Responsabilité des prestataires d'hébergement : les modalités d'une injonction visant à empêcher la réapparition d'un contenu illicite selon la CJUE

L'autorité nationale (juridiction ou autorité administrative compétente) peut faire injonction à un prestataire d'hébergement d'empêcher la réapparition d'une information qu'elle a jugée illicite, que cette information émane de son auteur d'origine ou d'un tiers.

Elle peut également enjoindre au prestataire d'hébergement d'empêcher la réapparition d'une information « équivalente » à celle jugée illicite, à certaines conditions seulement.

L'autorité nationale peut donner à de telles injonctions une portée mondiale, dans le cadre du droit international pertinent.

La responsabilité au titre des contenus illicites en ligne paraît à la croisée des chemins : son socle juridique, issu de la directive 2000/31/CE du 8 juin 2000 relative au commerce électronique (« la directive »), transposée en droit français par la loi no 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (dite « LCEN »), se trouve « rogné » par l'émergence, au niveau européen ou national, de régimes spéciaux visant à lutter contre certaines catégories de contenus illicites (atteintes au droit d'auteur aux droits voisins1, contenus dits « haineux »2, catégorie que l'on est en droit de trouver diffuse).

Ces régimes ou projets de régimes spéciaux et catégoriels ont en effet en commun de créer, pour certains types de contenus illicites seulement, des mécanismes de responsabilité « hybrides », à mi-chemin, pourrait-on dire, entre celui, exceptionnel, des prestataires techniques3, issu de la directive 2000/31/CE, et celui des éditeurs de services de communication au public en ligne, qui n'est autre que le droit commun. Ces régimes d'exception, qui n'en reviennent pas pour autant audit droit commun, révèlent que, aux yeux des législateurs et sans doute d'une partie au moins des acteurs eux-mêmes, le socle issu de la directive 2000/31/CE trouve aujourd'hui ses limites. Témoigne également de cette tendance la promotion de différents mécanismes d'autorégulation ou de corégulation4.

Ce qui frappe, à l'étude de ces régimes spéciaux adoptés ou en cours d'adoption, comme des mécanismes de régulation précités, c'est que le « dogme » sur lequel reposait jusqu'à présent le régime dérogatoire de responsabilité des prestataires d'hébergement5, à savoir leur absence de capacité de contrôle sur les contenus « stockés » et diffusés via leurs services, induisant leur « neutralité » technique, semble dépassé. Au contraire, leur capacité d'action sur lesdits contenus est en réalité au cœur de ces nouveaux régimes spéciaux ainsi que des mécanismes de régulation, puisque les uns comme les autres attendent des opérateurs concernés qu'ils identifient, à l'aide de moyens techniques de détection et de filtrage, les contenus illicites, notamment pour en prévenir la

diffusion.
Et pourtant, le régime de responsabilité des fournisseurs d'hébergement issu de la directive 2000/31/CE perdure, et concerne sans doute encore une part substantielle des contenus illicites en ligne (par exemple : diffamations et injures « de droit commun »6, atteintes à la vie privée et au droit à l'image, dénigrement de produits, etc.).
C'est dans ce contexte incertain, où nombre d'acteurs du web ne savent plus très bien quelle « casquette » endosser (hébergeur, fournisseur d'un service de partage…) tandis que le régime des prestataires d'hébergement apparaît déjà vieux et fatigué, que la Cour de justice devait répondre à une question relative à certaines modalités d'application, importante en pratique, de ce régime.
Selon quelles modalités une autorité nationale peut-elle ordonner à un prestataire d'hébergement d'empêcher la réapparition, sur son service, d'un contenu qu'elle a jugé illicite ?
Telle est en substance la question à laquelle répond l'arrêt rapporté, rendu sur question préjudicielle en interprétation de la directive 2000/31/CE relative au commerce électronique, et plus particulièrement de ses articles 15, paragraphe 1, 14, paragraphe 3, et 18, paragraphe 1.
D'un côté, l'article 15, paragraphe 1, interdit d'imposer aux prestataires techniques, dont les prestataires d'hébergement, une obligation générale de surveillance des informations qu'ils stockent, ou de rechercher activement des informations illicites.
De l'autre, les articles 14, paragraphe 3, et 18, paragraphe 1, de la directive énoncent respectivement, en substance, que les juridictions ou autorités administratives nationales doivent pouvoir exiger d'un prestataire technique, notamment d'hébergement, qu'il mette un terme à une violation*ou la prévienne*, et que les États membres doivent veiller à ce que les recours juridictionnels prévus à cette fin permettent l'adoption rapide des mesures adéquates.
Il s'agissait donc de concilier l'interdiction d'imposer aux prestataires d'hébergement une obligation générale de surveillance des informations qu'ils stockent avec la nécessité de protéger efficacement les droits des tiers susceptibles d'être violés par des contenus en ligne, en particulier en prévenant de nouvelles atteintes.
Les circonstances du litige au principal étaient les suivantes. Un utilisateur de Facebook avait partagé sur ce réseau social un article consacré au parti politique des écologistes autrichiens, favorable à maintien d'un revenu minimum pour les réfugiés. Ce partage avait généré, selon les modalités techniques usuelles du réseau social, ce qu'il est convenu d'appeler un « aperçu vignette » du site d'origine de l'article, reproduisant son titre, un bref résumé de cet article, ainsi qu'une photo d'illustration, au sein de laquelle apparaissait la requérante, députée au Nationalrat (le Conseil national autrichien), présidente du groupe parlementaire du parti en cause et porte-parole fédéral de ce parti. L'utilisateur avait assorti ce partage d'un commentaire affublant cette représentante du peuple de divers noms d'oiseau tout en lui imputant des pratiques contraires à la loi, dont il suffira de dire ici qu'ils portaient indéniablement atteinte à sa réputation. Ce point, admis par les juridictions nationales successivement saisies du litige, ne faisait pas débat devant la Cour.
La députée avait d'abord écrit à Facebook pour lui demander de supprimer notamment ce

