PRISE de POSITION pour l'audience

du Contrôleur Européen de la Protection des données sur les réponses écrites des parties visées à l'article 23 du Statut

dans l'affaire C-470/21 La Quadrature du Net e.a. ('LQDN II')

Monsieur le Président, Mesdames et Messieurs les Juges, Monsieur l'Avocat Général,

Le contrôleur européen de la protection des données exprime sa gratitude pour l'invitation à cette importante audience devant le *plenum* de la Cour.

La première question pour réponse écrite vise à explorer quelles conditions matérielles et procédurales peuvent être envisagées, autres qu'un contrôle préalable par une juridiction ou une autorité administrative indépendante ayant la qualité de tiers.

Commençons par des considérations sur le niveau d'ingérence avec les droits fondamentaux pertinents.

Ce niveau d'ingérence découle de plusieurs éléments et cette affaire démontre qu'il est difficile de le réduire à la dichotomie ingérence 'grave' versus ingérence non grave.

Tout d'abord, comme souligné par l'Avocat Général (point 102) s'agissant des personnes concernées, les données traitées par la HADOPI ne concernent pas l'ensemble des personnes ayant un accès à internet.

Le Contrôleur convient qu'il s'agit d'un nombre encore potentiellement élevé de personnes puisque dans beaucoup de réseaux pair à pair, les téléchargeurs (downloaders) sont aussi téléverseurs (uploaders, ou plutôt, seeders) comme d'ailleurs discuté dans l'arrêt MICM. Il faut toutefois tenir compte du fait que les réseaux pair à pair peuvent être utilisés pour bien d'autres activités que le partage d'œuvres et qu'il s'agit uniquement d'identifier des personnes suspectées de mettre à disposition des oeuvres sans autorisation.

Venant maintenant aux données personnelles dont l'accès est sollicité, elles sont exhaustivement listées par la loi française.

Même s'il ne peut être exclu que dans le cas particulier d'un abonné qui mettrait à disposition de manière répétée un type d'œuvres particulier, certaines

1

conclusions sur sa vie privée puissent être tirées, de telles conclusions n'iraient pas aussi loin que celles que l'on peut tirer de la connaissance de données de trafic et localisation dont il était question dans d'autres affaires. Là aussi, nous sommes d'accord avec le point 101 des Conclusions de M. l'Avocat général. Dans cette affaire, il n'est pas question de données qui pourraient permettre de reconstruire l'ensemble des activités en ligne de l'utilisateur et engendrer un sentiment de surveillance généralisée.

Passons maintenant aux risques. Le nombre et la nature des garanties requises dépendent des risques, pour la vie privée et la protection des données, découlant de la conservation et de l'accès aux données.

S'agissant des risques engendrés par le traitement en cause, je me pencherai par conséquent sur les risques que la Cour évoque dans sa première question pour réponse écrite.

- les faux positifs et

- les abus,

notamment dans le cadre des traitements automatisées tant par les organisations professionnelles, dans le premier type de traitement en amont, que par la HADOPI, dans le traitement en aval.

S'agissant du traitement automatisé par les organisations de défense des droit d'auteur, d'abord.

Le Contrôleur sait d'expérience qu'il n'est pas toujours facile de disposer des détails techniques concernant les faux positifs par les sociétés qui développent des technologies de détection. Ce cas ne fait pas exception.
De plus, de manière générale, tout traitement automatisé n'est pas exempt d'erreurs.

Cela dit, le Contrôleur a analysé le système tel que mentionné dans le rapport visé par le gouvernement français dans ses réponses écrites, le « rapport Znaty » commissionné par la HADOPI. Ce rapport est daté de 2012 et concerne le recours par les organisations d'ayant-droits à un prestataire de services spécifique, la société TMG.

Or, la révision manuelle des fichiers repérés en ligne grâce à l'empreinte numérique réduit considérablement le risque de faux positifs. La base de données des fichiers avec les œuvres de référence est de notre avis suffisamment à l'abri des faux positifs à ce stade.

