

N° 433539 La Quadrature du Net et autres

10^{ème} et 9^{ème} chambres réunies

Séance du 3 avril 2026

Décision du 30 avril 2026

CONCLUSIONS

Mme Charline NICOLAS, Rapporteuse publique

La présente affaire est aussi ancienne que complexe et vous aurez l'occasion aujourd'hui de la solder, à défaut de pouvoir la simplifier.

A la croisée des chemins entre protection des droits d'auteur et protection de la vie privée, elle vous invite à tirer les conséquences de la réponse apportée le 30 avril 2024 par l'assemblée plénière de la Cour de Justice de l'Union européenne à une question préjudicielle, que vous lui aviez soumise (CE, 15 juillet 2021, *La Quadrature du Net et autres*, n° 433539, Inédite), portant sur les modalités de recueil de certaines données dans le cadre de la procédure dite de « réponse graduée » à l'encontre du téléchargement illégal d'œuvres protégées par le droit d'auteur et mise en œuvre, en vertu de l'article L. 331-25 du code de la propriété intellectuelle (devenu depuis l'article L. 331-20 du même code), par la Haute autorité pour la diffusion des œuvres et la protection des droits sur internet (HADOPI)¹, devenue depuis la loi du 25 octobre 2021², l'Autorité de régulation de la communication audiovisuelle et numérique (ARCOM).

¹ Au titre de ses missions de protection des œuvres et des objets auxquels est attaché un droit d'auteur ou un droit voisin à l'égard des atteintes à ces droits commises sur les réseaux de communication électroniques utilisés par la fourniture de services de communication au public en ligne (2° de l'article L. 331-13 du CPI dans

Ces conclusions ne sont pas libres de droits. Leur citation et leur exploitation commerciale éventuelles doivent respecter les règles fixées par le code de la propriété intellectuelle. Par ailleurs, toute rediffusion, commerciale ou non, est subordonnée à l'accord du rapporteur public qui en est l'auteur.

S'adaptant constamment à l'évolution des technologies numériques, les atteintes aux droits d'auteur sur internet peuvent prendre différentes formes (streaming, téléchargement direct...), parmi lesquelles figure le « pair à pair » (« *peer to peer* »), particulièrement bon marché, qui permet, en synthèse, de partager des fichiers numérisés entre ordinateurs reliés entre eux, à l'aide d'un logiciel ou d'une application spécifique.

Face à cette pratique, le législateur français, par les lois des 12 juin 2009 et 28 octobre 2009³, a choisi de mettre en place **un mécanisme dit de « riposte graduée »**, qui a inspiré certains pays, dont le Royaume Uni, mais qui semble minoritaire dans l'Union européenne.

Par rapport à d'autres systèmes mis en œuvre, celui-ci présente deux caractéristiques.

Il repose, en premier lieu, sur l'obligation, fixée à l'article L. 336-3 du CPI, du titulaire de l'accès à internet de veiller à ce que son 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'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits, **et sur la sanction de la méconnaissance de cette obligation, mais qui n'intervient qu'à l'issue d'une phase préalable d'information visant à responsabiliser les internautes dès la commission des premiers faits**. Concrètement, saisie de faits de mise à disposition de contenus en ligne portant atteinte aux droits d'auteur ou aux droits voisins, la commission de protection des droits de l'Autorité envoie au titulaire de l'accès à internet, par l'intermédiaire du fournisseur d'accès à internet, une première « recommandation » rappelant l'obligation de surveillance de son accès à internet ainsi que les sanctions encourues, puis en cas de renouvellement de faits dans les six mois, une deuxième recommandation par courrier électronique, doublé cette fois-ci d'un envoi postal. Et

sa version en vigueur à la date du décret du 5 mars 2010, devenu, s'agissant de l'ARCOM, 1° de l'article L. 331-12 du CPI).