commentaire. Face à l'insuccès de cette démarche, elle saisit le tribunal de commerce de Vienne en référé, qui fit notamment injonction à Facebook de cesser la diffusion de la photographie représentant la requérante, dès lors qu'elle était accompagnée du même commentaire*ou d'allégations de contenu équivalent*, jusqu'à la clôture définitive de l'action au fond.
La juridiction d'appel confirma cette injonction s'agissant du commentaire jugé illicite, mais l'infirma en ce qu'il imposait également au réseau social d'empêcher la diffusion de contenus*équivalents*, dès lors que ceux-ci ne lui avaient pas été préalablement notifiés par la requérante au principal ou des tiers.
Chacune des parties forma un recours à l'encontre de cette décision devant la Cour suprême autrichienne (Oberster Gerichtshof), laquelle estima que, selon sa propre jurisprudence, la solution retenue en première instance par le tribunal de commerce de Vienne était proportionnée, dès lors que le contenu en cause avait été notifié au moins une fois au prestataire d'hébergement.
Néanmoins, la Cour suprême autrichienne, éprouvant des doutes quant à l'interprétation du droit de l'Union applicable en ces circonstances, décida de surseoir à statuer et de poser à la Cour de justice la question préjudicielle à laquelle répond l'arrêt rapporté.
En substance, la Cour juge en premier lieu que l'autorité nationale peut faire injonction à un prestataire d'hébergement d'empêcher la réapparition d'une information qu'elle a jugée illicite, que cette information émane de son auteur d'origine ou d'un tiers ; en second lieu, elle décide que l'autorité nationale peut également enjoindre au prestataire d'hébergement d'empêcher la réapparition d'une information « équivalente » à celle jugée illicite, à certaines conditions seulement ; en troisième lieu, elle estime que l'autorité nationale peut donner à de telles injonctions une portée mondiale, « dans le cadre du droit international pertinent »7.
Par ces réponses, la Cour précise la portée matérielle (I) et territoriale (II) de l'injonction faite par un juge national à un hébergeur de supprimer une information (ou d'empêcher sa réapparition) qu'elle a jugée illicite.**I - La portée matérielle de l'injonction faite à un hébergeur de supprimer une information jugée illicite ou d'en bloquer l'accès**Au préalable, il ne fait pas de doute que la juridiction nationale (ou l'autorité administrative compétente) saisie d'une demande de retrait ou de blocage d'une information illicite en ligne peut, sur le fondement de son droit national transposant l'article 14 de la directive 2000/31/CE, faire injonction à l'hébergeur de cette information, non seulement de la retirer ou d'en bloquer l'accès, mais également d'empêcher que son auteur ne la publie à nouveau en ligne via son service. En effet, l'article 14, paragraphe 3, de la directive réserve la possibilité, pour les droits nationaux, d'exiger notamment de l'hébergeur qu'il*prévienne*une violation et son article 18, paragraphe 1, le confirme, en exigeant que les recours juridictionnels prévus par ces droits nationaux permettent l'adoption rapide des mesures visant notamment à *prévenir*de nouvelles atteintes. Par ailleurs, le considérant 47 de la directive précise que l'interdiction d'instaurer à la charge des hébergeurs une obligation générale de surveillance des informations qu'ils stockent ne vaut pas pour les obligations de surveillance applicables à un cas *spécifique*, et en particulier à celles résultant de décisions des autorités nationales conformément à

