeuvre des dispositions nécessaires au plein respect des exigences européennes méconnues par le décret du 5 mars 2010 impliquent de différer de douze mois les effets de l'annulation prononcée, il ne ressort pas des pièces du dossier que l'annulation avec effet immédiat du refus d'abroger les dispositions contestées se heurte à une nécessité impérieuse de nature à justifier, à titre exceptionnel, de déroger au principe selon lequel le juge national ne peut moduler les effets d'une annulation contentieuse qui résulte de la méconnaissance du droit de l'Union européenne. Les conclusions de la ministre de la culture tendant à ce que les effets de l'annulation soient modulés dans le temps doivent donc être rejetées.

21. En deuxième lieu, l'annulation de la décision du Premier ministre refusant d'abroger le décret du 5 mars 2010 implique seulement qu'il lui soit enjoint d'abroger ce décret dans la seule mesure où ses dispositions méconnaissent les exigences qui découlent du droit de l'Union européenne, sans qu'il soit besoin d'assortir cette injonction d'une astreinte.

22. En troisième lieu, l'annulation prononcée par la présente décision implique nécessairement que l'ARCOM s'abstienne de faire application des dispositions législatives qui, pour les motifs énoncés ci-dessus, méconnaissent les exigences qui découlent du droit de l'Union européenne. Afin d'assurer la continuité de sa mission de lutte contre la contravention de négligence caractérisée, qui concourt notamment aux objectifs fixés par la directive européenne du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information, l'ARCOM ne peut, dans l'attente de l'édiction des dispositions nécessaires au respect des exigences mentionnées au point 5, continuer de demander aux opérateurs de communications électroniques l'accès aux données à caractère personnel relatives aux abonnés dont les adresses IP lui ont été transmises par les personnes chargées de veiller à la protection du droit d'auteur et des droits voisins, que s'il est établi que ces données ont été conservées par ces opérateurs dans les conditions énoncées au point 5. Toutefois, ces conditions de conservation n'étant pas exigibles pour la poursuite d'un objectif entrant dans le champ de la criminalité grave, l'ARCOM peut, sans être tenue d'en vérifier l'application, demander un tel accès aux opérateurs de communications électroniques lorsque les faits dont elle est saisie sont susceptibles de constituer les délits définis aux articles L. 335-2, L. 335-3 ou L. 335-4 du code de la propriété intellectuelle et d'entrer dans le champ de la criminalité grave.

23. En dernier lieu, l'annulation prononcée par la présente décision ne fait pas obstacle à ce que, dans l'attente de l'édiction des dispositions nécessaires au respect des exigences mentionnées au point 8, le membre et les agents de l'ARCOM mentionnés au point 12 accèdent aux données d'identité d'une personne à la seule fin de lui adresser la première ou la seconde des deux recommandations successives prévues par l'article L. 331-20 du code de la propriété intellectuelle.

24. Il y a lieu, dans les circonstances de l'espèce, de mettre à la charge de l'Etat à verser aux associations La Quadrature du Net, French Data Network, Franciliens.net et Fédération des fournisseurs d'accès à internet associatifs la somme de 1 000 euros pour chacune, au titre de l'article L. 761-1 du code de justice administrative.

D E C I D E :

Article 1er : La décision du Premier ministre, en tant qu'elle refuse d'abroger les dispositions du décret n° 2010-236 du 5

mars 2010 qui méconnaissent, pour les motifs énoncés par la présente décision, les exigences du droit de l'Union européenne, est annulée.
Article 2 : Il est enjoint au Premier ministre d'abroger les dispositions du décret du 5 mars 2010 dans la mesure énoncée à l'article 1er.
Article 3 : L'annulation prononcée à l'article 1er comporte pour l'ARCOM les obligations définies par les motifs de la présente décision.
Article 4 : L'Etat versera aux associations La Quadrature du Net, French Data Network, Franciliens.net et Fédération des fournisseurs d'accès à internet associatifs une somme de 1 000 euros pour chacune, au titre de l'article L. 761-1 du code de justice administrative.
Article 5 : Le surplus des conclusions de la requête est rejeté.
Article 6 : La présente décision sera notifiée à l'association La Quadrature du Net, première dénommée, au Premier ministre, à la ministre de la culture, à l'Autorité de régulation de la communication audiovisuelle et numérique et à la Commission nationale de l'informatique et des libertés.