² Loi n° 2021-1382 du 25 octobre 2021 relative à la régulation et à la protection de l'accès aux œuvres culturelles à l'ère numérique.

³ Loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet et loi n° 2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur internet.

Voir s'agissant du Royaume-Uni, le Digital Economy Act du 18 avril 2010 (<http://www.legislation.gov.uk/ukpga/2010/24contents>)

Ces conclusions ne sont pas libres de droits. Leur citation et leur exploitation commerciale éventuelles doivent respecter les règles fixées par le code de la propriété intellectuelle. Par ailleurs, toute rediffusion, commerciale ou non, est subordonnée à l'accord du rapporteur public qui en est l'auteur.

si dans un délai d'un an suivant cette deuxième recommandation, de nouveaux faits sont constatés, l'ARCOM peut saisir le Procureur de la République aux fins de poursuites pénales. Les recommandations mentionnent la date et l'heure auxquelles les faits susceptibles de constituer un manquement ont été constatés, précisent le contenu des œuvres ou objets protégés concernés par ce manquement et indiquent les coordonnées postales et électroniques où leur destinataire peut adresser, s'il le souhaite, des observations à l'autorité.

A défaut d'avoir mis en place un moyen de sécurisation de son accès ou d'avoir mis en œuvre ce moyen avec diligence, constituant ainsi une « négligence caractérisée », le contrevenant risque une amende prévue pour les contraventions de cinquième classe, soit une amende de 1500 euros pour une personne physique et 7500 euros pour une personne morale⁴. Cette sanction ne peut être prononcée qu'en cas d'échec de la démarche pédagogique décrite précédemment. Il peut par ailleurs être poursuivi pour le délit de contrefaçon (prévu aux articles L. 335-2 et suivants du CPI), puni de trois ans d'emprisonnement et de 300 000 euros d'amendes. Enfin, en cas de négligence caractérisée ou de délit de contrefaçon, une peine complémentaire de suspension de la connexion à internet peut être prononcée par l'autorité judiciaire (le Conseil constitutionnel ayant censuré une disposition prévoyant que l'HADOPI puisse prononcer une telle sanction : décision n° 2009-580 DC du 10 juin 2009).

Ce mécanisme, à mi-chemin entre incitation et coercition, semble particulièrement efficace, toutes choses égales par ailleurs, puisque selon le bilan 2025 de la « lutte contre le piratage » publié par l'ARCOM en mars 2026⁵, il est constaté une tendance baissière de l'audience des services et applications de pair à pair depuis 2018, près de 75 % des abonnés ne réitèrent pas leur manquement à chaque phase de la procédure. Ainsi, au cours de l'année passée, sur les 80 000 premiers avertissements envoyés, 17 000 ont fait l'objet d'un deuxième avertissement et parmi ces derniers, 3400 ont donné lieu à un constat de négligence et 1300 à une décision de transmission à l'autorité judiciaire. Enfin, 631 suites judiciaires et 300 sanctions pécuniaires prononcées sont recensées pour l'année 2025.

La deuxième caractéristique de ce mécanisme, en second lieu, est qu'il repose sur l'exercice par une autorité administrative indépendante du pouvoir de constater les atteintes aux droits d'auteur, à la différence d'autres systèmes font reposer cette

⁴ Article R. 335-5 du CPI

⁵ https://www.arcom.fr/sites/default/files/2026-03/Arcom_Bilan%202025_Lutte_Piratage.pdf

Ces conclusions ne sont pas libres de droits. Leur citation et leur exploitation commerciale éventuelles doivent respecter les règles fixées par le code de la propriété intellectuelle. Par ailleurs, toute rediffusion, commerciale ou non, est subordonnée à l'accord du rapporteur public qui en est l'auteur.

responsabilité sur les fournisseurs d'internet. **A ce titre, elle est placée au centre d'une organisation de flux de données spécifique lui permettant d'identifier les individus** qui partagent illégalement des contenus protégés. Cette organisation de flux de données constitue l'objet du décret du 5 mars 2010 relatif au traitement automatisé de données à caractère personnel dénommé « système de gestion des mesures pour la protection des œuvres sur internet », dont la création a été autorisée par l'article L. 331-29 du CPI, dans sa version alors applicable, et dont le refus implicite d'abrogation est aujourd'hui contesté devant vous par les associations requérantes.