leur législation.
Or l'injonction faite par l'autorité nationale à un prestataire d'hébergement de bloquer l'accès à une information qu'elle a jugée illicite et que l'auteur initial de cette information voudrait publier à nouveau, vise à prévenir une nouvelle atteinte et est limitée à un cas spécifique, puisqu'il suffit à ce prestataire, pour la respecter, de surveiller les nouvelles informations émises par ce seul utilisateur de son service.
En d'autres termes, il ne lui est pas imposé, alors, de procéder à une surveillance généralisée de la totalité ou de la quasi-totalité des informations qu'il stocke.
La question est plus délicate lorsque l'injonction s'étend aux informations, identiques ou équivalentes, mises en ligne*par d'autres utilisateurs*du service d'hébergement.
Pourtant, nous l'avons vu, la Cour de justice admet dans ces deux cas la validité d'une telle injonction au regard du droit de l'Union et, en particulier, de l'article 15, paragraphe 1, de la directive, qui fulmine l'interdiction d'une obligation générale de surveillance à la charge des hébergeurs.
Il convient d'examiner l'hypothèse de l'injonction d'empêcher la réapparition d'une information identique, quel que soit son auteur, dont la Cour admet la conformité au droit de l'Union sans condition (A), puis celle de l'injonction d'empêcher la réapparition d'une information « équivalente », dont la conformité au droit de l'Union est soumise, selon la Cour, à certaines conditions (B).
Nous nous essayerons ensuite à une appréciation critique de ces solutions (C).**A – L'injonction faite à un hébergeur d'empêcher la réapparition d'une information identique à celle jugée illicite, quel qu'en soit l'auteur**L'hypothèse est celle où l'autorité nationale, ayant jugé une information illicite, fait injonction au prestataire d'hébergement de cette information de bloquer l'accès à toute information identique ou de supprimer une telle information de son service, que cette information émane de l'auteur de celle initialement jugée illicite ou de tout autre utilisateur dudit service.
La Cour ne définit pas ce qu'elle entend par une information « identique » à celle jugée illicite. Les conclusions de l'avocat général précisent que deux situations sont ainsi visées : d'une part les reproductions « manuelles et exactes » de l'information qualifiée d'illicite et, d'autre part, les reproductions « automatisées » de ladite information, effectuées grâce à la fonction de « partage », en l'occurrence proposée par Facebook8.
Ceci précisé, la Cour juge, on l'a dit, qu'une telle injonction est conforme au droit de l'Union et, en particulier, qu'elle n'impose pas au prestataire d'hébergement de surveiller de manière générale les contenus qu'il stocke, ni de rechercher activement des informations illicites, ce qui serait contraire à l'article 15, paragraphe 1, de la directive 2000/31/CE. Et cela que les nouvelles informations qui seraient bloquées par l'hébergeur en application de cette injonction émanent de l'auteur de l'information originaire jugée illicite ou de tout autre utilisateur de son service.
La Cour justifie cette solution de manière succincte.
Après avoir observé, notamment, que selon l'article 18, paragraphe 1, de la directive, les mesures efficaces prises par les juridictions nationales doivent mettre un terme à « toute » violation9 et que,

en vertu du considérant 52 de la directive, les recours juridictionnels internes doivent être efficaces, elle relève que selon le considérant 47 de cette même directive, déjà cité, l'interdiction d'obligation générale de surveillance édictée par l'article 15, paragraphe 1, ne s'applique pas aux « cas spécifiques ». Et d'ajouter en substance qu'un tel cas spécifique correspond notamment à la situation en cause au principal, où une information précise, stockée par le prestataire d'hébergement à la demande d'un utilisateur de son service, a été analysée puis jugée illicite par la juridiction nationale.

Dans la mesure, poursuit la Cour, où la diffusion rapide des informations stockées par l'hébergeur (en l'occurrence, faut-il le rappeler, un réseau social planétaire) crée un risque réel de voir cette information illicite être partagée et ainsi se propager, il est « légitime » que la juridiction nationale ayant jugé cette information illicite fasse injonction audit hébergeur de bloquer les informations identiques à cette dernière, « quel que soit l'auteur de la demande de stockage » de ces informations – lire : quel que soit l'utilisateur de son service.

Et d'affirmer, en guise de conclusion, qu'une telle injonction ne revient pas à imposer à l'hébergeur une obligation générale de surveillance des informations ou contenus qu'il stocke, « eu égard en particulier à l'identité » de l'information déclarée illicite et de celle dont il est exigé qu'il empêche la réapparition (ou à tout le moins qu'il en bloque l'accès ou la supprime).