La vérification automatisée qui suit, et qui consiste à associer une certaine adresse IP utilisée pour mettre à disposition des œuvres protégées, en s'appuyant sur des techniques de hachage numérique, ne peut jamais être considérée exempte d'erreurs mais paraît fiable à l'étude de ce rapport dont malheureusement nous n'avons pas pu voir les annexes.

Passons maintenant au traitement par la HADOPI.

A la lumière des explications fournies, le Contrôleur estime que le risque d'occurrence de faux positifs à ce stade est réduit même si d'importants points d'interrogations restent, liés aux sources disponibles pour apprécier ce risque. Dans une optique globale toutefois ce risque ne semble pas apte à affecter de manière décisive la proportionnalité des mesures en question dans l'affaire au principal[1]. Nous restons à disposition pour fournir toute information complémentaire.

S'agissant de la conséquence la plus grave pour les personnes concernées, c'est à dire les conséquences qui découlent de la saisine du Procureur de la République, il faut remarquer que cette saisine fait l'objet d'un contrôle préalable humain et individualisé et non d'un traitement automatisé.

S'agissant des risques de détournement par des tiers d'un nombre potentiellement élevé des données personnelles traitées par l'HADOPI, de l'avis du Contrôleur ces risques sont intrinsèques à potentiellement tout traitement des données qui ne serait pas suffisamment sécurisé au regard des principes d'intégrité et de confidentialité établis par le droit à la protection des données de l'Union.

Les risques d'abus existent toujours. De l'avis du Contrôleur la jurisprudence de la Cour tient compte pour évaluer ces risques du volume de données traitées et de la quantité des personnes concernées et de la possibilité de constituer une forme de profilage.

C'est la raison pour laquelle, le Contrôleur attache de l'importance aux mesures techniques et organisationnelles prévues en l'espèce et décrites par le gouvernement français dans ses écritures aux fins de limiter le risque d'abus par des tiers[2].

---

[1] Les réponses reçues des opérateurs sont vérifiées par échantillon (point 17 des réponses FR du 16 juin 2022) ou dans le cadre d'une demande complémentaire qui s'opère en cas de demande d'accès ou rectification par les abonnés concernés (point 22 FR 16 Juin 2022).

[2] En particulier, le décret 2010-236 prévoit à son article 3 les délais de conservation par l'autorité publique HADOPI des données reçues et listées exhaustivement à l'annexe du

Dans le cas d'espèce, les risques liés au traitement de données par l'HADOPI semblent suffisamment limités et encadrés.

Passons donc aux questions plus techniques. Le Contrôleur va encore une fois traiter d'abord les questions qui tiennent aux risques (c) et (d) pour ensuite aborder les questions concernant davantage les conditions matérielles et procédurales adaptées aux risques.

II. 2) c) La conservation des adresses IP par les fournisseurs de services de communication électroniques.

Compte tenu de ce que, comme l'a souligné l'Avocat Général au point 88 de ses conclusions, « *la conservation des données et l'accès à ces données ne sauraient se concevoir isolément* », nous rejoignons sa lecture quant au caractère proportionné des ingérences en cause dans la présente affaire, notamment dans la mesure où, et pour autant que, ces données aient été conservées en conformité avec la directive vie privée.

Nous comprenons l'exigence de ne pas mettre à mal l'efficacité de la lutte contre les infractions pénales, en particulier lorsqu'elles sont commises en ligne et que l'adresse IP de la source de connexion constitue le seul moyen d'investigation pour identifier la personne à laquelle cette adresse était attribuée au moment de la commission de l'infraction.

Comme mentionné par certains Etats membres, tel que l'Estonie, les adresses IP des abonnés sont retenues par les fournisseurs de services de communication électroniques plutôt pour des raisons techniques, qui tiennent essentiellement à la gestion du réseau[3].

---

même décret, qui incluent l'adresse IP, les données d'identité et les « informations relatives aux œuvres ou objets protégés concernés par les faits ».

Le contrôleur souligne aussi parmi les mesures de sauvegarde mentionnées par le gouvernement français la nature d'autorité indépendante de l'HADOPI, l'obligation d'obtenir un avis de l'autorité de protection des données émis sur les traitements en question ainsi que la circonstance que le système de traitement des données de la HADOPI est déconnecté de l'internet (point 20 FR 16 juin 2022).

