



Fiche thématique

Commerce électronique

et obligations contractuelles

Avant-propos

La réglementation du commerce électronique est au cœur de la directive 2000/31/CE¹ relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur, qui énonce les règles portant sur les exigences en matière d'établissement et d'information de prestataires de services de la société de l'information, ainsi que sur la responsabilité des prestataires intermédiaires.

Toutefois, le commerce électronique touche à une variété de domaines de la vie économique qui échappent à la réglementation de ladite directive, tels que les jeux de hasard, les questions relatives aux accords ou pratiques régis par le droit sur les ententes ainsi que la fiscalité (voir l'article 1^{er}, paragraphe 5, de la directive sur le commerce électronique, portant sur l'objectif et le champ d'application de ladite directive). De même, les droits d'auteur et les droits voisins, les droits des marques, la protection des consommateurs et la protection des données à caractère personnel relèvent du domaine du commerce électronique, mais sont régis par un ensemble de directives et règlements spéciaux.

La présente fiche thématique dresse une vue d'ensemble de la jurisprudence prononcée jusqu'au 30 avril 2024 en la matière. À cette fin, elle classe les arrêts principaux portant sur cet éventail de domaines dans deux sections, d'une part, les aspects relatifs aux obligations contractuelles entre les parties, et d'autre part, le cadre juridique régissant le commerce électronique.

Dans le cadre de cette fiche, les arrêts de la Cour, jugés les plus importants en la matière, ont été retenus, la plupart d'entre eux ayant été rendus par la grande chambre.

¹ 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 (« directive sur le commerce électronique ») (JO 2000, L 178, p. 1).

Liste des actes visés

RÈGLEMENTS

Règlement (CE) n° 40/94 du Conseil, du 20 décembre 1993, sur la marque communautaire (JO 1994, L 11, p. 1).

Règlement (CE) n° 2790/1999 de la Commission, du 22 décembre 1999, concernant l'application de l'article 81, paragraphe 3, du traité à des catégories d'accords verticaux et de pratiques concertées (JO 1999, L 336, p. 21).

Règlement (CE) n° 44/2001 du Conseil, du 22 décembre 2000, concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale (JO 2001, L 12, p. 1).

Règlement (CE) n° 864/2007 du Parlement européen et du Conseil, du 11 juillet 2007, sur la loi applicable aux obligations non contractuelles (Rome II) (JO 2007, L 199, p. 40).

Règlement (CE) n° 593/2008 du Parlement européen et du Conseil, du 17 juin 2008, sur la loi applicable aux obligations contractuelles (Rome I) (JO 2008, L 177, p. 6).

Règlement (UE) n° 330/2010 de la Commission, du 20 avril 2010, concernant l'application de l'article 101, paragraphe 3, du traité sur le fonctionnement de l'Union européenne à des catégories d'accords verticaux et de pratiques concertées (JO 2010, L 102, p. 1).

Règlement (UE) 2015/2120 du Parlement européen et du Conseil, du 25 novembre 2015, établissant des mesures relatives à l'accès à un internet ouvert et modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques et le règlement (UE) n° 531/2012 concernant l'itinérance sur les réseaux publics de communications mobiles à l'intérieur de l'Union (JO 2015, L 310, p. 1, et rectificatif JO 2016, L 27, p. 14).

Règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO 2016, L 119, p. 1).

Règlement (UE) 2017/1001 du Parlement européen et du Conseil, du 14 juin 2017, sur la marque de l'Union européenne (JO 2017, L 154, p. 1).

RÈGLEMENT D'EXÉCUTION

Règlement d'exécution (UE) n° 282/2011 du Conseil, du 15 mars 2011, portant mesures d'exécution de la directive 2006/112/CE relative au système commun de taxe sur la valeur ajoutée (JO 2011, L 77, p. 1).

DIRECTIVES

Directive 84/450/CEE du Conseil, du 10 septembre 1984, relative au rapprochement des dispositions législatives, réglementaires et administratives des États membres en matière de publicité trompeuse, telle que modifiée par la directive 2005/29/CE (JO 1984, L 250, p. 17).

Directive 89/104/CEE du Conseil, du 21 décembre 1988, rapprochant les législations des États membres sur les marques (JO 1989, L 40, p. 1).

Directive 93/13/CEE du Conseil, du 5 avril 1993, concernant les clauses abusives dans les contrats conclus avec les consommateurs (JO 1993, L 95, p. 29).

Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO 1995, L 281, p. 31).

Directive 97/7/CE du Parlement européen et du Conseil, du 20 mai 1997, concernant la protection des consommateurs en matière de contrats à distance (JO 1997, L 144., p. 19).

Directive 98/34/CE du Parlement européen et du Conseil, du 22 juin 1998, prévoyant une procédure d'information dans le domaine des normes et réglementations techniques et des règles relatives aux services de la société de l'information (JO 1998, L 204, p. 37), telle que modifiée par la directive 98/48/CE du Parlement européen et du Conseil, du 20 juillet 1998 (JO 1998, L 217, p. 18) (ci-après la « directive 98/34 »).

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 (« directive sur le commerce électronique ») (JO 2000, L 178, p. 1).

Directive 2001/29/CE du Parlement européen et du Conseil, du 22 mai 2001, sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information (JO 2001, L 167, p. 10).

Directive 2001/83/CE du Parlement européen et du Conseil, du 6 novembre 2001, instituant un code communautaire relatif aux médicaments à usage humain (JO 2001, L 311, p. 67), telle que modifiée par la directive 2011/62/UE du Parlement européen et du Conseil, du 8 juin 2011 (JO 2011, L 174, p. 74).

Directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO 2002, L 201, p. 37), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009 (JO 2009, L 337, p. 11).

Directive 2004/48/CE du Parlement européen et du Conseil, du 29 avril 2004, relative au respect des droits de propriété intellectuelle (JO 2004, L 157, p. 45 et rectificatif JO 2004, L 195, p. 16).

Directive 2005/29/CE du Parlement européen et du Conseil, du 11 mai 2005, relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs dans le marché intérieur et modifiant la directive 84/450/CEE du Conseil et les directives 97/7/CE, 98/27/CE et 2002/65/CE du Parlement européen et du Conseil et le règlement (CE) n° 2006/2004 du Parlement européen et du Conseil (JO 2005, L 149, p. 22).

Directive 2006/112/CE du Conseil, du 28 novembre 2006, relative au système commun de taxe sur la valeur ajoutée (JO 2006, L 347, p. 1).

Directive 2006/114/CE du Parlement européen et du Conseil, du 12 décembre 2006, en matière de publicité trompeuse et de publicité comparative (JO 2006, L 376, p. 21).

Directive 2006/115/CE du Parlement européen et du Conseil, du 12 décembre 2006, relative au droit de location et de prêt et à certains droits voisins du droit d'auteur dans le domaine de la propriété intellectuelle (JO 2006, L 376, p. 28).

Directive 2006/123/CE du Parlement européen et du Conseil, du 12 décembre 2006, relative aux services dans le marché intérieur (JO 2006, L 376, p. 36).

Directive 2007/64/CE du Parlement européen et du Conseil, du 13 novembre 2007, concernant les services de paiement dans le marché intérieur, modifiant les directives 97/7/CE, 2002/65/CE, 2005/60/CE ainsi que 2006/48/CE et abrogeant la directive 97/5/CE (JO 2007, L 319, p. 1).

Directive 2009/22/CE du Parlement européen et du Conseil, du 23 avril 2009, relative aux actions en cessation en matière de protection des intérêts des consommateurs (JO 2009, L 110, p. 30).

Directive 2009/24/CE du Parlement européen et du Conseil, du 23 avril 2009, concernant la protection juridique des programmes d'ordinateur (JO 2009, L 111, p. 16).

Directive (UE) 2015/1535 du Parlement européen et du Conseil, du 9 septembre 2015, prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information (JO 2015, L 241, p. 1).

Directive (UE) 2019/790 du Parlement européen et du Conseil, du 17 avril 2019, sur le droit d'auteur et les droits voisins dans le marché unique numérique et modifiant les directives 96/9/CE et 2001/29/CE (JO 2019, L 130, p. 92).

DÉCISIONS

Décision de la Commission du 26 juillet 2000 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » et par les questions souvent posées y afférentes, publiés par le ministère du commerce des États-Unis (JO 2000, L 215, p.7).

Décision de la Commission du 5 février 2010 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement européen et du Conseil (JO 2010, L 39, p. 5), telle que modifiée par la décision d'exécution (UE) 2016/2297 de la Commission du 16 décembre 2016 (JO 2016, L 344, p. 100).

Décision d'exécution (UE) 2016/1250 de la Commission, du 12 juillet 2016, conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis (JO 2016, L 207, p. 1).

Table des matières

AVANT-PROPOS	3
LISTE DES ACTES VISES	4
I. RELATIONS CONTRACTUELLES ENTRE LES PARTIES	9
1. Conclusion du contrat	9
2. Loi applicable/compétence judiciaire.....	13
3. Protection des consommateurs.....	19
4. Protection des données à caractère personnel	25
5. Droit d'auteur	56
II. CADRE JURIDIQUE RÉGISSANT LE COMMERCE ÉLECTRONIQUE	69
1. Publicité	69
2. Responsabilité des prestataires intermédiaires	82
3. Droit de la concurrence.....	89
4. Vente de médicaments et de dispositifs médicaux en ligne.....	96
5. Jeux de hasard	102
6. Économie du partage	105
7. TVA.....	111

I. Relations contractuelles entre les parties

1. Conclusion du contrat

Arrêt du 5 juillet 2012, Content Services (C-49/11, EU:C:2012:419)

La société Content Services exploitait une filiale à Mannheim (Allemagne) et proposait différents services en ligne sur son site Internet, rédigé en langue allemande et accessible également en Autriche. Par ce site, il était notamment possible de télécharger des logiciels gratuits ou des versions d'essai de logiciels payants. Avant de passer leur commande, les internautes devaient remplir un formulaire d'inscription et cocher une case désignée dans le formulaire pour déclarer qu'ils acceptaient les clauses générales de vente et qu'ils renonçaient à leur droit de rétractation.

Ces informations n'étaient pas directement présentées aux internautes. Ces derniers pouvaient toutefois les visualiser en cliquant sur un lien figurant sur la page qu'ils remplissaient pour la conclusion dudit contrat. La conclusion d'un contrat était impossible si ladite case n'avait pas été cochée. Ensuite, l'internaute concerné recevait, de la part de Content Services, un courriel qui ne comportait aucune information sur le droit de rétractation, mais de nouveau un lien pour les visualiser. L'Oberlandesgericht Wien (tribunal régional supérieur de Vienne, Autriche) a posé à la Cour une question préjudiciable portant sur l'interprétation de l'article 5, paragraphe 1, de la directive 97/7/CE². Il a demandé si une pratique commerciale qui consiste à ne rendre accessibles au consommateur les informations prévues à cette disposition que par un lien sur un site Internet de l'entreprise concernée satisfait aux exigences de ladite disposition.

Selon la Cour, l'article 5, paragraphe 1, de la directive 97/7/CE doit être interprété en ce sens que cette pratique commerciale ne satisfait pas aux exigences de ladite disposition, dès lors que ces informations ne sont ni « fournies » par cette entreprise ni « reçues » par le consommateur et qu'un site Internet ne peut être considéré comme un « support durable ».

En effet, le consommateur doit recevoir la confirmation desdites informations, sans qu'un comportement actif de celui-ci ne soit requis. En outre, pour qu'un site Internet soit considéré comme un support durable, il doit garantir au consommateur, de manière analogue à un support papier, la possession des informations mentionnées à cette disposition pour lui permettre de faire valoir, le cas échéant, ses droits. À cet égard, il doit permettre au consommateur de stocker les informations qui lui ont été adressées personnellement, garantir l'absence d'altération de leur contenu ainsi que

² Directive 97/7/CE du Parlement européen et du Conseil, du 20 mai 1997, concernant la protection des consommateurs en matière de contrats à distance (JO 1997, L 144, p. 19).

leur accessibilité pendant une durée appropriée, et offrir au consommateur la possibilité de les reproduire telles quelles.

Arrêt du 25 janvier 2017, BAWAG (C-375/15, EU:C:2017:38)

La banque BAWAG, qui exerçait son activité sur le territoire autrichien, utilisait une clause contractuelle standardisée en vue de l'adhésion des consommateurs aux services bancaires en ligne (« e-banking »).

Selon ladite clause, « les informations et explications que la banque doit fournir au client ou mettre à sa disposition seront transmises par voie postale ou par voie électronique, dans le cadre du e-banking ». Les informations pouvaient être transmises par le biais d'un système de messagerie intégré dans les comptes en ligne. Les consommateurs pouvaient consulter, reproduire et télécharger les courriels. Les messages qui se trouvaient dans les comptes en ligne « e-banking » y subsistaient sans modification et n'étaient pas supprimés pendant une période adaptée aux fins de l'information de ces consommateurs, de telle sorte qu'ils pouvaient être consultés et reproduits à l'identique par voie électronique ou imprimés. Toutefois, les consommateurs n'étaient pas informés, par une autre voie, de la réception d'un nouveau courriel.

L'Oberster Gerichtshof (Cour suprême, Autriche) a saisi la Cour à titre préjudiciel afin de savoir si l'article 41, paragraphe 1, de la directive 2007/64/CE³, lu en combinaison avec l'article 36, paragraphe 1, de la même directive, doit être interprété en ce sens qu'une information transmise par le biais de la boîte électronique intégrée dans une plateforme de banque en ligne est « fournie sur un support durable ».

D'après la Cour, il convient de considérer que certains sites Internet doivent être qualifiés de « supports durables », au sens de l'article 4, point 25, de ladite directive.

Toutefois, les modifications du contrat-cadre, qui sont transmises par le prestataire de services de paiement à l'utilisateur de ces services au moyen d'une boîte aux lettres électronique, ne sauraient être considérées comme étant fournies sur un support durable que si les deux conditions suivantes sont réunies :

- ce site Internet permet uniquement à cet utilisateur de stocker et reproduire des informations de manière qu'il puisse y accéder pendant une durée appropriée ;
- la transmission de ces informations est accompagnée d'un comportement actif du prestataire de services de paiement destiné à porter à la connaissance de cet utilisateur la disponibilité desdites informations.

L'envoi d'un courriel à l'adresse habituellement utilisée par l'utilisateur de ces services pour communiquer avec d'autres personnes, et dont les parties ont convenu de

³ Directive 2007/64/CE du Parlement européen et du Conseil, du 13 novembre 2007, concernant les services de paiement dans le marché intérieur, modifiant les directives 97/7/CE, 2002/65/CE, 2005/60/CE ainsi que 2006/48/CE et abrogeant la directive 97/5/CE (JO 2007, L 319, p. 1).

l'utilisation dans un contrat-cadre conclu entre le prestataire de services de paiement et cet utilisateur, peut également constituer un tel comportement. L'adresse ainsi choisie ne saurait, cependant, être celle dédiée audit utilisateur sur le site Internet de banque en ligne géré par le prestataire de services de paiement.

Arrêt du 15 septembre 2020 (grande chambre), Telenor Magyarország (C-807/18 et C-39/19, EU:C:2020:708)

La société Telenor, établie en Hongrie, fournit notamment des services d'accès à Internet. Parmi les services proposés à ses clients figurent deux offres groupées d'accès préférentiel (dites à « tarif nul ») ayant pour particularité que le trafic de données généré par certains services et applications spécifiques n'est pas décompté dans la consommation du volume de données acheté par les clients. En outre, ces derniers peuvent, une fois épuisé ce volume de données, continuer à utiliser sans restrictions ces applications et ces services spécifiques, pendant que des mesures de blocage ou de ralentissement du trafic sont appliquées aux autres applications et services disponibles.

Après avoir ouvert deux procédures visant à contrôler la conformité de ces deux offres groupées avec le règlement 2015/2120 établissant des mesures relatives à l'accès à un Internet ouvert⁴, l'autorité hongroise des communications et des médias a adopté deux décisions par lesquelles elle a considéré que celles-ci ne respectaient pas l'obligation générale de traitement égal et non discriminatoire du trafic énoncée à l'article 3, paragraphe 3, de ce règlement et que Telenor devait y mettre fin.

Saisie de deux recours par cette dernière, la Fővárosi Törvényszék (cour de Budapest-Capitale, Hongrie) a décidé d'interroger la Cour à titre préjudiciel afin de savoir comment doivent être interprétés et appliqués les paragraphes 1 et 2 de l'article 3 du règlement 2015/2120, qui garantissent un certain nombre de droits⁵ aux utilisateurs finals de services d'accès à Internet et qui interdisent aux fournisseurs de tels services de mettre en place des accords ou des pratiques commerciales limitant l'exercice de ces droits, ainsi que le paragraphe 3 de cet article 3, qui énonce une obligation générale de traitement égal et non discriminatoire du trafic.

Dans son arrêt du 15 septembre 2020, la Cour, statuant en grande chambre, a interprété pour la première fois le règlement 2015/2120, qui consacre le principe essentiel d'ouverture d'Internet (plus familièrement dénommé « neutralité du Net »).

S'agissant, en premier lieu, de l'interprétation de l'article 3, paragraphe 2, du règlement 2015/2120, lu conjointement avec l'article 3, paragraphe 1, de ce règlement, la

⁴ Règlement (UE) 2015/2120 du Parlement européen et du Conseil, du 25 novembre 2015, établissant des mesures relatives à l'accès à un internet ouvert et modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques et le règlement (UE) n° 531/2012 concernant l'itinérance sur les réseaux publics de communications mobiles à l'intérieur de l'Union (JO 2015, L 310, p. 1, et rectificatif JO 2016, L 27, p. 14).

⁵ Droit pour les utilisateurs finals d'accéder aux applications, aux contenus et aux services ainsi que de les utiliser, mais également droit de fournir des applications, des contenus et des services ainsi que d'utiliser les terminaux de leur choix.

Cour a observé que la seconde de ces dispositions prévoit que les droits qu'elle garantit aux utilisateurs finals de services d'accès à Internet ont vocation à être exercés « par l'intermédiaire de leur service d'accès à Internet », et que la première disposition exige qu'un tel service n'implique pas de limitation de l'exercice de ces droits. Par ailleurs, il découle de l'article 3, paragraphe 2, dudit règlement que les services d'un fournisseur d'accès à Internet donné doivent être évalués au regard de cette exigence, par les autorités réglementaires nationales⁶ et sous le contrôle des juridictions nationales compétentes, en prenant en considération tant les accords conclus par ce fournisseur avec les utilisateurs finals que les pratiques commerciales mises en œuvre par ledit fournisseur.

Dans ce contexte, la Cour, après avoir apporté un ensemble de précisions générales sur le sens des notions d'« accords », de « pratiques commerciales » et d'« utilisateurs finals »⁷ figurant dans le règlement 2015/2120, a estimé que la conclusion d'accords par lesquels des clients donnés souscrivent à des offres groupées combinant un « tarif nul » et des mesures de blocage ou de ralentissement du trafic lié à l'utilisation de services et d'applications autres que les services et applications spécifiques relevant de ce « tarif nul » est susceptible de limiter l'exercice des droits des utilisateurs finals, au sens de l'article 3, paragraphe 2, de ce règlement, sur une partie significative du marché. En effet, de telles offres groupées sont de nature à amplifier l'utilisation des applications et des services privilégiés et, corrélativement, à raréfier l'utilisation des autres applications et des autres services disponibles, compte tenu des mesures par lesquelles le fournisseur de services d'accès à Internet rend cette dernière utilisation techniquement plus difficile, voire impossible. En outre, plus le nombre de clients qui concluent de tels accords est important, plus l'incidence cumulée de ces accords est susceptible, compte tenu de son ampleur, d'engendrer une limitation importante de l'exercice des droits des utilisateurs finals, voire de porter atteinte à l'essence même de ces droits.

En second lieu, s'agissant de l'interprétation de l'article 3, paragraphe 3, du règlement 2015/2120, la Cour a relevé que, pour constater une incompatibilité avec cette disposition, aucune évaluation de l'incidence de mesures de blocage ou de ralentissement du trafic sur l'exercice des droits des utilisateurs finals n'est requise. En effet, cette disposition ne prévoit pas une telle exigence pour apprécier le respect de l'obligation générale de traitement égal et non discriminatoire du trafic y figurant. En outre, la Cour a jugé que, dès lors que des mesures de ralentissement ou de blocage du trafic sont fondées non pas sur des différences objectives entre les exigences techniques en matière de qualité de service de certaines catégories spécifiques de trafic, mais sur des considérations d'ordre commercial, ces mesures sont à considérer, en tant que telles, comme étant incompatibles avec ladite disposition.

⁶ Sur le fondement de l'article 5 du règlement 2015/2120.

⁷ Cette dernière notion englobe toutes les personnes physiques ou morales qui utilisent ou qui demandent un service de communication électronique accessible au public. Par ailleurs, elle inclut aussi bien les personnes physiques ou morales qui utilisent ou qui demandent des services d'accès à Internet en vue d'accéder à des contenus, à des applications et à des services que celles qui s'appuient sur l'accès à Internet pour fournir des contenus, des applications et des services.

En conséquence, des offres groupées telles que celles soumises au contrôle de la juridiction de renvoi sont, de manière générale, susceptibles de violer tant le paragraphe 2 de l'article 3 du règlement 2015/2120 que le paragraphe 3 de cet article, étant précisé que les autorités et les juridictions nationales compétentes peuvent les examiner d'emblée au regard de la seconde de ces dispositions.

2. Loi applicable/compétence judiciaire

Arrêt du 28 juillet 2016, Verein für Konsumenteninformation (C-191/15, EU:C:2016:612)

L'entreprise Amazon EU Sàrl, établie au Luxembourg, procédait à des ventes électroniques de biens à des consommateurs établis dans différents États membres. Dans l'affaire au principal, l'association autrichienne de défense des intérêts des consommateurs (Verein für Konsumenteninformation) avait introduit une action en cessation, fondée sur la directive 2009/22/CE⁸, et alléguant que les clauses contractuelles utilisées par Amazon étaient contraires à des interdictions légales ou aux bonnes pratiques.

Saisi par l'association autrichienne, l'Oberster Gerichtshof (Cour suprême, Autriche) a cherché à savoir si une clause figurant dans les conditions générales de vente d'un contrat conclu par voie électronique entre un professionnel et un consommateur, selon laquelle la loi de l'État membre du siège de ce professionnel régit ce contrat, est abusive au sens de l'article 3, paragraphe 1, de la directive 93/13/CEE⁹. En outre, l'Oberster Gerichtshof s'est demandé si le traitement de données à caractère personnel par une entreprise est soumis, en vertu de l'article 4, paragraphe 1, sous a), de la directive 95/46/CE¹⁰, au droit de l'État membre vers lequel cette entreprise dirige ses activités.

Selon la Cour, les règlements Rome I¹¹ et Rome II¹² doivent être interprétés en ce sens que la loi applicable à une telle action en cessation doit être déterminée conformément à l'article 6, paragraphe 1, du règlement Rome II, dès lors que les atteintes à l'ordre juridique résultent de l'utilisation de clauses abusives. En revanche, la loi applicable à l'appréciation de la clause contractuelle en cause doit être déterminée en application du

⁸ Directive 2009/22/CE du Parlement européen et du Conseil, du 23 avril 2009, relative aux actions en cessation en matière de protection des intérêts des consommateurs (JO 2009, L 110, p. 30).

⁹ Directive 93/13/CEE du Conseil, du 5 avril 1993, concernant les clauses abusives dans les contrats conclus avec les consommateurs (JO 1993, L 95, p. 29).

¹⁰ Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO 1995, L 281, p. 31).

¹¹ Règlement (CE) n° 593/2008 du Parlement européen et du Conseil, du 17 juin 2008, sur la loi applicable aux obligations contractuelles (Rome I) (JO 2008, L 177, p. 6).

¹² Règlement (CE) n° 864/2007 du Parlement européen et du Conseil, du 11 juillet 2007, sur la loi applicable aux obligations non contractuelles (Rome II) (JO 2007, L 199, p. 40).

règlement Rome I, que cette appréciation soit effectuée dans le cadre d'une action individuelle ou dans celui d'une action collective.

Toutefois, il découle de l'article 6, paragraphe 2, du règlement Rome I que le choix de la loi applicable est sans préjudice de l'application des dispositions impératives prévues par la loi du pays où résident les consommateurs dont les intérêts sont défendus au moyen d'une action en cessation. Ces dispositions peuvent comprendre celles qui transposent la directive 93/13/CEE, pour autant qu'elles assurent un niveau de protection plus élevé au consommateur.

Ainsi, une clause, qui n'a pas fait l'objet d'une négociation individuelle, selon laquelle la loi de l'État membre du siège du professionnel régit le contrat conclu par voie électronique avec un consommateur est abusive au sens de l'article 3, paragraphe 1, de la directive 93/13/CEE, pour autant qu'elle induise ce consommateur en erreur en lui donnant l'impression que seule la loi de cet État s'applique au contrat, sans l'informer du fait qu'il bénéficie également de la protection des dispositions impératives du droit qui seraient applicables en l'absence de cette clause.

Par ailleurs, l'article 4, paragraphe 1, sous a), de la directive 95/46/CE doit être interprété en ce sens qu'un traitement de données à caractère personnel effectué par une entreprise de commerce électronique est régi par le droit de l'État membre vers lequel cette entreprise dirige ses activités s'il s'avère que cette entreprise procède au traitement des données en question dans le cadre des activités d'un établissement situé dans cet État membre. Il convient d'évaluer tant le degré de stabilité de l'installation que la réalité de l'exercice des activités dans l'État membre en question.

Arrêt du 7 décembre 2010 (grande chambre), Pammer et Alpenhof (C-585/08 et C-144/09, EU:C:2010:740)

Les affaires jointes Pammer et Alpenhof portent sur deux litiges principaux concernant des questions similaires. Dans l'affaire Pammer, un consommateur domicilié en Autriche s'était opposé à une compagnie de navires de charge, établie en Allemagne, au sujet du remboursement du prix du voyage. Ce consommateur s'était plaint que le navire et le déroulement du voyage ne correspondaient pas à la description donnée sur le site Internet de l'agence, également établie en Allemagne, qui avait joué le rôle d'intermédiaire en offrant de tels voyages.

La juridiction autrichienne de première instance s'était estimée compétente. La juridiction d'appel, en revanche, avait déclaré que les juridictions autrichiennes étaient incompétentes. La question préjudicielle de l'Oberster Gerichtshof (Cour suprême, Autriche) visait à savoir comment il convient d'interpréter la notion de contrat combinant voyage et hébergement pour un prix forfaitaire au sens de l'article 15, paragraphe 3, pour lequel les dispositions de la section 4 du chapitre II du règlement

(CE) n° 44/2001¹³ sont applicables. Dans un deuxième temps, le juge de renvoi a souhaité savoir si le fait que l'attention du consommateur autrichien a été attirée sur le voyage par la consultation du site Internet de l'agence intermédiaire, sans que la réservation du voyage soit effectuée via Internet, suffit pour pouvoir constater la compétence des juridictions autrichiennes.

La deuxième affaire, Alpenhof, avait opposé une société autrichienne exploitant un hôtel et ayant son siège en Autriche, à un consommateur domicilié en Allemagne au sujet du paiement d'une facture pour des prestations hôtelières convenues par échange de courriels sur la base des informations fournies sur le site Internet de la société requérante. Les juridictions autrichiennes avaient rejeté le recours, en estimant qu'elles étaient incompétentes.

Selon la Cour, un contrat ayant pour objet un voyage en cargo peut constituer un contrat de transport qui, pour un prix forfaitaire, combine voyage et hébergement si ledit voyage en cargo comporte, pour un prix forfaitaire, également le logement et que ce voyage excède 24 heures.

Afin de déterminer si un commerçant, dont l'activité est présentée sur son site Internet ou sur celui d'un intermédiaire, peut être considéré comme « dirigeant » son activité vers l'État membre sur le territoire duquel le consommateur a son domicile, il convient de vérifier si ce commerçant envisageait de commercer avec des consommateurs domiciliés dans un ou plusieurs États membres.

Les éléments suivants, dont la liste n'est pas exhaustive, sont susceptibles de constituer des indices permettant de considérer que l'activité du commerçant est dirigée vers l'État membre du domicile du consommateur, à savoir la nature internationale de l'activité, la mention d'itinéraires à partir d'autres États membres pour se rendre au lieu où le commerçant est établi, l'utilisation d'une langue ou d'une monnaie autres que la langue ou la monnaie habituellement utilisées dans l'État membre dans lequel est établi le commerçant avec la possibilité de réserver et de confirmer la réservation dans cette autre langue. En revanche, la simple accessibilité du site Internet du commerçant ou de celui de l'intermédiaire dans l'État membre sur le territoire duquel le consommateur est domicilié est insuffisante. Il en va de même de la mention d'une adresse électronique ainsi que d'autres coordonnées ou de l'emploi d'une langue ou d'une monnaie qui sont la langue et/ou la monnaie habituellement utilisées dans l'État membre dans lequel le commerçant est établi.

Arrêt du 6 septembre 2012, Mühlleitner (C-190/11, [EU:C:2012:542](#))

L'affaire au principal opposait la consommatrice M^{me} Daniela Mühlleitner, domiciliée en Autriche, à des vendeurs de voitures domiciliés à Hambourg, en Allemagne, au sujet de

¹³ Règlement (CE) n° 44/2001 du Conseil, du 22 décembre 2000, concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale (JO 2001, L 12, p. 1).

l'achat d'une voiture. Après avoir relevé leurs coordonnées sur leur site Internet, M^{me} Mühlleitner avait téléphoné aux vendeurs depuis l'Autriche, où elle avait reçu par la suite une offre par courriel. La conclusion du contrat avait cependant eu lieu chez les vendeurs en Allemagne.

Par la suite, la juridiction de première instance, le Landesgericht Wels (le tribunal régional, Autriche), avait rejeté le recours en se déclarant incompétente.

L'Oberlandesgericht Linz (tribunal régional supérieur de Linz, Autriche) avait confirmé la décision en rappelant qu'un site Internet purement « passif » ne suffisait pas pour considérer qu'une activité est dirigée vers l'État du consommateur. M^{me} Mühlleitner avait introduit un recours en « Revision » contre ce jugement devant l'Oberster Gerichtshof (Cour suprême, Autriche). Celui-ci a renvoyé à la Cour la question de savoir si l'application de l'article 15, paragraphe 1, sous c), du règlement Bruxelles I¹⁴ suppose que le contrat entre le consommateur et le professionnel ait été conclu à distance.

La Cour a dit pour droit que l'article 15, paragraphe 1, sous c), du règlement (CE) n° 44/2001, doit être interprété en ce sens qu'il n'exige pas que le contrat entre le consommateur et le professionnel ait été conclu à distance.

En premier lieu, cette disposition ne conditionne pas explicitement son application au fait que les contrats soumis à son champ d'application aient été conclus à distance. En deuxième lieu, s'agissant de l'interprétation téléologique de ladite disposition, l'adjonction d'une condition liée à la conclusion des contrats de consommation à distance irait à l'encontre de l'objectif poursuivi par cette disposition, notamment celui de la protection des consommateurs, parties faibles au contrat. En troisième lieu, la condition essentielle à laquelle est subordonnée l'application de l'article 15, paragraphe 1, sous c), dudit règlement est celle liée à l'activité commerciale ou professionnelle dirigée vers l'État du domicile du consommateur. À cet égard, tant la prise de contact à distance que la réservation d'un bien ou d'un service à distance ou, a fortiori, la conclusion d'un contrat de consommation à distance sont des indices de rattachement du contrat à une telle activité.

Arrêt du 17 octobre 2013, Emrek (C-218/12, [EU:C:2013:666](#))

M. Emrek, domicilié à Sarrebruck (Allemagne), était à la recherche d'une voiture et avait appris par des connaissances l'existence de l'entreprise de M. Sabranovic. Ce dernier exploitait à Spicheran (France) une entreprise de commercialisation de véhicules d'occasion. Il tenait également un site Internet qui contenait les coordonnées de son entreprise, y compris des numéros de téléphone français et un numéro de téléphone portable allemand, assortis des préfixes internationaux respectifs. Toutefois, M. Emrek n'avait pas pris connaissance de l'entreprise par le site Internet. Ainsi, M. Emrek, en

¹⁴ Règlement (CE) n° 44/2001 du Conseil, du 22 décembre 2000, concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale (JO 2001, L 12, p. 1).

qualité de consommateur, avait conclu avec M. Sabranovic, dans l'établissement de ce dernier, un contrat écrit de vente d'un véhicule d'occasion.