On se contentera de relever, à ce stade, que la Cour procède essentiellement par suite d'affirmations plutôt que par démonstration, et que l'assimilation de la situation concrète en cause à un « cas spécifique » faisant exception, par la grâce du considérant 47 de la directive, à l'interdiction générale de surveillance des informations stockées par l'hébergeur, est justifiée exclusivement par l'identification précise de l'information qu'il est fait injonction à ce dernier de bloquer : il s'agit des informations identiques à celle jugée initialement illicite, à l'exclusion de toutes les autres.

En d'autres termes, cette identification précise de l'information que l'hébergeur devra bloquer en application de l'injonction judiciaire suffit à considérer que cette injonction porte sur un cas spécifique n'imposant pas audit hébergeur de surveiller l'ensemble, ou une partie substantielle, des informations qu'il stocke.

Nous verrons que cette affirmation est discutable (v. *infra*, C), mais il convient d'abord de présenter la seconde hypothèse réglée par la Cour, qui pose la même difficulté.**B – L'injonction faite à un hébergeur d'empêcher la réapparition d'une information équivalente à celle jugée illicite, quel qu'en soit l'auteur**Cette seconde hypothèse est celle où l'autorité nationale fait injonction à l'hébergeur de bloquer ou de rendre l'accès impossible à des informations non plus identiques, mais équivalentes à celle qu'elle a jugée illicite.

La Cour est un peu plus prolixe sur cette notion d'information « équivalente » que sur celle d'information « identique » : elle indique que sont visées les informations véhiculant un message dont le contenu est « en substance inchangé » par rapport à celui de l'information jugée illicite et qui, dès lors, en diverge très peu. Elle précise que ce qui importe n'est pas l'emploi de certains termes combinés d'une certaine manière, autrement dit, si l'on comprend bien, la forme du

message, mais le fond de ce dernier, autrement dit le propos qu'il véhicule : l'information est équivalente à celle initialement jugée illicite si ce propos l'est lui-même.
On peut, au passage, ne pas partager totalement ce point de vue, la forme d'un message étant parfois constitutive de son illicéité : il suffit de penser aux critères d'appréciation de la diffamation, de maniement subtil et délicat. C'est dire que l'identification d'une information équivalente à l'information initiale pourrait être moins simple que n'a l'air de le penser la Cour. C'est sans doute pourquoi, nous allons le voir, elle a tout de même pris la précaution de subordonner la validité d'une injonction portant sur de telles informations équivalentes à des conditions qui apparaissent comme des garde-fous au manque de précision qui affecte cette notion.
Relevons, au préalable, que les conclusions de l'avocat général sont, sur ce point encore, plus précises que l'arrêt rapporté : selon ce dernier, les informations « équivalentes » sont celles qui « divergent à peine » de l'information initiale, jugée illicite, et visent notamment les hypothèses où cette dernière est reproduite avec une erreur de frappe ou ayant une syntaxe ou une ponctuation nuancée. Il admet néanmoins que cette notion d'information équivalente pourrait être plus large, sans autre précision.
De fait, à lire l'arrêt rapporté, l'avocat général s'est fait une conception plus restrictive de la notion que celle que retient la Cour.
Quoi qu'il en soit, cette dernière juge que l'autorité nationale peut faire injonction à l'hébergeur de bloquer l'accès à, ou de supprimer de son service, les informations seulement équivalentes à celle qu'elle a jugée illicite, que ces informations émanent de l'auteur de l'information initiale ou de tout autre utilisateur du service, aux conditions suivantes :
– en premier lieu, l'autorité nationale doit identifier (dans son injonction) des éléments spécifiques que l'on doit ensuite retrouver dans l'information équivalente, qui sont notamment : le nom de la personne concernée (c'est-à-dire la « victime » du message initial illicite), les circonstances dans lesquelles la violation initiale a été constatée et un « contenu » équivalent à celui déclaré illicite (comprendre : un propos en substance identique et, pour cette raison, également illicite) ;
– en second lieu, la Cour précise que les différences entre la formulation de l'information initiale, jugée illicite, et celle des informations équivalentes faisant l'objet de l'injonction ne doivent pas être telles qu'elles imposent à l'hébergeur de procéder « à une appréciation autonome » de leur illicéité. Autrement dit, si l'on comprend bien, l'illicéité des informations équivalentes visées par l'injonction doit être évidente, sans que l'hébergeur ait à l'apprécier par lui-même ;
– et la Cour de préciser à ce sujet, en troisième et dernier lieu, que le prestataire d'hébergement doit ainsi pouvoir recourir « à des moyens techniques et à des moyens de recherche automatisés », en d'autres termes, à un ou des outils d'intelligence artificielle.
À ces conditions, estime la Cour, l'injonction faite par la juridiction nationale sera suffisamment efficace pour protéger les droits de la personne visée par l'information illicite, sans imposer une obligation excessive à l'hébergeur. Et la Cour conclut qu'une telle injonction n'est pas de nature à imposer à l'hébergeur une obligation générale de surveillance des informations qu'il stocke.

