N° 433539
Le Quadrature du Net et autres

10ème et 9ème chambres réunies
Séance du 16 juin 2021
Lecture du 5 juillet 2021

CONCLUSIONS

M. Alexandre LALLET, rapporteur public

Cette affaire devrait, hélas, réjouir des millions d'internautes puisqu'elle met en jeu, indirectement, l'existence même de la Haute autorité pour la diffusion des œuvres et la protection des droits sur internet, la HADOPI. Il est à peine nécessaire de rappeler que cette autorité publique indépendante a notamment pour mission de détecter et prévenir les manquements à l'obligation de sécurisation de l'accès internet contre le téléchargement illégal et les autres atteintes au droit d'auteur et au droit voisin sur internet.

Pour ce faire, les agents assermentés désignés par les organismes de défense professionnelle, les organismes de gestion collective et le Centre national du cinéma et de l'image animée se connectent aux applications de partage de fichiers dites peer-to-peer, comme le très populaire *BitTorrent*, téléchargent des œuvres présélectionnées et relèvent les adresses IP de toutes celles et tous ceux qui les mettent à sa disposition, ainsi que les dates et heures, les protocoles de pair-à-pair utilisés, les pseudonymes, les noms des fichiers et les fournisseurs d'accès à internet auprès desquels l'accès a été souscrit. Ces éléments sont fournis à la commission de protection des droits de la HADOPI à l'appui des saisines des organismes compétents[1]. Sur cette base, la commission sollicite les opérateurs afin de mettre un nom sur chaque adresse IP. Elle est alors en mesure d'adresser aux contrevenants, via les opérateurs[2], une première recommandation rappelant les sanctions encourues, à savoir une contravention de cinquième classe en cas de négligence caractérisée et le délit de contrefaçon, dans le cadre du dispositif dit de « réponse graduée ». En cas de nouveau manquement dans le délai de six mois, la seconde recommandation est envoyée par la même voie, et par courrier à l'adresse postale également fournie par l'opérateur[3]. En cas de récidive dans le délai d'un an, une lettre de notification est adressée par courrier[4], et le procureur de la République peut être saisi par la commission de protection des droits.

---

[1] L'article R. 331-35 du code de la propriété intellectuelle subordonne la recevabilité des saisines à la fourniture de ces informations.
[2] Le dernier alinéa de l'article R. 331-37 du CPI précise que les opérateurs sont tenus d'adresser par voie électronique à l'abonné chacune des recommandations dans un délai de 24 heures suivant sa transmission par la commission de protection des droits.
[3] Art. L. 331-25 du CPI.

On le voit, la HADOPI est tributaire de la conservation et de la mise à disposition de certaines données concernant les utilisateurs des réseaux, sans lesquelles elle ne peut tout simplement plus exercer cette mission de protection des droits. L'article L. 34-1 du code des postes et des communications électroniques impose précisément aux fournisseurs d'accès à internet une obligation de conservation aux fins de l'exercice de cette mission. Sans évoquer spécifiquement cet objectif, l'article 6 de la loi pour la confiance dans l'économie numérique (LCEN) de 2004 prévoit également une obligation de conservation pour les données des créateurs de contenus sur internet, à la charge tant des fournisseurs d'accès que des hébergeurs. L'article L. 331-21 du code de la propriété intellectuelle organise l'accès des agents assermentés et habilités de la HADOPI aux données ainsi conservées. Dans sa version initiale, il ne comportait aucune restriction quant à la nature des données susceptibles d'être recueillies, tout en mettant l'accent, à titre d'illustration, sur l'identité, l'adresse postale, l'adresse électronique et les coordonnées téléphoniques de l'abonné dont l'accès a été abusivement utilisé. En pratique, seules ces données sont recueillies, comme on l'a vu.

Les données collectées auprès des opérateurs par les agents de la HADOPI sont versées, avec d'autres, dans un traitement de données à caractère personnel baptisé « Système de gestion des mesures pour la protection des œuvres sur internet », autorisé dans son principe par l'article L. 331-29 du CPI et dont les caractéristiques précises sont fixées par un décret n° 2010-236 du 5 mars 2010.