En synthèse, l'HADOPI, à travers le traitement contesté, met en relation successivement deux traitements de données personnelles distincts :

En amont, des agents assermentés et agréés désignés par les organismes d'ayants droits (à savoir ceux de défense professionnelle, les sociétés de perception et de répartition des droits et le Centre national du cinéma et de l'image animée), collectent sur les réseaux de pair à pair, les adresses IP des internautes dont l'accès à internet a été utilisé à des fins de reproduction, de représentation, de mise à disposition d'œuvres protégées sans autorisation de leurs auteurs.

En vertu de l'article L. 331-24 alors applicable, ils saisissent la commission de protection des droits de l'HADOPI des constats ainsi réalisés, lesquels comportent un certain nombre d'informations, dont la liste figure au 1° de l'annexe du décret du 5 mars 2010 parmi lesquelles la date et l'heure des faits, le protocole utilisé, le pseudonyme utilisé par l'abonné, le nom du fichier et le fournisseur d'accès à internet auprès duquel l'accès a été souscrit, ou encore le nom des huissiers ayant établis les constats et des ayant droit à la demande desquels ces constats ont été établis.

En aval, à partir de ces éléments, les agents assermentés habilités par l'Autorité recueillent auprès des opérateurs de communications électroniques les noms et coordonnées des abonnés correspondant aux adresses IP précédemment collectées leur permettant d'identifier les abonnés en cause. Le 2° de l'annexe I du décret énumère ainsi les différents éléments relatifs à l'identité et aux coordonnées de l'abonné. Ce droit de communication auprès de ces opérateurs est fondé sur le 3^{ème} alinéa de l'article L. 331-21 du CPI qui a été déclaré conforme sur ce point par le Conseil constitutionnel dans sa décision n°2020-841 QPC du 20 mai 2020,

suite à la QPC que vous lui aviez transmise⁶ (les éléments censurés par le juge constitutionnel n'ayant pas été repris par les dispositions réglementaires). Du côté des opérateurs, l'article L. 34-1 du code des postes et des télécommunications électroniques (CPCE) leur impose de conserver certaines données selon certaines finalités (notamment en vue de la prévention et de répression de la criminalité, de la délinquance grave et des autres manquements graves), par dérogation à leur obligation d'effacer ou de rendre anonyme toute donnée relative au trafic.

Après cette présentation du cadre légal et opérationnel applicable caractéristique du mécanisme, il est temps d'en venir à la requête.

Précisons à titre liminaire que le décret du 5 mars 2010 a été modifié par un décret du 24 décembre 2021 pour tirer les conséquences de la fusion de l'HADOPI avec le CSA et la création de l'ARCOM, mais que ce toilettage ne rend pas sans objet la requête de la Quadrature du Net.

Précisons en outre et pour mémoire, que dans votre décision précédente du 5 juillet 2011, vous avez écarté les moyens de légalité externe et les moyens de légalité interne tirés de l'inconstitutionnalité de l'article L. 331-21 du CPI et de la méconnaissance de 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 (dite directive « *e-privacy* ») en ce que le décret prévoit le recueil des données relatives à l'identité civile dans le cadre de la lutte contre des infractions dépourvues de gravité ainsi qu'en ce que les personnes dont les données sont recueillies ne disposent pas de voie de recours. Nous n'y reviendrons donc pas.

Pour l'examen qui vous occupe aujourd'hui, nous commencerons par le moyen qui a justifié le renvoi d'une question préjudicielle à la Cour.