On comprend l'idée générale : les conditions énoncées par la Cour de justice imposent à la juridiction nationale d'identifier, dans son injonction, les critères (nom de la victime de l'information initiale, circonstances de sa constatation, substance du message véhiculé) permettant de déceler les informations équivalentes (à l'information originaire jugée illicite), dont elle exige en conséquence du fournisseur d'hébergement qu'il en empêche la réapparition. Cette identification doit être suffisamment précise pour permettre à ce dernier de mettre en œuvre cette injonction en ayant recours à des outils automatisés, sans avoir à apprécier, au cas par cas, si telle information est effectivement illicite, ou non. Autrement dit, cette illicéité doit « découler » de l'identification opérée par le juge.

On reste cependant perplexe quant à la faisabilité pratique d'une telle solution : quand on connaît l'appréciation subtile qu'implique la mise en œuvre des qualifications de diffamation, d'injure ou même de dénigrement de produit ou services, définir les « circonstances » de la constatation initiale d'une information illicite ainsi que la teneur du message véhiculé, de manière à permettre l'identification automatisée d'informations équivalentes qui seront également considérées comme illicites, pourra dans certains cas relever de la gageure.

Quoi qu'il en soit, on constatera que, à l'instar de la première hypothèse considérée, la Cour de justice procède par voie d'affirmations, le fait que l'injonction n'impose pas à l'hébergeur, aux conditions qu'elle définit, une obligation générale de surveillance étant énoncé en forme de postulat sans reposer sur une justification construite et argumentée.

Or cette affirmation, loin d'être évidente, peut être discutée.**C – Appréciation critique**

Indépendamment des difficultés pratiques de mise en œuvre qui ont été évoquées, et de l'incertitude sur les contours exacts de la notion d'information « équivalente », la solution adoptée par la Cour de justice dans les deux hypothèses présentées soulève une difficulté de principe.

Rappelons, en effet, que cette solution permet à une juridiction nationale de faire injonction à un prestataire d'hébergement de bloquer ou de rendre l'accès impossible à une information identique ou équivalente (dans ce second cas aux conditions présentées ci-avant) à celle qu'elle a jugée illicite,*quelle que soit, dans les deux cas, la source de ces informations*, c'est-à-dire que ces informations identiques ou équivalentes proviennent de l'auteur de l'information initiale ou de*tout autre utilisateur*du service d'hébergement.

Or, comme l'a reconnu l'avocat général lui-même dans ses conclusions, faire injonction à un prestataire d'hébergement de bloquer une information quel que soit l'utilisateur qui est à son origine revient à lui imposer d'identifier, parmi toutes les informations qu'il stocke, l'information visée, et donc à surveiller la totalité de ces informations.

Et que l'information recherchée soit précisément identifiée et définie dans l'injonction comme étant une information identique ou équivalente à une information déjà jugée illicite n'y change rien : pour bloquer une telle information ou empêcher sa réapparition le prestataire d'hébergement ne peut faire autrement que d'analyser, fût-ce au moyen d'outils automatisés, la totalité des informations dont ses utilisateurs sollicitent le stockage (pour reprendre la terminologie de la Cour).

En d'autres termes, l'affirmation selon laquelle la situation en cause au principal correspond au « cas spécifique » visé par le considérant 47 de la directive, excluant l'obligation générale de surveillance prohibée par son article 15, au motif que l'injonction porte sur des informations (plus ou moins) précisément identifiées apparaît comme un leurre.

Certes, si l'injonction portait sur des informations non identifiées ou identifiées mais beaucoup plus nombreuses, elle imposerait de plus fort une obligation générale de surveillance des informations stockées par l'hébergeur, et porterait en outre une atteinte excessive à la liberté d'entreprendre de ce dernier en mettant à sa charge des mesures impliquant des coûts excessifs, sans parler de l'atteinte à la liberté d'expression et au droit à la vie privée des utilisateurs, comme l'a jugé précédemment la Cour. Mais l'on ne peut selon nous en déduire,*a contrario*, que l'injonction ciblée sur des informations plus ou moins précisément identifiées ne conduit pas également à imposer une telle obligation à l'hébergeur. Certes, elle est moins attentatoire à sa liberté d'entreprendre, comme aux droits fondamentaux des utilisateurs. Mais l'étendue de l'obligation de surveillance qu'elle implique à la charge de cet hébergeur est un fait difficilement contestable : pour respecter l'injonction, celui-ci devrait analyser toutes les informations que ses utilisateurs souhaitent publier en ligne.

Et, malgré (à moins que ce ne soit à cause de) les précautions édictées par la Cour sous forme de conditions relatives aux informations équivalentes, on peut être inquiet de ce qu'une telle analyse soit opérée exclusivement au moyen d'outils automatisés, et douter que la liberté d'expression soit ainsi réellement garantie.