Les quatre associations requérantes vous demandent d'annuler le refus d'abroger ce décret.

Contrairement à ce que soutient la ministre, il ne peut être donné acte d'aucun désistement d'office dès lors qu'un mémoire complémentaire, annoncé dans la requête sommaire, a bien été produit dans le délai de trois mois. Le ministre ne pouvait pas le savoir, il est vrai, puisque ce mémoire ne lui a pas été transmis. Mais le caractère contradictoire de la procédure a été respecté dès lors que le mémoire produit le 6 mai dernier par les associations comporte, en la précisant, l'ensemble de l'argumentation de fond à laquelle le ministre a du reste répondu hier.

1. Au titre de la **légalité externe**, vous pourrez rappeler que l'article L. 232-4 du code des relations entre le public et l'administration dont les requérants se prévalent, qui frappe d'illégalité les décisions implicites dont l'administration s'abstient de fournir les motifs sur demande, ne s'applique qu'aux décisions qui doivent être motivées[5]. Or le refus d'abroger un acte réglementaire n'a pas à l'être[6].

---

[4] Art. R. 331-40 du CPI.

[5] V. par ex. CE, 6 juin 2018, *B…*, n° 400042, aux T. sur un autre point

[6] V. par ex., CE, 25 septembre 2020, *UDAF et France Liberté Voyage*, n° 437524. Rappelons qu'un tel moyen, mettant en cause les vices propres de la décision de refus d'abroger (et non la légalité externe de la décision dont l'abrogation est réclamée), n'est pas inopérant par principe (à la différence des moyens de légalité externe visant la décision dont l'abrogation est réclamée) et que son bien-fondé doit s'apprécier en se plaçant à la date de la décision attaquée (CE, 23 décembre 2020, *Association autisme espoir vers l'école*, n° 428284, au Rec.).

2. Les requérants vous demandent ensuite de **tirer les conséquences de la décision du Conseil constitutionnel du 20 mai 2020**[7], rendue à la suite de la transmission d'une QPC soulevée dans la présente affaire. Par l'ablation chirurgicale de l'adverbe « notamment », cette décision abroge, à compter du 31 décembre 2020, les dispositions de l'article L. 331-21 du CPI en tant qu'elles permettent à la HADOPI d'accéder à des données autres que celles relatives à l'identité et aux coordonnées des internautes contrevenants.

S'agissant d'un contentieux de refus d'abroger que vous tranchez en 2021, vous devez tenir compte de cette censure. Mais elle n'implique aucune modification du décret de 2010 et, en particulier, du 2° de son annexe qui énumère les données recueillies auprès des opérateurs qui peuvent être versées dans le traitement litigieux.

Comme on vient de le dire, l'article L. 331-21 du CPI, déclaré conforme à la Constitution sur ce point, permet justement le recueil de l'identité et des coordonnées de l'internaute. Il n'y a, à cet égard, aucune difficulté à inclure dans « l'adresse postale » de l'abonné évoquée par ce texte non seulement l'adresse déclarée au moment de la souscription de l'abonnement, mais aussi, comme l'envisage l'annexe au décret, l'adresse de l'installation téléphonique de l'abonné, qui peut être différente. C'est parfaitement conforme à l'intention du législateur, qui a entendu permettre à la HADOPI de se mettre en relation par tous moyens avec l'internaute afin de l'avertir du manquement et des sanctions encourues.

Le nom du fournisseur d'accès à internet, quant à lui, est fourni à l'appui des saisines (art R. 331-35 CPI). Et s'il s'agit d'un fournisseur qui utilise les ressources techniques d'un autre, identifié dans la saisine, son identité est fournie à ce dernier par la HADOPI. Le décret pouvait parfaitement faire figurer cette donnée parmi les données conservées dans le traitement[8].

3. Est allusivement invoqué un moyen d'**erreur manifeste d'appréciation** qui est parfaitement vain, puisqu'il est indispensable que la HADOPI puisse recueillir et traiter de telles données pour les besoins de la mission que lui a confiée le législateur.