Les associations requérantes soutiennent que l'accès par des agents de la HADOPI aux données de connexion conservées par les opérateurs, à savoir celles relatives à l'identité civile de l'utilisateur, au trafic et à la localisation, méconnaît la directive « *e-privacy* », dès lors que cet accès n'était pas préalablement autorisé par un juge ou une autorité administrative indépendante présentant des garanties d'impartialité.

⁶ CE, 12 février 2020, La Quadrature du Net et autres, n° 433539, Inédite.

Ce moyen prend appui sur l'arrêt de la CJUE *Tele2 Sverige AB* rendu le 21 décembre 2016⁷ et confirmé depuis⁸ portant sur l'interprétation de l'article 15 de la directive *e-privacy*, lequel permet, sous réserve que la mesure soit nécessaire, appropriée et proportionnée, de déroger à certains droits prévus par la directive, en particulier au principe de confidentialité des communications, notamment en vue d'assurer la prévention et la recherche d'infractions pénales.

Dans cette affaire, étaient en cause des mesures nationales prévoyant une conservation généralisée et indifférenciée de l'ensemble des données des utilisateurs d'internet relatives au trafic et de localisation, soit, selon la Cour, des données susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, (telles que les habitudes de la vie quotidienne, les lieux de séjour, les déplacements...). **Elle en déduisait que l'ingérence dans les droits fondamentaux qui en résultait devait être qualifiée « particulièrement grave », et partant, que seule la lutte contre la criminalité grave était susceptible de justifier une telle mesure.**

Au regard de ces éléments, et en particulier de l'absence de limitation de l'accès à ces données aux seules fins de lutte contre la criminalité grave, la Cour en a conclu que l'accès à ces données par les autorités publiques devait être soumis à un contrôle préalable par une juridiction ou une autorité administrative indépendante permettant de garantir que cet accès soit limité au strict nécessaire⁹.

Face aux conséquences d'une éventuelle interprétation stricte de cette décision pour une procédure qui implique près d'un million d'accès par an aux données conservées par les

⁷ CJUE, 21 décembre 2016 *Tele2 Sverige AB c/ Post-och telestyrelsen et Secretary of State for the Home Department c/ Tom Watson et autres* (C 203/15 et C 698/15).

⁸ CJUE, 2 mars 2021 *H.K. / Prokuratuur* (C 746/18).

⁹ *L'article 15, paragraphe 1, de la directive 2002/58, telle que modifiée par la directive 2009/136, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale régissant la protection et la sécurité des données relatives au trafic et des données de localisation, en particulier l'accès des autorités nationales compétentes aux données conservées, sans limiter, dans le cadre de la lutte contre la criminalité, cet accès aux seules fins de lutte contre la criminalité grave, sans soumettre ledit accès à un contrôle préalable par une juridiction ou une autorité administrative indépendante, et sans exiger que les données en cause soient conservées sur le territoire de l'Union.*

opérateurs et qui ne relève pas, s’agissant de l’infraction de « négligence caractérisée » de la criminalité grave, nous comprenons que vous avez souhaité inciter la Cour à un certain pragmatisme en lui demandant d’une part, si les données d’identité civile (nom et adresses) sont au nombre des données relatives au trafic et à la localisation qui sont soumises à une exigence de contrôle préalable, d’autre part, si au regard de la faible sensibilité de ces données, l’absence d’un tel contrôle est contraire à la directive *e-privacy*, et *enfin*, si tel est le cas, si la mise en place d’un contrôle automatisé sous certaines conditions est possible.

Dans un premier temps, la Cour n’est pas restée indifférente aux conditions particulières de la riposte graduée mise en place par le législateur français.