Par la suite, M. Emrek a introduit une action contre M. Sabranovic en matière de garantie devant l'Amtsgericht Saarbrücken (tribunal de district de Sarrebrück, Allemagne). Ladite juridiction a jugé qu'elle n'était pas compétente. M. Emrek a interjeté appel de cette décision devant la juridiction de renvoi, le Landgericht Saarbrücken (tribunal régional de Sarrebrück, Allemagne). Cette dernière a cherché à savoir s'il faut, pour l'application de l'article 15, paragraphe 1, sous c), du règlement (CE) n° 44/2001, un lien de causalité entre les activités du commerçant dirigées vers l'État membre du domicile du consommateur au moyen d'Internet et la conclusion de contrats.

La Cour a rappelé qu'elle a identifié, dans son arrêt Pammer et Alpenhof (C-585/08 et C-144/09), une liste non exhaustive d'indices susceptibles d'aider une juridiction nationale à apprécier si la condition essentielle de l'activité commerciale dirigée vers l'État membre du domicile du consommateur est remplie.

Elle a conclu que l'article 15, paragraphe 1, sous c), du règlement (CE) n° 44/2001, doit être interprété en ce sens qu'il n'exige pas l'existence d'un lien de causalité entre le moyen employé pour diriger l'activité commerciale ou professionnelle vers l'État membre du domicile du consommateur, à savoir un site Internet, et la conclusion du contrat avec ce consommateur. Toutefois, l'existence d'un tel lien de causalité constitue un indice de rattachement du contrat à une telle activité.

Arrêt du 21 mai 2015, El Majdoub (C-322/14, EU:C:2015:334)

Le litige au principal concernait la vente d'un véhicule automobile par le biais d'un site Internet. Les conditions générales de vente accessibles sur ce site contenaient une convention attributive de juridiction en faveur d'un tribunal situé dans un État membre. La fenêtre contenant lesdites conditions générales de vente ne s'ouvrait pas automatiquement lors de l'enregistrement ni lors de chaque opération d'achat, l'acheteur devant cocher une case spécifique pour accepter ces conditions.

La Cour a été appelée par le Landgericht Krefeld (tribunal régional de Krefeld, Allemagne) à établir si la validité d'une clause attributive de juridiction est remise en cause dans l'hypothèse de l'emploi de la technique d'acceptation par « clic ».

En premier lieu, concernant la réalité du consentement des intéressés, qui est l'un des objectifs de l'article 23, paragraphe 1, du règlement (CE) n° 44/2001, la Cour a constaté que l'acheteur en cause au principal avait accepté les conditions générales en cause de manière expresse, en cochant la case correspondante sur le site Internet du vendeur concerné. En second lieu, elle a jugé qu'il ressort d'une interprétation littérale de l'article 23, paragraphe 2, de ce règlement que celui-ci exige que la « possibilité » soit offerte de consigner durablement la convention attributive de juridiction, indépendamment de la question de savoir si le texte des conditions générales a

effectivement été consigné durablement par l'acheteur après ou avant qu'il ait coché la case indiquant qu'il accepte lesdites conditions.

À cet égard, la Cour a observé que la finalité de cette disposition est d'assimiler certaines formes de transmissions électroniques à la forme écrite, en vue de simplifier la conclusion des contrats par voie électronique, la transmission des informations concernées étant réalisée également si ces informations sont accessibles au moyen d'un écran. Pour que la transmission électronique puisse offrir les mêmes garanties, notamment en matière de preuve, il suffit qu'il soit « possible » de sauvegarder et d'imprimer les informations avant la conclusion du contrat. Par conséquent, dès lors que la technique d'acceptation par « clic » rend possible l'impression et la sauvegarde du texte des conditions générales avant la conclusion du contrat, la circonstance que la page Internet contenant ces conditions ne s'ouvre pas automatiquement lors de l'enregistrement sur le site Internet et lors de chaque opération d'achat ne saurait remettre en cause la validité de la convention attributive de juridiction. Une telle technique d'acceptation constitue, dès lors, une transmission par voie électronique au sens de l'article 23, paragraphe 2, du règlement (CE) n° 44/2001.

Arrêt du 25 janvier 2018, Schrems (C-498/16, EU:C:2018:37)

M. Maximilian Schrems était un utilisateur privé du réseau social Facebook depuis 2008. Il avait initié des actions publiques contre la société Facebook Ireland Limited. En outre, depuis l'année 2011, il avait ouvert une page Facebook qu'il avait enregistrée et créée lui-même, afin d'informer les internautes de son action. Il avait fondé une association à but non lucratif, ayant pour objectif la réalisation du droit fondamental à la protection des données et le soutien financier de procès modèles.

Dans le cadre d'un litige opposant M. Maximilian Schrems à Facebook Ireland Limited, au sujet de demandes de constatation, de cessation, d'information, de reddition de comptes de Facebook, l'Oberster Gerichtshof (Cour suprême, Autriche) s'est interrogé sur la question de savoir si l'article 15 du règlement (CE) n° 44/2001 doit être interprété de sorte qu'une personne perd sa qualité de consommateur si, après avoir utilisé un compte privé Facebook pendant plusieurs années, elle publie des livres, perçoit des honoraires pour des conférences ou gère des sites Internet. La juridiction de renvoi s'est demandé également si l'article 16 dudit règlement doit être interprété en ce sens qu'un consommateur peut faire valoir en même temps que ses propres droits relevant d'un contrat de consommateur, des droits similaires d'autres consommateurs qui sont domiciliés soit dans le même État membre, soit dans un autre État membre, soit dans un État tiers.

La Cour a précisé que la notion de « consommateur » doit être interprétée de manière autonome et restrictive. Pour déterminer si l'article 15 est applicable, la finalité du contrat conclu entre les parties doit avoir pour objet un usage autre que professionnel du bien ou du service concerné. En ce qui concerne une personne qui conclut un contrat

pour un usage se rapportant en partie à son activité professionnelle, le lien dudit contrat avec l'activité professionnelle de l'intéressé serait si tenu qu'il deviendrait marginal et, partant, n'aurait qu'un rôle négligeable dans le contexte de l'opération.

Ensuite, la Cour a relevé que le consommateur n'est protégé en tant que tel que s'il est personnellement demandeur ou défendeur dans une procédure. Dès lors, le demandeur qui n'est pas lui-même partie au contrat de consommation en cause ne saurait bénéficier du for du consommateur. Ces considérations doivent également valoir à l'égard d'un consommateur cessionnaire de droits d'autres consommateurs. En effet, l'article 16, paragraphe 1, implique nécessairement la conclusion d'un contrat par le consommateur avec le professionnel mis en cause.

Par ailleurs, une cession de créances ne saurait, en elle-même, avoir d'incidence sur la détermination de la juridiction compétente. Il s'ensuit que la compétence des juridictions ne saurait être établie au moyen d'une concentration de plusieurs droits dans le chef d'un seul requérant. Le règlement ne s'applique pas à l'action d'un consommateur comme dans le cas présent.

3. Protection des consommateurs

Arrêt du 16 octobre 2008, Bundesverband der Verbraucherzentralen (C-298/07, [EU:C:2008:572](#))

DIV, une compagnie d'assurance automobile, offrait ses services exclusivement sur Internet. Sur les pages de son site Internet, elle avait mentionné son adresse postale ainsi que son adresse de courrier électronique, mais pas son numéro de téléphone. Celui-ci n'était communiqué qu'après la conclusion d'un contrat d'assurance. En revanche, les personnes intéressées par les services de DIV avaient la possibilité de lui poser des questions au moyen d'un formulaire de contact sur Internet dont les réponses étaient communiquées par courrier électronique. Le Bundesverband der Verbraucherzentralen, fédération allemande des associations de consommateurs, avait cependant estimé que DIV était tenu d'indiquer son numéro de téléphone sur son site Internet. En effet, ce serait l'unique moyen de garantir une communication directe.

Par la suite, le Bundesgerichtshof (Cour fédérale de justice, Allemagne) a décidé de poser à la Cour la question de savoir si l'article 5, paragraphe 1, sous c), de la directive 2000/31/CE¹⁵ exige l'indication d'un numéro de téléphone.

La Cour de justice a jugé que l'article 5, paragraphe 1, sous c), de la directive 2000/31/CE doit être interprété en ce sens que le prestataire de services est tenu de fournir aux destinataires du service, avant toute conclusion de contrat avec ces derniers, en sus de

¹⁵ 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 (JO 2000, L 178, p. 1).

son adresse de courrier électronique, d'autres informations permettant une prise de contact rapide ainsi qu'une communication directe et efficace.

Ces informations ne doivent pas obligatoirement correspondre à un numéro de téléphone. Elles peuvent résider dans un formulaire de contact électronique, au moyen duquel les destinataires du service peuvent s'adresser au moyen d'Internet au prestataire de services et auquel celui-ci répond par courrier électronique, sauf dans des situations où un destinataire du service, se trouvant, après la prise de contact par voie électronique avec le prestataire de services, privé d'accès au réseau électronique, demande à ce dernier l'accès à une voie de communication non électronique.

Arrêt du 3 septembre 2009, Messner (C-489/07, [EU:C:2009:502](#))

M^{me} Messner, une consommatrice allemande, avait effectué une rétractation de l'achat d'un ordinateur portable au moyen d'Internet. Le vendeur de l'ordinateur avait refusé d'éliminer gratuitement un défaut apparu huit mois après l'achat. Par la suite, M^{me} Messner avait déclaré qu'elle révoquait le contrat de vente et avait proposé de renvoyer l'ordinateur portable au vendeur contre remboursement concomitant. Cette révocation avait été effectuée dans les délais prévus par le Bürgerliches Gesetzbuch (code civil allemand) dans la mesure où M^{me} Messner n'avait pas reçu les informations, prévues par les dispositions de ce code, de nature à faire courir le délai de rétractation. M^{me} Messner avait réclamé la somme de 278 euros devant l'Amtsgericht Lahr (tribunal de district de Lahr, Allemagne). Le vendeur s'était opposé à cette demande en justice en faisant valoir que M^{me} Messner lui devait, en tout état de cause, une indemnité compensatrice correspondant à quasiment huit mois pleins d'utilisation de l'ordinateur portable.

Dans son arrêt, la Cour a relevé que les dispositions de l'article 6, paragraphes 1, deuxième phrase, et 2, de la directive 97/7/CE¹⁶ doivent être interprétées en ce sens qu'elles s'opposent à ce qu'une réglementation nationale prévoie de manière générale la possibilité pour le vendeur de réclamer au consommateur une indemnité compensatrice pour l'utilisation d'un bien acquis par un contrat à distance dans le cas où ce dernier a exercé son droit de rétractation dans les délais.

En effet, dans le cas où le consommateur devrait verser une telle indemnité compensatrice pour le seul fait qu'il a eu la possibilité d'utiliser le bien pendant le temps où celui-ci s'est trouvé en sa possession, il ne pourrait exercer son droit de rétractation seulement contre paiement de ladite indemnité. Une telle conséquence serait en claire contradiction avec le libellé et la finalité de l'article 6, paragraphes 1, deuxième phrase, et 2, de la directive 97/7/CE et priverait notamment le consommateur de la possibilité de

¹⁶ Directive 97/7/CE du Parlement européen et du Conseil, du 20 mai 1997, concernant la protection des consommateurs en matière de contrats à distance (JO 1997, L 144, p. 19).

faire usage en toute liberté et sans aucune pression du délai de réflexion qui lui est accordé par cette directive.

De même, l'efficacité et l'effectivité du droit de rétractation seraient mises en cause s'il était imposé au consommateur de payer une indemnité compensatrice en raison de la simple circonstance d'avoir examiné et essayé le bien. Dans la mesure où le droit de rétractation a précisément pour but de donner cette possibilité au consommateur, le fait d'avoir recouru à celle-ci ne saurait avoir pour conséquence que le consommateur ne puisse exercer ledit droit qu'à la condition de payer une indemnité.

Toutefois, ces mêmes dispositions ne s'opposent pas à ce que le paiement d'une indemnité compensatrice pour l'utilisation du bien soit imposé au consommateur dans l'hypothèse où celui-ci aurait fait usage dudit bien d'une manière incompatible avec les principes de droit civil, tels que la bonne foi ou l'enrichissement sans cause, à la condition qu'il ne soit pas porté atteinte à la finalité de ladite directive et, notamment, à l'efficacité et à l'effectivité du droit de rétractation, ce qu'il incombe à la juridiction nationale de déterminer.

Arrêt du 15 avril 2010, Heinrich Heine (C-511/08, EU:C:2010:189)

Une entreprise de vente par correspondance, Heinrich Heine, prévoyait dans ses conditions générales de vente que le consommateur supporte, à titre de frais d'expédition, un forfait de 4,95 euros. Cette somme restait acquise au fournisseur même lorsque le consommateur exerçait son droit de rétractation. La Verbraucherzentrale Nordrhein-Westfalen, une association allemande de consommateurs, avait engagé contre Heinrich Heine une action en cessation de cette pratique, car elle estimait que, en cas de rétractation, les frais d'expédition ne devaient pas être imputés au consommateur. Selon le Bundesgerichtshof (Cour fédérale de justice, Allemagne), le droit allemand ne confère de manière explicite à l'acheteur aucun droit au remboursement des frais d'expédition de la marchandise commandée. Ayant cependant des doutes sur la compatibilité avec la directive 97/7/CE¹⁷ de la facturation des frais d'expédition des marchandises au consommateur même lorsque celui-ci a exercé son droit de rétractation, cette juridiction a demandé à la Cour de justice d'interpréter la directive.

Dans son arrêt, la Cour a constaté que l'article 6, paragraphes 1, premier alinéa, seconde phrase, et 2, de la directive 97/7/CE doit être interprété en ce sens qu'il s'oppose à une réglementation nationale qui permet au fournisseur, dans un contrat conclu à distance, d'imputer les frais d'expédition des marchandises au consommateur dans le cas où ce dernier exerce son droit de rétractation.

¹⁷ Directive 97/7/CE du Parlement européen et du Conseil, du 20 mai 1997, concernant la protection des consommateurs en matière de contrats à distance (JO 1997, L 144, p. 19).

En effet, ces dispositions n'autorisent le fournisseur à imputer au consommateur, en cas de rétractation de ce dernier, que les frais directs de renvoi des marchandises. Si les frais d'expédition devaient également être mis à la charge du consommateur, une telle imputation, qui serait nécessairement de nature à dissuader ce dernier d'exercer son droit de rétractation, irait à l'encontre de l'objectif même dudit article 6.

En outre, une telle imputation serait de nature à remettre en cause une répartition équilibrée des risques entre les parties dans les contrats conclus à distance, en faisant supporter au consommateur l'ensemble des charges liées au transport des marchandises.

Arrêt du 6 juillet 2017, Air Berlin (C-290/16, [EU:C:2017:523](#))

La compagnie aérienne allemande Air Berlin avait introduit dans ses conditions générales de vente une clause selon laquelle, lorsqu'un passager annulait sa réservation d'un vol au tarif économique ou ne se présentait pas à l'embarquement d'un tel vol, un montant de 25 euros était prélevé au titre des frais de traitement sur la somme devant lui être remboursée. Le Bundesverband der Verbraucherzentralen (Union fédérale allemande des centrales de consommateurs) avait estimé que cette clause était nulle en vertu du droit allemand, du fait qu'elle désavantageait les clients de façon indue. De plus, s'agissant de l'exécution d'une obligation légale, Air Berlin ne pouvait exiger des frais distincts. Le Bundesverband avait dès lors saisi les juridictions allemandes d'une action en cessation à l'encontre d'Air Berlin.

Dans le cadre de la même action, le Bundesverband avait contesté les pratiques d'Air Berlin en matière d'affichage des prix sur son site Internet. En effet, lors d'une simulation de réservation en ligne en 2010, le Bundesverband avait constaté que les taxes et redevances indiquées étaient très inférieures à celles effectivement perçues par les aéroports concernés. Le Bundesverband était d'avis que cette pratique pouvait induire le consommateur en erreur et qu'elle était contraire aux règles sur la transparence des prix prévues par le règlement de l'Union sur l'exploitation des services aériens¹⁸. Le Bundesgerichtshof (Cour fédérale de justice, Allemagne) a demandé à la Cour, d'une part, si le règlement (CE) n° 1008/2008 doit être interprété en ce sens que, lors de la publication de leurs tarifs des passagers, les transporteurs aériens doivent préciser le montant effectif des redevances et ne peuvent donc pas inclure pour partie ces dernières dans leurs tarifs des passagers et, d'autre part, si ledit règlement s'oppose à une application d'une réglementation nationale relative au droit des conditions générales de vente, fondée sur le droit de l'Union qui prévoit qu'il n'est pas possible de facturer des frais de traitement distincts aux clients qui ne se sont pas présentés à un vol ou qui ont annulé leur réservation.

¹⁸ Règlement (CE) n° 1008/2008 du Parlement européen et du Conseil, du 24 septembre 2008, établissant des règles communes pour l'exploitation de services aériens dans la Communauté (JO 2008, L 293, p. 3).

La Cour a répondu que l'article 23, paragraphe 1, troisième phrase, du règlement (CE) n° 1008/2008 doit être interprété en ce sens que, lors de la publication de leurs tarifs des passagers, les transporteurs aériens doivent préciser, de manière séparée, les montants dus par les clients au titre des taxes, des redevances aéroportuaires ainsi que des autres redevances, suppléments et droits, visés dans ce règlement. En outre, ils ne peuvent en conséquence inclure, même pour partie, ces éléments dans le tarif des passagers. L'article 23, paragraphe 1, du règlement (CE) n° 1008/2008 vise à garantir, notamment, l'information et la transparence des prix des services aériens au départ d'un aéroport situé sur le territoire d'un État membre et contribue, partant, à assurer la protection du client recourant à ces services. Au demeurant, une interprétation différente serait de nature à priver cette disposition de tout effet utile.

L'article 22, paragraphe 1, du règlement (CE) n° 1008/2008 doit être interprété en ce sens qu'il ne s'oppose pas à ce que l'application d'une réglementation nationale transposant la directive 93/13/CEE puisse conduire à déclarer nulle une clause figurant dans des conditions générales de vente qui permettent de facturer des frais de traitement forfaitaires distincts aux clients qui ne se sont pas présentés à un vol ou qui ont annulé leur réservation. La Cour constate à cet égard que les règles générales protégeant les consommateurs contre les clauses abusives s'appliquent également aux contrats de transport aérien.

Ainsi, le règlement (CEE) n° 2409/92, abrogé par le règlement n° 1008/2008, indiquait dans son cinquième considérant qu'il convenait « de compléter la libre fixation des tarifs par des dispositions appropriées visant à sauvegarder les intérêts des consommateurs et de l'industrie ».

Arrêt du 10 juillet 2019, Amazon EU (C-649/17, EU:C:2019:576)

L'entreprise Amazon EU Sàrl, établie à Luxembourg, propose la vente en ligne de divers produits. Dans l'affaire au principal, l'Union fédérale allemande des centrales et associations de consommateurs (ci-après l'« Union fédérale ») avait introduit devant un tribunal régional une action en cessation des pratiques d'Amazon EU en matière d'affichage des informations figurant sur son site Internet www.amazon.de et permettant au consommateur de contacter cette société. Cette juridiction ayant rejeté ledit recours, l'Union fédérale a formé un appel devant un tribunal régional supérieur qui a également été rejeté. De ce fait, l'Union fédérale a introduit un pourvoi en Revision devant la juridiction de renvoi, le Bundesgerichtshof (Cour fédérale de justice, Allemagne).

La demande de décision préjudiciale portait sur l'interprétation de l'article 6, paragraphe 1, sous c), de la directive 2011/83/UE¹⁹.

Premièrement, la Cour a rappelé que la possibilité, pour le consommateur, de contacter le professionnel rapidement et de communiquer avec lui efficacement, ainsi que le prévoit ladite disposition, revêt une importance fondamentale pour la sauvegarde et la mise en œuvre effective des droits du consommateur et, notamment, du droit de rétractation dont les modalités et les conditions d'exercice sont indiquées aux articles 9 à 16 de cette directive. Cependant, dans l'interprétation de ladite disposition, il convient d'assurer un juste équilibre entre un niveau élevé de protection des consommateurs et la compétitivité des entreprises, ainsi que l'énonce le considérant 4 de la directive 2011/83/UE, tout en respectant la liberté d'entreprise de l'entrepreneur, telle que consacrée à la charte des droits fondamentaux de l'Union européenne (ci-après la « Charte »).

La Cour a estimé qu'il incombe au juge national d'apprécier si, compte tenu de l'ensemble des circonstances dans lesquelles le consommateur prend contact avec le professionnel par l'intermédiaire d'un site Internet et notamment de la présentation et de la fonctionnalité de ce site, les moyens de communication mis à la disposition de ce consommateur par ce professionnel permettent au consommateur de contacter le professionnel rapidement et de communiquer avec lui efficacement, conformément à l'article 6, paragraphe 1, sous c), de la directive 2011/83/UE.

À cet égard, la Cour a souligné qu'une obligation inconditionnelle de mettre à disposition du consommateur, en toutes circonstances, un numéro de téléphone, voire de mettre en place une ligne téléphonique, ou de télécopieur, ou de créer une nouvelle adresse électronique pour permettre aux consommateurs de contacter le professionnel paraît disproportionnée.

La Cour a dès lors jugé qu'il convient d'interpréter les termes « lorsqu'ils sont disponibles », figurant à l'article 6, paragraphe 1, sous c), de la directive 2011/83/UE, en ce sens qu'ils visent les cas où le professionnel dispose d'un numéro de téléphone ou de télécopieur et qu'il ne les utilise pas uniquement à des fins autres que le contact avec les consommateurs. À défaut, cette disposition ne lui impose pas d'informer le consommateur de ce numéro de téléphone, voire de mettre en place une ligne téléphonique, ou de télécopieur, ou de créer une nouvelle adresse électronique pour permettre aux consommateurs de le contacter.

Deuxièmement, examinant si ce professionnel peut, dans des circonstances telles que celles de l'affaire au principal, recourir à des moyens de communication qui ne sont pas mentionnés à l'article 6, paragraphe 1, sous c), de la directive 2011/83/UE, tels qu'un système de messagerie instantanée ou de rappel téléphonique, la Cour a jugé que

¹⁹ Directive 2011/83/UE du Parlement européen et du Conseil, du 25 octobre 2011, relative aux droits des consommateurs, modifiant la directive 93/13/CEE du Conseil et la directive 1999/44/CE du Parlement européen et du Conseil et abrogeant la directive 85/577/CEE du Conseil et la directive 97/7/CE du Parlement européen et du Conseil (JO 2011, L 304, p. 64).

l'article 6, paragraphe 1, sous c), de la directive 2011/83/UE doit être interprété en ce sens que, si cette disposition impose au professionnel de mettre à la disposition du consommateur un moyen de communication de nature à satisfaire aux critères d'une communication directe et efficace, elle ne s'oppose pas à ce que ledit professionnel fournit d'autres moyens de communication que ceux énumérés dans ladite disposition aux fins de satisfaire à ces critères.

4. Protection des données à caractère personnel

Arrêt du 1^{er} octobre 2015, Weltimmo (C-230/14, [EU:C:2015:639](#))

Weltimmo, une société enregistrée en Slovaquie, exploitait un site Internet d'annonces immobilières concernant des biens situés en Hongrie. Dans ce cadre, elle traitait les données à caractère personnel des annonceurs. Les annonces étaient publiées gratuitement pendant un mois et devenaient payantes au terme de ce délai. De nombreux annonceurs avaient demandé, par courrier électronique, le retrait de leurs annonces à l'issue du premier mois et, par la même occasion, l'effacement des données à caractère personnel les concernant. Weltimmo n'avait toutefois pas procédé à cet effacement et avait facturé aux intéressés le prix de ses services. En l'absence de règlement des sommes facturées, Weltimmo avait communiqué les données à caractère personnel des annonceurs à des agences de recouvrement. Les annonceurs avaient déposé plainte auprès de l'autorité hongroise chargée de la protection des données. Celle-ci avait infligé à Weltimmo une amende de 10 millions de forints hongrois (HUF) (environ 32 000 euros) pour avoir violé la loi hongroise transposant la directive 95/46/CE²⁰.

Weltimmo a alors contesté la décision de l'autorité de contrôle devant les tribunaux hongrois. Appelée à connaître du litige en cassation, la Kúria (Cour suprême, Hongrie) a demandé à la Cour si ladite directive permettait à l'autorité de contrôle hongroise d'appliquer la loi hongroise adoptée sur la base de la directive et d'infliger l'amende prévue par cette loi.

La Cour a rappelé qu'il découle du considérant 19 de la directive 95/46/CE une conception souple de la notion d'établissement. Ainsi, afin de déterminer si une société, responsable d'un traitement de données, dispose d'un établissement dans un État membre autre que l'État membre ou le pays tiers où elle est immatriculée, il convient d'évaluer tant le degré de stabilité de l'installation que la réalité de l'exercice des activités dans cet autre État membre. Cela vaut tout particulièrement pour des entreprises qui s'emploient à offrir des services exclusivement sur Internet.

²⁰ Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO 1995, L 281, p. 31).

Selon la Cour, l'article 4, paragraphe 1, sous a), de la directive 95/46/CE, doit être interprété en ce sens qu'il permet l'application de la législation relative à la protection des données à caractère personnel d'un État membre autre que celui dans lequel le responsable du traitement de ces données est immatriculé, pour autant que celui-ci exerce, au moyen d'une installation stable sur le territoire de cet État membre, une activité effective et réelle. En revanche, est dénuée de pertinence la question de la nationalité des personnes concernées par ce traitement de données.

Dans l'hypothèse où l'autorité de contrôle d'un État membre parviendrait à la conclusion que le droit applicable est non pas le droit de cet État membre, mais celui d'un autre État membre, l'article 28, paragraphes 1, 3 et 6, de cette directive doit être interprété en ce sens que cette autorité de contrôle ne pourrait exercer les pouvoirs effectifs d'intervention. Partant, elle ne saurait infliger de sanctions sur la base du droit de l'État membre dont elle relève au responsable du traitement de ces données qui n'est pas établi sur le territoire de l'État membre dont elle relève. En effet, il découle des exigences résultant de la souveraineté territoriale de l'État membre concerné, du principe de légalité et de la notion d'État de droit que le pouvoir de répression ne peut, en principe, s'exercer en dehors des limites légales dans lesquelles une autorité administrative est habilitée à agir, dans le respect du droit de l'État membre dont elle relève.

Arrêt du 6 octobre 2015 (grande chambre), Schrems (C-362/14, [EU:C:2015:650](#))

M. Maximillian Schrems, un citoyen autrichien, utilisait Facebook depuis 2008. Des données fournies par M. Schrems à Facebook étaient transférées, en tout ou en partie, à partir de la filiale irlandaise de Facebook sur des serveurs situés sur le territoire des États-Unis, où elles faisaient l'objet d'un traitement. M. Schrems avait déposé une plainte auprès de l'autorité irlandaise de contrôle, considérant qu'au vu des révélations faites en 2013 par M. Edward Snowden au sujet des activités des services de renseignement des États-Unis (en particulier la National Security Agency ou « NSA »), le droit et les pratiques des États-Unis n'offraient pas de protection suffisante contre la surveillance, par les autorités publiques, des données transférées vers ce pays. L'autorité irlandaise avait rejeté la plainte, au motif notamment que, dans la décision 2000/520/CE²¹, la Commission avait considéré que, dans le cadre du régime dit de la « sphère de sécurité », les États-Unis assuraient un niveau adéquat de protection des données à caractère personnel transférées.

Saisie de l'affaire, la High Court (Haute Cour, Irlande) a souhaité savoir si cette décision de la Commission a pour effet d'empêcher une autorité nationale de contrôle

²¹ Décision 2000/520/CE de la Commission, du 26 juillet 2000, conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » et par les questions souvent posées y afférentes, publiés par le ministère du commerce des États-Unis d'Amérique (JO 2000, L 215, p. 7).

d'enquêter sur une plainte alléguant qu'un pays tiers n'assure pas un niveau de protection adéquat et, le cas échéant, de suspendre le transfert de données contesté.

La Cour a répondu que l'opération consistant à faire transférer des données à caractère personnel depuis un État membre vers un pays tiers constitue, en tant que telle, un traitement de données à caractère personnel au sens de l'article 2, sous b), de la directive 95/46/CE²², effectué sur le territoire d'un État membre. Les autorités nationales sont donc investies de la compétence de vérifier si un transfert de données à caractère personnel depuis l'État membre dont elles relèvent vers un pays tiers respecte les exigences posées par la directive 95/46.

Ainsi, aussi longtemps que la décision de la Commission n'a pas été déclarée invalide par la Cour, seule compétente pour constater l'invalidité d'un acte de l'Union, les États membres et leurs organes ne sauraient adopter des mesures contraires à cette décision, telles que des actes visant à constater avec effet contraignant que le pays tiers visé par ladite décision n'assure pas un niveau de protection adéquat. Dans l'hypothèse où une autorité de contrôle parvient à la conclusion que les éléments avancés au soutien d'une demande relative à la protection des droits et libertés à l'égard du traitement de ces données à caractère personnel sont dépourvus de fondement et rejette, de ce fait, cette dernière, la personne ayant introduit ladite demande doit avoir accès aux voies de recours juridictionnelles lui permettant de contester une telle décision lui faisant grief devant les juridictions nationales. Dans l'hypothèse contraire, où ladite autorité estime fondés les griefs avancés par la personne l'ayant saisie d'une telle demande, cette même autorité doit pouvoir ester en justice, conformément à l'article 28, paragraphe 3, premier alinéa, troisième tiret, de la directive 95/46/CE, lu à la lumière notamment de l'article 8, paragraphe 3, de la Charte.

L'article 25, paragraphe 6, de la directive 95/46/CE, lu à la lumière des articles 7, 8 et 47 de la Charte, doit être interprété en ce sens qu'une décision adoptée au titre de cette disposition, par laquelle la Commission constate qu'un pays tiers assure un niveau de protection adéquat, ne fait pas obstacle à ce qu'une autorité de contrôle d'un État membre examine la demande d'une personne relative à la protection de ses droits et libertés à l'égard du traitement des données à caractère personnel la concernant qui ont été transférées depuis un État membre vers ce pays tiers, lorsque cette personne fait valoir que le droit et les pratiques en vigueur dans celui-ci n'assurent pas un niveau de protection adéquat.

L'expression « niveau de protection adéquat » figurant à l'article 25, paragraphe 6, de la directive 95/46/CE doit être comprise comme exigeant que ce pays tiers assure effectivement, en raison de sa législation interne ou de ses engagements internationaux, un niveau de protection des libertés et droits fondamentaux substantiellement

²² Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO 1995, L 281, p. 31).

équivalent à celui garanti au sein de l'Union en vertu de cette directive, lue à la lumière de la Charte.

En effet, les principes de la « sphère de sécurité » sont uniquement applicables aux organisations américaines autocertifiées recevant des données à caractère personnel depuis l'Union, sans qu'il soit exigé que les autorités publiques américaines soient soumises au respect desdits principes. De surcroît, la décision 2000/520/CE rend possible des ingérences, fondées sur des exigences relatives à la sécurité nationale et à l'intérêt public ou sur la législation interne des États-Unis, dans les droits fondamentaux des personnes dont les données à caractère personnel sont ou pourraient être transférées depuis l'Union vers les États-Unis, sans comporter de constatation quant à l'existence, aux États-Unis, de règles à caractère étatique destinées à limiter les éventuelles ingérences dans ces droits et sans faire état de l'existence d'une protection juridique efficace contre des ingérences de cette nature.

En outre, la Commission a outrepassé la compétence qui lui est attribuée à l'article 25, paragraphe 6, de la directive 95/46/CE, lue à la lumière de la Charte, en adoptant l'article 3 de la décision 2000/520/CE, lequel est de ce fait invalide.

Arrêt du 1er octobre 2019, Planet49 (grande chambre) (C-673/17, [EU:C:2019:801](#))

Planet49 est une société organisatrice d'un jeu promotionnel sur le site Internet www.dein-macbook.de. Pour participer, les internautes devaient communiquer leurs nom et adresse sur une page web où se trouvaient des cases à cocher. La case autorisant l'installation des cookies était cochée par défaut.

Saisi d'un recours par la Fédération allemande des associations de consommateurs, le Bundesgerichtshof (Cour fédérale de justice, Allemagne) éprouvait des doutes sur la validité de l'obtention du consentement des utilisateurs au moyen de la case cochée par défaut ainsi que sur l'étendue de l'obligation d'information pesant sur le fournisseur de service.

La demande de décision préjudicielle portait essentiellement sur l'interprétation de la notion de « consentement » visée par la directive vie privée et communications électroniques, lue en combinaison avec la directive 95/46/CE, ainsi qu'avec le règlement général sur la protection des données.