4. Invoquant le droit de l'Union et, plus précisément, la directive *e-privacy* du 12 juillet 2002 et le RGPD, les associations se plaignent enfin de l'absence de garanties encadrant l'accès de la HADOPI aux données de connexion[9].

---

[7] Décision n° 2020-841 QPC.

[8] Formellement, les associations contestent aussi la légalité du recueil des adresses IP publiques, des protocoles de pair-à-pair et de l'identité des fournisseurs d'accès à internet correspondant à chaque adresse IP publique (accessible via le registre WHOIS). Mais cette argumentation est dénuée de portée. Ces données, qui sont publiques et ne nécessitent aucune réquisition auprès d'un opérateur, sont, on l'a dit, fournies spontanément à la HADOPI par les agents assermentés désignés par les organismes de gestion des droits. Elles ne relèvent pas du droit de communication régi par l'article L. 331-21 du CPI, seul en cause devant le Conseil constitutionnel.

[9] S'agissant des adresses IP, des protocoles de pair-à-pair et des fournisseurs d'accès correspondant aux adresses IP, la directive *e-privacy* ne s'applique pas puisque, comme indiqué à la note précédente, il s'agit de données rendues publiques par les internautes utilisant les applications de *peer-to-peer*, et non de données de trafic et de localisation dont les fournisseurs d'accès à internet devraient assurer la confidentialité et qu'ils devraient

Vous noterez que cet accès n'est pas organisé par le décret litigieux, mais par les dispositions du code de la propriété intellectuelle que nous avons rappelées. Le traitement de données n'en est, d'une certaine manière, qu'un « receleur ». Pour autant, l'opérance de cet ensemble de moyens ne nous paraît pas douteuse en tant qu'ils portent sur les données recueillies auprès des opérateurs par la HADOPI : en ce qu'il autorise un fichier contenant expressément ces données, le décret a bien pour objet et pour effet d'en autoriser la collecte, qui constitue un traitement de données à caractère personnel ou, si l'on préfère, l'une des opérations constitutives du traitement global géré par la Haute autorité. L'irrégularité éventuelle d'une telle collecte doit nécessairement rejaillir sur la légalité du décret dans cette mesure.

Il est possible de tirer trois griefs précis de l'argumentation en demande qui, pour le surplus, n'est pas assorti des précisions suffisantes en ce qu'elle se borne à asséner que le décret serait contraire au RGPD et à la Charte des droits fondamentaux de l'Union européenne.

4.1. Le premier grief reproche au décret de ne pas limiter le recueil des données conservées par les opérateurs à la **lutte contre la criminalité grave**. Que vous ayez participé à sa confection ou simplement lu la décision de l'Assemblée du contentieux du 21 avril dernier[10], vous n'ignorez pas que la Cour de justice de l'Union européenne a subordonné l'obligation de conservation par les opérateurs et l'accès par les autorités publiques aux données de trafic et de localisation stockées par les opérateurs à la condition qu'ils soient motivés soit par la sauvegarde de la sécurité nationale, soit par la lutte contre la criminalité grave ou la prévention des menaces graves à l'ordre public. Mais la Cour de justice a ménagé une souplesse pour les données relatives à l'identité civile de l'abonné, dans lesquelles elle a expressément inclus ses coordonnées, en admettant une obligation de conservation sans limitation de durée et un recueil administratif ou judiciaire pour la lutte contre toute infraction, y compris « non grave », en raison de la faible sensibilité de ces informations, qui ne fournissent pas d'informations sur les communications données (V. en particulier son arrêt *Ministerio fiscal* du 2 octobre 2018, C-207/16, repris par l'arrêt *LQDN et autres* du 6 octobre 2020, pt. 157)[11].

Or c'est justement de ces données qu'il s'agit ici. Dès l'instant que la HADOPI les recueille à la suite du constat d'un manquement à l'obligation de sécurisation de l'accès internet et en vue de prévenir des infractions pénales, elle s'inscrit bien dans un objectif de lutte contre les infractions, fussent-elles d'une gravité limitée. Il n'y a donc aucune difficulté à cet égard.

4.2. Vous n'aurez guère plus de peine à écarter le reproche suivant, qui tient à **l'absence de voies de recours** pour les personnes dont les données sont recueillies.