D’une part, s’agissant de l’accès aux adresses IP conservées aux fins de l’objectif de lutte contre les infractions pénales en général (et non de criminalité grave), elle a admis un tel principe dès lors que cet accès est autorisé à seule fin d’identifier la personne soupçonnée d’être impliquée dans de telles infractions et que les modalités de conservation de ces adresses, de manière étanche, évitent de tirer des conclusions sur la vie privée des personnes (nous y reviendrons). Elle a ainsi assoupli sa jurisprudence issue de son arrêt de grande chambre du 6 octobre 2020 *La Quadrature du Net*¹⁰ et celui précité *Tele2 Sverige* (au point 102) dans laquelle elle avait jugé que l’article 15 de la directive s’opposait à ce qu’une conservation généralisée et indifférenciée des adresses IP soit autorisée pour des objectifs autres que la lutte contre la criminalité grave, la prévention des menaces graves contre la sécurité publique ou la sauvegarde de la sécurité nationale.

D’autre part, elle a relevé, outre l’objectif d’intérêt général poursuivi par le dispositif de riposte graduée, le caractère limité des données recueillies relatives au trafic et à la localisation du titulaire d’accès qui ne permet pas un traçage exhaustif de son parcours de navigation, ainsi celui des données relatives à l’œuvre concernée (son titre essentiellement), et le caractère indispensable de ces données en vue de l’identification des auteurs d’infraction. Elle a par ailleurs fait état des garanties afférentes à cet accès, tirées notamment des obligations de confidentialité auxquelles sont soumis les agents assermentés de la Haute autorité.

¹⁰ C-511/18, C-512/18 et C-520/18.

S'écartant du contexte de l'affaire *Tele2 Sverige*, elle a ainsi jugé que l'ingérence que comporte « *l'accès aux données relatives à l'identité civile des utilisateurs des moyens de communications électroniques à seule fin d'identifier l'utilisateur concerné et sans que ces données puissent être associées aux communications effectuées* » ne saurait en principe être qualifiée de **grave** et que **l'exigence d'un contrôle préalable n'a donc pas vocation à s'appliquer dans ce cas** (points 132 et 133).

Dégageant ces principes de la situation d'espèce, la Cour aurait pu s'arrêter là, comme l'y invitait au demeurant son avocat général. **Mais elle a continué son raisonnement** en considérant qu'il ne saurait toutefois être exclu que, dans des « situations atypiques », les données mises à disposition de l'HADOPI, prises ensemble et au fur et à mesure que se déroule la procédure de riposte graduée, soient susceptibles de révéler des informations, le cas échéant sensibles, sur des aspects de la vie privée de la personne et de permettre d'établir son profil (au point 135).

Apportant ainsi un tempérament au principe qu'elle venait tout juste de dégager, la Cour en a conclu qu'un contrôle d'une juridiction ou d'une autorité administrative indépendante devait intervenir préalablement à la troisième étape de la réponse graduée, soit concrètement avant l'envoi de la lettre de notification à l'abonné à raison de la troisième réitération des faits.

Nous ne cachons pas une certaine perplexité face à cette solution parce que, d'une part, elle revient à imposer un même contrôle de l'accès aux données, alors que le risque d'ingérence dans le vie privée nous semble sans rapport dans le cas d'un traitement recueillant l'ensemble des données des internautes comme dans l'affaire *Tele2 Sverige*, et celui en cause rassemblant au mieux quelques titres d'œuvres, et d'autre part sa praticabilité, quoi qu'en dise la Cour, ne nous semble pas d'un abord spontané.

Et ce d'autant que répondant à la troisième question qui lui était posée, la Cour indique que ce contrôle ne saurait être entièrement automatisé et qu'ainsi, au regard des pratiques de l'HADOPI (qui vérifie essentiellement de manière automatisée si les procès-verbaux contiennent toutes les informations et données requises), un contrôle du système de traitement de données par un organisme indépendant tiers par rapport à l'autorité devrait intervenir à intervalles réguliers et être prévu par une mesure législative.

