CJUE et directive sur le commerce électronique – Partie 2 : Interdire la rediffusion de messages par un service de géolocalisation

Pauline Meyer, le 6 juillet 2026

Un État membre de l'UE peut interdire à des prestataires de services d'aide à la conduite par géolocalisation de rediffuser des messages d'utilisateurices susceptibles de révéler la localisation de certains contrôles.

Arrêt de la Cour de justice de l'Union européenne du 16 juin 2026, Affaires jointes C-188/24 et C-190/24

Affaire C-190/24

Coyote System est une entreprise française fournissant un service répondant à la qualification de « service électronique d'aide à la conduite ou à la navigation par géolocalisation ». L'art. L.130–11 du Code de la route prévoit, à des fins d'ordre, de sécurité et de sûreté publics, la mise en place d'un mécanisme permettant à l'autorité administrative compétente d'interdire aux exploitants de ce type de service de rediffuser, pendant une période et dans un périmètre géographique limités, les messages de leurs utilisateurs et utilisatrices susceptibles de révéler la localisation des contrôles d'alcoolémie et d'usage de stupéfiants ainsi que certaines opérations de police judiciaire. Ce mécanisme a été institué par le décret n° 2021–468 portant application de l'art. L. 130–11 du Code de la route. L'entreprise conteste l'interdiction de signaler ce type de contrôles routiers, rendue possible par ce décret, prononcée par l'Autorité de régulation de la communication audiovisuelle (Arcom) française.

Par trois questions préjudicielles, le Conseil d'État demande à la CJUE si le « domaine coordonné » de la directive sur le commerce électronique (art. 2 let. h et i de la directive) comprend l'interdiction pour les exploitants de service électronique d'aide à la conduite ou à la navigation par géolocalisation de rediffuser par leur service des messages et autres indications par des usagères et usagers lorsqu'ils sont susceptibles de permettre aux autres utilisateurs et utilisatrices de se soustraire à certains contrôles routiers. En outre, le Conseil d'État souhaite savoir si cette interdiction pourrait être imposée à des prestataires établis dans un autre État membre.

Finalement, il s'agit pour la CJUE d'examiner si l'interdiction d'imposer une obligation générale de surveillance (découlant de l'art. 15 de la directive) pourrait s'opposer à une telle interdiction. En effet, l'interdiction de rediffusion de messages prononcée par l'Arcom à Coyote System impliquerait un suivi et enregistrement généralisé des contenus partagés par ces utilisateurs et utilisatrices. Cette surveillance serait interdite par l'art. 15 de la directive si Coyote System est considéré comme un fournisseur d'hébergement au sens de l'art. 14 de la directive.

Principe du « pays d'origine » pour le « domaine coordonné »

La CJUE affirme que la mesure litigieuse fait partie du « domaine coordonné » consacré à l'art. 2 let. h de la directive. Celui-ci ne se limite pas aux exigences régies par les dispositions d'harmonisation de la directive, mais comprend en principe toutes les exigences à l'égard de l'accès ou à l'exercice d'un service de la société de l'information. Qui plus est, le domaine concerné par le décret ne tombe pas dans les domaines exclus par la directive. En effet, l'interdiction contestée implique une limitation des fonctionnalités courantes d'un tel service et fait partie du domaine coordonné en vertu de l'art. 2 let. h et i de la directive.

Selon le principe du « pays d'origine », consacré dans la directive sur le commerce électronique (consid. 22 de la directive), les services relevant du « domaine coordonné » sont soumis au seul droit de l'État membre d'établissement d'un prestataire de service de société de l'information.

Dérogations au principe du « pays d'origine »

L'application par la France de mesures à des prestataires établis dans d'autres États membres constitue une restriction à la libre circulation des services concernés, qui peut être permise moyennant que les mesures poursuivent des objectifs reconnus par la directive, qu'elles sont proportionnées, et que l'État membre prenant les mesures a, d'une part, demandé à l'État membre d'établissement de prendre lui-même les mesures appropriées, et, d'autre part, notifié cet État membre et la Commission européenne de son intention d'adopter de telles mesures (art. 3 par. 4 de la directive).

Dans l'affaire C-190/24, la mesure vise l'interdiction de rediffuser des informations relatives à certains contrôles routiers, et peut être justifiée par des raisons d'ordre, de sécurité et de sûreté publics. Concernant l'exigence de proportionnalité, la mesure française se concrétise par des décisions individuelles d'interdiction adoptées sur la base du droit national et semble pouvoir être proportionnée au vu des informations à disposition de la Cour.

Interdiction de l'obligation générale de surveillance et fournisseur d'hébergement

La CJUE doit répondre à la question de savoir si l'interdiction de l'obligation générale de surveillance de l'art. 15 de la directive empêche une réglementation nationale permettant d'interdire à cet exploitant la rediffusion d'informations relatives à certains contrôles routiers.

Cette question est conditionnée à celle de savoir si le prestataire est considéré comme un fournisseur d'hébergement au sens de l'art. 14 de la directive, ceux-ci faisant partie des prestataires auxquels un État membre ne peut pas imposer une obligation générale de surveillance. La Cour renvoie l'affaire au Conseil d'État avec la tâche de décider si l'entreprise est un fournisseur d'hébergement purement neutre (ayant un comportement purement technique, automatique et passif impliquant l'absence de connaissance ou de contrôle des contenus qu'il stocke) pouvant bénéficier d'exemptions de responsabilité pour les contenus stockés, ou s'il s'agit au contraire d'un fournisseur plus « actif », qui exerce un contrôle par la prédétermination, au moyen d'un algorithme et dans son intérêt, des conditions de la diffusion ou non et de l'ordre de priorité des informations sur son site Internet.