---

anonymiser ou effacer, conformément aux dispositions nationales de transposition de cette directive. Ces informations sont adressées spontanément à la HADOPI, et non recueillies auprès des opérateurs. Les moyens sont donc inopérants dans cette mesure.

[10] CE, Ass., 21 avril 2021, *French Data Network*, n° 393099-394922-397844-397851-424717, au Rec.

[11] L'Assemblée a pris sur elle de rattacher à cette catégorie l'ensemble des données relatives au compte et aux paiements effectués par un abonné internet, qui ne se rapportent pas aux communications effectuées ou à la localisation du téléphone portable.

Vous pourriez y lire une critique de l'article 7 du décret en tant qu'il écarte l'application du **droit d'opposition**. Précisons à titre liminaire que le traitement litigieux nous paraît relever non pas du RGPD invoqué mais de la directive dite « police-justice », qui s'applique aux traitements des autorités compétentes à des fins de prévention des infractions pénales. C'est donc l'article 110 de la loi du 6 janvier 1978 qui s'applique. Il permet d'écarter le droit d'opposition par une disposition expresse de l'acte de création du traitement. Et cette mise à l'écart est tout à fait justifiée par les besoins des procédures diligentées par la HADOPI.

Pour le surplus, il est loisible à toute personne de demander l'effacement des données qu'elle estime indûment collectées et conservées, en application du 3° de l'article 106 de la même loi, et de contester le refus qui lui serait opposé, soit par une plainte auprès de la CNIL, soit par un recours direct devant le juge administratif. Il n'existe donc aucune immunité contentieuse[12].

3.3. Le dernier grief est, de loin, le plus redoutable. Les requérantes soutiennent que **l'accès aux données de connexion est illégal dès l'instant qu'il n'est pas préalablement autorisé par un juge ou une autorité indépendante** présentant des garanties d'impartialité.

Tel qu'il était initialement formulé, le moyen semblait cibler l'accès des agents de la HADOPI aux données conservées dans leur propre traitement, c'est-à-dire la phase d'utilisation interne du fichier. Or à l'évidence, un tel accès n'a pas à faire l'objet d'un contrôle préalable.

Le dernier mémoire produit par les associations requérantes resitue le débat sur le bon terrain, en amont : celui de la phase de collecte des données par la HADOPI auprès des opérateurs. Il y a, cette fois, une vraie difficulté au regard de la jurisprudence de la Cour de justice qui exige que le recueil des données relatives au trafic et à la localisation auprès des opérateurs soit précédé d'un contrôle indépendant et impartial par une autorité administrative indépendante ou une autorité juridictionnelle[13].

Il vous faut vous interroger sur le point sur le point de savoir **si cette exigence vaut aussi pour le recueil des données d'identité civile et des coordonnées de l'utilisateur**, ou s'il est circonscrit aux données relatives aux communications et aux données de localisation du téléphone portable, qui sont, évidemment, les données les plus sensibles.

A la lettre, la décision d'Assemblée d'avril dernier opte pour l'acception large, puisqu'elle annule certains décrets d'application de la loi « renseignement » de 2015 en tant qu'ils

[12] Rappelons qu'en revanche, les recommandations adressées par la HADOPI en amont d'une procédure judiciaire sont insusceptibles de recours (CE, 19 octobre 2011, *French Data Network*, n° 342405, au Rec.), de sorte que l'éventuelle irrégularité du recueil des données auprès des opérateurs en amont de leur émission ne peut trouver de débouché contentieux à travers leur contestation. Et nous doutons fort que cette irrégularité puisse entraîner celle de la procédure pénale subséquente, qu'il s'agisse de la contravention de 5ème classe spécifique ou du délit de contrefaçon. Mais tout ceci ne résulte absolument pas du décret attaqué, qui n'avait pas à organiser une quelconque voie de recours ni à exclure par principe la conservation des données en raison du régime contentieux de leur recueil.

