DOCTRINE

RESPONSABILITÉ

DSA : irresponsabilité de principe des hébergeurs et obligations renforcées

Le Digital services Act maintient le principe d'irresponsabilité des fournisseurs de services numériques pour le contenu mis en ligne par des tiers en l'assortissant d'obligations de vigilance et de transparence renforcées selon le niveau de risque et les capacités financières des différents acteurs de l'économie numérique.

Le principe d'irresponsabilité des hébergeurs et autres fournisseurs de services numériques pour le contenu mis en ligne sur leurs sites a été établi d'abord aux Etats-Unis en 1996 par le Communication Decency Act[1] puis en 1998 par le Digital Millenium Copyright Act[2], puis dans l'Union européenne par la directive du 8 juin 2000 dite « *Directive commerce électronique* »[3], transposée en France en 2004 par la LCEN[4].

Il a indéniablement largement contribué au développement fulgurant de l'économie numérique. Cependant, cette irresponsabilité de principe semble de moins en moins acceptable, au vu du pouvoir d'influence des plus grandes plateformes, dans leur quasi-totalité américaines, qui pose de réels enjeux non seulement économiques mais aussi pour le respect des droits fondamentaux. Au cours des derniers mois, de nombreuses initiatives, de tous les camps politiques, ont remis en cause ce principe d'irresponsabilité.

Aux Etats-Unis, Donald Trump, réagissant à ce qu'il percevait comme sa censure par Twitter, a, par décret du 28 mai 2020[5], précisé l'interprétation de son administration de l'article 230(c) du Communication Decency Act, en indiquant que cette immunité ne devrait s'appliquer qu'aux hébergeurs modérant leurs sites pour en retirer les contenus obscènes, violents ou constitutifs de harcèlement mais pas lorsque ces derniers retirent du contenu à des fins politiques, ce qui les soumettrait alors au statut d'éditeurs et les priverait du bénéfice de l'irresponsabilité pour les contenus mis en ligne par des tiers.

La suspension définitive par Twitter du compte @realDonaldTrump, suite aux appels à l'insurrection effectués sur ce compte, démontre bien d'un côté la gigantesque influence de cette plateforme, dont le président Trump a largement bénéficié, et d'un autre côté les risques qui existent pour la liberté d'expression à laisser une société commerciale, sans contrôle judiciaire et sans règles clairement définies à l'avance, censurer un acteur politique majeur, ayant réuni 88 millions de voix, de son moyen d'expression privilégié.

A l'inverse, en France, la loi Avia[6] qui prévoyait une obligation pour les hébergeurs, sous peine d'un an de prison et 250 000 € d'amende, de retirer certains contenus illégaux dans les 24 heures de leur notification ou même dans un délai d'une heure pour l'incitation au terrorisme ou la pédopornographie[7] sur simple notice des internautes a été censurée par le Conseil constitutionnel comme attentatoire à la liberté d'expression et de communication.

La Commission européenne, dans le projet de règlement sur les services numériques qu'elle a présenté le 15 décembre dernier, dit le Digital services Act, essaie de trouver un équilibre entre d'une part l'irresponsabilité des fournisseurs de services numériques pour le contenu mis en ligne par des tiers et d'autre part les risques que la taille et la puissance des plateformes font courir aux libertés publiques, en assortissant cette irresponsabilité d'obligations de vigilance et de transparence renforcées selon le niveau de risque et les capacités financières des différents acteurs de l'économie numérique.

Le principe d'irresponsabilité de fournisseurs de services réaffirmé

Le projet de règlement présenté par la Commission reprend quasiment mot pour mot les articles 12, 13 et 14 de la directive « *commerce électronique* », distinguant toujours entre les fournisseurs de simple transport (mere conduit)

qui se bornent à la simple transmission de l'information tels que par exemple les fournisseurs d'accès à internet, les fournisseurs de stockage dit de « *caching* », qui fournissent de manière neutre des services de stockage de l'information et les fournisseurs de services d'hébergement, qui stockent les informations fournies par leur utilisateurs en vue de leur accès par des tiers. Les simples transporteurs demeurent totalement exempts de responsabilité, les prestataires de services de « *caching* » demeurent soumis à l'obligation de retirer l'information de leurs serveurs dès qu'ils ont connaissance que l'accès à ces informations est interdit et les fournisseurs d'hébergement demeurent soumis à l'obligation de retirer ces informations dès qu'ils ont connaissance de leur caractère illicite. La jurisprudence a abondamment affiné la notion d'hébergeur, depuis l'arrêt fondateur « *Google Adwords* »[8] en 2010 qui a posé comme critère essentiel pour l'acquisition de la qualité d'hébergeur « *l'absence de rôle actif de nature à lui confier une connaissance ou un contrôle des données stockées* » du fournisseur de services numériques. La répétition presque mot pour mot de ces articles permet de conserver l'acquis considérable de cette jurisprudence, ce qui est une réelle source de sécurité juridique.