En sorte que l'arrêt rapporté nous paraît constituer, sous couvert de continuité, sinon une rupture, du moins une évolution notable par rapport à la jurisprudence antérieure de la Cour et, en particulier, son arrêt*Sabam*.

D'aucuns contesteront peut-être cette évolution en invoquant la portée temporelle de l'injonction. En effet, dans l'affaire, la Cour avait pris soin de relever que l'injonction judiciaire, dont elle a jugé qu'elle imposait à l'hébergeur une obligation générale de surveillance interdite par l'article 15, paragraphe 1, de la directive 2000/31/CE, était, notamment, « illimitée dans le temps ». Or, dans l'affaire au principal, la juridiction nationale saisie et dont l'injonction était en cause était le juge des référés et ladite injonction était limitée temporellement, jusqu'à l'intervention d'une décision au fond. Et l'avocat général insiste à plusieurs reprises, dans ses conclusions, sur l'importance d'une limitation temporelle comme critère permettant d'affirmer que l'injonction en cause relève d'un cas spécifique visé par le considérant 47 de la directive et dérogeant à l'interdiction fulminée par l'article 15.

Néanmoins, force est de constater que ni la question préjudicielle, ni l'arrêt rapporté, n'évoque ce critère temporel, dont la Cour ne fait pas une condition de validité de l'injonction en cause au principal ; au demeurant, on ne trouve pas plus de trace d'un tel critère dans la directive elle-même. En sorte que s'il paraît légitime, éventuellement, d'en faire, à l'instar de la Cour dans l'affaire, un critère parmi d'autres de l'appréciation, ce critère ne peut suffire, seul, à notre sens, à caractériser le

cas spécifique excluant que l'obligation de surveillance soit considérée comme générale.
En définitive, la décision commentée nous paraît marquer une évolution notable dans l'appréciation par la Cour des obligations qui peuvent être mises à la charge des hébergeurs. Ce faisant, elle ne fait sans doute que s'inscrire dans l'évolution générale évoquée en introduction.
On ne peut s'empêcher de penser, cependant, que cette évolution induit une distorsion à un double niveau :
– d'une part, en affirmant l'absence d'une obligation générale de surveillance à la charge de l'hébergeur alors que, en pratique, il incombera à ce dernier de surveiller la totalité des informations stockées par les utilisateurs de son service ;
– d'autre part, en continuant d'appliquer la qualification d'hébergeur et le régime de responsabilité allégée qui y est associé à des prestataires dont il faut bien admettre qu'ils sont non seulement en capacité de contrôler les informations qu'ils stockent, mais aussi qu'ils procèdent effectivement à un tel contrôle, sur injonction du juge, voire de leur propre initiative dans une logique d'autorégulation.
C'est en réalité le principe même de l'application de ce régime aux opérateurs du web dit « 2.0 » qui est en cause.
Quoi qu'il en soit, l'arrêt rapporté se prononce également sur la portée territoriale de l'injonction qui peut être faite au prestataire d'hébergement.**II - La portée territoriale de l'injonction faite à un hébergeur de supprimer une information jugée illicite ou d'en bloquer l'accès**Quoique peu explicite, la question préjudicielle invitait également la Cour à se prononcer sur le point de savoir si l'injonction faite par une juridiction nationale à un hébergeur de bloquer ou de supprimer l'accès à une information identique ou équivalente à une information jugée par elle illicite pouvait avoir une portée mondiale.
La Cour répond que la directive 2000/31/CE ne s'y oppose pas, sous la réserve, néanmoins, du droit international pertinent, ce qui est sibyllin.
La justification de cette solution par la Cour est elle-même fort succincte : elle juge que la directive 2000/31/CE ne prévoit aucune limitation, notamment territoriale, à la portée des mesures que les États membres sont en droit d'adopter.
Néanmoins, comme, selon les considérants 58 et 60 de cette directive, la dimension mondiale du commerce électronique a conduit le législateur européen à considérer que les règles de l'Union (comprendre : énoncées par la directive) devaient rester en cohérence avec le droit international, les mesures adoptées au niveau national en application de la directive (et donc les injonctions telles que celle en cause au principal) doivent tenir « dûment » compte des règles dudit droit international.
De prime abord, on peut s'étonner de cette latitude laissée par la Cour aux juridictions nationales de conférer à leurs injonctions une portée mondiale, alors que, moins de dix jours avant l'arrêt rapporté, elle avait jugé que le déréférencement d'une page web ordonné par une juridiction nationale n'avait pas, en principe, de portée mondiale (tout en n'excluant pas, il est vrai, qu'une telle portée lui soit conférée dans certaines circonstances). Cette différence s'explique en réalité, selon l'avocat général, par les textes en cause dans les deux affaires : alors que le droit matériel des données