Si l'autorité française estime qu'il s'agit en effet d'un fournisseur d'hébergement, elle devra d'une part examiner si la mesure d'interdiction de rediffusion consiste en une mesure visant à bloquer l'accès à des informations illicites stockées sur la plateforme de Coyote System, à mettre fin à une activité illicite ou à une violation de ses services par les utilisateurs ou utilisatrices, ou à prévenir une telle activité une violation, permise par l'art. 14 par. 3 de la directive. D'autre part, elle devra examiner si cette mesure n'est pas admissible car elle implique une obligation générale de surveillance en vertu de l'art. 15 de la directive.

Selon la CJUE, cette interdiction de rediffuser des informations relatives à certains contrôles routiers prévue par la réglementation en cause n'oblige pas l'hébergeur à procéder à une appréciation autonome du contenu stocké, dès lors que la juridiction de renvoi française souligne expressément que l'exploitant d'un service électronique d'aide à la conduite ou à la navigation par géolocalisation peut se limiter à identifier les contenus visés de manière automatisée et sans devoir prendre connaissance du contenu des messages transmis par ses utilisateurs signalant de tels contrôles routiers.

La Cour a par ailleurs déjà admis par le passé qu'une injonction adressée à un hébergeur de supprimer des éléments illicites précis du contenu stocké, estimant qu'il ne s'agit pas d'une obligation de surveillance généralisée (art. 15 de la directive), en particulier lorsque, comme dans le cas présent, il est possible d'identifier les contenus au moyen de recherches automatisées (CJUE, Affaire Glawischnig-Piesczek, C-18/18). Par ailleurs, la Cour rappelle que la théo-

rie prévoit que l'interdiction de l'obligation de surveillance générale ne s'applique pas à un « cas spécifique ». Par conséquent, en l'occurrence, une injonction adressée à un hébergeur de supprimer des éléments illicites précis du contenu stocké n'est pas de nature à imposer à l'hébergeur une obligation de surveiller de manière générale les informations qu'il stocke.

Conclusion

En résumé, la CJUE conclut donc que, pour que l'interdiction d'imposer une obligation générale de surveillance de la directive sur le commerce électronique s'applique, il faut que le type de prestataire visé soit un fournisseur d'hébergement. Le prestataire qui prédétermine les conditions de diffusion d'informations au moyen d'un algorithme dans son intérêt ou celui de son service n'est pas couvert par la notion de fournisseur d'hébergement, ce qui implique que celui-ci ne peut pas se prévaloir de l'interdiction de l'imposition d'une obligation de surveillance générale.

Cependant, cette interdiction ne s'oppose pas non plus à ce qu'un État membre interdise à des fournisseurs d'hébergement de rediffuser, dans le cadre de leurs services d'aide à la conduite par géolocalisation, des informations relatives à certains contrôles routiers. En effet, cette interdiction ne concerne pas les obligations de surveillance applicables à un cas spécifique et ne fait pas obstacle aux décisions des autorités nationales prises conformément à la législation nationale (consid. 47 de la directive).

Commentaire

Cette décision suscite plusieurs réflexions. Tout d'abord, la CJUE confirme sa jurisprudence en indiquant que le prestataire qui stocke des informations de manière neutre est un fournisseur d'hébergement, à l'inverse du prestataire qui détermine par un algorithme et à son intérêt ou à l'intérêt de son service les conditions de diffusion de certains messages sur sa plateforme (réflexion reprise de la décision CJUE, Youtube et Cyando, C-682/18 et C-683/18). Il peut par ailleurs paraître étonnant que cette question n'ait pas du tout été examinée dans le cadre de l'affaire C-188/24 (commenté sur : swissprivacy.law/410/).

Ensuite, la Cour reprend aussi sa jurisprudence en admettant que l'interdiction spécifique imposée à un prestataire de services d'aide à la conduite ou à la navigation par géolocalisation de rediffuser des messages de ses utilisateurs et utilisatrices concernant certains types de contrôles routiers ne consiste pas en de la surveillance généralisée dans le cas où il n'a pas besoin de prendre connaissance du contenu des messages, car il peut identifier les messages par de moyens de recherches automatisés (CJUE, Affaire Glawischnig-Piesczek,

C-18/18).

En pratique, il est d'intérêt général que le contenu des messages transitant sur différentes plateformes ne soient pas surveillés de façon généralisée par les prestataires. Il semble également important de ne pas interpréter la décision de la Cour comme permettant la surveillance généralisée des messages envoyés par les utilisateurs et utilisatrices des plateformes. En outre, il convient de s'assurer que les prestataires ne prennent pas connaissance du contenu des messages, et que le respect des différentes exigences, en particulier de protection des données, soit garanti par la mise en place de garde-fous par ces entreprises.

Finalement, cette décision permet de se questionner quant à ce que le droit suisse prévoit pour encadrer la pratique des prestataires de services d'aide à la conduite ou à la navigation par géolocalisation, si un cas de figure similaire pourrait se produire en Suisse. La question reste ouverte sur la manière dont de tels cas seraient examinés juridiquement.

Proposition de citation : Pauline Meyer, CJUE et directive sur le commerce électronique – Partie 2 : Interdire la rediffusion de messages par un service de géolocalisation, 6 juillet 2026 *in* www.swissprivacy.law/411

Les articles de swissprivacy.law sont publiés sous licence creative commons CC BY 4.0.