L'article 6 du projet de règlement ajoute une précision importante concernant la conservation du bénéfice de ces exemptions lorsque le fournisseur de services numériques effectue volontairement des investigations afin de détecter le caractère illégal du contenu stocké par les utilisateurs. En effet, cette activité de modération pourrait être considérée comme l'exercice d'un contrôle sur les données stockées et priver le fournisseur de services numériques du bénéfice de l'exemption de responsabilité des hébergeurs, ce qui a pu faire hésiter certains hébergeurs à investir dans un véritable service de modération. C'est notamment cette interprétation qui a été retenue par le décret du président Trump cité ci-dessus. Ce frein à la présence systématique de services de modération est donc levé, même si le projet de règlement répète l'absence d'obligation générale de surveillance des fournisseurs de services numériques de la Directive commerce électronique.

Le projet de règlement définit également un cadre que les Etats membres doivent respecter lorsqu'ils ordonnent à un fournisseur de service numérique de retirer du contenu illégal ou de fournir des informations, telles que par exemple l'adresse IP de la personne qui a initialement mis en ligne le contenu illégal. Si les Etats membres sont libres de prévoir des procédures judiciaires ou administratives à cet effet, les ordonnances ou mises en demeure devront toutes inclure la justification du caractère illégal du contenu en mentionnant spécifiquement la disposition juridique enfreinte, la localisation du contenu illégal ainsi que toutes autres informations permettant de l'identifier ainsi que les recours disponibles pour le fournisseur de services numériques.

Les ordonnances ou mises en demeure devront également évaluer leur portée territoriale -ce qui semble étonnant puisqu'une juridiction ou une autorité administrative ne saurait généralement avoir de compétence que sur son propre territoire national- et être rédigées dans la langue déclarée par le fournisseur de services numériques. Les ordonnances ou mises en demeure concernant la fourniture d'information par les fournisseurs de services numériques sont soumises à des conditions de forme similaire. On peut s'interroger sur la proportionnalité et le respect du principe de subsidiarité par ces prescriptions normatives.
En particulier, la question de la langue semble conférer aux fournisseurs de services numériques un privilège absolument exorbitant, celui de désigner la langue dans laquelle les administrations et juridictions des Etats membres pourront communiquer avec lui, ce qui semble en violation manifeste des dispositions de l'article 2 de la Constitution française.

Il est à espérer que le Conseil ou le Parlement reviendront sur cette disposition et permettront aux juridictions et administrations nationales de s'adresser aux fournisseurs de services numériques dans la langue de leur Etat membre, et non dans celle choisie par le fournisseur.

Ce maintien de l'irresponsabilité de principe s'accompagne de nouvelles obligations, destinées à renforcer la transparence et assurer la neutralité des fournisseurs de services numériques. Ces nouvelles obligations sont différenciées selon la taille et les risques représentés par les différents fournisseurs de services numériques, les simples fournisseurs d'accès Internet présentant moins de risques que les plateformes disposant de centaines de millions d'utilisateurs.

Les nouvelles obligations applicables à tous les fournisseurs de services numériques

Tous les fournisseurs de services numériques devront disposer d'un point de contact unique pour communiquer avec les autorités nationales, dont les coordonnées devront être rendues publiques et dont la ou les langues utilisées, une de ces langues devant être celle du pays où le fournisseur de services numériques ou son représentant est établi. Les fournisseurs de services intermédiaires qui ne disposent pas d'un établissement au sein de l'Union européenne devront nommer un représentant dans l'un des Etats membres où ils offrent leurs services.

Comme le représentant prévu par le RGPD, ce représentant pourra être responsable en cas de violation du règlement par le fournisseur

de services intermédiaires, ce qui risque de fortement limiter le succès de ce mécanisme, du fait du faible nombre de volontaires pour exposer leur responsabilité personnelle pour le compte de tiers situés hors de l'Union européenne.