Premièrement, la Cour a observé que l'article 2, sous h), de la directive 95/46/CE, à laquelle renvoie l'article 2, sous f), de la directive vie privée et communications électroniques, définit le consentement comme étant « toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement ». Elle a relevé que l'exigence d'une « manifestation » de volonté de la personne concernée évoque clairement un comportement actif et non pas passif. Or, un consentement donné au moyen d'une case cochée par défaut n'implique pas un comportement actif de

la part de l'utilisateur d'un site Internet. En outre, la genèse de l'article 5, paragraphe 3, de la directive vie privée et communications électroniques, qui prévoit depuis sa modification par la directive 2009/136 que l'utilisateur doit avoir « donné son accord » au placement de cookies, tend à indiquer que le consentement de l'utilisateur ne peut dorénavant plus être présumé et doit résulter d'un comportement actif de ce dernier. Enfin, un consentement actif est désormais prévu par le règlement général sur la protection des données, dont l'article 4, point 11, requiert une manifestation de volonté prenant la forme, notamment, d'un « acte positif clair » et dont le considérant 32 exclut expressément qu'il y ait un consentement « en cas de silence, de cases cochées par défaut ou d'inactivité ».

La Cour a dès lors jugé que le consentement n'est pas valablement donné lorsque le stockage d'informations ou l'accès à des informations déjà stockées dans l'équipement terminal de l'utilisateur d'un site Internet est autorisé par une case cochée par défaut que l'utilisateur doit décocher pour refuser de donner son consentement.

Deuxièmement, la Cour a constaté que l'article 5, paragraphe 3, de la directive vie privée et communications électroniques vise à protéger l'utilisateur de toute ingérence dans sa vie privée, indépendamment du point de savoir si cette ingérence concerne ou non des données à caractère personnel. Il en résulte que la notion de « consentement » ne doit pas être interprétée différemment selon que les informations stockées ou consultées dans l'équipement terminal de l'utilisateur d'un site Internet constituent ou non des données à caractère personnel.

Troisièmement, la Cour a relevé que l'article 5, paragraphe 3, de la directive vie privée et communications électroniques exige que l'utilisateur ait donné son accord, après avoir reçu une information claire et complète, notamment sur la finalité du traitement. Or, une information claire et complète doit permettre à l'utilisateur de déterminer facilement les conséquences du consentement qu'il pourrait donner et garantir que ce consentement soit donné en pleine connaissance de cause. À cet égard, la Cour a considéré que la durée de fonctionnement des cookies ainsi que la possibilité ou non pour des tiers d'avoir accès à ces cookies font partie de l'information claire et complète devant être donnée à l'utilisateur d'un site Internet par le fournisseur de services.

Arrêt du 16 juillet 2020, Facebook Ireland et Schrems (C-311/18, EU:C:2020:559)

Le règlement général relatif à la protection des données²³ (RGPD) dispose que le transfert de telles données vers un pays tiers ne peut, en principe, avoir lieu que si le pays tiers en question assure un niveau de protection adéquat à ces données. Selon ce règlement, la Commission peut constater qu'un pays tiers assure, en raison de sa

²³ Règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (JO 2016, L 119, p. 1).

législation interne ou de ses engagements internationaux, un niveau de protection adéquat²⁴. En l'absence d'une telle décision d'adéquation, un tel transfert ne peut être réalisé que si l'exportateur des données à caractère personnel, établi dans l'Union, prévoit des garanties appropriées, pouvant notamment résulter de clauses types de protection des données adoptées par la Commission, et si les personnes concernées disposent de droits opposables et de voies de droit effectives²⁵.

Par ailleurs, le RGPD établit, de manière précise, les conditions dans lesquelles un tel transfert peut avoir lieu en l'absence d'une décision d'adéquation ou de garanties appropriées²⁶.

M. Maximillian Schrems, ressortissant autrichien résidant en Autriche, est un utilisateur de Facebook depuis 2008. Comme pour les autres utilisateurs résidant dans l'Union, les données à caractère personnel de M. Schrems sont, en tout ou en partie, transférées par Facebook Ireland vers des serveurs appartenant à Facebook Inc., situés sur le territoire des États-Unis, où elles font l'objet d'un traitement. M. Schrems a déposé une plainte auprès de l'autorité irlandaise de contrôle, visant, en substance, à faire interdire ces transferts. Il a soutenu que le droit et les pratiques des États-Unis n'offrent pas de protection suffisante contre l'accès, par les autorités publiques, aux données transférées vers ce pays. Cette plainte a été rejetée, au motif notamment que, dans sa décision 2000/520²⁷ (dite décision « sphère de sécurité »), la Commission avait constaté que les États-Unis assuraient un niveau adéquat de protection. Par un arrêt rendu le 6 octobre 2015, la Cour, saisie d'une question préjudicielle posée par la High Court (Haute Cour, Irlande), a jugé cette décision invalide (ci-après l'« arrêt Schrems I »)²⁸.

À la suite de l'arrêt Schrems I et de l'annulation consécutive, par la juridiction irlandaise, de la décision rejetant la plainte de M. Schrems, l'autorité de contrôle irlandaise a invité celui-ci à reformuler sa plainte compte tenu de l'invalidation, par la Cour, de la décision 2000/520. Dans sa plainte reformulée, M. Schrems maintient que les États-Unis n'offrent pas de protection suffisante des données transférées vers ce pays. Il demande de suspendre ou d'interdire, pour l'avenir, les transferts de ses données à caractère personnel depuis l'Union vers les États-Unis, que Facebook Ireland réalise désormais sur le fondement des clauses types de protection figurant à l'annexe de la décision 2010/87²⁹. Estimant que le traitement de la plainte de M. Schrems dépend, notamment, de la validité de la décision 2010/87, l'autorité de contrôle irlandaise a initié une procédure devant la High Court (Haute Cour) aux fins que celle-ci soumette à la Cour une demande de décision préjudicielle. Après l'ouverture de cette procédure, la

²⁴ Article 45 du RGPD.

²⁵ Article 46, paragraphe 1 et paragraphe 2, sous c), du RGPD.

²⁶ Article 49 du RGPD.

²⁷ Décision de la Commission du 26 juillet 2000 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » et par les questions souvent posées y afférentes, publiés par le ministère du commerce des États-Unis (JO 2000, L 215, p.7).

²⁸ Arrêt de la Cour du 6 octobre 2015, Schrems (C-362/14, [EU:C:2015:650](#)).

²⁹ Décision de la Commission du 5 février 2010 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement européen et du Conseil (JO 2010, L 39, p. 5), telle que modifiée par la décision d'exécution (UE) 2016/2297 de la Commission du 16 décembre 2016 (JO 2016, L 344, p. 100).

Commission a adopté la décision 2016/1250 relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis³⁰ (dite décision « bouclier de protection des données »).

Par sa demande de décision préjudiciale, la juridiction de renvoi interroge la Cour sur l'applicabilité du RGPD à des transferts de données à caractère personnel fondés sur des clauses types de protection figurant dans la décision 2010/87, sur le niveau de protection requis par ce règlement dans le cadre d'un tel transfert et sur les obligations incombant aux autorités de contrôle dans ce contexte. En outre, la High Court soulève la question de la validité tant de la décision 2010/87 que de la décision 2016/1250.

Par son arrêt de ce jour, la Cour constate que l'examen de la décision 2010/87 au regard de la charte des droits fondamentaux ne révèle aucun élément de nature à affecter sa validité. En revanche, elle déclare la décision 2016/1250 invalide.

La Cour estime, tout d'abord, que le droit de l'Union, et notamment le RGPD, s'applique à un transfert de données à caractère personnel effectué à des fins commerciales par un opérateur économique établi dans un État membre vers un autre opérateur économique établi dans un pays tiers, même si, au cours ou à la suite de ce transfert, ces données sont susceptibles d'être traitées à des fins de sécurité publique, de défense et de sûreté de l'État par les autorités du pays tiers concerné. Elle précise que ce type de traitement de données par les autorités d'un pays tiers ne saurait exclure un tel transfert du champ d'application du règlement.

En ce qui concerne le niveau de protection requis dans le cadre d'un tel transfert, la Cour juge que les exigences prévues à cet effet par les dispositions du RGPD, qui ont trait à des garanties appropriées, des droits opposables et des voies de droit effectives, doivent être interprétées en ce sens que les personnes dont les données à caractère personnel sont transférées vers un pays tiers sur le fondement de clauses types de protection des données doivent bénéficier d'un niveau de protection substantiellement équivalent à celui garanti au sein de l'Union par ce règlement, lu à la lumière de la Charte. Dans ce contexte, elle précise que l'évaluation de ce niveau de protection doit prendre en compte tant les stipulations contractuelles convenues entre l'exportateur des données établi dans l'Union et le destinataire du transfert établi dans le pays tiers concerné que, en ce qui concerne un éventuel accès des autorités publiques de ce pays tiers aux données ainsi transférées, les éléments pertinents du système juridique de celui-ci.

S'agissant des obligations incombant aux autorités de contrôle dans le contexte d'un tel transfert, la Cour juge que, à moins qu'il existe une décision d'adéquation valablement adoptée par la Commission, ces autorités sont notamment obligées de suspendre ou d'interdire un transfert de données à caractère personnel vers un pays tiers lorsqu'elles

³⁰ Décision d'exécution (UE) 2016/1250 de la Commission, du 12 juillet 2016, conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis (JO 2016, L 207, p. 1).

estiment, au regard des circonstances propres à ce transfert, que les clauses types de protection des données ne sont pas ou ne peuvent pas être respectées dans ce pays et que la protection des données transférées, requise par le droit de l'Union, ne peut pas être assurée par d'autres moyens, à défaut pour l'exportateur établi dans l'Union d'avoir lui-même suspendu ou mis fin à un tel transfert.

La Cour examine ensuite la validité de la décision 2010/87. Selon la Cour, la validité de cette décision n'est pas remise en cause par le seul fait que les clauses types de protection des données figurant dans celle-ci ne lient pas, en raison de leur caractère contractuel, les autorités du pays tiers vers lequel un transfert des données pourrait être opéré. En revanche, précise-t-elle, cette validité dépend du point de savoir si ladite décision comporte des mécanismes effectifs permettant, en pratique, d'assurer que le niveau de protection requis par le droit de l'Union soit respecté et que les transferts de données à caractère personnel, fondés sur de telles clauses, soient suspendus ou interdits en cas de violation de ces clauses ou d'impossibilité de les honorer. La Cour constate que la décision 2010/87 met en place de tels mécanismes. À cet égard, elle souligne, notamment, que cette décision instaure une obligation pour l'exportateur des données et le destinataire du transfert de vérifier, au préalable, que ce niveau de protection soit respecté dans le pays tiers concerné et qu'elle oblige ce destinataire à informer l'exportateur des données de son éventuelle incapacité de se conformer aux clauses types de protection, à charge alors pour ce dernier de suspendre le transfert de données et/ou de résilier le contrat conclu avec le premier.

La Cour procède, enfin, à l'examen de la validité de la décision 2016/1250 au regard des exigences découlant du RGPD, lu à la lumière des dispositions de la Charte garantissant le respect de la vie privée et familiale, la protection des données à caractère personnel et le droit à une protection juridictionnelle effective. À cet égard, la Cour relève que cette décision consacre, à l'instar de la décision 2000/520, la primauté des exigences relatives à la sécurité nationale, à l'intérêt public et au respect de la législation américaine, rendant ainsi possibles des ingérences dans les droits fondamentaux des personnes dont les données sont transférées vers ce pays tiers. Selon la Cour, les limitations de la protection des données à caractère personnel qui découlent de la réglementation interne des États-Unis portant sur l'accès et l'utilisation, par les autorités publiques américaines, de telles données transférées depuis l'Union vers ce pays tiers, et que la Commission a évaluées dans la décision 2016/1250, ne sont pas encadrées de manière à répondre à des exigences substantiellement équivalentes à celles requises, en droit de l'Union, par le principe de proportionnalité, en ce que les programmes de surveillance fondés sur cette réglementation ne sont pas limités au strict nécessaire. En se fondant sur les constatations figurant dans cette décision, la Cour relève que, pour certains programmes de surveillance, ladite réglementation ne fait ressortir d'aucune manière l'existence de limitations à l'habilitation qu'elle comporte pour la mise en œuvre de ces programmes, pas plus que l'existence de garanties pour des personnes non américaines potentiellement visées. La Cour ajoute que, si la même réglementation prévoit des exigences que les autorités américaines doivent respecter, lors de la mise en œuvre des

programmes de surveillance concernés, elle ne confère pas aux personnes concernées des droits opposables aux autorités américaines devant les tribunaux.

Quant à l'exigence de protection juridictionnelle, la Cour juge que, contrairement à ce que la Commission a considéré dans la décision 2016/1250, le mécanisme de médiation visé par cette décision ne fournit pas à ces personnes une voie de recours devant un organe offrant des garanties substantiellement équivalentes à celles requises en droit de l'Union, de nature à assurer tant l'indépendance du médiateur prévu par ce mécanisme que l'existence de normes habilitant ledit médiateur à adopter des décisions contraignantes à l'égard des services de renseignement américains. Pour toutes ces raisons, la Cour déclare la décision 2016/1250 invalide.

Arrêt du 2 mars 2021 (grande chambre), Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques) (C-746/18, [EU:C:2021:152](#))

Une procédure pénale a été engagée en Estonie contre H. K. des chefs de vol, d'utilisation de la carte bancaire d'un tiers et de violence à l'égard de personnes participant à une procédure en justice. H. K. a été condamnée pour ces infractions par un tribunal de première instance à une peine privative de liberté de deux ans. Cette décision a ensuite été confirmée en appel.

Les procès-verbaux sur lesquels s'appuie la constatation de ces infractions ont été établis, notamment, sur la base de données à caractère personnel générées dans le cadre de la fourniture de services de communications électroniques. La Riigikohus (Cour suprême, Estonie), devant laquelle un pourvoi en cassation a été introduit par H. K., a émis des doutes quant à la compatibilité avec le droit de l'Union³¹ des conditions dans lesquelles les services d'enquête ont eu accès à ces données.

Ces doutes concernent, en premier lieu, la question de savoir si la durée de la période pour laquelle les services d'enquête ont eu accès aux données constitue un critère permettant d'évaluer la gravité de l'ingérence que constitue cet accès dans les droits fondamentaux des personnes concernées. Ainsi, lorsque cette période est très brève ou que la quantité de données recueillies est très limitée, la juridiction de renvoi s'est interrogée sur le fait de savoir si l'objectif de lutte contre la criminalité en général, et pas seulement de lutte contre la criminalité grave, est susceptible de justifier une telle ingérence. En second lieu, la juridiction de renvoi a nourri des doutes quant à la possibilité de considérer le ministère public estonien, compte tenu des différentes missions qui lui sont confiées par la réglementation nationale, comme une autorité

³¹ Plus précisément, avec l'article 15, paragraphe 1, de la directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO 2002, L 201, p. 37), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009 (JO 2009, L 337, p. 11) (ci-après la « directive «vie privée et communications électroniques»), lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne (ci-après la « Charte »).

administrative « indépendante » au sens de l'arrêt Tele2 Sverige et Watson e.a.³², susceptible d'autoriser l'accès de l'autorité chargée de l'enquête aux données concernées.

Par son arrêt, prononcé en grande chambre, la Cour juge que la directive « vie privée et communications électroniques », lue à la lumière de la Charte, s'oppose à une réglementation nationale permettant l'accès des autorités publiques à des données relatives au trafic ou à des données de localisation, susceptibles de fournir des informations sur les communications effectuées par un utilisateur d'un moyen de communication électronique ou sur la localisation des équipements terminaux qu'il utilise et de permettre de tirer des conclusions précises sur sa vie privée, à des fins de prévention, de recherche, de détection et de poursuite d'infractions pénales, sans que cet accès soit circonscrit à des procédures visant à la lutte contre la criminalité grave ou à la prévention de menaces graves contre la sécurité publique. Selon la Cour, la durée de la période pour laquelle l'accès à ces données est sollicité et la quantité ou la nature des données disponibles pour une telle période n'a pas d'incidence à cet égard. En outre, la Cour considère que cette même directive, lue à la lumière de la Charte, s'oppose à une réglementation nationale donnant compétence au ministère public pour autoriser l'accès d'une autorité publique aux données relatives au trafic et aux données de localisation afin de mener une instruction pénale.

S'agissant des conditions dans lesquelles l'accès aux données relatives au trafic et aux données de localisation conservées par les fournisseurs de services de communications électroniques peut, à des fins de prévention, de recherche, de détection et de poursuite d'infractions pénales, être accordé à des autorités publiques, en application d'une mesure prise au titre de la directive « vie privée et communications électroniques »³³, la Cour rappelle ce qu'elle a jugé dans son arrêt La Quadrature du Net e.a.³⁴. Ainsi, cette directive n'autorise les États membres à adopter, entre autres à ces fins, des mesures législatives visant à limiter la portée des droits et des obligations prévus par cette directive, notamment l'obligation de garantir la confidentialité des communications et des données relatives au trafic³⁵, que dans le respect des principes généraux du droit de l'Union, parmi lesquels figure le principe de proportionnalité, et des droits fondamentaux garantis par la Charte³⁶. Dans ce cadre, la directive s'oppose à des mesures législatives imposant aux fournisseurs de services de communications électroniques, à titre préventif, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation.

En ce qui concerne l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales, poursuivi par la réglementation en cause, conformément au

³² Arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a. (C-203/15 et C-698/15, [EUC:2016970](#), point 120).

³³ Article 15, paragraphe 1, de la directive 2002/58.

³⁴ Arrêt du 6 octobre 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 et C-520/18, [EUC:2020:791](#), points 166 à 169).

³⁵ Article 5, paragraphe 1, de la directive 2002/58.

³⁶ En particulier, les articles 7, 8 et 11 ainsi que l'article 52, paragraphe 1, de la Charte.

principe de proportionnalité, la Cour considère que seuls les objectifs de lutte contre la criminalité grave ou de prévention de menaces graves pour la sécurité publique sont de nature à justifier l'accès des autorités publiques à un ensemble de données relatives au trafic ou de données de localisation, susceptibles de permettre de tirer des conclusions précises sur la vie privée des personnes concernées, sans que d'autres facteurs tenant à la proportionnalité d'une demande d'accès, tels que la durée de la période pour laquelle l'accès est sollicité à de telles données, puissent avoir pour effet que l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales en général soit susceptible de justifier un tel accès.

S'agissant de la compétence donnée au ministère public pour autoriser l'accès d'une autorité publique aux données relatives au trafic et aux données de localisation afin de diriger une instruction pénale, la Cour rappelle qu'il appartient au droit national de déterminer les conditions dans lesquelles les fournisseurs de services de communications électroniques doivent accorder aux autorités nationales compétentes l'accès aux données dont ils disposent. Toutefois, pour satisfaire à l'exigence de proportionnalité, une telle réglementation doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant des exigences minimales, de sorte que les personnes dont les données à caractère personnel sont concernées disposent de garanties suffisantes permettant de protéger efficacement ces données contre les risques d'abus. Cette réglementation doit être légalement contraignante en droit interne et indiquer en quelles circonstances et sous quelles conditions matérielles et procédurales une mesure prévoyant le traitement de telles données peut être prise, garantissant ainsi que l'ingérence soit limitée au strict nécessaire.

Selon la Cour, aux fins de garantir, en pratique, le plein respect de ces conditions, il est essentiel que l'accès des autorités nationales compétentes aux données conservées soit subordonné à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante et que la décision de cette juridiction ou de cette entité intervienne à la suite d'une demande motivée de ces autorités présentée, notamment, dans le cadre de procédures de prévention, de détection ou de poursuites pénales. En cas d'urgence dûment justifiée, le contrôle doit intervenir dans de brefs délais.

À cet égard, la Cour précise que le contrôle préalable requiert, entre autres, que la juridiction ou l'entité chargée d'effectuer ce contrôle dispose de toutes les attributions et présente toutes les garanties nécessaires en vue d'assurer une conciliation des différents intérêts et droits en cause. S'agissant plus particulièrement d'une enquête pénale, un tel contrôle exige que cette juridiction ou cette entité soit en mesure d'assurer un juste équilibre entre, d'une part, les intérêts liés aux besoins de l'enquête dans le cadre de la lutte contre la criminalité et, d'autre part, les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel des personnes dont les données sont concernées par l'accès. Lorsque ce contrôle est effectué non par une juridiction mais par une entité administrative indépendante, celle-

ci doit jouir d'un statut lui permettant d'agir, lors de l'exercice de ses missions, de manière objective et impartiale et doit être, à cet effet, à l'abri de toute influence extérieure.

D'après la Cour, il en résulte que l'exigence d'indépendance à laquelle doit satisfaire l'autorité chargée d'exercer le contrôle préalable impose que cette autorité ait la qualité de tiers par rapport à celle qui demande l'accès aux données, de sorte que la première soit en mesure d'exercer ce contrôle de manière objective et impartiale à l'abri de toute influence extérieure. En particulier, dans le domaine pénal, l'exigence d'indépendance implique que l'autorité chargée de ce contrôle préalable, d'une part, ne soit pas impliquée dans la conduite de l'enquête pénale en cause et, d'autre part, ait une position de neutralité vis-à-vis des parties à la procédure pénale. Or, tel n'est pas le cas d'un ministère public qui, comme c'est le cas du ministère public estonien, dirige la procédure d'enquête et exerce, le cas échéant, l'action publique. Il s'ensuit que le ministère public n'est pas en mesure d'effectuer le contrôle préalable susmentionné.

Arrêts du 6 octobre 2020 (grande chambre), Privacy International (C-623/17, [EU:C:2020:790](#)) et La Quadrature du Net e.a. (C-511/18, C-512/18 et C-520/18, [EU:C:2020:791](#))

Ces dernières années, la Cour de justice s'est prononcée, dans plusieurs arrêts, sur la conservation et l'accès aux données à caractère personnel dans le domaine des communications électroniques³⁷. La jurisprudence qui en découle, en particulier l'arrêt Tele2 Sverige et Watson e.a., dans lequel elle a notamment considéré que les États membres ne pouvaient pas imposer aux fournisseurs de services de communications électroniques une obligation de conservation généralisée et indifférenciée des données relatives au trafic et à la localisation, a suscité les préoccupations de certains États, craignant d'avoir été privés d'un instrument qu'ils estiment nécessaire à la sauvegarde de la sécurité nationale et à la lutte contre la criminalité.

C'est sur cette toile de fond que l'Investigatory Powers Tribunal (tribunal chargé des pouvoirs d'enquête, Royaume-Uni) (Privacy International, C-623/17), le Conseil d'État (France) (La Quadrature du Net e.a., affaires jointes C-511/18 et C-512/18) ainsi que la Cour constitutionnelle (Belgique) (Ordre des barreaux francophones et germanophone

³⁷ Ainsi, dans l'arrêt du 8 avril 2014, Digital Rights Ireland e.a (C-293/12 et C-594/12, [EU:C:2014:238](#)), la Cour a déclaré invalide la directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE (JO 2006, L 105, p. 54), au motif que l'ingérence dans les droits au respect de la vie privée et à la protection des données à caractère personnel, reconnus par la charte des droits fondamentaux de l'Union européenne (ci-après la « Charte »), que comportait l'obligation générale de conservation des données relatives au trafic et à la localisation prévue par cette directive n'était pas limitée au strict nécessaire. Dans l'arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a. (C-203/15 et C-698/15, [EU:C:2016:970](#)), la Cour a ensuite interprété l'article 15, paragraphe 1, de la directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO 2002, L 201, p. 37), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009 (JO 2009, L 337, p. 11) (ci-après la « directive "vie privée et communications électroniques" »). Cet article habilite les États membres - pour des raisons de protection, entre autres, de la sécurité nationale - à adopter des « mesures législatives » afin de limiter la portée de certains droits et obligations prévus par la directive. Enfin, dans l'arrêt du 2 octobre 2018, Ministerio Fiscal (C-207/16, [EU:C:2018:788](#)), la Cour a interprété ce même article 15, paragraphe 1, dans une affaire qui concernait l'accès des autorités publiques aux données relatives à l'identité civile des utilisateurs des moyens de communications électroniques.

e.a., C-520/18) ont été saisis de litiges concernant la légalité des réglementations adoptées par certains États membres dans ces domaines, prévoyant en particulier une obligation pour les fournisseurs de services de communications électroniques de transmettre à une autorité publique ou de conserver de manière généralisée ou indifférenciée les données des utilisateurs relatives au trafic et à la localisation.

Par deux arrêts prononcés en grande chambre, le 6 octobre 2020, la Cour juge tout d'abord que la directive « vie privée et communications électroniques » s'applique à des réglementations nationales imposant aux fournisseurs de services de communications électroniques de procéder, aux fins de la sauvegarde de la sécurité nationale et de la lutte contre la criminalité, à des traitements de données à caractère personnel, tels que leur transmission à des autorités publiques ou leur conservation. En outre, tout en confirmant sa jurisprudence issue de l'arrêt Tele2 Sverige et Watson e.a., sur le caractère disproportionné d'une conservation généralisée et indifférenciée des données relatives au trafic et à la localisation, la Cour apporte des précisions, notamment, quant à l'étendue des pouvoirs que reconnaît cette directive aux États membres en matière de conservation de telles données aux fins précitées.

Tout d'abord, la Cour prend soin de dissiper les doutes sur l'applicabilité de la directive « vie privée et communications électroniques » soulevés dans le cadre des présentes affaires. En effet, plusieurs États membres ayant soumis des observations écrites à la Cour ont exprimé un avis divergent à cet égard. Ils faisaient notamment valoir que cette directive ne trouverait pas à s'appliquer aux réglementations nationales en cause, dans la mesure où celles-ci ont pour finalité la sauvegarde de la sécurité nationale, qui relèverait de leur seule compétence, comme en témoignerait notamment l'article 4, paragraphe 2, troisième phrase, TUE. La Cour considère cependant que des réglementations nationales imposant aux fournisseurs de services de communications électroniques de conserver des données relatives au trafic et à la localisation ou encore de transmettre ces données aux autorités nationales de sécurité et de renseignement à cette fin relèvent du champ d'application de la directive.

Ensuite, la Cour rappelle que la directive « vie privée et communications électroniques »³⁸ ne permet pas que la dérogation à l'obligation de principe de garantir la confidentialité des communications électroniques et des données y afférentes et à l'interdiction de stocker ces données devienne la règle. Ceci implique que cette directive n'autorise les États membres à adopter, entre autres à des fins de sécurité nationale, des mesures législatives visant à limiter la portée des droits et des obligations prévus par cette directive, notamment l'obligation de garantir la confidentialité des communications et des données relatives au trafic³⁹, que dans le respect des principes

³⁸ Article 15, paragraphes 1 et 3, de la directive 2002/58.

³⁹ Article 5, paragraphe 1, de la directive 2002/58.

généraux du droit de l'Union, parmi lesquels figure le principe de proportionnalité, et des droits fondamentaux garantis par la Charte⁴⁰.

Dans ce cadre, la Cour considère, d'une part, dans l'affaire Privacy International, que la directive « vie privée et communications électroniques », lue à la lumière de la Charte, s'oppose à une réglementation nationale, imposant aux fournisseurs de services de communications électroniques, en vue de la sauvegarde de la sécurité nationale, la transmission généralisée et indifférenciée aux services de sécurité et de renseignement des données relatives au trafic et à la localisation. D'autre part, dans les affaires jointes La Quadrature du Net e.a., ainsi que dans l'affaire Ordre des barreaux francophones et germanophone e.a., la Cour estime que cette même directive s'oppose à des mesures législatives imposant aux fournisseurs de services de communications électroniques, à titre préventif, une conservation généralisée et indifférenciée des données relatives au trafic et à la localisation. En effet, ces obligations de transmission et de conservation généralisée et indifférenciée de telles données constituent des ingérences

particulièrement graves dans les droits fondamentaux garantis par la Charte, sans que le comportement des personnes dont les données sont concernées présente de lien avec l'objectif poursuivi par la réglementation en cause. De manière analogue, la Cour interprète l'article 23, paragraphe 1, du règlement général sur la protection des données⁴¹, lu à la lumière de la Charte, en ce sens qu'il s'oppose à une réglementation nationale imposant aux fournisseurs d'accès à des services de communication au public en ligne et aux fournisseurs de services d'hébergement la conservation généralisée et indifférenciée, notamment, des données à caractère personnel afférentes à ces services.

En revanche, la Cour estime que, dans des situations où l'État membre concerné fait face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, la directive « vie privée et communications électroniques », lue à la lumière de la Charte, ne s'oppose pas au fait d'enjoindre aux fournisseurs de services de communications électroniques de conserver de manière généralisée et indifférenciée des données relatives au trafic et à la localisation. Dans ce contexte, la Cour précise que la décision prévoyant cette injonction, pour une période temporellement limitée au strict nécessaire, doit faire l'objet d'un contrôle effectif, soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, afin de vérifier l'existence d'une de ces situations ainsi que le respect des conditions et des garanties prévues. Dans ces mêmes conditions, ladite directive ne s'oppose pas non plus à l'analyse automatisée des données, notamment celles relatives au trafic et à la localisation, de l'ensemble des utilisateurs de moyens de communications électroniques.

La Cour ajoute que la directive « vie privée et communications électroniques », lue à la lumière de la Charte, ne s'oppose pas à des mesures législatives permettant le recours à

⁴⁰ En particulier, les articles 7, 8 et 11 ainsi que l'article 52, paragraphe 1, de la Charte.

⁴¹ Règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO 2016, L 119, p. 1).

une conservation ciblée, temporellement limitée au strict nécessaire, des données relatives au trafic et à la localisation, qui soit délimitée, sur la base d'éléments objectifs et non discriminatoires, en fonction de catégories de personnes concernées ou au moyen d'un critère géographique. De même, cette directive ne s'oppose pas à de telles mesures prévoyant une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une communication, pour autant que la durée de conservation est limitée au strict nécessaire, ni à celles prévoyant une telle conservation des données relatives à l'identité civile des utilisateurs des moyens de communications électroniques, les États membres n'étant dans ce dernier cas pas tenus de limiter temporellement la conservation. Au surplus, ladite directive ne s'oppose pas à une mesure législative permettant le recours à une conservation rapide des données dont disposent les fournisseurs de services dès lors que se présentent des situations dans lesquelles survient la nécessité de conserver lesdites données au-delà des délais légaux de conservation des données aux fins de l'élucidation d'infractions pénales graves ou d'atteintes à la sécurité nationale, lorsque ces infractions ou atteintes ont déjà été constatées ou lorsque leur existence peut être raisonnablement soupçonnée.

En outre, la Cour juge que la directive « vie privée et communications électroniques », lue à la lumière de la Charte, ne s'oppose pas à une réglementation nationale imposant aux fournisseurs de services de communications électroniques de recourir au recueil en temps réel, notamment, des données relatives au trafic et à la localisation, lorsque ce recueil est limité aux personnes à l'égard desquelles il existe une raison valable de soupçonner qu'elles sont impliquées, d'une manière ou d'une autre, dans des activités de terrorisme et est soumis à un contrôle préalable, effectué soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, s'assurant qu'un tel recueil en temps réel n'est autorisé que dans la limite de ce qui est strictement nécessaire. En cas d'urgence, le contrôle doit intervenir dans de brefs délais.

Enfin, la Cour aborde la question du maintien des effets dans le temps d'une réglementation nationale jugée incompatible avec le droit de l'Union. À cet égard, elle juge qu'une juridiction nationale ne peut faire application d'une disposition de son droit national qui l'habilite à limiter dans le temps les effets d'une déclaration d'illégalité lui incombeant, à l'égard d'une réglementation nationale imposant aux fournisseurs de services de communications électroniques une conservation généralisée et indifférenciée des données relatives au trafic et à la localisation, jugée incompatible avec la directive « vie privée et communications électroniques », lue à la lumière de la Charte.

Ceci étant dit, afin de donner une réponse utile à la juridiction nationale, la Cour rappelle que l'admissibilité et l'appréciation d'éléments de preuve qui ont été obtenus par une conservation de données contraire au droit de l'Union, dans le cadre d'une procédure pénale ouverte à l'encontre de personnes soupçonnées d'actes de criminalité grave, relève, en l'état actuel du droit de l'Union, du seul droit national. Toutefois, la Cour précise que la directive « vie privée et communications électroniques », interprétée à la

lumière du principe d'effectivité, exige que le juge pénal national écarte des éléments de preuve qui ont été obtenus par une conservation généralisée et indifférenciée des données relatives au trafic et à la localisation incompatible avec le droit de l'Union, dans le cadre d'une telle procédure pénale, si les personnes soupçonnées d'actes de criminalité ne sont pas en mesure de prendre efficacement position sur ces éléments de preuve.