[3] Point 8 des réponses écrites de l'Estonie même s'il semble y avoir un problème dans la version FR qui se réfère au 'port block' comme à un dispositif de blocage et pas comme à la partie relative au port qui peut compléter un code IP.

Les raisons techniques sont les suivantes :

Quant au journal des sites web consultés, plusieurs gouvernements indiquent qu'un tel journal n'est pas tenu par les opérateurs de services de communication électroniques. La conservation d'un dit journal ne semble pas nécessaire ni pour des raisons techniques, ni de facturation.

De l'avis du Contrôleur, il ressort que pour les besoins techniques ou de facturation, les adresses IP ainsi que les données telles que l'horodatage ne devraient être conservées que pour une période relativement courte, ce qui explique peut-être la recherche de célérité dans la procédure mise en place en l'espèce. Nous sommes cependant dans l'impossibilité de déterminer davantage in abstracto la durée de conservation nécessaire car elle dépend en pratique d'une multitude de facteurs.

II. 2 d) Possibilité technique d'accéder, à partir des adresses IP, à des données de trafic et localisation et possibilités de traçage des activités en ligne.

Il est important à cet égard de distinguer les adresses IP de la source et de destination, comme cela résulte déjà de la jurisprudence, et les entités qui ont accès à ces adresses.

Les fournisseurs de services de communication en ligne pour effectuer ladite connexion, i.e. pour acheminer la communication, disposent des adresses IP de la source et de la destination de la communication.

Les fournisseurs de services de communication, partant, disposent de la capacité technique de déterminer :

- Une localisation approximative (au niveau d'une ville ou au niveau régional) tant de l'abonné que de la destination contactée ;

- Les destinations (sites web) visitées ;

- Le type de connexion (résidentielle, professionnelle ou mobile).

- allocation des adresses IP pour acheminer les communications, i.e. le routage [Réponses écrites de LQDN], para. 23, vérifier des problèmes sur les réseau (troubleshooting);
- prévention des abus (e.g., envoi en masse de messages non sollicités par une même adresse IP) [Réponses écrites de LQDN, para 23.] et des cyber-attaques, tel que les attaques de déni de service distribué (Denial of Service) ;
- Service de support à la clientèle pour les problèmes de connexion.

Une autorité telle que la HADOPI, ne disposant que des adresses IP de la source de la connexion, peut déterminer la localisation, au niveau régional, de l'abonné ayant mis à disposition[4] les œuvres protégées sur un réseau de pair à pair, pour autant que ce dernier n'utilise pas un mécanisme pour masquer l'adresse IP. Nous soulignons par ailleurs qu'une adresse IP peut être attribuée à une personne morale, sans qu'il soit possible de l'attribuer à la personne physique ayant accédé à l'internet à travers de ce même adresse IP 'externe'.

En considérant l'adresse IP de la source en possession de la HADOPI, le Contrôleur conclut en outre qu'il n'est pas possible pour cette dernière d'en tirer des données de trafic autres que les données qui lui ont été transmises[5].

II. 2) a) - 'Étanchéité'

Tout d'abord, le Contrôleur comprend que la législation française en cause n'impose pas d'obligation spécifique aux opérateurs de service de communication électroniques de conserver les adresses IP aux fins de lutte contre la violation des droits de propriété intellectuelle.

Il est vrai que les fournisseurs peuvent être tenus de conserver les adresses IP pour des finalités distinctes de celle de la facturation ou des raisons techniques, comme par exemple la conservation aux fins de la lutte contre la criminalité grave. Il est essentiel cependant que la jurisprudence de la Cour (Cfr. *Garda Siochana*, C-140/20, paras 98 à 100), clarifiant la hiérarchie des objectifs qui peuvent justifier des ingérences d'ampleurs différentes avec les droits fondamentaux, soit respectée[6].

Nous partageons l'analyse des États membres ayant répondu selon laquelle il existe des mesures garantissant l'étanchéité entre deux bases de données, ou assurant différents types de limitation à l'accès à une même base de données selon les finalités poursuivies par cet accès.