Les conditions générales devront également clairement indiquer les restrictions que les fournisseurs imposent à l'utilisation de leurs services, qui devront être appliquées de manière diligente, objective et proportionnée. De plus, un rapport annuel devra être publié concernant la modération effectuée, mentionnant le nombre d'ordonnances, mises en demeure ou notifications reçues concernant du contenu illicite et le type de contenu illicite, les initiatives de modérations des contenus prises par les fournisseurs et le nombre de plaintes reçues par le mécanisme interne de résolution des plaintes et les délais de traitement de ces plaintes. Ce rapport ne concerne toutefois pas les entreprises employant moins de 50 personnes ou ayant un chiffre d'affaires de moins de 10 millions d'euros. L'intérêt de faire établir un tel rapport par les simples fournisseurs de services de transport d'information et de caching ne semble cependant pas évident, puisqu'ils n'ont pas par définition d'activité de modération et il est à espérer que le Parlement et le Conseil limiteront cette obligation aux hébergeurs.

Les obligations graduées applicables aux hébergeurs et aux plateformes

Obligations applicables à tous les hébergeurs

Les fournisseurs de services d'hébergement devront mettre en place un mécanisme de notification des contenus illégaux beaucoup plus élaboré que celui défini à l'article 6.5 actuel de la LCEN. Afin d'éviter les notifications non valides, c'est désormais à l'hébergeur de configurer son mécanisme de notification pour que les informations transmises par l'internaute contiennent les informations demandées : justification du caractère illégal du contenu dénoncé, indication de la location du contenu (URL), nom et adresse électronique du plaignant et déclaration confirmant la bonne foi du plaignant.

L'article 14 du projet de règlement ne prévoit cependant pas de délai strictement défini pour répondre aux plaintes, mais uniquement une obligation de « *promptement* » délivrer un accusé de réception et de notifier « *sans retard indu* » la décision de retirer ou de maintenir le contenu objet de la plainte. Lorsque l'hébergeur décide de retirer un contenu estimé illégal, il devra en informer son producteur, au plus tard au moment de ce retrait, en lui fournissant les raisons de cette décision (fait et circonstances, y compris notification par un tiers du caractère illégal du contenu, base juridique utilisée pour trouver le contenu illégal ou non conforme aux conditions générales d'utilisation de l'hébergeur) ainsi que le cas échéant, l'utilisation de moyens automatisés pour parvenir à la décision, sa portée territoriale et les moyens de recours judiciaires et extrajudiciaires à la disposition du producteur du contenu retiré. Ces décisions devront être publiées sur un site Internet accessible au public géré par la Commission.

Obligations applicables uniquement aux plateformes

Les plateformes en ligne ayant un chiffre d'affaires de plus de 10 millions d'euros ou plus de 50 salariés sont soumises à des obligations renforcées par rapport à celles des simples hébergeurs.

Un système de résolution extra-judiciaire des différends est tout d'abord défini, qui impose aux plateformes de mettre à disposition de leurs utilisateurs un dispositif leur permettant de contester les décisions de retrait de contenu, de suspendre ou résilier l'accès au service ou à leur compte. Ces dispositifs devront être faciles à utiliser et la plateforme devra rétablir l'accès au contenu si l'utilisateur démontre de façon suffisante que son contenu n'était pas illégal. Contrairement au traitement des plaintes des visiteurs de la plateforme, ces dispositifs de traitement des plaintes des utilisateurs ne pourront pas être uniquement basés sur des traitements automatisés, ce qui ne signifie pas qu'ils ne pourront pas l'être partiellement. Si, après cette forme de recours gracieux, la plateforme refuse toujours de revenir sur sa décision de retrait du contenu (ou d'interdiction d'accès au site), les utilisateurs pourront la contester auprès d'organismes tiers indépendants agréés par le Coordinateur national des services numériques. S'ils prévalent, ils se verront remboursés de tous leurs honoraires et frais raisonnables par la plateforme qui ne bénéficie cependant pas de la réciproque. Le projet de règlement institue également une sorte de procureurs privés, dont les alertes devront être traitées en priorité, en créant les « *lanceurs d'alerte de confiance* » (trusted flaggers) qui seront des entités agréées par le Coordinateur des services numériques au vu de leurs compétences et de leur indépendance.

Les plateformes seront soumises, si le règlement est adopté en l'état, à des obligations de surveillance et de sanction de leurs utilisateurs, puisqu'elles devront suspendre ceux qui fournissent fréquemment du contenu illégal ou effectuent des alertes infondées, ainsi que communiquer aux autorités des États membres les informations leur permettant de soupçonner la commission d'un crime ou d'un délit concernant la vie ou la sécurité des personnes. Elles devront également, si elles permettent la conclusion de contrats avec des commerçants, collecter des informations sur ces commerçants, permettant leur éventuelle poursuite : nom, adresse, téléphone, adresse e-mail, document d'identification (probablement l'extrait K-bis en France), coordonnées bancaires si le commerçant est une personne physique, numéro d'enregistrement au registre du commerce et des sociétés, déclaration du respect du droit de l'UE par les produits et services offerts par le commerçant.