Quoi qu'il en soit, au regard des termes de la réponse de la Cour, il ne fait guère de doute que le décret du 5 mars 2010, et en particulier le I de son article 4 qui permet aux agents de l'ARCOM d'accéder aux données d'identité du titulaire d'accès, ne satisfait pas les exigences relatives à l'existence d'un contrôle préalable au stade de la troisième étape de la riposte graduée puisqu'il ne le prévoit pas. Et force est de constater que le pouvoir réglementaire s'est abstenu de compléter ce décret en ce sens depuis l'arrêt du 30 avril 2024. Le constat de l'illégalité du refus de l'abroger dans cette mesure nous semble donc imparable.

Mais il y a plus problématique encore, et cette difficulté se trouve en amont.

Dans son arrêt du 30 avril 2024, la Cour ne s'en est en effet pas tenue au strict examen des questions posées, mais s'est prononcée sur la conformité au droit de l'Union européenne des conditions de conservation des adresses IP des fournisseurs de services de communications électroniques, estimant qu'une conservation préalable d'adresses IP non conforme à la directive du 12 juillet 2002 s'opposerait à l'accès de ces données par l'HADOPI.

Si comme nous l'avons mentionné précédemment, la Cour a assoupli sa jurisprudence concernant la conservation des adresses IP de manière générale et indifférenciée en vue de la lutte contre les infractions pénales en général, ce n'est qu'à la condition que cette conservation ne puisse engendrer des ingérences graves dans la vie privée de la personne concernée. Or celles-ci ne pouvaient être exclues, selon elle, dans des situations atypiques.

Pour s'en assurer, et alors que la directive posait une exigence générale vis-à-vis des fournisseurs d'internet de prendre les mesures d'ordre technique et organisationnel appropriées permettant d'assurer une protection efficace des données conservées contre tout accès illicite à ces données, la Cour a précisé cette exigence dans son arrêt, laquelle consiste à prévoir une « séparation étanche » doit être garantie entre chaque catégorie de données, y compris les données relatives à l'identité civile et les adresses IP, et les autres catégories de données conservées, la fiabilité de cette séparation devant, en outre, faire l'objet d'un contrôle régulier par une autorité tierce.

Vous remarquerez que le dispositif de l'arrêt « miroite » sur ce point avec sa motivation en ce que la Cour impose ces garanties pour exclure que « hormis dans des situations atypiques », cet accès puisse permettre de tirer des conclusions précises sur la vie privée. Il nous semble qu'en tout état de cause, il convient de lire l'arrêt comme imposant cette exigence technique dans toutes les situations.

Cela n'a pas échappé aux requérantes lesquelles, dans le dernier état de leurs écritures, soutiennent que le décret contesté est illégal en ce qu'il permet l'accès de l'ARCOM à des données qui ne sont pas conservées selon les modalités requises par la jurisprudence de la CJUE.

Comme le reconnaît elle-même la ministre en défense, aucune disposition législative, en particulier l'article L. 34-1 du CPCE (lequel n'évoque au demeurant que la criminalité grave), ou réglementaire ne prévoit de règles spécifiques concernant la conservation des données par les fournisseurs d'accès à internet aux fins de lutte contre les infractions pénales en général. Par conséquent, l'arrêt de la Cour implique nécessairement de compléter le droit existant pour prévoir une telle obligation.

Nous n'avons en tout état de cause guère de doute au vu du raisonnement de la Cour (point 59 de son arrêt) que cette illégalité rejaillit sur celle du décret en tant qu'il permet, au I de son article, aux agents de l'ARCOM à des fins de lutte contre la contravention de négligence caractérisée, d'accéder à des données dont les modalités de conservation ne sont pas régies par des dispositions prévoyant une séparation étanche conformément au droit de l'Union européenne.

A ce stade du raisonnement, disons-le, le plus dur reste à faire car vous devrez tirer les conséquences de ces deux motifs d'illégalité sur la décision de refus d'abrogation, puis celles d'une annulation partielle (« en tant que ») de cette dernière, le cas échéant.