[13] Sauf urgence dûment justifiée, qui permet un contrôle *ex post* à bref délai.

permettent le recueil des données de connexion sans contrôle préalable conforme aux exigences européennes, sans distinguer entre les différentes catégories de données, ce qu'elle fait par ailleurs, en amont, quand elle examine la question du régime applicable à la conservation des données. Mais aussi vrai que les conclusions du rapporteur public étaient discrètes sur ce point, on ne peut pas considérer la question comme véritablement tranchée par cette décision, qui avait, comme vous le savez, quelques autres détails à régler…

Il ne fait aucun doute, d'abord, que ces données d'identité civile sont au nombre des **données relatives au trafic et des données de localisation**, relevant du champ d'application de la directive *e-privacy*[14]. D'une part, l'adresse de l'installation téléphonique peut être regardée comme une donnée de localisation de l'équipement terminal, même si, à l'évidence, elle est beaucoup moins intrusive que le bornage du téléphone mobile[15]. D'autre part, les données relatives au trafic visées par la directive *e-privacy*, dont la définition est reprise au 18° de l'article L. 32 du code des postes et des communications électroniques, incluent les données traitées en vue de la facturation des prestations. Or les données d'identité et au moins certaines coordonnées sont utilisées à cette fin. Enfin, et surtout, il n'est pas demandé aux opérateurs de transmettre leur fichier clients, ou même d'obtenir confirmation auprès d'eux qu'une personne nommément désignée est abonnée chez eux, mais de mettre en relation une adresse IP donnée[16], donc une communication ou un ensemble de communications, avec un utilisateur. Bref, il s'agit d'identifier la personne qui a consulté un site internet voire un contenu donné. Cette information doit être regardée comme une donnée relative au trafic. On comprend donc que la Cour de justice ait appliqué la directive *e-privacy* à la conservation et à l'accès aux données d'identité civile de l'abonné détenus par les fournisseurs d'accès à internet et les opérateurs télécom[17]. Quant aux hébergeurs, c'est le RGPD qui leur est applicable, et son champ d'application inclut toutes les données à caractère personnel, ce que sont évidemment l'ensemble des informations en cause.

Si ces données d'identité civile relèvent donc bien du champ de la directive *e-privacy* et du RGPD, leur conservation et leur accès obéissent toutefois à un régime plus libéral que les autres données de connexion, comme nous l'avons vu pour ce qui concerne les motifs d'accès. Or on peut se demander si ce libéralisme ne doit pas s'étendre à la question du contrôle de l'accès. En effet, ce garde-fou posé par la Cour de justice, allant d'ailleurs au-delà de ce qu'exige la Cour européenne des droits de l'homme, s'explique avant tout par la sensibilité des données et les conclusions très précises qu'elles permettent de tirer sur la vie privée.

---

[14] V. les pts. 51 et suivants dans lequel elle indique que « *l'accès des autorités nationales compétentes aux données conservées* » doit être subordonné à un contrôle préalable, lequel doit assurer un juste équilibre entre les intérêts liés aux besoins de l'enquête dans le cadre de la « lutte contre la criminalité » (sans distinction formelle entre grave et non grave) et les droits fondamentaux.

[15] Au point 157 de l'arrêt *LQDN et autres* du 6 octobre 2020, la Cour indique en creux que les coordonnées des utilisateurs, notamment les adresses, fournissent des informations sur les communications données.

[16] Sauf utilisation d'une adresse IP fixe, qui est plutôt l'exception, l'adresse IP est dynamique et change occasionnellement, en particulier au redémarrage de la box.

[17] Cf. en particulier les points 158 et 159 de l'arrêt *LQDN et autres*.

Cela étant, il faut bien admettre que la lettre des arrêts de la Cour ne distingue pas. Ni l'arrêt *Digital Rights Ireland* de 2014, ni l'arrêt *Télé2 Sverige*, ni, plus récemment, l'arrêt *H.K. c/ Prokuratuur* ne comporte d'exclusion formelle des données d'identité civile du champ du contrôle préalable. La Cour exige d'ailleurs que ce contrôle ménage un juste équilibre entre les droits fondamentaux et la « *lutte contre la criminalité* »[18], sans se limiter à la criminalité grave. Or on l'a dit, seules les données d'identité civile peuvent être recueillies pour la criminalité « ordinaire », ce qui pourrait laisser entendre qu'elles sont elles-mêmes bien soumises à ce régime.