Au vu de ces informations, la plateforme devra faire des efforts raisonnables pour vérifier l'identité des personnes qui proposent des biens et services, c'est-à-dire leur existence réelle, mais uniquement en utilisant les bases de données disponibles gratuitement dans l'Union européenne ou en formulant des demandes auprès des commerçants, mais en pratique, toute société-écran pourra librement continuer à commercer sur les plateformes.

Il est à espérer que le Conseil et le Parlement renforceront ces vérifications, en incluant par exemple des informations sur les bénéficiaires effectifs de ces sociétés à partir d'un certain seuil de chiffre d'affaires, et permettront la création par les plateformes de listes rouges suite à des fraudes des sociétés de bénéficiaires effectifs établis hors de l'Union européenne, afin de lutter plus efficacement contre les fraudes qui profitent de l'opacité permise par le commerce sur Internet.

Les plateformes devront publier tous les ans le nombre de plaintes résolues par voie alternative de résolution des litiges, les décisions rendues et les délais de règlement des procédures, le nombre de suspensions prononcées, toute utilisation de moyens automatiques de modérations des contenus ainsi que, tous les six mois, le nombre de moyen d'utilisateurs mensuel dans chaque Etat membre.

Si elles permettent la publicité sur leur site, les plateformes devront clairement identifier ces publicités, permettre l'identification de l'annonceur et communiquer des informations sur les principaux paramètres utilisés pour déterminer le destinataire de la publicité.

Au vu de la sensibilité de cette information, ce dernier point risque de générer un lobbying intense, les critères de ciblage utilisés étant un secret commercial d'une valeur réelle dont la publication générale et sans filtre ne nous semble pas souhaitable.

Obligations applicables aux plateformes de très grande taille

Le considérant 56 du projet de règlement dispose que les très grandes plateformes, dont le nombre d'utilisateurs actifs dépasse 10% de la population de l'Union européenne, peuvent causer des risques sociétaux systémiques de par l'influence qu'elle exercent sur la sécurité en ligne, la formation de l'opinion et du discours public et le commerce en ligne, alors qu'elles sont créées généralement uniquement pour maximiser les profits de leur propriétaire, basés sur la publicité et le traitement de données personnelles.

Par conséquent, le projet de règlement impose à ces très grandes plateformes de procéder au moins une fois par an à une étude des risques que leur fonctionnement et l'utilisation de leurs services dans l'Union européenne présente concernant la dissémination en ligne de contenu illicite, le respect des droits fondamentaux à la vie privée et familiale, de la liberté d'expression et de l'information, l'interdiction des discriminations et les droits de l'enfants tels que définis dans la Charte des Droits fondamentaux et la manipulation intentionnelle de leurs services pouvant avoir des conséquences négatives sur la protection de la santé publique, des mineurs, du discours civique, du processus électoral ou de la sécurité publique. Une fois ces études achevées, les très grandes plateformes devront mettre en place des mesures de nature à y remédier, par exemple en adaptant leur modération ou en collaborant avec des lanceurs d'alerte de confiance.

Tous les ans, ces plateformes devront faire l'objet d'un audit par un tiers indépendant concernant leur respect de toutes leurs nouvelles obligations au titre du projet de règlement, c'est-à-dire les mécanismes de notification de contenus illégaux, de règlement interne et extra-judiciaire des différends, de surveillance et de sanction, de transparence et d'étude des risques. Si le rapport d'audit établit des points de non-conformité et formule des recommandations, les très grandes plateformes devront dans un délai d'un mois établir un rapport de mise en œuvre de l'audit détaillant la façon dont ces recommandations ont été mises en œuvre et si elles ne l'ont pas été, la justification de cette absence de mise en œuvre.

Les obligations de transparence des très grandes plateformes sont également renforcées, avec une obligation d'indiquer les logiques sous-jacentes aux recommandations, de conserver pendant une année après la fin d'une publication, de manière accessible au public, le contenu de la publicité, l'identité de l'annonceur, la période d'affichage de la publicité, ses paramètres de ciblage et le nombre total d'utilisateurs du service ayant reçu communication de la publicité et le nombre total d'utilisateurs visés. Tous les rapports (modération, étude de risque, mise en œuvre des études de risque) devront être rendus publics.