personnelles, qui fonde les demandes de déréférencement, est, on le sait, harmonisé au niveau européen, ce qui justifie qu'une injonction prise sur le fondement de ce droit ait une portée seulement européenne, tel n'est pas le cas des règles relatives à la protection de la réputation d'autrui, en cause dans l'affaire au principal. Or, relève par ailleurs l'avocat général, les injonctions faites aux hébergeurs sur le fondement de la directive 2000/31/CE relèvent du droit national.
En simplifiant, il résulte en substance de ces deux constats que la portée territoriale d'une injonction prise sur le fondement de cette directive ne relève pas du droit de l'Union mais du droit international public et privé non harmonisé. Et ce droit n'exclut pas qu'une injonction prononcée par un juge national puisse produire des effets extraterritoriaux, même si, selon l'avocat général, les juridictions nationales devraient plutôt, dans ce cas, adopter une attitude « d'autolimitation » en « n'allant pas au-delà de ce qui est nécessaire » pour assurer la protection de la personne lésée, et en respectant ainsi les règles de la « courtoisie internationale ».
L'avocat général relève par ailleurs que si les règles de compétence juridictionnelle, qui résultent du règlement (UE) no 1215/2012 du 12 décembre 2012 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale, sont quant à elles harmonisées au niveau de l'Union, elles n'excluent pas que la juridiction qu'elles désignent comme compétente prononce une injonction visant au retrait d'informations au-delà du territoire de l'État membre concerné, dans la mesure où l'étendue territoriale de sa compétence est universelle. En effet, selon la jurisprudence de la Cour, cette juridiction nationale est compétente pour statuer sur l'intégralité du dommage (en tout cas lorsqu'il s'agit de la juridiction de l'État membre du centre des intérêts de la victime et en matière d'atteinte à l'honneur ou à la réputation).
En synthèse, l'absence d'harmonisation, au niveau européen, des règles matérielles en cause au principal aboutit à ce résultat paradoxal que l'injonction prononcée par une juridiction nationale peut avoir un effet mondial, tandis que si les règles matérielles en cause en principal sont harmonisées, l'injonction prononcée par le juge national doit plutôt voir ses effets limités au territoire de l'Union.
Mais cela n'est, au fond, qu'une conséquence logique de la portée du droit de l'Union : ce qui échappe à sa sphère d'influence ne saurait, par définition, être limité par lui. Dès lors, la question en cause relève des seules règles du droit international, lesquelles peuvent, dans certains cas, admettre qu'une mesure nationale produise des effets extraterritoriaux. Il n'appartient simplement pas à la Cour de justice d'interférer.
Telle est en substance, croyons-nous, le sens de l'arrêt rapporté sur cette dernière question.
À prendre un peu de recul, on peut trouver que cet arrêt, en tout cas pour ce qui concerne ses réponses à la portée matérielle des injonctions faites à l'hébergeur, illustre fort bien l'idée que le juge, et spécialement le juge européen, décide d'abord de la solution qui lui paraît adéquate, et l'habille ensuite. La lecture comparée de l'arrêt rapporté et de l'arrêtde 2012 donne, à cet égard, le sentiment qu'il suffit à la Cour de justice d'utiliser à bon escient les considérants des textes qu'elle interprète, en sélectionnant ceux qui vont dans le sens souhaité, ainsi que les autres règles disponibles et notamment la Charte des droits fondamentaux, pour justifier la solution qui lui paraît

juste. Peut-être ne faut-il pas le regretter : c'est sans doute ce qui confère à la jurisprudence son adaptabilité.

Auteur(s) :

Vincent Varet - Docteur en droit - Avocat au barreau de Paris

Notes de bas de page :