Arrêt du 5 avril 2022 (grande chambre), Commissioner of An Garda Síochána e.a. (C-140/20, EU:C:2022:258)

Dans la présente affaire, la demande de décision préjudiciale a été présentée par la Supreme Court (Cour suprême, Irlande) dans le cadre d'une procédure civile engagée par une personne condamnée à la réclusion à perpétuité pour un meurtre commis en Irlande. Cette dernière contestait la compatibilité avec le droit de l'Union de certaines dispositions de la loi nationale relative à la conservation des données générées dans le cadre des communications électroniques⁴². En vertu de cette loi⁴³, des données relatives au trafic et des données de localisation afférentes à des appels téléphoniques de l'inculpé avaient été conservées par les fournisseurs de services de communication électroniques et rendues accessibles aux autorités de police. Les doutes émis par la juridiction de renvoi portaient notamment sur la compatibilité avec la directive « vie privée et communications électroniques »⁴⁴, lue à la lumière de la Charte⁴⁵, d'un régime de conservation généralisée et indifférenciée de ces données, en lien avec la lutte contre la criminalité grave.

Par son arrêt, prononcé en grande chambre, la Cour confirme, tout en précisant sa portée, la jurisprudence issue de l'arrêt *La Quadrature du Net e.a.*, en rappelant que la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation afférentes aux communications électroniques n'est pas autorisée aux fins de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique. Elle confirme également la jurisprudence issue de l'arrêt *Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques)*⁴⁶, notamment quant à l'obligation de subordonner l'accès des autorités nationales compétentes auxdites données conservées à un contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante, à l'égard d'un fonctionnaire de police.

⁴² Communication (Retention of Data) Act 2011 [loi sur les communications (conservation des données)]. Cette loi a été adoptée a fin de transposer dans l'ordre juridique irlandais la directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE (JO 2006, L 105, p. 54).

⁴³ La loi autorise, pour des raisons allant au-delà de celles inhérentes à la protection de la sécurité nationale, la conservation préventive, généralisée et indifférenciée des données relatives au trafic et des données de localisation de tous les abonnés pour une durée de deux ans.

⁴⁴ Plus précisément, l'article 15, paragraphe 1, de la directive 2002/58.

⁴⁵ Notamment des articles 7, 8, 11 et 52, paragraphe 1, de la Charte.

⁴⁶ Arrêt du 2 mars 2021, *Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques)* (C-746/18, [EU:C:2021:152](#))

La Cour juge, en premier lieu, que la directive « vie privée et communications électroniques », lue à la lumière de la Charte, s’oppose à des mesures législatives prévoyant, à titre préventif, aux fins de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation. En effet, compte tenu, d’une part, des effets dissuasifs sur l’exercice des droits fondamentaux⁴⁷ que cette conservation est susceptible d’entraîner et, d’autre part, de la gravité de l’ingérence qu’elle comporte, une telle conservation doit constituer l’exception et non la règle au système mis en place par cette directive, de manière à ce que ces données ne puissent faire l’objet d’une conservation systématique et continue.

La criminalité, même particulièrement grave, ne peut être assimilée à une menace pour la sécurité nationale, dans la mesure où une telle assimilation serait susceptible d’introduire une catégorie intermédiaire entre la sécurité nationale et la sécurité publique, aux fins d’appliquer à la seconde les exigences inhérentes à la première.

En revanche, la directive « vie privée et communications électroniques », lue à la lumière de la Charte, ne s’oppose pas à des mesures législatives prévoyant, aux fins de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation ciblée des données relatives au trafic et des données de localisation qui soit délimitée, sur la base d’éléments objectifs et non discriminatoires, en fonction de catégories de personnes concernées ou au moyen d’un critère géographique, pour une période temporellement limitée au strict nécessaire, mais renouvelable. Elle ajoute qu’une telle mesure de conservation visant des lieux ou des infrastructures fréquentés régulièrement par un nombre très élevé de personnes ou des lieux stratégiques, tels que des aéroports, des gares, des ports maritimes ou des zones de péages, est susceptible de permettre aux autorités compétentes d’obtenir des informations sur la présence, dans ces lieux ou zones géographiques, des personnes y utilisant un moyen de communication électronique et d’en tirer des conclusions sur leur présence et leur activité dans lesdits lieux ou zones géographiques aux fins de la lutte contre la criminalité grave. En tout état de cause, l’existence éventuelle de difficultés pour définir précisément les hypothèses et les conditions dans lesquelles une conservation ciblée peut être effectuée ne saurait justifier que des États membres prévoient une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation.

Cette directive, lue à la lumière de la Charte, ne s’oppose pas non plus à des mesures législatives prévoyant, aux mêmes fins, une conservation généralisée et indifférenciée des adresses IP attribuées à la source d’une connexion, pour une période temporellement limitée au strict nécessaire, ainsi que des données relatives à l’identité civile des utilisateurs de communications électroniques. S’agissant de ce dernier aspect, la Cour précise plus particulièrement que ni la directive « vie privée et communications

⁴⁷ Consacrés aux articles 7 à 11 de la Charte.

électroniques » ni aucun autre acte du droit de l'Union ne s'opposent à une législation nationale, ayant pour objet la lutte contre la criminalité grave, en vertu de laquelle l'acquisition d'un moyen de communication électronique, tel qu'une carte SIM prépayée, est subordonnée à la vérification de documents officiels établissant l'identité civile de l'acheteur et à l'enregistrement, par le vendeur, des informations en résultant, le vendeur étant le cas échéant tenu de donner accès à ces informations aux autorités nationales compétentes.

Il n'en va pas différemment pour ce qui est des mesures législatives prévoyant, toujours aux fins de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, le recours à une injonction faite aux fournisseurs de services de communications électroniques, au moyen d'une décision de l'autorité compétente soumise à un contrôle juridictionnel effectif, de procéder, pour une durée déterminée, à la conservation rapide (« quick freeze ») des données relatives au trafic et des données de localisation dont ils disposent. En effet, seule la lutte contre la criminalité grave et, a fortiori, la sauvegarde de la sécurité nationale sont de nature à justifier une telle conservation, à la condition que cette mesure ainsi que l'accès aux données conservées respectent les limites du strict nécessaire. La Cour rappelle qu'une telle mesure de conservation rapide peut être étendue aux données relatives au trafic et aux données de localisation afférentes à des personnes autres que celles qui sont soupçonnées d'avoir projeté ou commis une infraction pénale grave ou une atteinte à la sécurité nationale, pour autant que ces données puissent, sur la base d'éléments objectifs et non discriminatoires, contribuer à l'élucidation d'une telle infraction ou d'une telle atteinte à la sécurité nationale, telles que les données de la victime de celle-ci ainsi que celles de son entourage social ou professionnel.

Cependant, la Cour indique, ensuite, que toutes les mesures législatives susmentionnées doivent assurer, par des règles claires et précises, que la conservation des données en cause est subordonnée au respect des conditions matérielles et procédurales y afférentes et que les personnes concernées disposent de garanties effectives contre les risques d'abus. Les différentes mesures de conservation des données relatives au trafic et des données de localisation peuvent, selon le choix du législateur national et tout en respectant les limites du strict nécessaire, être appliquées conjointement.

En outre, la Cour précise qu'autoriser, aux fins de la lutte contre la criminalité grave, un accès à des telles données conservées de manière généralisée et indifférenciée, pour faire face à une menace grave pour la sécurité nationale, serait contraire à la hiérarchie des objectifs d'intérêt général pouvant justifier une mesure prise au titre de la directive « vie privée et communications électroniques »⁴⁸. En effet, ceci reviendrait à permettre que l'accès puisse être justifié par un objectif d'une importance moindre que celui ayant

⁴⁸ Cette hiérarchie est consacrée dans la jurisprudence de la Cour, et notamment dans l'arrêt du 6 octobre 2020, *La Quadrature du Net e.a. (C-511/18, C-512/18 et C-520/18, EUC:2020:791)*, points 135 et 136. En vertu de cette hiérarchie, la lutte contre la criminalité grave est d'une importance moindre que la sauvegarde de la sécurité nationale.

justifié la conservation, à savoir la sauvegarde de la sécurité nationale, risquant ainsi de priver de tout effet utile l'interdiction de procéder à une conservation généralisée et indifférenciée aux fins de la lutte contre la criminalité grave.

En deuxième lieu, la Cour décide que la directive « vie privée et communications électroniques », lue à la lumière de la Charte, s'oppose à une réglementation nationale, en vertu de laquelle le traitement centralisé des demandes d'accès à des données conservées par les fournisseurs de services de communications électroniques, émanant de la police dans le cadre de la recherche et de la poursuite d'infractions pénales graves, incombe à un fonctionnaire de police, même lorsque celui-ci est assisté par une unité instituée au sein de la police jouissant d'un certain degré d'autonomie dans l'exercice de sa mission et dont les décisions peuvent faire ultérieurement l'objet d'un contrôle juridictionnel. En effet, d'une part, un tel fonctionnaire ne remplit pas les exigences d'indépendance et d'impartialité qui s'imposent à une autorité administrative exerçant le contrôle préalable des demandes d'accès aux données émanant des autorités nationales compétentes, dans la mesure où il n'a pas la qualité de tiers par rapport à ces autorités. D'autre part, si la décision d'un tel fonctionnaire peut faire l'objet d'un contrôle juridictionnel exercé a posteriori, ce contrôle ne peut pas se substituer à un contrôle indépendant et, sauf cas d'urgence dûment justifiée, préalable.

En troisième lieu, enfin, la Cour confirme sa jurisprudence selon laquelle le droit de l'Union s'oppose à ce qu'une juridiction nationale limite dans le temps les effets d'une déclaration d'invalidité qui lui incombe, en vertu du droit national, à l'égard d'une législation nationale imposant aux fournisseurs de services de communications électroniques une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, en raison de l'incompatibilité de cette législation avec la directive « vie privée et communications électroniques ». Cela étant, la Cour rappelle que l'admissibilité des éléments de preuve obtenus au moyen d'une telle conservation relève, conformément au principe d'autonomie procédurale des États membres, du droit national, sous réserve du respect notamment des principes d'équivalence et d'effectivité.

Arrêt du 20 septembre 2022 (grande chambre), SpaceNet et Telekom Deutschland (C-793/19 et C-794/19, [EU:C:2022:702](#))

Dans les présentes affaires jointes, deux demandes de décision préjudicielle ont été présentées par le Bundesverwaltungsgericht (Cour administrative fédérale, Allemagne), qui a été saisi d'un recours en Revision par la République fédérale d'Allemagne contre deux arrêts ayant accueilli les recours formés par deux sociétés, SpaceNet AG (affaire C-793/19) et Telekom Deutschland GmbH (affaire C-794/19), fournissant des services d'accès à Internet. Par ces recours, ces sociétés contestaient l'obligation qu'impose la

réglementation allemande⁴⁹ de conserver des données relatives au trafic et des données de localisation afférentes aux communications électroniques de leurs clients.

Les doutes émis par la juridiction de renvoi portaient notamment sur la compatibilité avec la directive « vie privée et communications électroniques »⁵⁰, lue à la lumière de la charte des droits fondamentaux de l'Union européenne (ci-après la « Charte »)⁵¹ et de l'article 4, paragraphe 2, TUE, d'une réglementation nationale qui impose aux fournisseurs de services de communications électroniques accessibles au public, notamment aux fins de la répression des infractions pénales graves ou de la prévention d'un risque concret pour la sécurité nationale, la conservation généralisée et indifférenciée de l'essentiel des données relatives au trafic et des données de localisation des utilisateurs de ces services, en prévoyant une durée de conservation de plusieurs semaines, ainsi que des règles visant à garantir une protection efficace des données conservées contre les risques d'abus ainsi que contre tout accès illicite à ces données.

Par son arrêt, la Cour, réunie en grande chambre, confirme, tout en précisant sa portée, la jurisprudence issue de l'arrêt *La Quadrature du Net e.a.*, et, plus récemment, de l'arrêt *Commissioner of An Garda Síochána e.a.*⁵². Elle rappelle notamment que la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation afférentes aux communications électroniques n'est pas autorisée, à titre préventif, aux fins de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique.

La Cour commence par confirmer l'applicabilité de la directive « vie privée et communications électroniques » à la réglementation nationale en cause, puis effectue un rappel didactique des principes issus de sa jurisprudence, avant de procéder à un examen détaillé des caractéristiques de la réglementation nationale en cause, mises en exergue par la juridiction de renvoi.

En ce qui concerne, tout d'abord, l'étendue des données conservées, la Cour relève que l'obligation de conservation prévue par la réglementation nationale en cause s'étend à un ensemble très large de données relatives au trafic et de données de localisation et qu'elle concerne la quasi-totalité des personnes composant la population sans que celles-ci se trouvent, même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales. Elle relève également que cette réglementation impose la conservation, sans motif, généralisée et non différenciée d'un point de vue personnel, temporel et géographique, de l'essentiel des données relatives au trafic et des données de localisation dont l'étendue correspond, en substance, à celle des données conservées dans les affaires ayant conduit à l'arrêt *La Quadrature du Net e.a.* Partant, eu égard à

⁴⁹ Dispositions combinées de l'article 113a, paragraphe 1, et de l'article 113b du Telekommunikationsgesetz (loi sur les télécommunications), du 22 juin 2004 (BGBI. 2004 I, p. 1190), dans sa version applicable au litige au principal.

⁵⁰ Plus précisément, l'article 15, paragraphe 1, de la directive 2002/58.

⁵¹ Articles 6 à 8, 11 et 52, paragraphe 1, de la Charte.

⁵² Arrêt du 5 avril 2022, *Commissioner of An Garda Síochána e.a.* (C-140/20, [EUC-2022-258](#)).

cette jurisprudence, la Cour considère qu'une obligation de conservation des données telle que celle en cause en l'espèce ne peut être considérée comme étant une conservation ciblée des données.

Ensuite, s'agissant de la durée de conservation des données, la Cour rappelle qu'il ressort de la directive « vie privée et communications électroniques »⁵³ que la durée de conservation prévue par une mesure nationale imposant une obligation de conservation généralisée et indifférenciée est, certes, un facteur pertinent, parmi d'autres, afin de déterminer si le droit de l'Union s'oppose à une telle mesure, ladite directive exigeant que cette durée soit « limitée ». Toutefois, la gravité de l'ingérence découle du risque, notamment eu égard à leur nombre et à leur variété, que les données conservées, prises dans leur ensemble, permettent de tirer des conclusions très précises concernant la vie privée de la ou des personnes dont les données ont été conservées et, en particulier, fournissent les moyens d'établir le profil de la ou des personnes concernées, qui est une information tout aussi sensible, au regard du droit au respect de la vie privée, que le contenu même des communications. Partant, la conservation des données relatives au trafic ou des données de localisation présente en tout état de cause un caractère grave, indépendamment de la durée de la période de conservation, de la quantité ou de la nature des données conservées, lorsque l'ensemble de données conservées est susceptible de permettre de tirer de telles conclusions⁵⁴.

Enfin, en ce qui concerne les garanties visant à protéger les données conservées contre les risques d'abus et contre tout accès illicite, la Cour relève, en se fondant sur la jurisprudence antérieure, que la conservation des données et l'accès à celles-ci constituent des ingérences distinctes dans les droits fondamentaux des personnes concernées, nécessitant une justification distincte. Il en découle qu'une législation nationale assurant le plein respect des conditions résultant de la jurisprudence en matière d'accès aux données conservées ne saurait, par nature, être susceptible ni de limiter ni même de remédier à l'ingérence grave dans les droits des personnes concernées qui résulterait de la conservation généralisée de ces données.

Par ailleurs, afin de répondre à des arguments présentés devant elle, la Cour relève, en premier lieu, qu'une menace pour la sécurité nationale doit être réelle et actuelle ou, à tout le moins, prévisible, ce qui suppose la survenance de circonstances suffisamment concrètes, pour pouvoir justifier une mesure de conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, pendant une durée limitée. Une telle menace se distingue donc, par sa nature, sa gravité et le caractère spécifique des circonstances qui la constituent, du risque général et permanent de survenance de tensions ou de troubles, même graves, à la sécurité

⁵³ Plus précisément, de l'article 15, paragraphe 1, deuxième phrase, de la directive 2002/58.

⁵⁴ Voir, en ce qui concerne l'accès à de telles données, arrêt du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques) (C-746/18, [EUC2021:152](#), point 39).

publique ou celui d'infractions pénales graves. Ainsi, la criminalité, même particulièrement grave, ne peut être assimilée à une menace pour la sécurité nationale.

Elle relève, en second lieu, que le fait d'autoriser, aux fins de la lutte contre la criminalité grave, un accès à des données relatives au trafic et des données de localisation conservées de manière généralisée et indifférenciée, pour faire face à une menace grave pour la sécurité nationale, serait contraire à la hiérarchie des objectifs d'intérêt général pouvant justifier une mesure prise au titre de la directive « vie privée et communications électroniques »⁵⁵. En effet, ceci reviendrait à permettre que l'accès puisse être justifié par un objectif d'une importance moindre que celui ayant justifié la conservation, à savoir la sauvegarde de la sécurité nationale, ce qui risquerait de priver de tout effet utile l'interdiction de procéder à une conservation généralisée et indifférenciée aux fins de la lutte contre la criminalité grave.

La Cour conclut, en confirmant sa jurisprudence antérieure, que la directive « vie privée et communications électroniques », lue à la lumière de la Charte, s'oppose à des mesures législatives nationales prévoyant, à titre préventif, aux fins de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation.

En revanche, elle ne s'oppose pas à des mesures législatives nationales permettant, aux fins de la sauvegarde de la sécurité nationale, le recours à une injonction faite aux fournisseurs de services de communications électroniques de procéder à une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, dans des situations où l'État membre concerné fait face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible. À cet égard, la Cour précise que la décision prévoyant cette injonction peut faire l'objet d'un contrôle effectif soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, visant à vérifier l'existence d'une de ces situations ainsi que le respect des conditions et des garanties devant être prévues, et ladite injonction ne pouvant être émise que pour une période temporellement limitée au strict nécessaire, mais renouvelable en cas de persistance de cette menace.

Cette directive, lue à la lumière de la Charte, ne s'oppose pas non plus à des mesures législatives nationales prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation ciblée des données relatives au trafic et des données de localisation qui soit délimitée, sur la base d'éléments objectifs et non discriminatoires, en fonction de catégories de personnes concernées ou au moyen d'un

⁵⁵ Cette hiérarchie est consacrée dans la jurisprudence de la Cour, et notamment dans l'arrêt *La Quadrature du Net e.a.*, aux points 135 et 136. En vertu de cette hiérarchie, la lutte contre la criminalité grave est d'une importance moindre que la sauvegarde de la sécurité nationale.

critère géographique, pour une période temporellement limitée au strict nécessaire, mais renouvelable.

Il en est de même pour ce qui est des mesures législatives nationales prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion, pour une période temporellement limitée au strict nécessaire, ainsi que des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques, dont il est constant que la conservation est susceptible de contribuer à la lutte contre la criminalité grave, pour autant que ces données permettent d'identifier les personnes ayant utilisé de tels moyens dans le contexte de la préparation ou de la commission d'un acte relevant de la criminalité grave.

Il n'en va pas différemment pour ce qui est des mesures législatives nationales permettant, aux fins de la lutte contre la criminalité grave et, a fortiori, de la sauvegarde de la sécurité nationale, le recours à une injonction faite aux fournisseurs de services de communications électroniques, au moyen d'une décision de l'autorité compétente soumise à un contrôle juridictionnel effectif, de procéder, pour une durée déterminée, à la conservation rapide des données relatives au trafic et des données de localisation dont disposent ces fournisseurs de services.

Cependant, la Cour indique que toutes les mesures susmentionnées doivent assurer, par des règles claires et précises, que la conservation des données en cause est subordonnée au respect des conditions matérielles et procédurales y afférentes et que les personnes concernées disposent de garanties effectives contre les risques d'abus. Ces différentes mesures peuvent, selon le choix du législateur national et tout en respectant les limites du strict nécessaire, être appliquées conjointement.

Arrêt du 15 juin 2021 (grande chambre), Facebook Ireland e.a. (C-645/19, EU:C:2021:483)

Le 11 septembre 2015, le président de la Commission belge de la protection de la vie privée, (ci-après la « CPVP ») a saisi le Nederlandstalige rechtbank van eerste aanleg Brussel (tribunal de première instance néerlandophone de Bruxelles, Belgique), d'une action en cessation à l'encontre de Facebook Ireland, Facebook Inc. et Facebook Belgium, visant à mettre un terme à des violations, prétendument commises par Facebook, de la législation relative à la protection des données. Ces violations consistaient notamment en la collecte et l'utilisation d'informations sur le comportement de navigation des internautes belges, détenteurs ou non d'un compte Facebook, au moyen de différentes technologies, telles que les cookies, les modules sociaux⁵⁶ ou les pixels.

⁵⁶ Par exemple, les boutons « J'aime » ou « Partager ».

Le 16 février 2018, ce tribunal s'est déclaré compétent pour statuer sur cette action et, sur le fond, a jugé que le réseau social Facebook n'avait pas suffisamment informé les internautes belges de la collecte et de l'usage des informations concernées. Par ailleurs, le consentement donné par les internautes à la collecte et au traitement desdites informations a été jugé non valable.

Le 2 mars 2018, Facebook Ireland, Facebook Inc. et Facebook Belgium ont interjeté appel de ce jugement devant le Hof van beroep te Brussel (cour d'appel de Bruxelles, Belgique), la juridiction de renvoi dans la présente affaire. Devant cette juridiction, l'Autorité belge de protection des données (ci-après l'« APD ») a agi en tant que successeur légal du président de la CPVP. La juridiction de renvoi s'est déclarée uniquement compétente pour statuer sur l'appel interjeté par Facebook Belgium.

La juridiction de renvoi a éprouvé des doutes au sujet de l'incidence de l'application du mécanisme de « guichet unique » prévu par le règlement relatif à la protection des données⁵⁷ sur les compétences de l'APD et s'est posée, plus particulièrement, la question de savoir si, pour les faits postérieurs à l'entrée en vigueur du RGPD, à savoir le 25 mai 2018, l'APD peut agir contre Facebook Belgium, dès lors que c'est Facebook Ireland qui a été identifié comme responsable du traitement des données concernées. En effet, depuis cette date et notamment en application du principe de « guichet unique » prévu par le RGPD, seul le Commissaire irlandais à la protection des données serait compétent pour intenter une action en cessation, sous le contrôle des juridictions irlandaises.

Dans son arrêt, rendu en grande chambre, la Cour précise les pouvoirs des autorités nationales de contrôle dans le cadre du RGPD. Ainsi, elle juge notamment que ce règlement autorise, sous certaines conditions, une autorité de contrôle d'un État membre à exercer son pouvoir de porter toute présumée violation du RGPD devant une juridiction de cet État et d'ester en justice en ce qui concerne un traitement de données transfrontalier⁵⁸, alors qu'elle n'est pas l'autorité chef de file pour ce traitement.

En premier lieu, la Cour précise les conditions dans lesquelles une autorité nationale de contrôle, n'ayant pas la qualité d'autorité chef de file en ce qui concerne un traitement transfrontalier, doit exercer son pouvoir de porter toute présumée violation du RGPD devant une juridiction d'un État membre et, le cas échéant, d'ester en justice afin d'assurer l'application de ce règlement. Ainsi, d'une part, le RGPD doit conférer à cette autorité de contrôle une compétence pour adopter une décision constatant que ce traitement méconnaît les règles prévues par ce règlement et, d'autre part, ce pouvoir

⁵⁷ Règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO 2016, L 119, p. 1, ci-après le « RGPD »). Aux termes de l'article 56, paragraphe 1, du RGPD : « Sans préjudice de l'article 55, l'autorité de contrôle de l'établissement principal ou de l'établissement unique du responsable du traitement ou du sous-traitant est compétente pour agir en tant qu'autorité de contrôle chef de file concernant le traitement transfrontalier effectué par ce responsable du traitement ou ce sous-traitant ».

⁵⁸ Au sens de l'article 4, point 23, du RGPD.

doit être exercé dans le respect des procédures de coopération et de contrôle de la cohérence prévues par ce règlement⁵⁹.

En effet, pour les traitements transfrontaliers, le RGPD prévoit le mécanisme du « guichet unique »⁶⁰, qui est fondé sur une répartition des compétences entre une « autorité de contrôle chef de file » et les autres autorités nationales de contrôle concernées. Ce mécanisme exige une coopération étroite, loyale et efficace entre ces autorités, afin d'assurer une protection cohérente et homogène des règles relatives à la protection des données à caractère personnel et ainsi préserver son effet utile. Le RGPD consacre à cet égard la compétence de principe de l'autorité de contrôle chef de file pour adopter une décision constatant qu'un traitement transfrontalier méconnaît les règles prévues par ce règlement⁶¹, tandis que la compétence des autres autorités nationales de contrôle pour adopter une telle décision, même à titre provisoire, constitue l'exception⁶². Cependant, dans l'exercice de ses compétences, l'autorité de contrôle chef de file ne saurait s'affranchir d'un dialogue indispensable ainsi que d'une coopération loyale et efficace avec les autres autorités de contrôle concernées. De ce fait, dans le cadre de cette coopération, l'autorité de contrôle chef de file ne peut ignorer les points de vue des autres autorités de contrôle concernées et toute objection pertinente et motivée formulée par l'une de ces dernières autorités a pour effet de bloquer, à tout le moins temporairement, l'adoption du projet de décision de l'autorité de contrôle chef de file.

La Cour précise par ailleurs que la circonstance qu'une autorité de contrôle d'un État membre qui n'est pas l'autorité de contrôle chef de file s'agissant d'un traitement de données transfrontalier ne puisse exercer le pouvoir de porter toute prévue violation du RGPD devant une juridiction de cet État et d'ester en justice que dans le respect des règles de répartition des compétences décisionnelles entre l'autorité de contrôle chef de file et les autres autorités de contrôle⁶³ est conforme aux articles 7, 8 et 47 de la charte des droits fondamentaux de l'Union européenne, garantissant à la personne concernée, respectivement, le droit à la protection de ses données à caractère personnel et le droit à un recours effectif.

En deuxième lieu, la Cour juge que, en cas de traitement de données transfrontalier, l'exercice du pouvoir d'une autorité de contrôle d'un État membre, autre que l'autorité de contrôle chef de file, d'intenter une action en justice⁶⁴ ne requiert pas que le responsable du traitement ou le sous-traitant pour le traitement transfrontalier de données à caractère personnel visé par cette action dispose d'un établissement principal ou d'un autre établissement sur le territoire de cet État membre. Cependant,

⁵⁹ Prévues aux articles 56 et 60 du RGPD.

⁶⁰ Article 56, paragraphe 1, du RGPD.

⁶¹ Article 60, paragraphe 7, du RGPD.

⁶² L'article 56, paragraphe 2, et l'article 66 du RGPD consacrent les exceptions au principe de la compétence décisionnelle de l'autorité de contrôle chef de file.

⁶³ Prévues aux articles 55 et 56, lus conjointement avec l'article 60 du RGPD.

⁶⁴ En vertu de l'article 58, paragraphe 5, du RGPD.

l'exercice de ce pouvoir doit relever du champ d'application territoriale du RGPD⁶⁵, ce qui suppose que le responsable du traitement ou le sous-traitant pour le traitement transfrontalier dispose d'un établissement sur le territoire de l'Union.

En troisième lieu, la Cour dit pour droit que, en cas de traitement de données transfrontalier, le pouvoir d'une autorité de contrôle d'un État membre, autre que l'autorité de contrôle chef de file, de porter toute présumée violation du RGPD devant une juridiction de cet État et, le cas échéant, d'ester en justice peut être exercé tant à l'égard de l'établissement principal du responsable du traitement qui se trouve dans l'État membre dont relève cette autorité qu'à l'égard d'un autre établissement de ce responsable, pour autant que l'action en justice vise un traitement de données effectué dans le cadre des activités de cet établissement et que ladite autorité soit compétente pour exercer ce pouvoir.

Cependant, la Cour précise que l'exercice de ce pouvoir suppose que le RGPD soit d'application. En l'occurrence, les activités de l'établissement du groupe Facebook situé en Belgique étant indissociablement liées au traitement des données à caractère personnel en cause au principal, dont Facebook Ireland est le responsable s'agissant du territoire de l'Union, ce traitement est effectué « dans le cadre des activités d'un établissement du responsable du traitement » et partant, relève bien du champ d'application du RGPD.

En quatrième lieu, la Cour juge que, lorsqu'une autorité de contrôle d'un État membre qui n'est pas l'« autorité de contrôle chef de file » a intenté, avant la date d'entrée en vigueur du RGPD, une action en justice visant un traitement transfrontalier de données à caractère personnel, cette action peut être maintenue, en vertu du droit de l'Union, sur le fondement des dispositions de la directive relative à la protection des données⁶⁶, laquelle demeure applicable en ce qui concerne les infractions aux règles qu'elle prévoit commises jusqu'à la date à laquelle cette directive a été abrogée. En outre, cette action peut être intentée par cette autorité pour des infractions commises après la date d'entrée en vigueur du RGPD, pour autant que ce soit dans l'une des situations où, à titre d'exception, ce règlement confère à cette même autorité une compétence pour adopter une décision constatant que le traitement de données concerné méconnaît les règles prévues par ce règlement et dans le respect des procédures de coopération que ce dernier prévoit.

En cinquième et dernier lieu, la Cour reconnaît l'effet direct de la disposition du RGPD en vertu de laquelle chaque État membre prévoit, par la loi, que son autorité de contrôle a le pouvoir de porter toute violation de ce règlement à l'attention des autorités judiciaires et, le cas échéant, d'ester en justice. Par conséquent, une telle autorité peut invoquer

⁶⁵ L'article 3, paragraphe 1, du RGPD prévoit que ce règlement s'applique au traitement des données à caractère personnel effectué « dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union ».

⁶⁶ Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO 1995, L 281, p. 31).

cette disposition pour intenter ou reprendre une action contre des particuliers, même si elle n'a pas été spécifiquement mise en œuvre dans la législation de l'État membre concerné.

Arrêt du 30 avril 2024 (assemblée plénière), La Quadrature du Net e.a. (Données personnelles et lutte contre la contrefaçon) (C-470/21, [EU:C:2024:370](#))

Ces dernières années, la Cour a été appelée, à plusieurs reprises, à se prononcer sur la conservation et l'accès aux données à caractère personnel dans le domaine des communications électroniques et a établi, par conséquent, une riche jurisprudence en la matière⁶⁷. Saisie à titre préjudiciel par le Conseil d'État (France), l'assemblée plénière de la Cour développe cette jurisprudence en apportant des précisions concernant, d'une part, les conditions dans lesquelles une conservation généralisée d'adresses IP par des fournisseurs de services de communications électroniques peut ne pas être regardée comme entraînant une ingérence grave dans les droits au respect de la vie privée, à la protection des données à caractère personnel ainsi qu'à la liberté d'expression garantis par la Charte⁶⁸, ainsi que, d'autre part, la possibilité, pour une autorité publique, d'accéder à certaines données à caractère personnel conservées dans le respect de telles conditions, dans le cadre de la lutte contre les infractions aux droits de propriété intellectuelle commises en ligne.

En l'occurrence, quatre associations ont présenté au Premier ministre (France) une demande d'abrogation du décret relatif au traitement automatisé de données à caractère personnel⁶⁹. Cette demande n'ayant pas été suivie d'effet, ces associations ont saisi le Conseil d'État d'un recours tendant à l'annulation de cette décision implicite de rejet. Selon elles, ce décret ainsi que les dispositions qui en constituent la base légale⁷⁰ méconnaissent le droit de l'Union.

En vertu de la législation française, la Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet (Hadopi), afin de pouvoir identifier les responsables d'atteintes aux droits d'auteur ou aux droits voisins commises en ligne, est autorisée à accéder à certaines données que les fournisseurs de services de communications électroniques sont tenus de conserver. Ces données portent sur l'identité civile d'une personne concernée correspondant à son adresse IP collectée préalablement par des organismes d'ayants droit. Une fois que le titulaire de l'adresse IP utilisée pour des activités portant une telle atteinte est identifié, la Hadopi suit la procédure dite de

⁶⁷ Voir, notamment, arrêts du 21 décembre 2016, Tele2 Sverige et Watson e.a. (C-203/15 et C-698/15, [EU:C:2016:970](#)), du 2 octobre 2018, Ministerio Fiscal (C-207/16, [EU:C:2018:788](#)), du 6 octobre 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 et C-520/18, [EU:C:2020:791](#)), du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques) (C-746/18, [EU:C:2021:152](#)), du 17 juin 2021, M.I.C.M. (C-597/19, [EU:C:2021:492](#)), et du 5 avril 2022, Commissioner of An Garda Síochána e.a. (C-140/20, [EU:C:2022:258](#)).

⁶⁸ Articles 7, 8 et 11 de la charte des droits fondamentaux de l'Union européenne (ci-après la « Charte »).

⁶⁹ Décret n° 2010-236, du 5 mars 2010, relatif au traitement automatisé de données à caractère personnel autorisé par l'article L. 331-29 du code de la propriété intellectuelle dénommé « Système de gestion des mesures pour la protection des œuvres sur internet » (JORF n° 56 du 7 mars 2010, texte n° 19), tel que modifié par le décret n° 2017-924, du 6 mai 2017, relatif à la gestion des droits d'auteur et des droits voisins par un organisme de gestion de droits et modifiant le code de la propriété intellectuelle (JORF n° 109 du 10 mai 2017, texte n° 176).