Enfin, elles devront nommer une personne responsable du respect de ce nouveau règlement, qui devra être le point de contact des Coordinateurs de services numériques, organiser et superviser les audits, informer les salariés des obligations de la société et surveiller le respect par la plateforme de ses obligations au titre de ce règlement.

Création d'un cadre institutionnel de la réglementation des hébergeurs de données

Contrairement à la directive « *commerce électronique* », le projet de règlement Digital Services Act prévoit la création d'une véritable infrastructure institutionnelle destinée à assurer son respect par les fournisseurs de services numériques, dont de nombreux éléments semblent directement inspirés du RGPD.

DOCTRINE

Il prévoit tout d'abord l'adoption de codes de conduite volontaires par les acteurs de l'industrie et approuvés par la Commission, la création de responsables de la conformité et de représentants pour les fournisseurs non établis dans l'Union veuropéenne, qui sont tous des éléments présents dans le RGPD.
Comme dans le RGPD, chaque Etat membre devra désigner une autorité indépendante, dénommée le Coordinateur des services numériques, qui sera en charge du respect du règlement. Au vu de la loi Avia, il semble probable que cette responsabilité reviendrait, en France, au Conseil supérieur de l'Audiovisuel, bien que le projet de règlement prévoit que les compétences du Coordinateur des services numériques puissent être partagées entre plusieurs autorités.

Ces Coordinateurs nationaux devront coopérer les uns avec les autres au niveau européen au sein d'un Comité, afin de coordonner leurs actions, adopter une interprétation commune du règlement et superviser les mesures prises par un ou plusieurs Coordinateurs nationaux concernant une plateforme de très grande taille.

Le Coordonnateur de l'Etat membre d'établissement d'un fournisseur de service (ou de son représentant si le fournisseur n'est pas établi dans l'Union européenne) aura compétence pour s'assurer du respect de ses obligations. Comme les autorités de contrôle du RGPD, ces Coordinateurs auront des pouvoirs d'enquête, d'injonction et de sanction, dont les montants sont même supérieurs à ceux prévus par le RGPD, puisqu'ils pourront aller jusqu'à 6% du chiffre d'affaires de service sanctionné.

Ils pourront recevoir et instruire directement les plaintes des utilisateurs et devront établir des rapports annuels de leur activité. Le projet de règlement Digital Services Act, s'il est perfectible, nous semble donc constituer une bonne base pour la réglementation des fournisseurs de services numériques. Le juge est en effet mal armé pour réguler ces activités, au vu du nombre de contentieux qu'elles peuvent générer et de la rapidité nécessaire à leur résolution.

Seul un mécanisme amiable géré tout d'abord par les plateformes puis un mécanisme contentieux extrajudiciaire permettent de concilier les exigences de faible coût, rapidité et traitement de masse nécessaires à la régulation des informations échangées sur Internet. Le rôle du juge demeurera cependant essentiel pour orienter les décisions prises par les plateformes et les organismes extrajudiciaires de résolution des différends, puisqu'il dispose de la légitimité nécessaire pour la prise des décisions fondamentales à la conciliation entre les exigences de la liberté de communication et la protection des individus, sur la base de la loi votée démocratiquement.

Ce rôle du juge mériterait d'être souligné dans le projet de règlement, en précisant que les décisions des organismes extra-judiciaires de résolution des conflits entre les plateformes et leurs utilisateurs demeureront susceptibles de recours devant les juridictions, pour éviter que ces mécanismes ne se transforment en arbitrage privé obligatoire.

Marc LEMPERIERE
Avocat associé
ALMAIN

Notes

(1) Communications Decency Act, section 230.(c), 47 U.S.C. 230©

(2) Digital Millennium Copyright Act, public law 105–304—OCT. 28, 1998,

(3) Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur

(4) Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique

(5) Executive Order on Preventing Online Censorship, 28 mai 2020

(6) Loi visant à lutter contre les contenus haineux sur Internet

(7) Décision n°2020-801 DC du 18 juin 2020 Loi visant à lutter contre les contenus haineux sur Internet

(8) CJUE, 23 mars 2010, aff.C-236/08 à C-238/08, Sté Google c/ Sté Louis Vuitton Malletier

Vous avez envie de vous exprimer sur un sujet qui vous tient à cœur, de partager votre analyse avec la communauté des lecteurs d'Expertises, d'exposer un point de vue différent sur un article déjà publié, de lancer un débat sur un thème émergent, ou simplement de commenter l'actualité du droit du numérique ?

Contactez la rédactrice en chef d'Expertises Sylvie Rozenfeld sr@expertises.info