En premier lieu, et contrairement aux conclusions des associations requérantes, nous ne vous proposons pas d'annuler la décision de refus d'abrogation du décret dans sa totalité. Nous ne sommes en effet pas dans l'hypothèse de votre décision *T...* (CE, 27 juillet 2001, n° 222509, au Rec.) dans laquelle l'absence de mesures propres à assurer le respect des conditions requises, entache l'acte réglementaire dans son ensemble. Concrètement, non seulement seules les dispositions du I de l'article 4 de ce décret sont concernées, mais en outre elles ne doivent être annulées qu'en tant qu'elles permettent certains types d'accès. Par exemple, l'ARCOM pourra ainsi continuer de recevoir les procès-verbaux des agents assermentés des représentants des ayants droits pour les premiers faits et lors d'une première réitération.

En second lieu, il vous faudra répondre à la demande de la ministre visant à différer d'une durée de douze mois les effets de l'annulation prononcée. Au soutien de sa demande, elle se prévaut de l'exigence de sanctions contre les atteintes aux droits d'auteur qui découlerait de la directive 2001/29/CE du 22 mai 2002 sur l'harmonisation des certains aspects du droit d'auteur et des droits voisins dans la société de l'information.

Mais d'une part, cette directive n'impose pas la mise en œuvre d'un mécanisme de riposte graduée tel que celui mis en place. D'autre part, l'application de votre décision *Association AC* (CE, Ass., 11 mai 2004, n°s 255886 et a., au Rec.), lorsqu'est en cause la méconnaissance du droit de l'Union européenne, emprunte une voie étroite : elle ne peut se faire qu'« à titre exceptionnel et en présence d'une nécessité impérieuse » (CE, Ass., 19 juillet 2017, *Association nationale des opérateurs détaillants en énergie*, n° 370321, au Rec.). Vous l'avez admis dans quelques cas où les conséquences de l'annulation sont particulièrement graves (s'agissant de l'annulation d'une décision administrative en cas de risque de rupture d'approvisionnement d'un produit sanguin : CE, 23 juillet 2014, *Sté Octapharma France*, n° 349717, au Rec. ; s'agissant de l'annulation d'un arrêté relatif aux tarifs réglementés de vente d'électricité applicables aux consommateurs non résidentiels en France métropolitaine continentale en raison de l'importante charge financière pesant sur ces consommateurs et aux incertitudes sur les conséquences en chaîne notamment en matière des restitutions financières dues par les fournisseurs d'électricité : CE, 23 juillet 2023, *Sté Ekwateur*, n° 462612, Inédite)

En l'espèce, les conséquences d'une annulation « sèche » n'entravera pas nécessairement la répression des atteintes les plus graves aux droits d'auteur et aux droits voisins, à savoir le délit de contrefaçon, qui peut être poursuivi sans mettre en œuvre la réponse graduée et en tout état de cause sans conservation étanche de la part des opérateurs des adresses IP dès lors qu'il relève de la criminalité grave. A titre infiniment subsidiaire, vous pourrez relever que le ministre a demandé cet effet différé il y a plus d'un an, sans pour autant prendre, depuis, les mesures exigées. Vous pourrez rejeter ses conclusions sur ce point.

En troisième lieu, l'annulation du refus d'abroger « en tant que » implique nécessairement à nos yeux que le décret du 5 mars 2010 soit abrogé dans la seule mesure des illégalités relevées. Par conséquent, vous pourrez enjoindre au Premier ministre d'abroger le décret dans cette seule mesure également.