⁷⁰ Notamment l'article L. 331-21, troisième à cinquième alinéas, du code de la propriété intellectuelle.

« réponse graduée ». Concrètement, elle est habilitée à envoyer, à cette personne, deux recommandations qui s'apparentent à des avertissements et, si les activités persistent, une lettre lui notifiant que ses activités sont susceptibles de poursuites pénales. Enfin, elle est en droit de saisir le ministère public en vue de la poursuite de ladite personne⁷¹.

Dans ce contexte, le Conseil d'État a interrogé la Cour sur l'interprétation de la directive « vie privée et communications électroniques », lue à la lumière de la Charte⁷².

En premier lieu, s'agissant de la conservation des données relatives à l'identité civile et des adresses IP correspondantes, la Cour souligne que toute conservation généralisée et indifférenciée des adresses IP ne constitue pas nécessairement une ingérence grave dans les droits au respect de la vie privée, à la protection des données à caractère personnel ainsi qu'à la liberté d'expression garantis par la Charte.

L'obligation d'assurer une telle conservation peut être justifiée par l'objectif de la lutte contre les infractions pénales en général, lorsqu'il est effectivement exclu que cette conservation puisse engendrer des ingérences graves dans la vie privée de la personne concernée en raison de la possibilité de tirer des conclusions précises sur celle-ci moyennant, notamment, une mise en relation de ces adresses IP avec un ensemble de données de trafic ou de localisation.

Partant, un État membre qui entend imposer aux fournisseurs de services de communications électroniques une telle obligation doit s'assurer que les modalités de conservation de ces données excluent que puissent être tirées des conclusions précises sur la vie privée des personnes concernées.

La Cour précise que les modalités de conservation doivent, à cet effet, concerter la structure même de la conservation qui, en substance, doit être organisée de manière à garantir une séparation effectivement étanche des différentes catégories de données conservées. Ainsi, les règles nationales relatives à ces modalités doivent assurer que chaque catégorie de données, y compris les données relatives à l'identité civile et les adresses IP, est conservée de manière pleinement séparée des autres catégories de données conservées et que cette séparation est effectivement étanche, moyennant un dispositif informatique sécurisé et fiable. De plus, dans la mesure où ces règles prévoient la possibilité d'une mise en relation des adresses IP conservées avec l'identité civile de la personne concernée à des fins de lutte contre des infractions, elles ne doivent permettre une telle mise en relation que par l'usage d'un procédé technique performant ne remettant pas en cause l'efficacité de la séparation étanche de ces catégories de données. La fiabilité de cette séparation doit faire l'objet d'un contrôle

⁷¹ À compter du 1^{er} janvier 2022, la Hadopi a été fusionnée avec le Conseil supérieur de l'audiovisuel (CSA), autre autorité publique indépendante, pour constituer l'Autorité de régulation de la communication audiovisuelle et numérique (ARCOM). La procédure de réponse graduée est toutefois restée en substance inchangée.

⁷² Article 15, paragraphe 1, de la directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO 2002, L 201, p. 37), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009 (JO 2009, L 337, p. 11) (ci-après la « directive "vie privée et communications électroniques" »), lue à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte.

régulier par une autorité publique tierce. Pour autant que la législation nationale applicable prévoit de telles exigences strictes, l'ingérence résultant de cette conservation des adresses IP ne saurait être qualifiée de « grave ».

Dès lors, la Cour conclut que, en présence d'un dispositif législatif garantissant qu'aucune combinaison de données ne permettra de tirer des conclusions précises sur la vie privée des personnes dont les données sont conservées, la directive « vie privée et communications électroniques », lue à la lumière de la Charte, ne s'oppose pas à ce qu'un État membre impose une obligation de conservation généralisée et indifférenciée des adresses IP, pour une durée ne dépassant pas le strict nécessaire, aux fins d'un objectif de lutte contre les infractions pénales en général.

En deuxième lieu, en ce qui concerne l'accès à des données relatives à l'identité civile correspondant à des adresses IP, la Cour dit pour droit que la directive « vie privée et communications électroniques », lue à la lumière de la Charte, ne s'oppose pas, en principe, à une réglementation nationale permettant l'accès, par une autorité publique, à ces données conservées par les fournisseurs de services de communications électroniques de manière séparée et effectivement étanche, à la seule fin que cette autorité puisse identifier les titulaires de ces adresses soupçonnés d'être responsables d'atteintes aux droits d'auteur et aux droits voisins sur Internet et prendre des mesures à leur égard. Dans un tel cas, la réglementation nationale doit interdire aux agents disposant d'un tel accès, premièrement, de divulguer sous quelque forme que ce soit des informations sur le contenu des fichiers consultés par ces titulaires, sauf aux seules fins de saisir le ministère public, deuxièmement, d'effectuer tout traçage du parcours de navigation de ces titulaires et, troisièmement, d'utiliser ces adresses IP à des fins autres que celle de l'adoption de ces mesures.

Dans ce contexte, la Cour rappelle notamment que, même si la liberté d'expression et la confidentialité des données à caractère personnel sont des préoccupations primordiales, ces droits fondamentaux ne sont pas pour autant absous. En effet, dans le cadre d'une mise en balance des droits et intérêts en cause, ceux-ci doivent parfois s'effacer devant d'autres droits fondamentaux et des impératifs d'intérêt général tels que la défense de l'ordre public et la prévention des infractions pénales ou la protection des droits et libertés d'autrui. Tel est, en particulier, le cas lorsque la prépondérance accordée auxdites préoccupations primordiales est de nature à entraver l'efficacité d'une enquête pénale, notamment en rendant impossible ou excessivement difficiles l'identification effective de l'auteur d'une infraction pénale et l'imposition d'une sanction à son égard.

Dans ce même contexte, la Cour se réfère également à sa jurisprudence selon laquelle, s'agissant de la lutte contre les infractions pénales portant atteinte aux droits d'auteur ou aux droits voisins commises en ligne, la circonstance que l'accès aux adresses IP peut constituer le seul moyen d'investigation permettant l'identification de la personne concernée tend à établir que la conservation de ces adresses et l'accès à celles-ci sont strictement nécessaires à la réalisation de l'objectif poursuivi et répondent donc à

l'exigence de proportionnalité. Ne pas permettre un tel accès comporterait d'ailleurs un réel risque d'impunité systémique d'infractions pénales commises en ligne ou dont la commission ou la préparation est facilitée par les caractéristiques propres à Internet. Or, l'existence d'un tel risque constitue une circonstance pertinente afin d'apprécier, dans le cadre d'une mise en balance des différents droits et intérêts en présence, si une ingérence dans les droits au respect de la vie privée, à la protection des données personnelles ainsi qu'à la liberté d'expression est une mesure proportionnée au regard de l'objectif de lutte contre les infractions pénales.

En troisième lieu, en se prononçant sur le point de savoir si l'accès de l'autorité publique à des données relatives à l'identité civile correspondant à une adresse IP doit être subordonné à un contrôle préalable par une juridiction ou une entité administrative indépendante, la Cour considère que l'exigence d'un tel contrôle s'impose lorsque, dans le contexte d'une réglementation nationale, cet accès comporte le risque d'une ingérence grave dans les droits fondamentaux de la personne concernée en ce sens qu'il pourrait permettre à cette autorité publique de tirer des conclusions précises sur la vie privée de cette personne et, le cas échéant, d'établir son profil détaillé. Inversement, cette exigence d'un contrôle préalable n'a pas vocation à s'appliquer lorsque l'ingérence dans les droits fondamentaux ne peut être qualifiée de grave.

À cet égard, la Cour précise que, dans le cas où un dispositif de conservation garantissant une séparation effectivement étanche des différentes catégories de données conservées est mis en place, l'accès de l'autorité publique aux données relatives à l'identité civile correspondant aux adresses IP n'est, en principe, pas subordonné à l'exigence d'un contrôle préalable. En effet, un tel accès à seule fin d'identifier le titulaire d'une adresse IP ne constitue pas, en règle générale, une ingérence grave dans les droits susvisés.

Toutefois, la Cour n'exclut pas que, dans des situations atypiques, un risque existe que, dans le cadre d'une procédure telle que la procédure de réponse graduée en cause au principal, l'autorité publique puisse tirer des conclusions précises sur la vie privée de la personne concernée, notamment lorsque cette personne se livre à des activités portant atteinte aux droits d'auteur ou aux droits voisins, sur des réseaux de pair à pair, de manière répétée, voire à grande échelle, en lien avec des œuvres protégées de types particuliers, révélant des informations, le cas échéant sensibles, sur la vie privée de ladite personne.

En l'occurrence, un titulaire d'une adresse IP peut être particulièrement exposé à un tel risque lorsque l'autorité publique est appelée à décider de saisir ou non le ministère public en vue de sa poursuite. En effet, l'intensité de l'atteinte au droit au respect de la vie privée est susceptible de croître au fur et à mesure que la procédure de réponse graduée, qui opère selon un processus séquentiel, parcourt les différentes étapes qui la composent. L'accès de l'autorité compétente à l'ensemble des données relatives à la personne concernée et cumulées au cours des différentes étapes de cette procédure peut permettre de tirer des conclusions précises sur la vie privée de celle-ci. Par

conséquent, la réglementation nationale doit prévoir un contrôle préalable qui doit intervenir avant que l'autorité publique puisse mettre en relation des données d'identité civile et un tel ensemble de données, et avant l'éventuel envoi de la lettre de notification constatant que cette personne s'est livrée à des faits susceptibles de poursuites pénales. Ce contrôle doit par ailleurs préserver l'efficacité de la procédure de réponse graduée en permettant en particulier d'identifier les cas de nouvelle réitération possible du comportement infractionnel en cause. À cette fin, cette procédure doit être organisée et structurée de manière à ce que les données d'identité civile d'une personne correspondant à des adresses IP préalablement collectées sur Internet ne soient pas automatiquement susceptibles d'être mises en relation, par les personnes chargées de l'examen des faits au sein de l'autorité publique compétente, avec des éléments dont cette dernière dispose déjà et qui pourraient permettre de tirer des conclusions précises sur la vie privée de cette personne.

En outre, s'agissant de l'objet du contrôle préalable, la Cour relève que, dans les cas où la personne concernée est soupçonnée d'avoir commis une infraction relevant des infractions pénales en général, la juridiction ou l'entité administrative indépendante en charge de ce contrôle doit refuser l'accès lorsque ce dernier permettrait à l'autorité publique de tirer des conclusions précises sur la vie privée de ladite personne. En revanche, même un accès permettant de tirer de telles conclusions précises devrait être autorisé dans les cas où la personne concernée est soupçonnée d'avoir commis des délits considérés par l'État membre concerné comme portant atteinte à un intérêt fondamental de la société et relevant ainsi des formes graves de criminalité.

La Cour précise également qu'un contrôle préalable ne saurait en aucun cas être entièrement automatisé puisque, s'agissant d'une enquête pénale, un tel contrôle exige la mise en balance, d'une part, des intérêts légitimes liés à la lutte contre la criminalité et, d'autre part, du respect de la vie privée et de la protection des données à caractère personnel. Cette mise en balance nécessite l'intervention d'une personne physique, celle-ci étant d'autant plus nécessaire que l'automaticité et la grande échelle du traitement de données en cause emportent des risques pour la vie privée.

Ainsi, la Cour conclut que la possibilité, pour les personnes chargées de l'examen des faits au sein de l'autorité publique, de mettre en relation des données relatives à l'identité civile d'une personne correspondant à une adresse IP avec les fichiers comportant des éléments permettant de connaître le titre d'œuvres protégées dont la mise à disposition sur Internet a justifié la collecte des adresses IP par des organismes d'ayants droit doit être subordonnée, dans des hypothèses de nouvelle réitération d'une activité portant atteinte aux droits d'auteur ou aux droits voisins par une même personne, à un contrôle par une juridiction ou une entité administrative indépendante. Ce contrôle ne peut être entièrement automatisé et doit intervenir préalablement à une telle mise en relation, susceptible dans de telles hypothèses de permettre que soient tirées des conclusions précises sur la vie privée de ladite personne dont l'adresse IP a

été utilisée pour des activités pouvant porter atteinte aux droits d'auteur ou aux droits voisins.

En quatrième et dernier lieu, la Cour note que le système de traitement de données utilisé par l'autorité publique doit faire l'objet, à intervalles réguliers, d'un contrôle par un organisme indépendant et ayant la qualité de tiers par rapport à cette autorité publique. Ce contrôle vise à vérifier l'intégrité du système, y compris les garanties effectives contre les risques d'accès et d'utilisation abusifs ou illicites de ces données, ainsi que son efficacité et sa fiabilité pour détecter les éventuels manquements.

Dans ce cadre, la Cour observe que, en l'occurrence, le traitement automatisé des données à caractère personnel effectué par l'autorité publique sur la base des informations relatives aux contrefaçons constatées par les organismes d'ayants droit est susceptible de comporter un certain nombre de faux cas positifs et surtout le risque qu'un nombre de données potentiellement très élevé soit détourné par des tiers à des fins abusives ou illicites, ce qui explique la nécessité d'un tel contrôle.

En outre, elle ajoute que ce traitement doit respecter les règles spécifiques de protection des données à caractère personnel prévues par la directive 2016/680⁷³. En effet, en l'espèce, même si l'autorité publique ne dispose pas de pouvoirs décisionnels propres dans le cadre de la procédure dite de réponse graduée, elle doit être qualifiée d'« autorité publique » impliquée dans la prévention et la détection des infractions pénales, et relève donc de son champ d'application. Ainsi, les personnes impliquées dans une telle procédure doivent bénéficier d'un ensemble de garanties matérielles et procédurales prescrit par la directive 2016/680, dont il appartient à la juridiction de renvoi de vérifier qu'elles sont prévues par la législation nationale.

5. Droit d'auteur

Arrêt du 3 juillet 2012 (grande chambre), UsedSoft (C-128/11, EU:C:2012:407)

La société Oracle développait et distribuait, notamment par téléchargement via Internet, des programmes d'ordinateur fonctionnant sur le mode « client/serveur ». Le client téléchargeait directement une copie du programme sur son ordinateur. Le droit d'utilisation incluait le droit de stocker de manière permanente la copie de ce programme sur un serveur et de permettre à 25 utilisateurs d'y accéder. Les contrats de licence prévoient que le client acquérait un droit d'utilisation à durée indéterminée, non cessible et réservé à un usage professionnel interne. UsedSoft, une entreprise

⁷³ Directive (UE) 2016/680 du Parlement européen et du Conseil, du 27 avril 2016, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (JO 2016, L 119, p. 89).

allemande, commercialisait des licences rachetées aux clients d'Oracle. Les clients de UsedSoft, non encore en possession du logiciel, le téléchargeaient directement, après avoir acquis une licence « d'occasion », à partir du site Internet d'Oracle. Les clients qui disposaient déjà de ce logiciel pouvaient acheter, de façon complémentaire, une licence ou une partie de la licence pour des utilisateurs supplémentaires. Dans ce cas, les clients téléchargeaient le logiciel vers la mémoire centrale des stations de travail de ces autres utilisateurs.

Oracle a assigné UsedSoft devant les juridictions allemandes afin de lui faire interdire cette pratique. Le Bundesgerichtshof (Cour suprême fédérale, Allemagne) a saisi la Cour de justice afin qu'elle interprète, dans ce contexte, la directive 2009/24/CE⁷⁴ concernant la protection juridique des programmes d'ordinateur.

Selon la Cour, l'article 4, paragraphe 2, de la directive 2009/24/CE doit être interprété en ce sens que le droit de distribution de la copie d'un programme d'ordinateur est épuisé si le titulaire du droit d'auteur, qui a autorisé, fût-ce à titre gratuit, le téléchargement de cette copie sur un support informatique au moyen d'Internet, a également conféré, moyennant le paiement d'un prix destiné à lui permettre d'obtenir une rémunération correspondant à la valeur économique de la copie de l'œuvre dont il est propriétaire, un droit d'usage de ladite copie, sans limitation de durée.

Le téléchargement d'une copie d'un programme d'ordinateur et la conclusion d'un contrat de licence d'utilisation se rapportant à celle-ci forment un tout indivisible. Lesdites opérations impliquent le transfert du droit de propriété de la copie du programme d'ordinateur concerné. À cet égard, il est indifférent que la copie du programme d'ordinateur ait été mise à la disposition du client au moyen d'un téléchargement ou au moyen d'un support matériel tel qu'un CD-ROM ou un DVD.

De surcroît, les articles 4, paragraphe 2, et 5, paragraphe 1, de la directive 2009/24/CE doivent être interprétés en ce sens que, en cas de revente d'une licence d'utilisation emportant la revente d'une copie d'un programme d'ordinateur téléchargée à partir du site Internet du titulaire du droit d'auteur, licence qui avait été initialement octroyée au premier acquéreur, le second acquéreur de ladite licence ainsi que tout acquéreur ultérieur de cette dernière pourront se prévaloir de l'épuisement du droit de distribution prévu à l'article 4, paragraphe 2, de cette directive et bénéficier du droit de reproduction.

Arrêt du 10 novembre 2016, Vereniging Openbare Bibliotheeken (C-174/15, EU:C:2016:856)

Aux Pays-Bas, le prêt de livres électroniques par les bibliothèques publiques ne relevait pas du régime de prêt public applicable aux livres traditionnels. Les bibliothèques publiques mettaient des livres électroniques à la disposition du public sur Internet, sur

⁷⁴ Directive 2009/24/CE du Parlement européen et du Conseil, du 23 avril 2009, concernant la protection juridique des programmes d'ordinateur (JO 2009, L 111, p. 16).

la base d'accords de licence avec les titulaires de droits. La Vereniging Openbare Bibliotheeken (VOB), une association regroupant toutes les bibliothèques publiques aux Pays-Bas, était d'avis que le régime pour les livres traditionnels devrait s'appliquer également au prêt numérique. Dans ce cadre, elle avait assigné en justice Stichting Leenrecht, une fondation chargée de la collecte de la rémunération due aux auteurs, afin d'obtenir un jugement déclaratoire en ce sens. Le recours de la VOB concernait les prêts organisés selon le modèle one copy, one user, à savoir le prêt d'une copie de livre sous forme numérique effectué en plaçant cette copie sur le serveur d'une bibliothèque publique et en permettant à un utilisateur de reproduire ladite copie par téléchargement sur son propre ordinateur, étant entendu qu'une seule copie peut être téléchargée pendant la période de prêt et que, après l'expiration de cette période, la copie téléchargée par cet utilisateur n'est plus utilisable par celui-ci. Saisi du litige, le Rechtbank Den Haag (tribunal de La Haye, Pays-Bas) a demandé à la Cour de justice si l'article 1^{er}, paragraphe 1, l'article 2, paragraphe 1, sous b), et l'article 6, paragraphe 1, de la directive 2006/115/CE⁷⁵, relative au droit de location et de prêt et à certains droits voisins du droit d'auteur dans le domaine de la propriété intellectuelle, doivent être interprétés en ce sens que la notion de « prêt » couvre un tel prêt d'une copie de livre sous forme numérique et si ladite directive s'oppose à une telle pratique.

Selon la Cour, l'article 1^{er}, paragraphe 1, l'article 2, paragraphe 1, sous b), et l'article 6, paragraphe 1, de la directive 2006/115/CE doivent être interprétés en ce sens que la notion de « prêt », au sens de ces dispositions, couvre le modèle one copy, one user.

En effet, il y a lieu d'entendre la notion de « location » d'objets, figurant à l'article 2, paragraphe 1, sous a), de la directive 2006/115/CE, comme portant exclusivement sur les objets tangibles, et la notion de « copies », figurant à l'article 1^{er}, paragraphe 1, de cette directive, comme portant, s'agissant de la location, exclusivement sur les copies fixées sur un support physique. Une telle conclusion est, par ailleurs, corroborée par l'objectif poursuivi par ladite directive. En effet, le considérant 4 de celle-ci énonce, notamment, que le droit d'auteur doit s'adapter aux réalités économiques nouvelles, telles que les nouvelles formes d'exploitation.

En outre, le droit de l'Union doit être interprété en ce sens qu'il ne s'oppose pas à ce à ce qu'un État membre soumette l'application de l'article 6, paragraphe 1, de la directive 2006/115/CE à la condition que la copie du livre sous forme numérique mise à disposition par la bibliothèque publique ait été mise en circulation par une première vente ou un premier autre transfert de propriété de cette copie dans l'Union par le titulaire du droit de distribution au public ou avec son consentement, au sens de l'article 4, paragraphe 2, de la directive 2001/29/CE⁷⁶. Les États membres ne sauraient être empêchés de fixer, le cas échéant, des conditions supplémentaires susceptibles

⁷⁵ Directive 2006/115/CE du Parlement européen et du Conseil, du 12 décembre 2006, relative au droit de location et de prêt et à certains droits voisins du droit d'auteur dans le domaine de la propriété intellectuelle (JO 2006, L 376, p. 28).

⁷⁶ Directive 2001/29/CE du Parlement européen et du Conseil, du 22 mai 2001, sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information (JO 2001, L 167, p. 10).

d'améliorer la protection des droits d'auteur au-delà de ce qui est prévu explicitement à ladite disposition.

L'article 6, paragraphe 1, de la directive 2006/115/CE doit être interprété en ce sens qu'il s'oppose à ce que l'exception de prêt public qu'il prévoit s'applique à la mise à disposition par une bibliothèque publique d'une copie de livre sous forme numérique dans le cas où cette copie a été obtenue à partir d'une source illégale.

Arrêt du 8 septembre 2016, GS Media (C-160/15, [EU:C:2016:644](#))

GS Media exploitait le site Internet GeenStijl, qui était l'un des dix sites les plus fréquentés dans le domaine des actualités aux Pays-Bas. En 2011, GS Media avait publié un article et un lien renvoyant les lecteurs vers un site australien où des photos de Mme Dekker avaient été mises à disposition. Ces photos étaient publiées sur le site australien sans le consentement de Sanoma, l'éditeur de la revue mensuelle Playboy qui détenait les droits d'auteur des photos en question. Malgré les sommations de Sanoma, GS Media avait refusé de supprimer l'hyperlien en question. Quand le site australien avait supprimé les photos sur demande de Sanoma, GeenStijl avait publié un nouvel article qui contenait lui aussi un lien vers un autre site, sur lequel on pouvait voir les photos en question. Ce dernier site avait aussi accédé à la demande de Sanoma de supprimer les photos. Les internautes visitant le forum de GeenStijl avaient ensuite placé de nouveaux liens renvoyant à d'autres sites où les photos pouvaient être consultées. Selon Sanoma, GS Media a porté atteinte au droit d'auteur. Saisi en cassation, le Hoge Raad der Nederlanden (Cour suprême des Pays-Bas) a interrogé la Cour de justice à ce sujet. En effet, en vertu de la directive 2001/29/CE⁷⁷, chaque acte de communication d'une œuvre au public doit être autorisé par le titulaire du droit d'auteur.

Selon la Cour, l'article 3, paragraphe 1, de la directive 2001/29/CE doit être interprété en ce sens que, afin d'établir si le fait de placer, sur un site Internet, des liens hypertextes vers des œuvres protégées, librement disponibles sur un autre site Internet sans l'autorisation du titulaire du droit d'auteur, constitue une « communication au public » au sens de cette disposition, il convient de déterminer si ces liens sont fournis sans but lucratif par une personne qui ne connaissait pas ou ne pouvait raisonnablement pas connaître le caractère illégal de la publication de ces œuvres sur cet autre site Internet ou si, au contraire, lesdits liens sont fournis dans un tel but, hypothèse dans laquelle cette connaissance doit être présumée.

Lorsqu'il est établi qu'une personne savait ou devait savoir que le lien hypertexte qu'elle a placé donne accès à une œuvre illégalement publiée sur Internet, par exemple en raison du fait qu'elle en a été averti par les titulaires du droit d'auteur, il y a lieu de

⁷⁷ Directive 2001/29/CE du Parlement européen et du Conseil, du 22 mai 2001, sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information (JO 2001, L 167, p. 10).

considérer que la fourniture de ce lien constitue une « communication au public », au sens de l'article 3, paragraphe 1, de la directive 2001/29/CE. Lorsque le placement de liens hypertexte est effectué dans un but lucratif, il peut être attendu de l'auteur d'un tel placement qu'il réalise les vérifications nécessaires pour s'assurer que l'œuvre concernée n'est pas illégalement publiée sur le site auquel mènent lesdits liens hypertextes. Dans de telles circonstances, et pour autant que cette présomption réfragable ne soit pas renversée, l'acte consistant à placer un lien hypertexte vers une œuvre illégalement publiée sur Internet constitue une « communication au public », au sens de l'article 3, paragraphe 1, de la directive 2001/29/CE.

Arrêt du 14 juin 2017, Stichting Brein (C-610/15, [EU:C:2017:456](#))

Ziggo et XS 4ALL étaient des fournisseurs d'accès à Internet. Une partie importante de leurs abonnés utilisait la plateforme de partage en ligne « The Pirate Bay ». Cette plateforme permettait aux utilisateurs de partager et de télécharger, par fragments (« torrents »), des œuvres qui se trouvaient sur leurs propres ordinateurs. Les fichiers en question étaient, dans leur grande majorité, des œuvres protégées par le droit d'auteur, sans que les titulaires du droit n'aient autorisé les administrateurs et les utilisateurs de cette plateforme à effectuer des actes de partage. Stichting Brein, une fondation néerlandaise qui défend les intérêts des titulaires du droit d'auteur, avait saisi les juridictions néerlandaises pour qu'elles ordonnent à Ziggo et à XS 4ALL de bloquer les noms de domaines et les adresses IP de « The Pirate Bay ».

Le Hoge Raad der Nederlanden (Cour suprême des Pays-Bas) a souhaité en substance savoir si une plateforme de partage telle que « The Pirate Bay » effectue une « communication au public » au sens de la directive 2001/29/CE⁷⁸ et peut dès lors enfreindre le droit d'auteur.

La Cour a jugé que la notion de « communication au public », au sens de l'article 3, paragraphe 1, de la directive 2001/29/CE doit être interprétée en ce sens qu'elle couvre la mise à disposition et la gestion, sur Internet, d'une plateforme de partage qui, par l'indexation de métadonnées relatives à des œuvres protégées et la fourniture d'un moteur de recherche, permet aux utilisateurs de cette plateforme de localiser ces œuvres et de les partager dans le cadre d'un réseau de pair à pair (peer-to-peer).

Il y a lieu de relever, ainsi qu'il ressort du considérant 23 de la directive 2001/29/CE, que le droit d'auteur de communication au public, visé au article 3, paragraphe 1, couvre toute transmission ou retransmission d'une œuvre au public non présent au lieu d'origine de la communication, par fil ou sans fil, y compris la radiodiffusion.

La Cour a déjà jugé, à cet égard, que le fait de fournir, sur un site Internet, des liens cliquables vers des œuvres protégées publiées sans aucune restriction d'accès sur un

⁷⁸ Directive 2001/29/CE du Parlement européen et du Conseil, du 22 mai 2001, sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information (JO 2001, L 167, p. 10).

autre site offre aux utilisateurs du premier site un accès direct auxdites œuvres. Tel est aussi le cas de la vente d'un lecteur multimédia sur lequel ont été préinstallés des modules complémentaires, disponibles sur Internet, contenant des liens hypertextes renvoyant à des sites Internet librement accessibles au public sur lesquels ont été mises à disposition des œuvres protégées par le droit d'auteur sans l'autorisation des titulaires de ce droit. Ainsi, il peut être déduit de cette jurisprudence que, en principe, tout acte par lequel un utilisateur donne, en pleine connaissance de cause, accès à ses clients à des œuvres protégées est susceptible de constituer un « acte de communication », au sens de l'article 3, paragraphe 1, de la directive 2001/29/CE.

Pour relever de la notion de « communication au public », au sens de l'article 3, paragraphe 1, de la directive 2001/29/CE, il faut que les œuvres protégées soient effectivement communiquées à un public. La notion de « public » comporte un certain seuil de minimis. Ainsi, il convient de savoir non seulement combien de personnes ont accès à la même œuvre parallèlement, mais également combien d'entre elles ont successivement accès à celle-ci.

Arrêt du 29 juillet 2019 (grande chambre), Funke Medien NRW(C-469/17, [EU:C:2019:623](#))

La société Funke Medien exploitait le portail Internet du quotidien allemand Westdeutsche Allgemeine Zeitung. La République fédérale d'Allemagne, estimant que Funke Medien avait violé son droit d'auteur sur certains rapports concernant la situation militaire « classifiés à diffusion restreinte » et établis par le gouvernement allemand, avait introduit une action en cessation dirigée contre cette dernière. Ce recours a été accueilli par un tribunal régional, puis confirmée en appel par un tribunal régional supérieur. Par son pourvoi en Revision, introduit devant la juridiction de renvoi, le Bundesgerichtshof (Cour fédérale de justice, Allemagne), Funke Medien a maintenu ses conclusions tendant au rejet de l'action en cessation.

À titre liminaire, la Cour a rappelé que des rapports de situation militaire ne sont susceptibles d'être protégés par le droit d'auteur qu'à la condition, laquelle doit être vérifiée par le juge national dans chaque cas d'espèce, que ces rapports constituent une création intellectuelle de leur auteur reflétant la personnalité de ce dernier et se manifestant par les choix libres et créatifs de celui-ci lors de l'élaboration desdits rapports.

D'après la Cour, les dispositions de la directive 2001/29/CE prévoyant les droits exclusifs des auteurs à la reproduction et à la communication au public de leurs œuvres constituent des mesures d'harmonisation complète du contenu matériel des droits qui y sont visés. En revanche, la Cour a considéré que les dispositions de la directive 2001/29/CE permettant une dérogation auxdits droits concernant les comptes rendus d'événements d'actualité et les citations ne constituent pas des mesures d'harmonisation complète de la portée des exceptions ou des limitations qu'elles comportent. Cependant, la marge d'appréciation des États membres dans la mise en

œuvre de ces dispositions doit s'exercer dans les limites imposées par le droit de l'Union, et ce afin de maintenir un juste équilibre entre, d'une part, l'intérêt des titulaires de droits à la protection de leur droit de propriété intellectuelle, garantie par la Charte, et, d'autre part, les droits et intérêts des utilisateurs d'œuvres ou d'objets protégés, en particulier leur liberté d'expression et d'information, également garantie par la Charte, ainsi que l'intérêt général.

Ensuite, la Cour a précisé que la liberté d'expression et d'information n'est pas susceptible de justifier, en dehors des exceptions et des limitations prévues par la directive 2001/29/CE, une dérogation aux droits exclusifs des auteurs à la reproduction et à la communication au public de leurs œuvres, autre que celle prévue par ladite directive. À cet égard, la Cour a rappelé que la liste des exceptions et des limitations prévues par la directive 2001/29/CE revêt un caractère exhaustif.

Enfin, selon la Cour, dans le cadre de la mise en balance qu'il incombe au juge national d'effectuer, au regard de l'ensemble des circonstances de l'espèce concernée, entre, d'une part, les droits exclusifs des auteurs à la reproduction et à la communication au public de leurs œuvres et, d'autre part, les droits des utilisateurs d'objets protégés visés par les dispositions dérogatoires de la directive 2001/29/CE concernant les comptes rendus d'événements d'actualité et les citations, celui-ci doit se fonder sur une interprétation de ces dispositions qui, tout en respectant leur libellé et en préservant leur effet utile, soit pleinement conforme aux droits fondamentaux garantis par la Charte.

Arrêt du 29 juillet 2019 (grande chambre), Spiegel Online (C-516/17, [EU:C:2019:625](#))

La société Spiegel Online exploitait un portail d'informations sur Internet du même nom. M. Volker Beck, qui était membre du Bundestag (Parlement fédéral, Allemagne), contestait, devant un tribunal régional, la mise à disposition des textes complets de ses manuscrit et article sur le site Internet de Spiegel Online. M. Beck considérait ladite publication comme une atteinte à son droit d'auteur. Cette juridiction a fait droit aux conclusions de M. Beck. Déboutée de son appel, Spiegel Online a formé un pourvoi en Revision devant la juridiction de renvoi, le Bundesgerichtshof (Cour fédérale de justice, Allemagne).

La Cour a estimé que les dispositions de la directive 2001/29/CE permettant une dérogation aux droits exclusifs de l'auteur concernant les comptes rendus d'événements d'actualité et les citations laissent aux États membres une marge d'appréciation pour leur transposition en droit national, mais qu'elles ne constituent pas des mesures d'harmonisation complète. Cependant, la marge d'appréciation des États membres dans la mise en œuvre de ces dispositions doit s'exercer dans les limites imposées par le droit de l'Union, et ce afin de maintenir un juste équilibre entre, d'une part, l'intérêt des titulaires de droits à la protection de leur droit de propriété intellectuelle, garantie par la Charte, et, d'autre part, les droits et intérêts des utilisateurs d'œuvres ou d'objets

protégés, en particulier leur liberté d'expression et d'information, également garantie par la Charte, ainsi que l'intérêt général.