Cette exigence n'aurait rien d'incongru dans son principe. D'une part, il n'est pas complètement anodin de connaître le nom de l'abonné qui se cache derrière une adresse IP relevée sur un site internet ou correspondant au téléchargement d'une œuvre donnée – disons, par exemple, un film pornographique. D'autre part, dans la plupart des régimes de recueil administratif des données de connexion, l'accès aux données d'identité civile donne lieu à un contrôle préalable. C'est le cas de l'administration fiscale[19], de l'Autorité des marchés financiers[20] ou encore de l'Autorité de la concurrence[21], avec la saisine préalable d'un contrôleur des demandes de données de connexion[22]. Pour les douanes, ce contrôle est confié au procureur de la République (art. 65 *quinquies*). Aucun des textes applicables à ces autorités ne distingue entre les données d'identité civile et les autres données. Enfin, pour les services de renseignement, l'accès aux données d'identité civile suppose de saisir la Commission nationale de contrôle des techniques de renseignement (CNCTR). Le deuxième alinéa de l'article L. 851-1 du code de la sécurité intérieure prévoit simplement que cette saisine peut émaner directement des services, sans validation par le ministre, pour recueillir les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, en raison de leur plus faible sensibilité. Mais il y a bien un contrôle préalable, même s'il ne respecte les standards européens que sous les réserves posées par l'Assemblée du contentieux. Il en va de même pour l'autorité judiciaire.

D'une certaine manière, c'est plutôt le régime de la HADOPI qui semble constituer une anomalie dans ce paysage[23]. Mais elle s'explique assez bien :

- d'une part, elle ne porte que sur ces données, et uniquement aux fins de prévenir le défaut de sécurisation du poste informatique. Il y a là une différence fondamentale avec les autorités que nous avons mentionnées, qui sont susceptibles d'accéder à bien d'autres catégories de données et de procéder ainsi à des recoupements donnant une image précise de la vie privée des utilisateurs, et pour des finalités très variées, notamment pour la prévention et la poursuite d'infractions pénales extraordinairement

[18] V. par exemple l'arrêt *H.K* du 2 mars 2021, pt. 52.
[19] Article L. 96 G du livre des procédures fiscales.
[20] Article L. 621-10-2 du code monétaire et financier.
[21] Article L. 450-3-3 du code de commerce.
[22] C'est aussi le cas des services de renseignement avec l'avis de la CNCTR (même si l'Assemblée du contentieux a jugé que cette procédure ne respectait pas les standards européens).
[23] On notera toutefois que le droit de communication des données d'identification des personnes ouvert à l'inspection du travail par l'article L. 8113-5-2 du code du travail ne fait pas intervenir le contrôle d'un tiers.

diverses. En l'espèce, ce ne sont donc pas seulement les données elles-mêmes, mais l'ensemble du traitement de recueil qui présente une faible sensibilité en termes d'ingérence dans la vie privée. On peut comprendre que le législateur n'ait pas estimé devoir subordonner un tel accès à un contrôle externe ;

- d'autre part, un contrôle systématique et humain préalablement à chaque réquisition de donnée serait évidemment incompatible avec le caractère industriel du recours à cette technique. Le ministre vous rappelle que la HADOPI peut traiter jusqu'à 70 000 saisines des ayants droit chaque jour. Celle-ci émet par ailleurs 1 à 2 millions de recommandations chaque année. On voit mal comment organiser un examen juridictionnel ou administratif préalablement à tout accès, sauf, bien sûr, à plomber encore un peu plus les finances publiques en recrutant massivement des contrôleurs et en acceptant de les exposer à d'importants risques psycho-sociaux. Or nous l'avons dit en introduisant notre propos, l'accès massif à ces données constitue l'un des principaux outils de travail de la HADOPI, sans lequel son existence même serait remise en cause. A nos yeux, un contrôle préalable ne pourrait qu'être automatisé, c'est-à-dire fondé sur un algorithme de contrôle permettant de s'assurer, d'une part, que les adresses IP sur lesquelles portent les réquisitions sont uniquement celles qui ont été portées à la connaissance de la HADOPI par les prestataires privés en charge de la surveillance et, d'autre part, que les données recueillies correspondent uniquement à celles que la HADOPI est autorisée à recueillir. Il n'est pas nécessaire, et même très inopportun, de consacrer des moyens humains à de telles vérifications. Pour le surplus, un contrôle *a posteriori*, par échantillonnage, permet de s'assurer de l'absence d'abus ou d'accès illicite, pratique qui expose son auteur à de lourdes sanctions pénales.