Reste, en quatrième lieu et dans la logique de votre décision d'Assemblée du 28 juin 2001 V... (n° 213229, au Rec.) (voir également CE 30 juillet 2014 *La Cimade*, n° 375430, au Rec. ou encore CE, 12 octobre 2020, *Sté Vert Marine*, n° 419146, aux T.), à vous déterminer sur la nécessité de prendre des mesures transitoires indiquant la marche à suivre dans l'attente des dispositions législatives et réglementaires nécessaires à la mise en conformité avec le droit de l'Union européenne. Comme vous le savez, ces mesures transitoires peuvent être prononcées en l'absence même de conclusions à fins d'injonction sur ce point (CE 5/4 SSR, 3 décembre 2010, *Société SMP Technologie et association de tireurs*, n° 332540, aux T.).

Au regard du faible risque d'ingérence grave dans les droits fondamentaux résultant de « situations atypiques » d'un côté, et de l'objectif de sauvegarde de la propriété intellectuelle et de la création culturelle poursuivi par le mécanisme de la réponse graduée, de l'autre, nous sommes convaincus de leur nécessité.

S'agissant de l'accès de l'ARCOM aux adresses IP conservées par les opérateurs de services de communications électroniques, vous ne serez pas insensible à la réponse de la ministre à une mesure supplémentaire d'instruction qui indique qu'en pratique, ces préconisations sont respectées par les quatre principaux fournisseurs d'accès internet en France (SFR, Free, Orange et Bouygues Telecom) lesquels conservent notamment les adresses IP séparément des éléments d'identité Aussi, afin de limiter l'atteinte à la conformité du droit de l'Union tout en maintenant l'accès de l'ARCOM à ces données, il pourrait être exigé des opérateurs, lorsqu'ils sont sollicités par l'autorité, qu'ils apportent la preuve d'une séparation étanche effective de ces données. La mesure transitoire envisagée ne consisterait ainsi pas à déroger aux exigences de fond posées par la CJUE, mais seulement à l'exigence formelle d'édicter une réglementation contraignante en la matière.

Cette mesure permettrait, en outre et à cette condition, à l'ARCOM de continuer à mettre en œuvre le mécanisme de riposte graduée, à tout le moins jusqu'au deuxième avertissement. S'agissant de la troisième étape, dans l'attente de la mise en place d'un contrôle par une juridiction ou une entité administrative indépendante, elle pourra stocker les adresses IP recueillies par les représentants des ayants-droits en vue de les relier à une identité civile, une fois ces mesures édictées. Encore faudra-il que les durées de conservation de ces différentes données le permettent, ce qui, dans le silence de l'article L. 34-1 du CPCE s'agissant de la durée de conservation des adresses IP pour les besoins de lutte contre la criminalité « non grave », peut poser question. Toutefois, dans son arrêt du 30 avril 2024, la Cour a jugé qu' «

un tel objectif de lutte contre les infractions pénales en général permet de justifier qu'il soit donné accès aux données de trafic et de localisation qui ont été stockées et donc conservées dans la mesure et pour la durée nécessaires à la commercialisation des services, à la facturation et à la fourniture de services à valeur ajoutée », ce qui en application de l'article R. 10-14 CPCE est plafonné à 1 an

Et dans les deux cas, si l'ARCOM dispose de suffisamment d'éléments matériels établissant le délit de contrefaçon et suffisamment tôt, elle ne sera pas tenue de respecter ces mesures transitoires qui ne valent qu'en vue de la constatation d'une infraction de négligence caractérisée.

PCM, nous concluons :

- **à l'annulation de la décision du Premier ministre en tant qu'elle refuse d'abroger les dispositions du I de l'article 4 d décret du 5 mars 2010 dans la mesure où elles méconnaissent les exigences qui découlent du droit de l'Union européenne ;**
- **à ce qu'il soit enjoint au Premier ministre d'abroger les dispositions du I de l'article 4 du décret dans cette mesure ;**
- **à ce que l'Etat soit condamné à verser, au titre des dispositions de l'article L 761-1 du code de justice administrative, la somme globale de 4 000 euros aux associations la Quadrature du Net, French Data Network, Franciliens.net et Fédération des fournisseurs d'accès à internet associatifs ;**
- **et au rejet du surplus des conclusions.**