S'agissant de la liberté d'expression et d'information, la Cour a précisé qu'elle n'est pas susceptible de justifier, en dehors des exceptions et des limitations prévues par la directive 2001/29/CE, une dérogation aux droits exclusifs des auteurs à la reproduction et à la communication au public de leurs œuvres, autre que celle prévue par ladite directive. À cet égard, la Cour a rappelé que la liste des exceptions et des limitations prévues par cette directive revêt un caractère exhaustif.

Par ailleurs, selon la Cour, dans le cadre de la mise en balance qu'il incombe au juge national d'effectuer, au regard de l'ensemble des circonstances de l'espèce concernée, entre, d'une part, les droits exclusifs des auteurs à la reproduction et à la communication au public de leurs œuvres et, d'autre part, les droits des utilisateurs d'objets protégés visés par les dispositions dérogatoires de la directive 2001/29/CE concernant les comptes rendus d'événements d'actualité et les citations, celui-ci doit se fonder sur une interprétation de ces dispositions qui, tout en respectant leur libellé et en préservant leur effet utile, soit pleinement conforme aux droits fondamentaux garantis par la Charte.

En premier lieu, la Cour a jugé que la disposition dérogatoire de la directive 2001/29/CE concernant les comptes rendus d'événements d'actualité s'oppose à une règle nationale restreignant l'application de l'exception ou de la limitation prévue à cette disposition aux cas dans lesquels une demande préalable d'autorisation en vue d'utiliser une œuvre protégée à des fins de compte rendu d'événements d'actualité n'est pas raisonnablement possible. En effet, la survenance d'un événement d'actualité requiert, en règle générale, et particulièrement dans le cadre de la société de l'information, que l'information y relative puisse être communiquée rapidement, de sorte qu'elle se concilie mal avec une exigence d'obtention préalable du consentement de l'auteur, laquelle serait susceptible de rendre excessivement difficile, voire d'empêcher, la fourniture au public d'informations pertinentes en temps utile.

En second lieu, la Cour a jugé, premièrement, que la notion de « citations », visée à la disposition dérogatoire de la directive 2001/29/CE concernant les citations, couvre le renvoi, au moyen d'un lien hypertexte, à un fichier consultable de manière autonome. Dans ce contexte, elle a rappelé sa jurisprudence selon laquelle les liens hypertextes contribuent au bon fonctionnement d'Internet, lequel revêt une importance particulière pour la liberté d'expression et d'information, garantie par la Charte, ainsi qu'à l'échange d'opinions et d'informations dans ce réseau caractérisé par la disponibilité d'innombrables quantités d'informations. Deuxièmement, la Cour a jugé qu'une œuvre a déjà été mise licitement à la disposition du public lorsque celle-ci, telle qu'elle se présente de manière concrète, a préalablement été rendue accessible au public avec l'autorisation du titulaire du droit ou en vertu d'une licence non volontaire ou encore en vertu d'une autorisation légale. Il appartient au juge national de décider si une œuvre a

été mise à la disposition du public de manière licite, à la lumière du cas concret dont il est saisi et en tenant compte de toutes les circonstances de l'espèce.

Arrêt du 9 mars 2021 (grande chambre), VG Bild-Kunst (C-392/19, EU:C:2021:181)

Stiftung Preußischer Kulturbesitz (ci-après « SPK »), une fondation allemande, exploite la Deutsche Digitale Bibliothek, une bibliothèque numérique dédiée à la culture et au savoir mettant en réseau des institutions culturelles et scientifiques allemandes. Le site Internet de cette bibliothèque contient des liens vers des contenus numérisés stockés sur les portails Internet des institutions participantes. En tant que « vitrine numérique », la Deutsche Digitale Bibliothek ne stocke elle-même que des vignettes (thumbnails), à savoir des versions d'images dont la taille est réduite par rapport à leur taille originale.

VG Bild-Kunst, une société de gestion collective des droits d'auteur dans le domaine des arts visuels en Allemagne, subordonne la conclusion, avec SPK, d'un contrat de licence d'utilisation de son catalogue d'œuvres sous la forme de vignettes à l'inclusion d'une disposition selon laquelle SPK s'engage à mettre en œuvre, lors de l'utilisation des œuvres visées au contrat, des mesures techniques efficaces contre la transclusion (framing)⁷⁹, par des tiers, des vignettes de ces œuvres affichées sur le site de la Deutsche Digitale Bibliothek.

Estimant qu'une telle condition contractuelle n'était pas raisonnable au regard du droit d'auteur, SPK a introduit une action devant les juridictions allemandes visant à ce qu'il soit constaté que VG Bild-Kunst était tenue d'accorder la licence en question sans qu'elle soit subordonnée à la mise en œuvre de mesures destinées à empêcher la transclusion⁸⁰.

Dans ce contexte, le Bundesgerichtshof (Cour fédérale de justice, Allemagne) demande à la Cour de déterminer si cette transclusion doit être considérée comme une communication au public au sens de la directive 2001/29⁸¹, ce qui, dans l'affirmative, permettrait à VG Bild-Kunst d'imposer à SPK la mise en œuvre de ces mesures.

La Cour, réunie en grande chambre, juge que l'incorporation par transclusion, dans une page Internet d'un tiers, des œuvres protégées par le droit d'auteur et mises à la disposition du public en libre accès avec l'autorisation du titulaire du droit d'auteur sur un autre site Internet constitue une communication au public lorsque cette

⁷⁹ La technique de la transclusion (framing) consiste à diviser une page d'un site Internet en plusieurs cadres et à afficher dans l'un d'eux, au moyen d'un lien cliquable ou d'un lien Internet incorporé (inline linking), un élément provenant d'un autre site afin de dissimuler aux utilisateurs de ce site l'environnement d'origine auquel appartient cet élément.

⁸⁰ Selon le droit allemand, les sociétés de gestion collective ont l'obligation d'accorder à toute personne qui en fait la demande, à des conditions raisonnables, une licence d'utilisation des droits dont la gestion leur a été confiée. Toutefois, selon la jurisprudence allemande, les sociétés de gestion collective peuvent, à titre exceptionnel, refuser d'octroyer une licence, à condition que ce refus ne constitue pas un abus de monopole et sous réserve de pouvoir opposer à la demande de licence des intérêts légitimes supérieurs.

⁸¹ En vertu de l'article 3, paragraphe 1, de la directive 2001/29/CE du Parlement européen et du Conseil, du 22 mai 2001, sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information (JO 2001, L 167, p. 10), les États membres prévoient pour les auteurs le droit exclusif d'autoriser ou d'interdire toute communication au public de leurs œuvres.

incorporation contourne des mesures de protection contre la transclusion adoptées ou imposées par le titulaire du droit d'auteur.

Tout d'abord, la Cour indique que la modification de la taille des œuvres dans le contexte d'une transclusion ne joue aucun rôle dans l'appréciation de l'existence d'un acte de communication au public, tant que les éléments originaux de ces œuvres sont perceptibles.

Ensuite, la Cour relève, d'une part, que la technique de la transclusion constitue un acte de communication à un public, dans la mesure où elle a pour effet de mettre l'élément affiché à la disposition de l'ensemble des utilisateurs potentiels d'un site Internet.

D'autre part, elle rappelle que, dès lors que la technique de la transclusion utilise le même mode technique que celui déjà utilisé pour communiquer l'œuvre protégée au public sur le site Internet d'origine, à savoir celui d'Internet, cette communication ne satisfait pas à la condition d'un public nouveau et, par conséquent, ne relève pas d'une communication « au public » au sens de la directive 2001/29.

Néanmoins, la Cour précise que cette considération ne s'applique que dans une situation où l'accès aux œuvres concernées sur le site Internet d'origine n'est soumis à aucune mesure restrictive. En effet, dans cette situation, le titulaire des droits a autorisé dès l'origine la communication de ses œuvres à l'ensemble des internautes.

En revanche, la Cour souligne que, lorsque le titulaire des droits a mis en place ou imposé dès l'origine des mesures restrictives liées à la publication de ses œuvres, il n'a pas consenti à ce que des tiers puissent librement communiquer ses œuvres au public. Au contraire, il a voulu restreindre le public ayant accès à ses œuvres aux seuls utilisateurs d'un site Internet particulier.

Par conséquent, la Cour juge que, lorsque le titulaire du droit d'auteur a adopté ou imposé des mesures de restriction contre la transclusion, l'incorporation d'une œuvre dans une page Internet d'un tiers, par la technique de la transclusion, constitue une « mise à la disposition de cette œuvre à un public nouveau ». Cette communication au public doit, dès lors, recevoir l'autorisation des titulaires de droits concernés.

En effet, une approche contraire reviendrait à consacrer une règle d'épuisement du droit de communication. Or, cette règle priverait le titulaire du droit d'auteur de la possibilité d'exiger une rémunération appropriée pour l'utilisation de son œuvre. Ainsi, une telle approche méconnaîtrait le juste équilibre devant être maintenu, dans l'environnement numérique, entre, d'une part, l'intérêt des titulaires du droit d'auteur et des droits voisins à la protection de leur propriété intellectuelle, et, d'autre part, la protection des intérêts et des droits fondamentaux des utilisateurs d'objets protégés.

Enfin, la Cour précise que le titulaire du droit d'auteur ne peut limiter son consentement à la transclusion autrement qu'au moyen de mesures techniques efficaces. En effet, en l'absence de telles mesures, il pourrait être difficile de vérifier si ce titulaire a entendu s'opposer à la transclusion de ses œuvres.

Arrêt du 22 juin 2021 (grande chambre), YouTube et Cyando (C-682/18 et C-683/18, EU:C:2021:503)

Dans le litige à l'origine de la première affaire (C-682/18), Frank Peterson, un producteur de musique, poursuit YouTube et sa représentante légale Google devant les juridictions allemandes au sujet de la mise en ligne, sur YouTube, en 2008, de plusieurs phonogrammes sur lesquels il allègue détenir différents droits. Cette mise en ligne a été effectuée par des utilisateurs de cette plateforme sans son autorisation. Il s'agit de titres de l'album *A Winter Symphony* de l'artiste Sarah Brightman ainsi que d'enregistrements audio privés réalisés lors des concerts de sa tournée « *Symphony Tour* ».

Dans le litige à l'origine de la seconde affaire (C-683/18), la maison d'édition Elsevier poursuit Cyando devant les juridictions allemandes au sujet de la mise en ligne, sur sa plateforme d'hébergement et de partage de fichiers « *Uploaded* », en 2013, de différents ouvrages sur lesquels Elsevier détient les droits exclusifs. Cette mise en ligne a été effectuée par des utilisateurs de cette plateforme sans son autorisation. Il s'agit des œuvres *Gray's Anatomy for Students*, *Atlas of Human Anatomy* et *Campbell-Walsh Urology*, qui pouvaient être consultés sur *Uploaded* via les collections de liens rehabgate.com, avaxhome.ws et bookarchive.ws.

Le Bundesgerichtshof (Cour fédérale de justice, Allemagne), saisi de ces deux litiges, a soumis plusieurs questions préjudiciales à la Cour afin que cette dernière précise, entre autres, la responsabilité des exploitants de plateformes en ligne s'agissant des œuvres protégées par le droit d'auteur qui sont mises en ligne sur ces plateformes, de manière illicite, par leurs utilisateurs.

Cette responsabilité est examinée par la Cour sous le régime applicable à l'époque des faits résultant de la directive 2001/29 sur le droit d'auteur⁸², de la directive 2000/31 sur le commerce électronique⁸³, ainsi que de la directive 2004/48 relative au respect des droits de propriété intellectuelle⁸⁴. Les questions préjudiciales posées ne concernent pas le régime, entré en application postérieurement à l'époque des faits, institué par la directive 2019/790 sur le droit d'auteur et les droits voisins dans le marché unique numérique⁸⁵.

Dans son arrêt, rendu en grande chambre, la Cour juge notamment que, en l'état actuel du droit de l'Union, les exploitants de plateformes en ligne ne font pas, eux-mêmes, une

⁸² Directive 2001/29/CE du Parlement européen et du Conseil, du 22 mai 2001, sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information (JO 2001, L 167, p. 10).

⁸³ 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 (« directive sur le commerce électronique ») (JO 2000, L 178, p. 1).

⁸⁴ Directive 2004/48/CE du Parlement européen et du Conseil, du 29 avril 2004, relative au respect des droits de propriété intellectuelle (JO 2004, L 157, p. 45 et rectificatif JO 2004, L 195, p. 16).

⁸⁵ Directive (UE) 2019/790 du Parlement européen et du Conseil, du 17 avril 2019, sur le droit d'auteur et les droits voisins dans le marché unique numérique et modifiant les directives 96/9/CE et 2001/29/CE (JO 2019, L 130, p. 92). Cette directive met en place, pour les exploitants de plateformes en ligne, un nouveau régime de responsabilité spécifique pour les œuvres illégalement mises en ligne par les utilisateurs de ces plateformes. Cette directive, qui doit être transposée par chaque État membre dans son droit national au plus tard le 7 juin 2021, impose notamment à ces exploitants d'obtenir une autorisation des titulaires de droits, par exemple, en concluant un accord de licence, pour les œuvres mises en ligne par les utilisateurs de leur plateforme.

communication au public des contenus protégés par le droit d'auteur que leurs utilisateurs mettent illégalement en ligne, à moins que ces exploitants ne contribuent, au-delà de la simple mise à disposition des plateformes, à donner au public accès à de tels contenus en violation du droit d'auteur. Par ailleurs, la Cour juge que ces exploitants peuvent bénéficier de l'exonération de responsabilité, au sens de la directive 2000/31 sur le commerce électronique, à la condition qu'ils ne jouent pas un rôle actif de nature à leur conférer une connaissance et un contrôle des contenus téléversés sur leur plateforme.

En premier lieu, la Cour examine la question de savoir si l'exploitant d'une plateforme de partage de vidéos ou d'une plateforme d'hébergement et de partage de fichiers, sur laquelle des utilisateurs peuvent mettre illégalement à la disposition du public des contenus protégés, effectue lui-même, dans des conditions telles que celles en cause dans les présentes affaires, une « communication au public » de ces contenus, au sens de la directive 2001/29 sur le droit d'auteur⁸⁶. Tout d'abord, la Cour rappelle les objectifs et la définition de la notion de « communication au public » ainsi que les critères complémentaires devant être pris en compte dans le cadre de l'appréciation individualisée que cette notion implique.

Ainsi, la Cour souligne, parmi ces critères, le rôle incontournable joué par l'exploitant de la plateforme et le caractère délibéré de son intervention. En effet, celui-ci réalise un « acte de communication » lorsqu'il intervient, en pleine connaissance des conséquences de son comportement, pour donner à ses clients accès à une œuvre protégée, et ce notamment lorsque, en l'absence de cette intervention, ces clients ne pourraient, en principe, jouir de l'œuvre diffusée.

Dans ce contexte, la Cour juge que l'exploitant d'une plateforme de partage de vidéos ou d'une plateforme d'hébergement et de partage de fichiers, sur laquelle des utilisateurs peuvent mettre illégalement à la disposition du public des contenus protégés, n'effectue pas une « communication au public » de ceux-ci, au sens de la directive sur le droit d'auteur, à moins qu'il ne contribue, au-delà de la simple mise à disposition de la plateforme, à donner au public accès à de tels contenus en violation du droit d'auteur.

Tel est notamment le cas lorsque cet exploitant a concrètement connaissance de la mise à disposition illicite d'un contenu protégé sur sa plateforme et s'abstient de l'effacer ou d'en bloquer l'accès promptement, ou lorsque ledit exploitant, alors même qu'il sait ou devrait savoir que, d'une manière générale, des contenus protégés sont illégalement mis à la disposition du public par l'intermédiaire de sa plateforme par des utilisateurs de celle-ci, s'abstient de mettre en œuvre les mesures techniques appropriées qu'il est permis d'attendre d'un opérateur normalement diligent dans sa situation pour contrer de manière crédible et efficace des violations du droit d'auteur sur cette plateforme, ou

⁸⁶ Article 3, paragraphe 1, de la directive 2001/29 sur le droit d'auteur. En vertu de cette disposition, les États membres prévoient pour les auteurs le droit exclusif d'autoriser ou d'interdire toute communication au public de leurs œuvres, par fil ou sans fil, y compris la mise à la disposition du public de leurs œuvres de manière à ce que chacun puisse y avoir accès de l'endroit et au moment qu'il choisit individuellement.

encore lorsqu'il participe à la sélection de contenus protégés communiqués illégalement au public, fournit sur sa plateforme des outils destinés spécifiquement au partage illicite de tels contenus ou promeut sciemment de tels partages, ce dont est susceptible de témoigner la circonstance que l'exploitant a adopté un modèle économique incitant les utilisateurs de sa plateforme à procéder illégalement à la communication au public de contenus protégés sur celle-ci.

En deuxième lieu, la Cour se penche sur la question de savoir si un exploitant de plateformes en ligne peut bénéficier de l'exonération de responsabilité, prévue par la directive 2000/31 sur le commerce électronique⁸⁷, pour les contenus protégés que des utilisateurs communiquent illégalement au public par l'intermédiaire de sa plateforme. Dans ce contexte, la Cour examine si le rôle exercé par cet exploitant est neutre, c'est-à-dire si son comportement est purement technique, automatique et passif, impliquant l'absence de connaissance ou de contrôle des contenus qu'il stocke, ou si, au contraire, ledit exploitant joue un rôle actif de nature à lui conférer une connaissance ou un contrôle de ces contenus. À cet égard, la Cour juge que cet exploitant peut bénéficier de l'exonération de responsabilité, pourvu qu'il ne joue pas un rôle actif de nature à lui conférer une connaissance ou un contrôle des contenus téléchargés sur sa plateforme. La Cour précise sur ce point que, pour être exclu du bénéfice de l'exonération de responsabilité, prévue par cette directive, un tel exploitant doit avoir connaissance des actes illicites concrets de ses utilisateurs afférents à des contenus protégés qui ont été téléchargés sur sa plateforme.

En troisième lieu, la Cour précise les conditions dans lesquelles les titulaires des droits, en vertu de la directive 2001/29 sur le droit d'auteur⁸⁸, peuvent obtenir des injonctions judiciaires à l'encontre des exploitants de plateformes en ligne. Ainsi, elle juge que cette directive ne s'oppose pas à ce que, en vertu du droit national, le titulaire d'un droit d'auteur ou d'un droit voisin ne puisse obtenir une ordonnance sur requête contre l'exploitant, dont le service a été utilisé par un tiers pour porter atteinte à son droit sans que cet exploitant en ait eu connaissance, au sens de la directive 2000/31 sur le commerce électronique⁸⁹, qu'à la condition que, avant l'ouverture de la procédure judiciaire, cette atteinte a été préalablement notifiée à cet exploitant et celui-ci n'est pas intervenu promptement pour retirer le contenu en question ou en bloquer l'accès et pour veiller à ce que de telles atteintes ne se reproduisent pas.

⁸⁷ Article 14, paragraphe 1, de la directive 2000/31 sur le commerce électronique. Selon cette disposition, les États membres veillent à ce que, en cas de fourniture d'un service de la société de l'information consistant à stocker des informations fournies par un destinataire du service, le prestataire ne soit pas responsable des informations stockées à la demande d'un destinataire du service, à condition que le prestataire n'ait pas effectivement connaissance de l'activité ou de l'information illicites et, en ce qui concerne une demande en dommages et intérêts, n'ait pas connaissance de faits ou de circonstances selon lesquels l'activité ou l'information illicite est apparente, ou bien que le prestataire, dès le moment où il a de telles connaissances, agisse promptement pour retirer les informations ou rendre l'accès à celles-ci impossible.

⁸⁸ Article 8, paragraphe 3, de la directive 2001/29 sur le droit d'auteur. Selon cette disposition, les États membres veillent à ce que les titulaires des droits puissent demander qu'une ordonnance sur requête soit rendue à l'encontre des intermédiaires dont les services sont utilisés par un tiers pour porter atteinte à un droit d'auteur ou à un droit voisin.

⁸⁹ Article 14, paragraphe 1, sous a), de la directive 2000/31 sur le commerce électronique.

Il appartient toutefois aux juridictions nationales de s'assurer, dans l'application d'une telle condition, que celle-ci n'aboutit pas à ce que la cessation effective de l'atteinte soit retardée de façon à engendrer des dommages disproportionnés pour ce titulaire.

II. Cadre juridique régissant le commerce électronique

1. Publicité

Arrêt du 23 mars 2010 (grande chambre), Google France (C-236/08 à C-238/08, [EU:C:2010:159](#))

La société Google exploitait un moteur de recherche sur Internet et proposait entre autres un service de référencement payant dénommé « AdWords ». Ce service permettait à tout opérateur économique, moyennant la sélection d'un ou de plusieurs mots clés, de faire apparaître un lien promotionnel vers son site, accompagné d'un message publicitaire. Vuitton, titulaire de la marque communautaire « Vuitton », et d'autres titulaires de marques françaises avaient constaté que, lors de l'utilisation du moteur de recherche de Google, la saisie par les internautes des termes constituant ces marques faisait apparaître des liens vers des sites proposant des imitations de produits de Vuitton et vers des sites de concurrents d'autres titulaires de marques. La Cour de cassation (France) a interrogé la Cour de justice sur la légalité de l'emploi, en tant que mots clés dans le cadre d'un service de référencement sur Internet, de signes correspondant à des marques, sans que les titulaires de celles-ci n'aient donné leur consentement.

La Cour a jugé qu'un tel prestataire d'un service de référencement sur Internet ne fait pas un usage de ce signe au sens de l'article 5, paragraphes 1 et 2, de la directive 89/104/CEE⁹⁰ ou de l'article 9, paragraphe 1, du règlement (CE) n° 40/94⁹¹, même si ce dernier permet aux annonceurs de sélectionner des signes identiques à des marques en tant que mots clés, stocke ces signes et affiche les annonces de ses clients à partir de ces signes. L'usage d'un signe identique ou similaire à la marque du titulaire par un tiers implique que celui-ci fasse une utilisation du signe dans le cadre de sa propre communication commerciale et constitue un usage au sens de ladite directive, dans le cas où l'affichage a pour but d'induire les internautes en erreur sur l'origine de ses produits ou de ses services.

Le titulaire d'une marque est habilité à interdire à un annonceur de faire de la publicité lorsqu'elle permet difficilement à l'internaute moyen de savoir si les produits ou les

⁹⁰ Directive 89/104/CEE du Conseil, du 21 décembre 1988, rapprochant les législations des États membres sur les marques (JO 1989, L 40, p. 1).

⁹¹ Règlement (CE) n° 40/94 du Conseil, du 20 décembre 1993, sur la marque communautaire (JO 1994, L 11, p. 1).

services visés par l'annonce proviennent du titulaire de la marque ou d'un tiers. La fonction essentielle de la marque consiste notamment à permettre aux internautes de distinguer les produits ou les services du titulaire de cette marque de ceux qui ont une autre provenance.

Toutefois, des répercussions de l'usage du signe identique à la marque par des tiers ne constituent pas en soi une atteinte à la fonction de publicité de la marque. L'article 14 de la directive 2000/31/CE⁹² doit être interprété en ce sens que la règle y énoncée s'applique au prestataire d'un service de référencement sur Internet lorsque ce prestataire n'a pas joué un rôle actif de nature à lui confier une connaissance ou un contrôle des données stockées. Si le comportement est purement technique, automatique et passif, impliquant l'absence de connaissance ou de contrôle des données qu'il stocke, ledit prestataire ne peut être tenu responsable.

Arrêt du 11 juillet 2013, Belgian Electronic Sorting Technology (C-657/11, EU:C:2013:516)

Les entreprises Belgian Electronic Sorting Technology (BEST) et Visys concevaient, produisaient et commercialisaient des trieuses et des chaînes de triage à technologie laser. Visys avait été fondée par M. Peelaers, ancien employé de BEST. Ce dernier avait fait enregistrer, pour le compte de Visys, le nom de domaine « www.bestlasersorter.com ». Le contenu du site Internet hébergé sous ce nom de domaine était identique à celui des sites Internet usuels de Visys, accessibles sous les noms de domaine « www.visys.be » et « www.visysglobal.be ». Si les mots « Best Laser Sorter » étaient introduits dans le moteur de recherche google.be, ce dernier renvoyait, en tant que deuxième résultat de recherche, après le site Internet de BEST, au site Internet de Visys. Visys utilisait dans ses sites Internet, entre autres, les balises métas « Best+Helius, Best+Genius ». La juridiction de renvoi, le Hof van Cassatie (Cour de cassation, Belgique), a saisi la Cour afin de savoir si l'enregistrement et l'utilisation d'un nom de domaine, d'une part, et l'utilisation de balises métas (« metatags ») reprises dans les métadonnées (« metadata ») d'un site web, d'autre part, peuvent être considérés comme relevant de la notion de publicité au sens des directives 84/450/CEE⁹³ et 2006/114/CE⁹⁴.

La Cour a jugé que l'article 2, point 1, de la directive 84/450/CEE et l'article 2, sous a), de la directive 2006/114/CE, doivent être interprétés en ce sens que la notion de publicité, telle que définie par ces dispositions, couvre l'utilisation d'un nom de domaine ainsi que celle des balises métas dans les métadonnées d'un site Internet, dans une telle situation où le nom de domaine ou les balises métas constituées de mots clés (« keyword »

⁹² 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 (JO 2000, L 178, p. 1).

⁹³ Directive 84/450/CEE du Conseil, du 10 septembre 1984, relative au rapprochement des dispositions législatives, réglementaires et administratives des États membres en matière de publicité trompeuse, telle que modifiée par la directive 2005/29/CE (JO 1984, L 250, p. 17).

⁹⁴ Directive 2006/114/CE du Parlement européen et du Conseil, du 12 décembre 2006, en matière de publicité trompeuse et de publicité comparative (JO 2006, L 376, p. 21).

metatags ») font référence à certains produits ou à certains services ou encore au nom commercial d'une société et constituent une forme de communication, qui s'adresse aux consommateurs potentiels et suggère à ceux-ci qu'ils trouveront un site Internet en rapport avec lesdits produits ou services, ou encore avec ladite société.

En effet, la notion de publicité ne saurait être interprétée et appliquée de façon à ce que des démarches entreprises par un professionnel en vue de promouvoir la vente de ses produits ou de ses services, qui sont susceptibles d'influencer le comportement économique des consommateurs et, partant, d'affecter les concurrents de ce professionnel, échappent aux règles de concurrence loyale imposées par ces directives.

En revanche, n'est pas englobé par cette notion l'enregistrement, en tant que tel, d'un nom de domaine. En effet, il s'agit d'un acte purement formel qui, à lui seul, n'implique pas nécessairement la possibilité d'une prise de connaissance du nom de domaine par les consommateurs potentiels et qui n'est donc pas susceptible d'influencer le choix de ces derniers.

Arrêt du 4 mai 2017, Luc Vanderborgh (C-339/15, [EU:C:2017:335](#))

M. Luc Vanderborgh, un dentiste établi en Belgique, avait fait de la publicité pour des prestations de soins dentaires. Il avait installé un panneau indiquant son nom, sa qualité de dentiste, l'adresse de son site Internet ainsi que le numéro d'appel de son cabinet. En outre, il avait créé un site Internet informant les patients des différents types de traitement proposés au sein de son cabinet. Enfin, il avait inséré des annonces publicitaires dans des journaux locaux. À la suite d'une plainte émanant du Verbond der Vlaamse tandartsen, une association professionnelle de dentistes, des poursuites pénales avaient été engagées à l'encontre de M. Vanderborgh. En effet, le droit belge interdisait toute publicité relative à des prestations de soins buccaux et dentaires et imposait des exigences de discrétion. Saisi du litige, le Nederlandstalige rechtbank van eerste aanleg te Brussel (tribunal de première instance néerlandophone de Bruxelles, Belgique) a décidé d'interroger la Cour de justice à ce sujet.

Selon la Cour, la directive 2000/31/CE⁹⁵ doit être interprétée en ce sens qu'elle s'oppose à une législation nationale, telle que celle en cause au principal.

Le considérant 18 de la directive 2000/31/CE précise que la notion de « services de la société de l'information » englobe un large éventail d'activités économiques qui ont lieu en ligne. Par ailleurs, l'article 2, sous f), de cette directive précise que la notion de « communication commerciale » couvre notamment toute forme de communication destinée à promouvoir les services d'une personne exerçant une profession réglementée. Il s'ensuit que la publicité relative aux prestations de soins buccaux et dentaires, faite au moyen d'un site Internet, constitue un tel service. Le législateur de

⁹⁵ 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 (JO 2000, L 178, p. 1).

l'Union n'a pas exclu de professions réglementées du principe d'autorisation des communications commerciales en ligne prévu à l'article 8, paragraphe 1, de ladite directive. Si cette disposition permet de tenir compte des particularités des professions de santé dans l'élaboration des règles professionnelles y afférentes, en encadrant les formes et les modalités des communications commerciales en ligne en vue notamment de garantir qu'il ne soit pas porté atteinte à la confiance qu'ont les patients envers ces professions, il n'en demeure pas moins que ces règles professionnelles ne sauraient interdire de manière générale et absolue toute forme de publicité en ligne destinée à promouvoir l'activité d'une personne exerçant une telle profession.

L'article 56 TFUE doit être interprété en ce sens qu'il s'oppose à une législation nationale, telle que celle en cause au principal, qui interdit de manière générale et absolue toute publicité relative à des prestations de soins buccaux et dentaires.

S'agissant de la nécessité d'une restriction à la libre prestation des services telle que celle en cause au principal, il doit être tenu compte du fait que la santé et la vie des personnes occupent le premier rang parmi les biens et les intérêts protégés par le traité et qu'il appartient, en principe, aux États membres de décider du niveau auquel ils entendent assurer la protection de la santé publique.

En effet, tous les messages publicitaires interdits par cette législation ne sont pas susceptibles, en tant que tels, de produire les effets contraires aux objectifs mentionnés. Dans ces conditions, il y a lieu de considérer que les objectifs poursuivis par la législation en cause au principal pourraient être atteints au moyen de mesures moins restrictives.

Arrêt du 30 mars 2017, Verband Sozialer Wettbewerb eV (C-146/16, [EU:C:2017:243](#))

L'objet du litige était une annonce publicitaire publiée dans un journal par DHL Paket, qui exploitait la plateforme de vente en ligne « MeinPaket.de » sur laquelle des vendeurs professionnels proposaient des produits à la vente. Les biens présentés dans cette annonce, assortis d'un code, pouvaient être achetés auprès de vendeurs tiers via ladite plateforme. Une fois connecté au site, l'utilisateur pouvait introduire le code correspondant afin d'être renvoyé vers une page présentant le bien en question de manière plus détaillée et mentionnant le vendeur, dont les informations pertinentes pouvaient être consultées dans une rubrique destinée à cet effet.

Selon le Verband Sozialer Wettbewerb (VSW), une association à laquelle adhèrent notamment des fournisseurs d'articles électriques et électroniques ainsi que des vendeurs par correspondance, qui proposent à la vente des articles de toute nature, l'annonce publiée présentait une pratique commerciale déloyale. Selon le VSW, DHL Paket ne satisfaisait pas à son obligation d'indiquer l'identité et l'adresse géographique des fournisseurs utilisant sa plateforme de vente. Le VSW a soutenu une action en justice en demandant la cessation de cette activité publicitaire.

Saisie par le Bundesgerichtshof (Cour fédérale de justice, Allemagne), la Cour a jugé que l'article 7, paragraphe 4, de la directive 2005/29/CE⁹⁶ doit être interprété en ce sens qu'une annonce publicitaire, telle que celle en cause au principal, qui relève de la notion d'« invitation à l'achat » au sens de cette directive peut répondre à l'obligation d'information prévue par cette disposition.

Il incombe à la juridiction de renvoi d'examiner, au cas par cas, d'une part, si les limites d'espace dans le texte publicitaire justifient la mise à disposition d'informations sur le fournisseur uniquement au niveau de la plateforme de vente en ligne et, d'autre part, le cas échéant, si les informations exigées par l'article 7, paragraphe 4, sous b), de ladite directive concernant la plateforme de vente en ligne sont communiquées simplement et rapidement.