1. C'est le nouveau régime de responsabilité des « fournisseurs de services de partage de contenus en ligne », créé par le fameux art. 17 de la dir. (UE) 2019/790 du 17 avr. 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique et modifiant les dir. 96/9/CE et 2001/29/CE. Ces dispositions devraient être transposées dans le cadre du projet de loi relatif à la communication audiovisuelle et à la souveraineté culturelle à l'ère numérique, présenté en Conseil des ministres le 5 déc 2019.
2. Proposition de loi no 1785 dite « Avia » visant à lutter contre la haine sur internet, adoptée en première lecture par l'Assemblée nationale le 9 juill 2019, enregistrée au Sénat sous le no 645 et examinée en première lecture en séance publique le 17 déc 2019. Il est vrai que les modifications adoptées par le Sénat à l'occasion de sa première lecture vident largement de substance le projet initial et le régime spécial de responsabilité qu'il comportait. Mais, à l'heure où nous écrivons ces lignes, l'Assemblée nationale, à l'origine du projet, n'a pas dit son dernier mot.
3. Et, en particulier, celui des fournisseurs d'hébergement, principaux concernés en pratique.
4. Ainsi, la Commission européenne se félicite-t-elle, dans un communiqué de presse en date du 4 févr. 2019, de l'efficacité du code de bonne conduite mis en place sous son égide pour lutter contre les discours de haine illégaux en ligne ; v. égal. le rapport Créer un cadre français de responsabilisation des réseaux sociaux : agir en France avec une ambition européenne, remis au secrétaire d'État en charge du numérique, Cédric O, en mai 2019. En doctrine, v. not. R.-O. Maistre, Point d'étape, vers un nouveau modèle de régulation des contenus, Légipresse 2019. 459 ; K. Favro et C. Zolinsky, De la régulation des contenus haineux à la régulation des contenus (illicites), Légipresse 2019. 461.
5. Puisque c'est d'eux principalement qu'il s'agit.
6. C'est-à-dire ne constituant pas une injure à raison de la race, de la religion, de l'ethnie, du sexe, de l'orientation sexuelle ou du handicap, visées par la proposition de loi Avia.
7. Précisons ici, pour ne plus y revenir, que la Cour juge, au préalable, que la faculté pour une autorité nationale de faire une injonction telle que celle faisant l'objet de la question préjudicielle est indépendante de la responsabilité éventuelle du prestataire d'hébergement sur le fondement de l'art. 14, § 1, de la directive. Autrement dit, une telle injonction peut être ordonnée, que le prestataire ait supprimé l'information illicite promptement dès qu'il en a eu connaissance, ou non.
8. Concl. av. gén. M. Szpunar, 4 juin 2019, pt 56.

9. En tout cas dans certaines versions linguistiques du texte, non contredites par les autres.

10. Concl. préc., pt 67.

11. Concl. préc., pts 59 et 73 ; de manière assez curieuse, l'avocat général tirait d'ailleurs de ce constat une conclusion distincte selon que l'injonction porte sur une information identique (dans cette hypothèse, selon lui, le fait que l'injonction porte sur les informations émises par tous les utilisateurs du service ne porte pas atteinte à l'art. 15, § 1, car elle reste ciblée sur un cas spécifique) ou équivalente (dans cette seconde hypothèse, il estimait que l'injonction allait au-delà d'un cas spécifique et imposait à l'hébergeur une obligation générale de surveillance, en sorte qu'elle était contraire à l'art. 15, § 1 – il n'a pas été suivi par la Cour sur ce dernier point).

12. CJUE 16 févr. 2012, aff. C-360/10, Sabam c/ Netlog, not. pt 46, D. 2012. 549, obs. C. Manara ; ibid. 2343, obs. J. Larrieu, C. Le Stanc et P. Tréfigny ; ibid. 2836, obs. P. Sirinelli ; Légipresse 2012. 138 et les obs. ; ibid. 167, comm. O. Bustin ; RSC 2012. 163, obs. J. Francillon ; RTD eur. 2012. 957, obs. E. Treppoz ; ibid. 2013. 675, obs. F. Benoît-Rohmer.

13. Ibid.

14. Arrêt Sabam, préc., pt 45.

15. CJUE 24 sept. 2019, aff. C-507/17, Google Llc c/ CNIL, AJDA 2019. 1839 ; D. 2019. 2022, note J.-L. Sauron ; ibid. 2266, obs. J. Larrieu, C. Le Stanc et P. Tréfigny ; Dalloz IP/IT 2019. 631, obs. N. Martial-Braz ; Légipresse 2019. 515 et les obs. ; ibid. 687, note N. Mallet-Poujol.

16. Concl. préc., pts 78, 79 et 90.

17. Concl. préc., pt 88.

18. Concl. préc., pts 92, 93, 95 et 100.

19. Concl. préc., pts 84 à 86.

20. CJUE 25 oct. 2011, aff. C-509/09 et C-161/10, eDate ADvertising et a., Légipresse 2011. 586 et les obs. ; ibid. 2012. 95, Étude J.-S. Bergé ; D. 2011. 2662 ; ibid. 2012. 1228, obs. H. Gaudemet-Tallon et F. Jault-Seseke ; ibid. 1279, chron. T. Azzi ; ibid. 1285, chron. S. Bollée et B. Haftel ; ibid. 2331, obs. L. d'Avout et S. Bollée ; Rev. crit. DIP 2012. 389, note H. Muir Watt ; RTD com. 2012. 423, obs. A. Marmisse-d'Abbadie d'Arrast ; ibid. 554, obs. F. Pollaud-Dulian ; RTD eur. 2011. 847, obs. E. Treppoz.