Précisons en revanche que le fait que la HADOPI soit elle-même une autorité publique indépendante ne nous paraît pas déterminant : cette indépendance ne permet pas à ses agents de s'auto-contrôler. La jurisprudence de la Cour exige un contrôle tiers, l'indépendance devant se manifester à l'égard des personnes chargées du recueil des données. C'est la raison pour laquelle elle a estimé que le procureur de la République estonien, qui bénéficie en substance de la même indépendance que son homologue français, ne pouvait de lui-même autoriser les officiers de police judiciaire, qui mènent les investigations sous son autorité, à accéder aux données de connexion.

Cela étant, on peut tout à fait imaginer que ce contrôle soit organisé au sein de la Haute autorité, dès l'instant qu'est garantie une séparation fonctionnelle entre les services opérationnels et l'organe interne de contrôle, de la même façon que l'organe chargé de prononcer les sanctions peut être regardé comme indépendant de celui qui diligente les poursuites.

Ces considérations, qui ont trait aux modalités pratiques du contrôle, pourraient ne pas être dépourvues d'incidence sur le sort du litige. En effet, l'intervention préalable d'une juridiction ou d'une autorité administrative tierce requerrait *a minima* un décret, voire une loi au titre des garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques. A

l'inverse, on pourrait admettre qu'un contrôle allégé, mis en place au sein de la Haute autorité, le cas échéant de façon automatisée, relève du pouvoir d'organisation interne de son président, de sorte que la légalité du décret ne serait pas en cause. Seule sa mise en œuvre concrète serait illégale aussi longtemps que les données sont collectées sans ce contrôle.

Eu égard la difficulté de la question et à l'enjeu, qui dépasse même le seul cas de la HADOPI, nous pensons qu'il y a matière à un renvoi préjudiciel à la Cour de justice, qui porterait en substance sur les deux questions suivantes :

- eu égard, d'une part, à la faible sensibilité des données relatives à l'identité civile des utilisateurs, incluant leurs coordonnées, qui ne permettent pas de tirer des conclusions précises sur la vie privée d'une personne, d'autre part, à la possibilité pour toute personne d'avoir accès aux données à caractère personnel la concernant traitées par une autorité et d'en obtenir l'effacement s'il y a lieu et, enfin, des sanctions pénales applicables en cas d'accès abusif ou non autorisé à ces données, la directive *e-privacy* et le RGPD s'opposent-ils à une réglementation nationale prévoyant le recueil de ces données à partir de l'adresse IP des utilisateurs sans contrôle préalable par une juridiction ou une entité administrative indépendante dotée d'un pouvoir contraignant ?

- en cas de réponse affirmative à la première question, eu égard à la circonstance que seules ces données de faible sensibilité peuvent être recueillies par la HADOPI, autorité publique indépendante, que ce recueil a pour seule finalité la prévention d'agissements définis de façon précise, limitative et restrictive par la loi et 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 compromettrait l'accomplissement de la mission de service public qui lui est confiée en vue de protéger la propriété intellectuelle conformément au paragraphe 2 de l'article 17 de la Charte des droits fondamentaux de l'Union européenne, la législation européenne fait-elle obstacle à ce que ce contrôle soit effectué selon des modalités adaptées, tel qu'un contrôle automatisé, le cas échéant sous supervision humaine confiée à un service interne à cette autorité présentant des garanties d'indépendance et d'impartialité à l'égard des agents chargés de procéder à ce recueil ?

PCMNC au sursis à statuer jusqu'à ce que la Cour de justice réponde à ces questions.