Arrêt du 3 mars 2016, Daimler AG (C-179/15, EU:C:2016:134)

Együd Garage, une société hongroise spécialisée dans la vente et la réparation de voitures Mercedes, était liée par une convention de service après-vente avec Daimler, fabricant allemand des voitures Mercedes et titulaire de la marque internationale « Mercedes-Benz ». La société hongroise avait le droit d'utiliser cette marque et de faire apparaître la mention « réparateur Mercedes-Benz agréé » dans ses propres annonces. À la suite de la résiliation de cette convention, Együd Garage avait cherché à supprimer toute annonce sur Internet susceptible d'amener le public à considérer qu'elle entretenait toujours une relation contractuelle avec Daimler. Malgré les démarches entreprises, des annonces faisant apparaître une telle association avaient continué à être diffusées sur Internet et recensées par les moteurs de recherche. La Fővárosi Törvényszék (Cour de Budapest, Hongrie) a demandé à la Cour de justice si la directive 2008/95/CE sur les marques⁹⁷ permet à Daimler d'exiger d'un partenaire contractuel antérieur d'entreprendre des démarches approfondies pour éviter de porter préjudice à sa marque.

La Cour a jugé que l'usage d'une marque par un tiers, sans l'autorisation du titulaire, en vue d'annoncer au public que ce tiers effectue la réparation et l'entretien de produits revêtus de cette marque ou qu'il est spécialisé dans de tels produits, constitue un usage de la marque au sens de l'article 5, paragraphe 1, sous a), de la directive 2008/95/CE. Cela peut être interdit par le titulaire de la marque, à moins que l'article 6, relatif à la limitation des effets de la marque, ou l'article 7, relatif à l'épuisement du droit conféré par celle-ci, ne trouvent à s'appliquer. Un tel usage, lorsqu'il est fait en l'absence de

⁹⁶ Directive 2005/29/CE du Parlement européen et du Conseil, du 11 mai 2005, relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs dans le marché intérieur et modifiant la directive 84/450/CEE du Conseil et les directives 97/7/CE, 98/27/CE et 2002/65/CE du Parlement européen et du Conseil et le règlement (CE) n° 2006/2004 du Parlement européen et du Conseil (JO 2005, L 149, p. 22).

⁹⁷ Directive 2008/95/CE du Parlement européen et du Conseil, du 22 octobre 2008, rapprochant les législations des États membres sur les marques (JO 2008, L 299, p. 25).

consentement du titulaire de la marque, est susceptible de porter atteinte à la fonction d'indication d'origine de la marque.

L'article 5, paragraphe 1, sous a) et b), de ladite directive, doit être interprété en ce sens qu'il ne s'agit pas d'un usage lorsque cette annonce n'a pas été placée par ce tiers ou en son nom ou, dans l'hypothèse où cette annonce a été placée par ce tiers ou en son nom avec le consentement du titulaire, lorsque ce tiers a expressément exigé de l'exploitant du site Internet auprès duquel il avait commandé l'annonce de supprimer celle-ci ou la mention de la marque y figurant. Ne sauraient non plus être imputés à un annonceur des actes autonomes d'autres opérateurs économiques, tels que ceux d'exploitants de sites Internet de référencement, qui agissent non pas sur commande mais de leur propre initiative et en leur propre nom.

Dans ces deux hypothèses, le titulaire de la marque n'est pas habilité, en vertu de l'article 5, paragraphe 1, sous a) et b), de la directive 2008/95/CE, à agir à l'encontre de l'annonceur afin de lui faire interdire la mise en ligne de l'annonce comportant la mention de sa marque.

Arrêt du 22 décembre 2022 (grande chambre), Louboutin (Usage d'un signe contrefaisant sur un marché en ligne) (C-148/21 et C-184/21, [EU:C:2022:1016](#))

Depuis 2016, M. Louboutin, créateur français de chaussures et de sacs à main de luxe, a enregistré la couleur rouge, appliquée sur la semelle extérieure d'une chaussure à talon haut, comme marque de l'Union européenne.

Amazon exploite des sites Internet de vente en ligne de produits variés qu'elle propose tant directement, en son nom et pour son propre compte, qu'indirectement, en fournissant une place de marché en ligne à des vendeurs tiers. Cet exploitant offre également aux vendeurs tiers des services complémentaires de stockage et d'expédition de leurs produits.

M. Louboutin a constaté que, sur ces sites Internet, paraissent régulièrement des annonces de vente relatives à des chaussures à semelles rouges qui, selon lui, concernent des produits dont la mise en circulation n'a pas fait l'objet de son consentement. Invoquant une atteinte aux droits exclusifs conférés par la marque en cause, il a alors introduit deux actions en contrefaçon contre Amazon devant le Tribunal d'arrondissement de Luxembourg (Luxembourg)⁹⁸ et le Tribunal de l'entreprise francophone de Bruxelles (Belgique)⁹⁹.

Ces juridictions ont alors chacune décidé de saisir la Cour de plusieurs questions préjudiciales.

⁹⁸ Affaire C-148/21.

⁹⁹ Affaire C-184/21.

En substance, elles ont interrogé la Cour sur la question de savoir si le règlement sur la marque de l'Union européenne¹⁰⁰ doit être interprété en ce sens que l'exploitant d'un site Internet de vente en ligne intégrant, outre les propres offres à la vente de celui-ci, une place de marché en ligne est susceptible d'être considéré comme faisant lui-même usage d'un signe identique à une marque de l'Union européenne d'autrui pour des produits identiques à ceux pour lesquels cette marque est enregistrée, lorsque des vendeurs tiers proposent, sans le consentement du titulaire de ladite marque, de tels produits revêtus de ce signe à la vente, sur cette place de marché.

Elles se demandent, en particulier, si sont pertinents à cet égard les faits que cet exploitant recourt à un mode de présentation uniforme des offres publiées sur son site Internet, affichant en même temps les annonces relatives aux produits qu'il vend en son nom et pour son propre compte et celles relatives à des produits proposés par des vendeurs tiers sur ladite place de marché, qu'il fait apparaître son propre logo de distributeur renommé sur l'ensemble de ces annonces et qu'il offre aux vendeurs tiers, dans le cadre de la commercialisation de leurs produits, des services complémentaires consistant à leur fournir un soutien dans la présentation de leurs annonces, ainsi qu'au stockage et à l'expédition des produits proposés sur la même place de marché. Dans ce contexte, les juridictions de renvoi s'interrogent également sur le point de savoir s'il convient de prendre en considération, le cas échéant, la perception des utilisateurs du site Internet en question.

Réunie en grande chambre, la Cour a eu l'occasion d'apporter des précisions importantes sur la question de la responsabilité directe de l'exploitant d'un site Internet de vente en ligne intégrant une place de marché en ligne pour des atteintes aux droits du titulaire d'une marque de l'Union européen qui résultent du fait qu'un signe identique à cette marque figure dans des annonces des vendeurs tiers sur cette place de marché.

Pour rappel, en vertu du règlement sur la marque de l'Union¹⁰¹, l'enregistrement d'une marque de l'Union européenne confère à son titulaire le droit d'interdire à tout tiers de faire usage, dans la vie des affaires, d'un signe identique à cette marque pour des produits ou des services identiques à ceux pour lesquels celle-ci est enregistrée.

La Cour relève d'emblée que la notion de « faire usage » n'est pas définie par le règlement sur la marque de l'Union. Néanmoins, cette expression implique, d'une part, un comportement actif et une maîtrise, directe ou indirecte, de l'acte constituant l'usage. En effet, seul un tiers qui a une telle maîtrise est effectivement en mesure de cesser l'usage d'une marque fait sans le consentement de son titulaire.

¹⁰⁰ Plus précisément, l'article 9, paragraphe 2, sous a), du règlement (UE) 2017/1001 du Parlement européen et du Conseil, du 14 juin 2017, sur la marque de l'Union européenne (JO 2017, L 154, p. 1).

¹⁰¹ Article 9, paragraphe 2, sous a), du règlement (UE) 2017/1001 du Parlement européen et du Conseil, du 14 juin 2017, sur la marque de l'Union européenne (JO 2017, L 154, p. 1).

L'usage d'un signe identique ou similaire à une marque du titulaire par un tiers suppose, d'autre part, à tout le moins, que ce dernier fasse un usage du signe dans le cadre de sa propre communication commerciale. Une personne peut ainsi permettre à ses clients de faire usage de signes identiques ou similaires à des marques, sans faire elle-même un usage desdits signes. C'est ainsi que la Cour a considéré que, s'agissant de l'exploitant d'une place de marché en ligne, l'usage de signes identiques ou similaires à des marques, dans des offres à la vente affichées sur cette place de marché, est fait uniquement par les clients vendeurs de cet exploitant et non pas par celui-ci, dès lors qu'il n'utilise pas ce signe dans le cadre de sa communication commerciale.

La Cour observe toutefois que, dans le cadre de sa jurisprudence antérieure, elle n'était pas interrogée par rapport à l'incidence du fait que le site Internet de vente en ligne en question intègre, outre la place de marché en ligne, des offres à la vente de l'exploitant de ce site lui-même, tandis que les présentes affaires portent précisément sur cette incidence. Ainsi, en l'espèce, les juridictions de renvoi se demandent si, outre le vendeur tiers, l'exploitant d'un site Internet de vente en ligne intégrant une place de marché en ligne, tel qu'Amazon, fait également usage, dans sa propre communication commerciale, d'un signe identique à une marque d'autrui pour des produits identiques à ceux pour lesquels cette marque est enregistrée, de telle sorte qu'il pourrait être tenu pour responsable de l'atteinte aux droits du titulaire de cette marque, lorsque ce vendeur tiers propose de tels produits revêtus de ce signe à la vente, sur cette place de marché.

La Cour constate que cette question se pose indépendamment du fait que le rôle d'un tel exploitant puisse, le cas échéant, être examiné également sous l'angle d'autres règles de droit, et que, bien que l'appréciation d'un tel usage par l'exploitant appartient, au final, au juge national, elle peut fournir des éléments d'interprétation relevant du droit de l'Union susceptibles d'être utiles à cet égard.

À cet égard, s'agissant de la communication commerciale, la Cour précise que l'usage d'un signe identique à la marque d'autrui par l'exploitant d'un site Internet intégrant une place de marché en ligne dans sa propre communication commerciale suppose que ce signe apparaisse, aux yeux des tiers, comme faisant partie intégrante de celle-ci et, partant, comme relevant de son activité.

Dans ce contexte, la Cour rappelle que, dans une situation où le prestataire d'un service utilise un signe identique ou similaire à une marque d'autrui pour promouvoir des produits que l'un de ses clients commercialise à l'aide de ce service, ce prestataire fait lui-même usage de ce signe lorsqu'il utilise celui-ci de telle façon qu'il s'établit un lien entre ledit signe et les services fournis par ledit prestataire.

Ainsi, la Cour a déjà considéré qu'un tel prestataire ne fait pas lui-même usage d'un signe identique ou similaire à une marque d'autrui lorsque le service rendu par celui-ci n'est pas comparable à un service visant à promouvoir la commercialisation de produits revêtus de ce signe et n'implique pas la création d'un lien entre ce service et ledit signe,

dès lors que le prestataire en question n'apparaît pas au consommateur, ce qui exclut toute association entre ses services et le signe en cause.

En revanche, la Cour a jugé qu'un tel lien existe lorsque l'exploitant d'une place de marché en ligne fait, à l'aide d'un service de référencement sur Internet et à partir d'un mot clé identique à une marque d'autrui, de la publicité pour des produits de cette marque mis en vente par ses clients sur sa place de marché en ligne. En effet, une telle publicité crée, pour les internautes effectuant une recherche à partir de ce mot clé, une association évidente entre ces produits de marque et la possibilité de les acheter via ladite place de marché. C'est pour ce motif que le titulaire de cette marque est habilité à interdire à cet exploitant un tel usage, lorsque cette publicité porte atteinte au droit de marque en raison du fait qu'elle ne permet pas ou permet seulement difficilement à l'internaute normalement informé et raisonnablement attentif de savoir si ces produits proviennent du titulaire de cette marque ou d'une entreprise économiquement liée à celui-ci ou, au contraire, d'un tiers.

La Cour en déduit que, afin de déterminer si l'exploitant d'un site Internet de vente en ligne intégrant une place de marché en ligne fait lui-même usage d'un signe identique à une marque d'autrui, figurant dans les annonces relatives à des produits proposés par des vendeurs tiers sur cette place de marché, il convient d'apprécier si un utilisateur normalement informé et raisonnablement attentif de ce site Internet établit un lien entre les services de cet exploitant et le signe en question.

Dans cette perspective, pour apprécier si une annonce, publiée sur ladite place de marché par un vendeur tiers actif sur cette dernière, utilisant un signe identique à une marque d'autrui peut être considérée comme faisant partie de la communication commerciale de l'exploitant dudit site Internet, il y a lieu de vérifier si elle est susceptible d'établir un lien entre les services offerts par ce dernier et le signe en question, au motif qu'un utilisateur pourrait croire que c'est l'exploitant qui commercialise, en son nom et pour son propre compte, le produit pour lequel il est fait usage du signe en question.

La Cour souligne que, dans le cadre de cette appréciation globale des circonstances de l'espèce, revêtent une importance particulière notamment le mode de présentation des annonces, tant individuellement que dans leur ensemble, sur le site Internet en question ainsi que la nature et l'ampleur des services fournis par l'exploitant de celui-ci.

En ce qui concerne, d'une part, le mode de présentation des annonces, le droit de l'Union oblige à un affichage transparent des annonces sur Internet, de sorte qu'un utilisateur normalement informé et raisonnablement attentif puisse distinguer aisément les offres émanant de l'exploitant du site Internet de celles des vendeurs tiers actifs sur la place de marché en ligne. Or, la Cour estime que le recours par l'exploitant à un mode de présentation uniforme des offres publiées, affichant en même temps ses propres annonces et celles des vendeurs tiers et faisant apparaître son propre logo de distributeur renommé tant sur son site Internet que sur l'ensemble des annonces, est susceptible de rendre difficile une telle distinction et ainsi de donner l'impression que

c'est l'exploitant qui commercialise, en son nom et pour son propre compte, les produits offerts à la vente par ces vendeurs tiers.

D'autre part, la nature et l'ampleur des services fournis par l'exploitant d'une place de marché en ligne aux vendeurs, et notamment ceux consistant dans le stockage, l'expédition et la gestion des retours desdits produits, sont également susceptibles de donner l'impression, à un utilisateur informé et raisonnablement attentif, que ces produits sont commercialisés par l'exploitant et de créer ainsi un lien, aux yeux de ces utilisateurs, entre ces services et les signes figurant sur ces produits et dans les annonces des vendeurs tiers.

En conclusion, la Cour dit pour droit que l'exploitant d'un site Internet de vente en ligne intégrant, outre les propres offres à la vente de celui-ci, une place de marché en ligne est susceptible d'être considéré comme faisant lui-même usage d'un signe identique à une marque de l'Union européenne d'autrui pour des produits identiques à ceux pour lesquels cette marque est enregistrée, lorsque des vendeurs tiers proposent, sans le consentement du titulaire de ladite marque, de tels produits revêtus de ce signe à la vente, sur cette place de marché, si un utilisateur normalement informé et raisonnablement attentif de ce site établit un lien entre les services de cet exploitant et le signe en question, ce qui est notamment le cas lorsque, compte tenu de l'ensemble des éléments caractérisant la situation en cause, un tel utilisateur pourrait avoir l'impression que c'est ledit exploitant qui commercialise lui-même, en son nom et pour son propre compte, les produits revêtus dudit signe. La Cour ajoute que sont pertinents à cet égard les faits :

- que cet exploitant recourt à un mode de présentation uniforme des offres publiées sur son site Internet, affichant en même temps les annonces relatives aux produits qu'il vend en son nom et pour son propre compte et celles relatives à des produits proposés par des vendeurs tiers sur ladite place de marché,
- qu'il fait apparaître son propre logo de distributeur renommé sur l'ensemble de ces annonces,
- et qu'il offre aux vendeurs tiers, dans le cadre de la commercialisation des produits revêtus du signe en cause, des services complémentaires consistant notamment dans le stockage et l'expédition de ces produits.

Arrêt du 22 décembre 2022 (grande chambre), EUROAPTEKA (C-530/20, [EU:C:2022:1014](#))

« EUROAPTEKA » SIA est une société exerçant une activité pharmaceutique en Lettonie. Elle fait partie d'un groupe qui possède un réseau de pharmacies et de sociétés de distribution de médicaments au détail dans ce pays. En 2016, la Veselības inspekcijas Zāļu kontroles nodaļa (Inspection de la santé publique, service contrôle des médicaments, Lettonie) a interdit à EUROAPTEKA de diffuser une publicité relative à une vente en promotion offrant une réduction de 15 % sur le prix d'achat de tout médicament en cas d'achat d'au moins trois articles. Cette décision a été prise sur le

fondement d'une disposition nationale qui interdit d'inclure, dans la publicité faite auprès du public pour des médicaments non soumis à prescription médicale ni remboursables, des informations qui encouragent l'achat du médicament en justifiant la nécessité d'un tel achat par le prix du médicament, en annonçant une vente spéciale ou en indiquant que le médicament est vendu avec d'autres médicaments (y compris à un prix réduit) ou produits¹⁰².

Saisie, en 2020, d'un recours introduit par EUROAPTEKA contre cette disposition, la Latvijas Republikas Satversmes tiesa (Cour constitutionnelle, Lettonie) a interrogé la Cour à titre préjudiciel sur l'interprétation de la directive 2001/83¹⁰³.

Par son arrêt, la Cour, réunie en grande chambre, précise l'étendue de la notion de « publicité pour des médicaments », au sens de cette directive, notamment concernant des contenus qui visent non pas un médicament déterminé, mais des médicaments indéterminés. Par ailleurs, elle se prononce sur la compatibilité avec ladite directive d'une disposition nationale prévoyant des interdictions telles que celles en cause au principal, notamment sur le point de savoir si ces interdictions visent à favoriser l'usage rationnel des médicaments, au sens de la même directive.

En premier lieu, la Cour dit pour droit que la diffusion d'informations qui encouragent l'achat de médicaments en justifiant la nécessité d'un tel achat par leur prix, en annonçant une vente spéciale ou en indiquant que ces médicaments sont vendus avec d'autres médicaments, y compris à un prix réduit, ou d'autres produits, relève de la notion de « publicité pour des médicaments », au sens de la directive 2001/83, même lorsque ces informations visent non pas un médicament déterminé, mais des médicaments indéterminés.

Tout d'abord, d'un point de vue textuel, la Cour rappelle que l'article 86, paragraphe 1, de cette directive, qui contient la notion de « publicité pour des médicaments », fait systématiquement référence aux « médicaments » au pluriel. En outre, cette disposition définit cette notion de manière très large, comme couvrant « toute forme » de démarchage d'information, de prospection ou d'incitation, y compris, notamment, la « publicité pour les médicaments auprès du public ».

Ensuite, d'un point de vue contextuel, la Cour relève que les dispositions du titre VIII de la directive 2001/83, dont fait partie l'article 86, énoncent les règles générales et fondamentales relatives à la publicité pour les médicaments et que, partant, elles ont vocation à s'appliquer à toute action visant à promouvoir la prescription, la délivrance, la vente ou la consommation de médicaments.

¹⁰² Point 18.12 du Ministru kabineta noteikumi Nr. 378 « Zāļu reklamēšanas kārtība un kārtība, kādā zāļu ražotājs ir tiesīgs nodot ārstiem bezmaksas zāļu paraugus » (décret n° 378 du conseil des ministres portant « Modalités de publicité pour les médicaments et modalités selon lesquelles les fabricants de médicaments sont autorisés à fournir des échantillons gratuits de médicaments aux médecins », du 17 mai 2011 (Latvijas Vēstnesis, 2011, n° 78).

¹⁰³ Plus précisément, sont visés les articles 86, paragraphe 1, 87, paragraphe 3, et 90 de la directive 2001/83/CE du Parlement européen et du Conseil, du 6 novembre 2001, instituant un code communautaire relatif aux médicaments à usage humain (JO 2001, L 311, p. 67), telle que modifiée par la directive 2004/27/CE du Parlement européen et du Conseil, du 31 mars 2004 (JO 2004, L 136, p. 34).

Enfin, s'agissant des finalités poursuivies par la directive 2001/83, la Cour estime que l'objectif essentiel de sauvegarder la santé publique poursuivi par cette directive serait largement compromis si une activité de démarchage d'information, de prospection ou d'incitation visant à promouvoir la prescription, la délivrance, la vente ou la consommation de médicaments sans faire référence à un médicament déterminé ne devait pas relever de la notion de « publicité pour des médicaments » et, partant, devait échapper aux interdictions, aux conditions et aux restrictions prévues par cette directive en matière de publicité.

En effet, dans la mesure où une publicité pour des médicaments indéterminés, telle qu'une publicité visant toute une classe de médicaments destinés à traiter la même pathologie, peut également concerner des médicaments soumis à prescription médicale ou des médicaments remboursables, l'exclusion d'une telle publicité du champ d'application des dispositions de la directive 2001/83 en matière de publicité reviendrait à priver largement de leur effet utile les interdictions édictées par cette directive¹⁰⁴, en ce qu'elle ferait échapper à ces interdictions toute publicité ne visant pas spécifiquement un médicament relevant de cette classe.

En outre, la Cour considère qu'une publicité faite à l'égard d'un ensemble indéterminé de médicaments non soumis à prescription médicale ni remboursable peut, au même titre qu'une publicité faite à l'égard d'un seul médicament déterminé, être excessive et inconsidérée et, dès lors, nuire à la santé publique, en incitant les consommateurs à une utilisation irrationnelle ou à une surconsommation des médicaments concernés.

La Cour conclut que, nonobstant ce qui a été affirmé dans l'arrêt A (Publicité et vente de médicaments en ligne)¹⁰⁵ ainsi que dans l'arrêt DocMorris¹⁰⁶, la notion de « publicité pour des médicaments » visée par la directive 2001/83 couvre toute forme de démarchage d'information, de prospection ou d'incitation visant à promouvoir la prescription, la délivrance, la vente ou la consommation d'un médicament déterminé ou de médicaments indéterminés.

La Cour ajoute que, étant donné que la finalité du message constitue le trait caractéristique essentiel de cette notion et l'élément déterminant pour distinguer la publicité de la simple information, et que les activités de diffusion d'information visées par une disposition nationale telle que celle en cause au principal paraissent avoir une telle finalité promotionnelle, ces activités relèvent de ladite notion.

En second lieu, la Cour juge que les dispositions de la directive 2001/83¹⁰⁷ ne s'opposent pas à une disposition nationale qui impose des restrictions non prévues par cette directive, mais qui répondent à l'objectif essentiel de sauvegarde de la santé publique poursuivi par ladite directive, en interdisant d'inclure, dans la publicité auprès du public

¹⁰⁴ Article 88, paragraphe 1, sous a), et paragraphe 3, de la directive 2001/83.

¹⁰⁵ Arrêt du 1^{er} octobre 2020, A (Publicité et vente de médicaments en ligne) (C-649/18, [EUC:2020:764](#), point 50).

¹⁰⁶ Arrêt du 15 juillet 2021, DocMorris (C-190/20, [EUC:2021:609](#), point 20).

¹⁰⁷ Plus précisément, les articles 87, paragraphe 3, et 90 de la directive 2001/83.

faite à l'égard des médicaments non soumis à prescription médicale ni remboursables, des informations qui encouragent l'achat de médicaments en justifiant la nécessité d'un tel achat par le prix de ces médicaments, en annonçant une vente spéciale ou en indiquant que lesdits médicaments sont vendus avec d'autres médicaments, y compris à un prix réduit, ou d'autres produits.

Au soutien de cette interprétation, la Cour rappelle, premièrement, s'agissant de l'articulation entre l'exigence que cette publicité favorise l'usage rationnel des médicaments¹⁰⁸ et les restrictions visées par la directive 2001/83 sous forme d'une liste d'éléments publicitaires interdits¹⁰⁹, que le fait que cette directive ne comporte pas de règles spécifiques concernant un élément publicitaire donné ne fait pas obstacle à ce que, dans le but d'empêcher toute publicité excessive et inconsidérée pour des médicaments qui pourrait affecter la santé publique, les États membres interdisent¹¹⁰ un tel élément dans la mesure où celui-ci favoriserait l'usage irrationnel de médicaments.

Par conséquent, et quand bien même la directive 2001/83 autorise la publicité pour les médicaments non soumis à prescription médicale, les États membres doivent interdire, afin de prévenir la survenance de risques pour la santé publique conformément à l'objectif essentiel de sauvegarde de celle-ci, l'inclusion, dans la publicité auprès du public faite à l'égard de médicaments non soumis à prescription médicale ni remboursables, d'éléments qui sont de nature à favoriser l'usage irrationnel de tels médicaments.

Deuxièmement, s'agissant de savoir si tel est le cas des éléments visés par des interdictions telles que celles en cause au principal, la Cour relève que, en ce qui concerne les médicaments non soumis à prescription médicale ni remboursables, il est fréquent que le consommateur final évalue lui-même, sans l'assistance d'un médecin, l'utilité ou la nécessité d'acheter de tels médicaments. Or, ce consommateur ne dispose pas nécessairement de connaissances spécifiques et objectives lui permettant d'apprécier leur valeur thérapeutique. La publicité peut alors exercer une influence particulièrement importante sur l'évaluation et le choix effectués par ledit consommateur, tant en ce qui concerne la qualité du médicament que la quantité à acheter.

Dans ce contexte, des éléments de publicité tels que visés par la disposition nationale en cause au principal sont de nature à inciter les consommateurs à acheter des médicaments non soumis à prescription médicale ni remboursables en fonction d'un critère économique lié au prix de ces médicaments et, partant, sont susceptibles de conduire ces consommateurs à acheter et à consommer ces médicaments sans qu'il ait

¹⁰⁸ Exigence prévue à l'article 87, paragraphe 3, de la directive 2001/83.

¹⁰⁹ Restrictions visées à l'article 90 de la directive 2001/83.

¹¹⁰ Sur le fondement de l'article 87, paragraphe 3, de la directive 2001/83.

été procédé à une évaluation objective fondée sur les propriétés thérapeutiques de ces derniers et sur des besoins médicaux concrets.

Or, selon la Cour, une publicité qui détourne le consommateur de l'évaluation objective de la nécessité de prendre un médicament encourage l'utilisation irrationnelle et excessive de ce médicament. Une telle utilisation irrationnelle et excessive des médicaments peut également découler d'une publicité qui, à l'instar de celles portant sur des offres promotionnelles ou sur des ventes combinées de médicaments et d'autres produits, assimile des médicaments à d'autres produits de consommation, qui font généralement l'objet de remises et de réductions de prix liées au dépassement d'un certain niveau de dépenses.

La Cour conclut que, en ce qu'elle interdit la diffusion d'éléments de publicité qui encouragent l'utilisation irrationnelle et excessive des médicaments non soumis à prescription médicale ni remboursables - sans préjudice de la possibilité pour les pharmacies d'accorder des remises et des réductions de prix lors de la vente de ces médicaments et d'autres produits de santé - une disposition nationale telle que celle en cause au principal répond à l'objectif essentiel de sauvegarde de la santé publique et est donc compatible avec la directive 2001/83.

2. Responsabilité des prestataires intermédiaires

Arrêt du 3 octobre 2019, Glawischnig-Piesczek (C-18/18, [EU:C:2019:821](#))

Facebook Ireland exploite une plateforme mondiale de média social (ci-après « Facebook Service ») pour les utilisateurs situés en dehors des États-Unis d'Amérique et du Canada. M^{me} Glawischnig-Piesczek était députée au Nationalrat (Conseil national, Autriche), présidente du groupe parlementaire « die Grünen » (Les Verts), et porte-parole fédérale de ce parti politique. Le 3 avril 2016, un utilisateur de Facebook Service a partagé, sur sa page personnelle, un article du magazine d'information autrichien en ligne oe24.at intitulé « Les Verts : en faveur du maintien d'un revenu minimum pour les réfugiés », ce qui a eu pour effet de générer sur cette page un « aperçu vignette » du site d'origine, comportant le titre de cet article, un bref résumé de ce dernier ainsi qu'une photographie de M^{me} Glawischnig-Piesczek. Cet utilisateur a en outre publié, au sujet de cet article, un commentaire rédigé dans des termes dont la juridiction de renvoi a constaté qu'ils étaient de nature à porter atteinte à l'honneur de la requérante au principal, à l'injurier et à la diffamer. Cette contribution pouvait être consultée par chaque utilisateur de Facebook Service.

Par une lettre du 7 juillet 2016, M^{me} Glawischnig-Piesczek a, notamment, demandé à Facebook Ireland d'effacer ce commentaire. Facebook Ireland n'ayant pas retiré le commentaire en question, M^{me} Glawischnig-Piesczek a introduit un recours devant un

tribunal de commerce qui a enjoint à Facebook Ireland de cesser, immédiatement et jusqu'à la clôture définitive de la procédure relative à l'action en cessation, la publication et/ou la diffusion de photos de la requérante au principal. Facebook Ireland a rendu l'accès au contenu initialement publié impossible en Autriche.

Saisi en appel, un tribunal régional supérieur a confirmé l'ordonnance rendue en première instance s'agissant des allégations identiques. En revanche, il a jugé que la diffusion d'allégations de contenu équivalent ne devait cesser que s'agissant de celles qui étaient portées à la connaissance de Facebook Ireland par la requérante au principal, par des tiers ou d'une autre manière. Chacune des parties au principal a formé un recours en Revision devant l'Oberster Gerichtshof (Cour suprême, Autriche).

La demande de décision préjudiciale portait essentiellement sur l'interprétation de l'article 15, paragraphe 1, de la directive 2000/31/CE.

À titre liminaire, la Cour a souligné que, afin de pouvoir obtenir de l'hébergeur en cause qu'il prévienne toute nouvelle atteinte aux intérêts concernés, il est légitime que la juridiction compétente puisse exiger de cet hébergeur qu'il bloque l'accès aux informations stockées, dont le contenu est identique à celui déclaré illicite antérieurement, ou qu'il retire ces informations, quel que soit l'auteur de la demande de stockage de celles-ci.

Ensuite, selon la Cour, une juridiction d'un État membre est autorisée à enjoindre à un hébergeur de supprimer les informations qu'il stocke et dont le contenu est équivalent à celui d'une information déclarée illicite précédemment ou de bloquer l'accès à celles-ci, pour autant que la surveillance et la recherche des informations concernées par une telle injonction sont limitées à des informations véhiculant un message dont le contenu demeure, en substance, inchangé par rapport à celui ayant donné lieu au constat d'illicéité et comportant les éléments spécifiés dans l'injonction et que les différences dans la formulation de ce contenu équivalent par rapport à celle caractérisant l'information déclarée illicite précédemment ne sont pas de nature à contraindre l'hébergeur à procéder à une appréciation autonome de ce contenu.

Enfin, une telle juridiction est en droit d'enjoindre à un hébergeur de supprimer les informations visées par l'injonction ou de bloquer l'accès à celles-ci au niveau mondial, dans le cadre du droit international pertinent.

Arrêt du 8 décembre 2022 (grande chambre), Google (Déréférencement d'un contenu prétendument inexact) (C-460/20, [EU:C:2022:962](#))

Les requérants au principal, TU, qui occupe des postes à responsabilité et détient des participations dans différentes sociétés, et RE, qui était sa compagne et, jusqu'en mai 2015, fondée de pouvoir d'une de ces sociétés, ont fait l'objet de trois articles publiés sur un site Internet en 2015 par G LLC, exploitant de ce site Internet. Ces articles, dont l'un était illustré de quatre photographies représentant les requérants et suggérant que ces

derniers menaient une vie luxueuse, présentaient de manière critique le modèle d'investissement de plusieurs de leurs sociétés. L'accès à ces articles était possible par la saisie, dans le moteur de recherche exploité par Google LLC (ci-après « Google »), des noms et prénoms des requérants, tant isolément qu'en combinaison avec certains noms de sociétés. La liste de résultats renvoyait à ces articles au moyen d'un lien, ainsi qu'aux photographies affichées sous la forme de vignettes (« thumbnails »).

Les requérants au principal ont demandé à Google, en tant que responsable du traitement des données à caractère personnel effectué par son moteur de recherche, d'une part, de déréférencer de la liste de résultats de recherche les liens vers les articles en cause, au motif que ceux-ci contiendraient des allégations inexactes et des opinions diffamatoires, et, d'autre part, de retirer les vignettes de la liste des résultats de recherche. Google a refusé de faire droit à cette demande.

Ayant été déboutés tant en première instance qu'en appel, les requérants au principal ont saisi le Bundesgerichtshof (Cour fédérale de justice, Allemagne) d'un recours en Revision, dans le cadre duquel le Bundesgerichtshof a saisi la Cour à titre préjudiciel quant à l'interprétation du RGPD¹¹¹ et de la directive 95/46¹¹².

Par son arrêt, rendu en grande chambre, la Cour développe sa jurisprudence sur les conditions applicables aux demandes de déréférencement adressées à l'exploitant d'un moteur de recherche sur le fondement des règles relatives à la protection des données à caractère personnel¹¹³. En particulier, elle examine, d'une part, l'étendue des obligations et des responsabilités qui incombent à l'exploitant d'un moteur de recherche dans le traitement d'une demande de déréférencement fondée sur la prétendue inexactitude des informations figurant dans le contenu référencé et, d'autre part, la charge de la preuve imposée à la personne concernée en ce qui concerne cette inexactitude. Elle se prononce en outre sur la nécessité, aux fins de l'examen d'une demande de suppression de photographies affichées sous la forme de vignettes dans la liste des résultats d'une recherche d'images, de tenir compte du contexte initial de la publication de ces photographies sur Internet.