Il est cependant vrai qu'aucun système n'est à l'abri d'erreur ou de piratage. Comme relevé par certaines parties, la multiplication des bases des données avec des données semblables signifie aussi une multiplication des risques liés aux traitements.

---

[4] Dans certains réseaux en pratique tous les utilisateurs, ou au moins la grande majorité d'entre eux, deviennent des « seeders » et peuvent être considérés comme ayant mis à disposition des oeuvres protégés.

[5] Arrêt C-207/16 Ministerio Fiscal paras 40 - 42 : les données d'identité civile correspondant à une SIM card sont des données de trafic aux termes de la directive 2002/58.

[6] Ainsi, l'on ne peut pas utiliser des données conservées pour des finalités de lutte contre la criminalité grave pour des finalités de lutte contre une forme de criminalité qui n'est évidemment pas grave, telles que les violations de la propriété intellectuelle.

II. 2) b) Hypothèse d'une autre autorité administrative indépendante en charge d'une liste prédéterminée d'œuvres protégées

La Cour s'interroge enfin sur la possibilité de confier la mise à jour ou le contrôle de la liste des œuvres prédéterminées à une autorité autre que celle en charge de communiquer les recommandations.

L'avantage d'un tel système résiderait dans la séparation des informations : la Cour imagine peut-être que d'un côté, l'autorité qui communique la recommandation ne serait pas en mesure de connaître le contenu des œuvres illicitement partagées ; ce contenu serait connu seulement par l'autre autorité qui aurait le rôle de certifier, au moyen de techniques de hachage, qu'une certaine œuvre est protégée. D'un autre côté, cette « autre » autorité tierce n'aurait pas connaissance de l'identité civile correspondant à l'adresse IP.

Les autres parties ont souligné encore aujourd'hui la complexité d'une telle architecture.

Le Contrôleur estime utile de résumer de son point de vue les avantages et les inconvénients d'une telle solution :

- L'avantage de la séparation des informations disponibles est bien évidemment que la gravité de l'ingérence avec les droits fondamentaux diminue, car chaque acteur dispose de manière cloisonnée d'informations qui isolément ne permettent pas de tirer des conclusions précises sur la vie privée.

- Les inconvénients sont en effet multiples et même les parties requérantes au principal les ont soulignés dans leurs réponses écrites. De l'avis du Contrôleur, il faut souligner notamment trois aspects :

(i) le caractère limitatif et, vraisemblablement, les difficultés liées à la gestion d'une liste d'œuvres protégées systématiquement dépassée ou ne correspondant pas aux priorités des ayants droit ;

(ii) les coûts accrus pour l'État, qui est une circonstance à prendre en compte selon le droit à la protection des données personnelles de l'Union lors du choix des mesures les plus appropriées pour assurer la sécurité du traitement ;

(iii) l'impact qu'un telle mesure aurait quant au choix éminemment politique concernant les entités plus adaptées à déclencher la défense des droits de propriété intellectuelle. Des réponses écrites du gouvernement français[7], il

[7] Voir notamment para. 53

s’avère que la politique française de répression de ces infractions a fait le choix, pour ainsi dire, de « partir de l’initiative privée ».

****

Conclusions

Monsieur le Président, Mesdames et Messieurs les Juges, Monsieur l’Avocat Général,

nous apprécions l’opportunité donnée au Contrôleur d’apporter son éclairage sur les questions posées par la Cour dans cette affaire ainsi que l’attention que la Cour porte à travers sa jurisprudence à la protection de la vie privée, des données personnelles et aux autres droits fondamentaux.

L’absence d’autres moyens que les adresses IP de la source d’une connexion pour poursuivre des infractions pénales mêmes non graves commises exclusivement en ligne, en présence d’un niveau d’ingérence qui n’est pas aussi grave que celui relatif à la conservation généralisée et indifférenciée des données de trafic et localisation devrait être reconnue par la Cour. Nous rejoignons donc les conclusions de l’Avocat Général à cet égard.

Merci pour votre attention. Le Contrôleur reste à votre disposition pour répondre à toute autre question de la Cour.