En premier lieu, la Cour dit pour droit que, dans le cadre de la mise en balance entre, d'une part, les droits au respect de la vie privée et à la protection des données à caractère personnel, et, d'autre part, le droit à la liberté d'expression et d'information¹¹⁴, aux fins de l'examen d'une demande de déréférencement adressée à l'exploitant d'un moteur de recherche et visant à la suppression de la liste de résultats d'une recherche d'un lien qui mène vers un contenu comportant des informations prétendument

¹¹¹ Article 17, paragraphe 3, sous a), du règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO 2016, L 119, p. 1).

¹¹² Article 12, sous b), et article 14, premier alinéa, sous a), de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO 1995, L 281, p. 31).

¹¹³ Arrêts du 13 mai 2014, Google Spain et Google (C-131/12, [EUC:2014:317](#)), ainsi que du 24 septembre 2019, GC e.a. (Déréférencement de données sensibles) (C-136/17, [EUC:2019:773](#)) et Google (Portée territoriale du déréférencement) (C-507/17, [EUC:2019:772](#)).

¹¹⁴ Droits fondamentaux garantis respectivement par les articles 7, 8 et 11 de la charte des droits fondamentaux de l'Union européenne.

inexactes, ce déréférencement n'est pas soumis à la condition que la question de l'exactitude du contenu référencé ait été résolue, au moins à titre provisoire, dans le cadre d'un recours intenté par le demandeur contre le fournisseur de contenu.

À titre liminaire, afin d'examiner dans quelles conditions l'exploitant d'un moteur de recherche est tenu de faire droit à une demande de déréférencement et donc d'effacer de la liste des résultats, affichée à la suite d'une recherche effectuée à partir du nom de la personne concernée, le lien vers une page Internet sur laquelle figurent des allégations que cette personne estime inexactes, la Cour a notamment rappelé ce qui suit :

- dans la mesure où l'activité d'un moteur de recherche est susceptible d'affecter significativement et de manière additionnelle par rapport à celle des éditeurs de sites Internet les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel, l'exploitant de ce moteur, en tant que personne déterminant les finalités et les moyens de cette activité, doit assurer, dans le cadre de ses responsabilités, de ses compétences et de ses possibilités, que les garanties prévues par la directive 95/46 et le RGPD puissent développer leur plein effet et qu'une protection efficace et complète des personnes concernées puisse effectivement être réalisée ;
- lorsqu'il est saisi d'une demande de déréférencement, l'exploitant d'un moteur de recherche doit vérifier si l'inclusion du lien vers la page Internet en question dans la liste des résultats est nécessaire à l'exercice du droit à la liberté d'information des internautes potentiellement intéressés à avoir accès à cette page Internet au moyen d'une telle recherche, protégée par le droit à la liberté d'expression et d'information ;
- le RGPD consacre explicitement l'exigence d'une mise en balance entre, d'une part, les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel et, d'autre part, le droit fondamental à la liberté d'information.

Tout d'abord, la Cour relève que, si les droits au respect de la vie privée et à la protection des données à caractère personnel de la personne concernée prévalent, en règle générale, sur l'intérêt légitime des internautes à avoir accès à l'information en question, cet équilibre peut toutefois dépendre des circonstances pertinentes de chaque cas, notamment de la nature de cette information et de sa sensibilité pour la vie privée de la personne concernée, ainsi que de l'intérêt du public à disposer de ladite information, lequel peut varier, notamment, en fonction du rôle joué par cette personne dans la vie publique.

La question du caractère exact ou non du contenu référencé constitue également un élément pertinent dans le cadre de cette appréciation. C'est ainsi que, dans certaines circonstances, le droit à l'information des internautes et la liberté d'expression du fournisseur de contenu peuvent prévaloir sur les droits à la protection de la vie privée et à la protection des données à caractère personnel, notamment lorsque la personne concernée joue un rôle dans la vie publique. Cependant, ce rapport s'inverse lorsque, à

tout le moins, une partie des informations visées par la demande de déréférencement ne présentant pas un caractère mineur au regard de l'ensemble du contenu se révèlent inexactes. Dans une telle hypothèse, le droit d'informer et le droit d'être informé ne sauraient être pris en compte, car ils ne peuvent inclure le droit de diffuser de telles informations et d'y avoir accès.

Ensuite, s'agissant, d'une part, des obligations relatives à l'établissement du caractère exact ou non des informations figurant dans le contenu référencé, la Cour précise que la personne qui demande le déréférencement, en raison de l'inexactitude de telles informations, est tenue d'établir l'inexactitude manifeste de ces informations ou, à tout le moins, d'une partie de ces informations ne présentant pas un caractère mineur au regard de l'ensemble de ce contenu. Toutefois, afin d'éviter de faire peser sur cette personne une charge excessive susceptible de nuire à l'effet utile du droit au déréférencement, il lui incombe uniquement de fournir les éléments de preuve qu'il peut être, compte tenu des circonstances du cas d'espèce, raisonnablement exigé de rechercher de sa part. En principe, cette personne ne saurait être tenue de produire, dès le stade précontentieux, à l'appui de sa demande de déréférencement, une décision juridictionnelle obtenue contre l'éditeur du site Internet, même sous la forme d'une décision prise en référé.

D'autre part, quant aux obligations et responsabilités imposées à l'exploitant du moteur de recherche, la Cour souligne que ce dernier doit, aux fins de vérifier si un contenu peut continuer à être inclus dans la liste de résultats des recherches effectuées par l'intermédiaire de son moteur de recherche à la suite d'une demande de déréférencement, se fonder sur l'ensemble des droits et des intérêts en présence ainsi que sur l'ensemble des circonstances du cas d'espèce. Toutefois, cet exploitant ne saurait être obligé d'enquêter sur les faits et, à cette fin, d'organiser un échange contradictoire avec le fournisseur de contenu visant à obtenir des éléments manquants sur l'exactitude du contenu référencé. Une obligation à contribuer à l'établissement du caractère exact ou non du contenu référencé ferait peser sur ledit exploitant une charge dépassant ce qui peut raisonnablement être attendu de lui au regard de ses responsabilités, compétences et possibilités. Cette solution comporterait un risque sérieux que des contenus qui répondent à un besoin d'information légitime et prépondérant du public soient déréférencés et qu'il devienne ainsi difficile de les trouver sur Internet. Ainsi, il existerait un risque réel d'effet dissuasif sur l'exercice de la liberté d'expression et d'information si un tel exploitant procérait à un déréférencement de manière quasiment systématique, en vue d'éviter d'avoir à supporter la charge d'enquêter sur les faits pertinents pour établir le caractère exact ou non du contenu référencé.

Par conséquent, lorsque le demandeur de déréférencement présente des éléments de preuve établissant le caractère manifestement inexact des informations figurant dans le contenu référencé ou, à tout le moins, d'une partie de ces informations ne présentant pas un caractère mineur au regard de l'ensemble de celui-ci, l'exploitant du moteur de

recherche est tenu d'y faire droit. Il en va de même lorsque ce demandeur présente une décision de justice prise contre l'éditeur du site Internet et qui repose sur le constat que des informations figurant dans le contenu référencé, qui ne présentent pas un caractère mineur au regard de l'ensemble de celui-ci, sont, au moins à première vue, inexactes. En revanche, si le caractère inexact de telles informations n'apparaît pas de manière manifeste au vu des éléments de preuve fournis par le demandeur, l'exploitant du moteur de recherche n'est pas tenu, en l'absence d'une telle décision de justice, de faire droit à la demande de déréférencement. Lorsque les informations en cause sont susceptibles de contribuer à un débat d'intérêt général, il y a lieu, au regard de l'ensemble des circonstances du cas d'espèce, d'accorder une importance particulière au droit à la liberté d'expression et d'information.

Enfin, la Cour ajoute que, lorsque l'exploitant d'un moteur de recherche ne donne pas suite à une demande de déréférencement, la personne concernée doit pouvoir saisir l'autorité de contrôle ou l'autorité judiciaire pour que celle-ci effectue les vérifications nécessaires et ordonne à ce responsable d'adopter les mesures qui s'imposent. À cet égard, ce sont notamment les autorités judiciaires qui doivent assurer la pondération des intérêts concurrents, car elles sont les mieux placées pour effectuer une mise en balance complexe et approfondie, qui tienne compte de tous les critères et de tous les éléments établis par la jurisprudence pertinente.

En second lieu, la Cour dit pour droit que, dans le cadre de la mise en balance des droits fondamentaux susvisés, aux fins de l'examen d'une demande de déréférencement tendant à ce que soient supprimées des résultats d'une recherche d'images effectuée à partir du nom d'une personne physique des photographies affichées sous la forme de vignettes qui représentent cette personne, il y a lieu de tenir compte de la valeur informative de ces photographies indépendamment du contexte initial de leur publication sur la page Internet dont elles sont issues. Cependant, il y a lieu de prendre en considération tout élément textuel qui accompagne directement l'affichage de ces photographies dans les résultats de recherche et qui est susceptible d'apporter un éclairage sur la valeur informative de celles-ci.

Pour parvenir à cette conclusion, la Cour souligne que les recherches d'images effectuées par l'intermédiaire d'un moteur de recherche sur Internet à partir du nom d'une personne sont soumises aux mêmes principes que ceux applicables aux recherches de pages Internet et des informations qui y sont contenues. Elle indique que l'affichage, à la suite d'une recherche par nom, sous la forme de vignettes, de photographies de la personne concernée, est de nature à constituer une ingérence particulièrement importante dans les droits à la protection de la vie privée et des données à caractère personnel de cette personne.

Partant, lorsque l'exploitant d'un moteur de recherche est saisi d'une demande de déréférencement tendant à ce que soient supprimées des résultats d'une recherche d'images effectuée à partir du nom d'une personne des photographies affichées sous la forme de vignettes qui représentent cette personne, il doit vérifier si l'affichage des

photographies en question est nécessaire à l'exercice du droit à la liberté d'information des internautes potentiellement intéressés à avoir accès à ces photographies au moyen d'une telle recherche.

Or, dans la mesure où le moteur de recherche affiche des photographies de la personne concernée en dehors du contexte dans lequel celles-ci sont publiées sur la page Internet référencée, le plus souvent en vue d'illustrer les éléments textuels que contient cette page, il y a lieu de déterminer si ce contexte doit néanmoins être pris en considération lors de la mise en balance des droits et des intérêts concurrents à effectuer. Dans ce cadre, la question de savoir si ladite appréciation doit également inclure le contenu de la page Internet dans laquelle figure la photographie dont la suppression de l'affichage sous la forme d'une vignette est demandée dépend de l'objet et de la nature du traitement en cause.

En ce qui concerne, premièrement, l'objet du traitement en cause, la Cour note que la publication de photographies en tant que moyen de communication non verbal est susceptible d'avoir un impact plus fort sur les internautes que les publications textuelles. En effet, les photographies sont, en tant que telles, un moyen important d'attirer l'attention des internautes et peuvent susciter l'intérêt à accéder aux articles qu'elles illustrent. Or, en raison notamment du fait qu'elles se prêtent souvent à plusieurs interprétations, leur affichage dans la liste des résultats de la recherche en tant que vignettes peut entraîner une ingérence particulièrement grave dans le droit de la personne concernée à la protection de son image, ce qui doit être pris en compte dans le cadre de la mise en balance entre les droits et les intérêts concurrents. Une mise en balance distincte s'impose selon que sont en cause, d'une part, des articles pourvus de photographies publiées par l'éditeur de la page Internet et qui, insérées dans leur contexte d'origine, illustrent les informations fournies dans ces articles et les opinions qui y sont exprimées, et, d'autre part, des photographies affichées sous la forme de vignettes dans la liste de résultats par l'exploitant d'un moteur de recherche en dehors du contexte dans lequel celles-ci ont été publiées sur la page Internet d'origine.

À cet égard, la Cour rappelle que non seulement le motif justifiant la publication d'une donnée à caractère personnel sur un site Internet ne coïncide pas forcément avec celui qui s'applique à l'activité des moteurs de recherche, mais aussi que, même lorsque tel est le cas, le résultat de la mise en balance des droits et des intérêts en cause à effectuer peut diverger selon qu'il s'agit du traitement effectué par l'exploitant d'un moteur de recherche ou de celui effectué par l'éditeur de cette page Internet. D'une part, les intérêts légitimes justifiant ces traitements peuvent être différents et, d'autre part, les conséquences qu'ont lesdits traitements pour la personne concernée, notamment pour sa vie privée, ne sont pas nécessairement les mêmes¹¹⁵.

¹¹⁵ Voir arrêt Google Spain et Google (C-131/12, [EUC:2014:317](#)), point 86.

S'agissant, deuxièmement, de la nature du traitement effectué par l'exploitant du moteur de recherche, la Cour constate que, en repérant les photographies de personnes physiques publiées sur Internet et en les affichant séparément, dans les résultats d'une recherche d'images, sous la forme de vignettes, l'exploitant d'un moteur de recherche offre un service qui implique un traitement de données à caractère personnel autonome et distinct du traitement de l'éditeur de la page Internet dont sont extraites les photographies ainsi que du traitement, dont cet exploitant est également responsable, relatif au référencement de cette page.

Par conséquent, une appréciation autonome de l'activité de l'exploitant du moteur de recherche, consistant en l'affichage des résultats d'une recherche d'images, sous la forme de vignettes, s'impose, car l'atteinte additionnelle aux droits fondamentaux qui résulte d'une telle activité peut être particulièrement intense du fait de l'agrégation, lors d'une recherche par nom, de toutes les informations relatives à la personne concernée qui se trouvent sur Internet. Dans le cadre de cette appréciation autonome, il y a lieu de tenir compte du fait que cet affichage constitue en soi le résultat recherché par l'internaute, indépendamment de sa décision ultérieure d'accéder ou non à la page Internet d'origine.

La Cour observe, toutefois, qu'une telle mise en balance spécifique, qui prend en compte la nature autonome du traitement effectué par l'exploitant du moteur de recherche, est sans préjudice de la pertinence éventuelle d'éléments textuels pouvant directement accompagner l'affichage d'une photographie dans la liste des résultats d'une recherche, de tels éléments étant susceptibles d'apporter un éclairage sur la valeur informative de cette photographie pour le public et, partant, d'influer sur la mise en balance des droits et des intérêts en présence.

3. Droit de la concurrence

Arrêt du 13 octobre 2011, Pierre Fabre (C-439/09, [EU:C:2011:649](#))

La société Pierre Fabre Dermo-Cosmétique (PFDC) avait pour activité la fabrication et la commercialisation de produits cosmétiques par l'intermédiaire de pharmaciens, sur le marché européen. Les produits en cause n'entraient pas dans la catégorie des médicaments. Toutefois, les contrats de distribution de ces produits précisaient que les ventes devaient exclusivement être réalisées dans un espace physique et en présence d'un diplômé en pharmacie, limitant ainsi en pratique toute forme de vente sur Internet. L'Autorité française de la concurrence avait décidé que, du fait de l'interdiction de facto de toute vente sur Internet, les accords de distribution de PFDC constituaient des accords anticoncurrentiels contraires aussi bien à la législation française qu'au droit de la concurrence de l'Union européenne. PFDC a introduit un recours contre cette décision devant la cour d'appel de Paris (France), laquelle a demandé à la Cour de justice si une

interdiction générale et absolue de vendre sur Internet constitue une restriction de la concurrence « par objet », si un tel accord peut bénéficier d'une exemption par catégorie et si, lorsque l'exemption par catégorie est inapplicable, cet accord peut bénéficier d'une exemption individuelle au titre de l'article 101, paragraphe 3, TFUE.

La Cour a répondu que l'article 101, paragraphe 1, TFUE doit être interprété en ce sens qu'une clause contractuelle, dans le cadre d'un système de distribution sélective, constitue une restriction par objet au sens de cette disposition si, à la suite d'un examen individuel, cette clause n'est pas objectivement justifiée. En effet, une telle clause contractuelle réduit considérablement la possibilité d'un distributeur agréé de vendre les produits contractuels aux clients situés en dehors de son territoire contractuel ou de sa zone d'activité. Elle est donc susceptible de restreindre la concurrence dans ce secteur.

Il existe, toutefois, des exigences légitimes, telles que le maintien du commerce spécialisé capable de fournir des prestations spécifiques pour des produits de haute qualité et technicité, qui justifient une réduction de la concurrence par les prix au bénéfice d'une concurrence portant sur d'autres éléments que les prix. À cet égard, l'organisation d'un système de distribution sélective ne relève pas de l'interdiction de l'article 101, paragraphe 1, TFUE, pour autant que le choix des revendeurs s'opère en fonction de critères objectifs de caractère qualitatif, fixés d'une manière uniforme à l'égard de tous les revendeurs potentiels et appliqués de façon non discriminatoire, que les propriétés du produit en cause nécessitent, pour en préserver la qualité et en assurer le bon usage, un tel réseau de distribution et, enfin, que les critères définis n'aillettent pas au-delà de ce qui est nécessaire. S'agissant, en particulier, de la vente de produits cosmétiques et d'hygiène corporelle, l'objectif de préserver l'image de prestige de ces produits ne saurait constituer un objectif légitime pour restreindre la concurrence.

L'article 4, sous c), du règlement (CE) n° 2790/1999¹¹⁶, doit être interprété en ce sens que l'exemption par catégorie prévue à l'article 2 dudit règlement ne s'applique pas aux accords verticaux qui ont pour objet la restriction des ventes actives ou des ventes passives aux utilisateurs finals par les membres d'un système de distribution sélective qui opèrent en tant que détaillants sur le marché, sans préjudice de la possibilité d'interdire à un membre du système d'opérer à partir d'un lieu d'établissement non autorisé.

Arrêt du 6 décembre 2017, Coty Germany (C-230/16, [EU:C:2017:941](#))

Coty Germany vendait des produits cosmétiques de luxe en Allemagne. Afin de préserver son image de luxe, elle commercialisait certaines de ses marques par

¹¹⁶ Règlement (CE) n° 2790/1999 de la Commission, du 22 décembre 1999, concernant l'application de l'article 81, paragraphe 3, du traité à des catégories d'accords verticaux et de pratiques concertées (JO 1999, L 336, p. 21).

l'intermédiaire d'un réseau de distribution sélective, c'est-à-dire par des distributeurs agréés. Les points de vente de ces derniers devaient respecter un certain nombre d'exigences en termes d'environnement, d'aménagement et d'agencement. De plus, les distributeurs agréés étaient autorisés à vendre les produits en question sur Internet, dans la mesure où ils se servaient de leur propre vitrine électronique ou bien de plateformes tierces non agréées sans que l'intervention de ces dernières soit visible pour le consommateur. En revanche, il leur était expressément interdit de vendre en ligne les produits par l'intermédiaire de plateformes tierces opérant de façon visible à l'égard des consommateurs.

Coty Germany a introduit un recours devant les juridictions allemandes contre l'un de ses distributeurs agréés, Parfümerie Akzente, afin qu'il lui soit interdit, en application de cette clause contractuelle, de distribuer les produits de Coty par l'intermédiaire de la plateforme « *amazon.de* ». Ayant des doutes sur le caractère licite de cette clause au regard du droit de la concurrence de l'Union, le Oberlandgericht Frankfurt am Main (tribunal régional supérieur de Francfort-sur-le-Main, Allemagne) a interrogé la Cour de justice à cet égard.

Selon la Cour, l'article 101, paragraphe 1, TFUE doit être interprété en ce sens qu'un tel système de distribution sélective destiné à préserver l'image de luxe de ces produits est conforme à cette disposition, pour autant que le choix des revendeurs s'opère en fonction de critères objectifs de caractère qualitatif, fixés d'une manière uniforme à l'égard de tous les revendeurs potentiels et appliqués de façon non discriminatoire, et que les critères définis n'aillent pas au-delà de ce qui est nécessaire.

En outre, l'article 4 du règlement (UE) n° 330/2010¹¹⁷ doit être interprété en ce sens que l'interdiction faite aux membres d'un système de distribution sélective de produits de luxe, qui opèrent en tant que distributeurs sur le marché, d'avoir recours de façon visible à des entreprises tierces pour les ventes par Internet ne constitue pas une restriction de la clientèle, au sens de l'article 4, sous b), ni une restriction des ventes passives aux utilisateurs finals, au sens de l'article 4, sous c), dudit règlement.

Arrêt du 4 juillet 2023 (grande chambre), Meta Platforms e.a. (Conditions générales d'utilisation d'un réseau social) (C-252/21, [EU:C:2023:537](#))

La société Meta Platforms est propriétaire du réseau social en ligne « *Facebook* », qui est gratuit pour les utilisateurs privés. Le modèle économique de ce réseau social se fonde sur le financement par la publicité en ligne, qui est faite sur mesure pour ses utilisateurs individuels. Une telle publicité est techniquement rendue possible par l'établissement automatisé de profils détaillés des utilisateurs du réseau et des services en ligne proposés au niveau du groupe Meta. Ainsi, afin de pouvoir utiliser ledit réseau social, les

¹¹⁷ Règlement (UE) n° 330/2010 de la Commission, du 20 avril 2010, concernant l'application de l'article 101, paragraphe 3, du traité sur le fonctionnement de l'Union européenne à des catégories d'accords verticaux et de pratiques concertées (JO 2010, L 102, p. 1).

utilisateurs doivent, au moment de leur inscription, accepter les conditions générales établies par Meta Platforms, qui renvoient aux politiques d'utilisation des données et des cookies fixées par cette société. En vertu de ces dernières, outre les données que ces utilisateurs fournissent directement lors de leur inscription, Meta Platforms collecte également des données relatives aux activités desdits utilisateurs à l'intérieur et à l'extérieur du réseau social et les met en relation avec les comptes Facebook des utilisateurs concernés. Quant à ces dernières données, également désignées comme des « données off Facebook », il s'agit, d'une part, des données concernant la consultation de pages Internet et d'applications tierces et, d'autre part, des données relatives à l'utilisation d'autres services en ligne appartenant au groupe Meta (dont Instagram et WhatsApp). L'aperçu global des données ainsi collectées permet de tirer des conclusions détaillées sur les préférences et les intérêts de ces mêmes utilisateurs.

Par décision du 6 février 2019, le Bundeskartellamt (autorité fédérale de la concurrence, Allemagne) a interdit à Meta Platforms, d'une part, de subordonner, dans les conditions générales alors en vigueur¹¹⁸, l'utilisation du réseau social Facebook par des utilisateurs privés résidant en Allemagne au traitement de leurs données off Facebook et, d'autre part, de procéder, sans leur consentement, au traitement de ces données. En outre, l'autorité fédérale de la concurrence lui a imposé d'adapter ces conditions générales, de sorte qu'il en ressorte clairement que lesdites données ne seront pas collectées, mises en relation avec les comptes d'utilisateurs Facebook et utilisées sans le consentement des utilisateurs concernés. Enfin, cette autorité a souligné qu'un tel consentement n'était pas valide lorsqu'il constituait une condition pour l'utilisation du réseau social. Elle a motivé sa décision par le fait que le traitement des données en cause, qui ne serait pas conforme au RGPD¹¹⁹, constituerait une exploitation abusive de la position dominante de Meta Platforms sur le marché des réseaux sociaux en ligne.

Meta Platforms a introduit un recours contre cette décision devant l'Oberlandesgericht Düsseldorf (tribunal régional supérieur de Düsseldorf, Allemagne). Nourrissant des doutes, d'une part, quant à la possibilité pour des autorités de la concurrence de contrôler la conformité d'un traitement de données à caractère personnel avec les exigences formulées dans le RGPD et, d'autre part, sur l'interprétation et l'application de certaines dispositions de ce règlement, le tribunal régional supérieur de Düsseldorf a saisi la Cour à titre préjudiciel.

Par son arrêt, la Cour, réunie en grande chambre, se prononce sur la compétence d'une autorité de la concurrence nationale pour constater la non-conformité d'un traitement de données à caractère personnel avec le RGPD, ainsi que sur son articulation avec les compétences des autorités nationales chargées du contrôle de la protection des

¹¹⁸ Le 31 juillet 2019, Meta Platforms a introduit de nouvelles conditions générales indiquant expressément que l'utilisateur, au lieu de payer pour l'utilisation des produits Facebook, déclare consentir aux annonces publicitaires.

¹¹⁹ Règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO 2016, L 119, p. 1, et rectificatif JO 2018, L 127, p. 2, ci-après le « RGPD »).

données¹²⁰. Par ailleurs, elle apporte des précisions sur la possibilité du traitement, par un opérateur d'un réseau social, de données à caractère personnel « sensibles » de ses utilisateurs, sur les conditions de licéité du traitement des données effectué par un tel opérateur ainsi que sur la validité du consentement, donné aux fins d'un tel traitement par ces utilisateurs, à une entreprise en position dominante sur le marché national des réseaux sociaux en ligne.

En premier lieu, s'agissant de la compétence d'une autorité de la concurrence pour constater la non-conformité avec le RGPD d'un traitement de données à caractère personnel, la Cour considère que, sous réserve du respect de son obligation de coopération loyale¹²¹ avec les autorités de contrôle de la protection des données, une telle autorité peut constater, dans le cadre de l'examen d'un abus de position dominante de la part d'une entreprise¹²², que les conditions générales d'utilisation fixées par cette entreprise en matière de traitement des données à caractère personnel et leur mise en œuvre ne sont pas conformes à ce règlement, lorsque ce constat est nécessaire pour établir l'existence d'un tel abus. Cependant, lorsqu'une autorité de la concurrence relève une violation du RGPD dans le cadre du constat d'un abus de position dominante, elle ne se substitue pas aux autorités de contrôle.

Ainsi, compte tenu du principe de coopération loyale, lorsque les autorités de la concurrence sont amenées, dans l'exercice de leurs compétences, à examiner la conformité avec les dispositions du RGPD d'un comportement d'une entreprise, elles doivent se concerter et coopérer loyalement avec les autorités de contrôle nationales concernées ou avec l'autorité de contrôle chef de file. L'ensemble de ces autorités sont alors tenues de respecter leurs pouvoirs et compétences respectifs, de manière à ce que les obligations découlant du RGPD ainsi que les objectifs de ce règlement soient respectés et que leur effet utile soit préservé. Il s'ensuit que, lorsque, dans le cadre de l'examen visant à constater un abus de position dominante de la part d'une entreprise, une autorité de la concurrence considère qu'il est nécessaire d'examiner la conformité d'un comportement de cette entreprise à l'égard des dispositions du RGPD, ladite autorité doit vérifier si ce comportement ou un comportement similaire a déjà fait l'objet d'une décision par l'autorité de contrôle nationale compétente ou par l'autorité de contrôle chef de file ou bien encore par la Cour. Si tel est le cas, l'autorité de la concurrence ne peut s'en écarter, tout en restant libre d'en tirer ses propres conclusions sous l'angle de l'application du droit de la concurrence.

Lorsqu'elle nourrit des doutes sur la portée de l'appréciation effectuée par l'autorité de contrôle nationale compétente ou l'autorité de contrôle chef de file, lorsque le comportement en cause ou un comportement similaire fait, en même temps, l'objet d'un examen de la part de ces autorités, ou encore lorsque, en l'absence d'enquête desdites autorités, elle considère qu'un comportement d'une entreprise n'est pas

¹²⁰ Au sens des articles 51 à 59 du RGPD.

¹²¹ Consacrée à l'article 4, paragraphe 3, TUE.

¹²² Au sens de l'article 102 TFUE.

conforme aux dispositions du RGPD, l'autorité de la concurrence doit consulter ces autorités et solliciter leur coopération, afin de lever ses doutes ou de déterminer s'il y a lieu d'attendre l'adoption d'une décision par l'autorité de contrôle concernée avant d'entamer sa propre appréciation. En l'absence d'objection de leur part ou de réponse dans un délai raisonnable, l'autorité de la concurrence peut poursuivre sa propre enquête.

En deuxième lieu, s'agissant du traitement de catégories particulières de données à caractère personnel¹²³, la Cour estime que, dans le cas où un utilisateur d'un réseau social en ligne consulte des sites Internet ou des applications en rapport avec une ou plusieurs de ces catégories et, le cas échéant, y insère des données en s'inscrivant ou en effectuant des commandes en ligne, le traitement de données à caractère personnel par l'opérateur de ce réseau social en ligne¹²⁴ doit être considéré comme un « traitement portant sur des catégories particulières de données à caractère personnel », au sens de l'article 9, paragraphe 1, du RGPD, lorsqu'il permet de révéler des informations relevant d'une de ces catégories particulières, que ces informations concernent un utilisateur de ce réseau ou toute autre personne physique. Un tel traitement de données est en principe interdit, sous réserve de certaines dérogations¹²⁵.

À ce dernier égard, la Cour précise que, lorsqu'un utilisateur d'un réseau social en ligne consulte des sites Internet ou des applications en rapport avec une ou plusieurs desdites catégories particulières de données, il ne rend pas manifestement publiques¹²⁶ les données relatives à cette consultation, collectées par l'opérateur de ce réseau social en ligne à travers des cookies ou des technologies d'enregistrement similaires. Par ailleurs, lorsqu'il insère des données dans de tels sites Internet ou dans de telles applications ou lorsqu'il active des boutons de sélection intégrés à ces sites et à ces applications, tels que les boutons « j'aime » ou « partager », ou les boutons permettant à l'utilisateur de s'identifier sur ces sites ou applications en utilisant les identifiants de connexion liés à son compte d'utilisateur du réseau social, son numéro de téléphone ou son adresse électronique, un tel utilisateur ne rend manifestement publiques les données ainsi insérées ou résultant de l'activation de ces boutons que dans le cas où il a explicitement exprimé son choix au préalable, le cas échéant sur la base d'un

¹²³ Visées à l'article 9, paragraphe 1, du RGPD. Cette disposition prévoit que « [l]e traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits. »

¹²⁴ Ce traitement consiste en la collecte, au moyen d'interfaces intégrées, de cookies ou de technologies d'enregistrement similaires, des données issues de la consultation de ces sites et de ces applications ainsi que des données insérées par l'utilisateur, en la mise en relation de l'ensemble de ces données avec le compte du réseau social de celui-ci et en l'utilisation desdites données par cet opérateur.

¹²⁵ Prévues à l'article 9, paragraphe 2, du RGPD. Cette disposition énonce : « [l]e paragraphe 1 ne s'applique pas si l'une des conditions suivantes est remplie :

a) la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques, sauf lorsque le droit de l'Union ou le droit de l'État membre prévoit que l'interdiction visée au paragraphe 1 ne peut pas être levée par la personne concernée ; [...] ;
e) le traitement porte sur des données à caractère personnel qui sont manifestement rendues publiques par la personne concernée ;
f) le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ou chaque fois que des juridictions agissent dans le cadre de leur fonction juridictionnelle ;
[...]. ».

¹²⁶ Au sens de l'article 9, paragraphe 2, sous e), du RGPD.

paramétrage individuel effectué en toute connaissance de cause, de rendre les données le concernant publiquement accessibles à un nombre illimité de personnes.

En troisième lieu, en ce qui concerne plus généralement les conditions de licéité d'un traitement de données à caractère personnel, la Cour rappelle que, en vertu du RGPD, le traitement de données est licite si, et dans la mesure où, la personne concernée y a consenti pour une ou plusieurs finalités spécifiques¹²⁷. En l'absence d'un tel consentement, ou lorsque ce consentement n'a pas été donné de manière libre, spécifique, éclairée et univoque, un tel traitement est néanmoins justifié lorsqu'il répond à l'une des exigences de nécessité¹²⁸, qui doivent être interprétées strictement. Or, le traitement de données à caractère personnel de ses utilisateurs effectué par un opérateur d'un réseau social en ligne ne peut être considéré comme étant nécessaire à l'exécution du contrat auquel ces utilisateurs sont parties qu'à la condition que ce traitement soit objectivement indispensable pour réaliser une finalité faisant partie intégrante de la prestation contractuelle destinée auxdits utilisateurs, de telle sorte que l'objet principal du contrat ne pourrait être atteint en l'absence de ce traitement.

En outre, selon la Cour, le traitement de données en cause ne peut être considéré comme étant nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers qu'à la condition que ledit opérateur ait indiqué aux utilisateurs auprès desquels les données ont été collectées un intérêt légitime poursuivi par leur traitement, que ce traitement soit opéré dans les limites du strict nécessaire pour la réalisation de cet intérêt légitime et qu'il ressorte d'une pondération des intérêts opposés, au regard de l'ensemble des circonstances pertinentes, que les intérêts ou les libertés et les droits fondamentaux de ces utilisateurs ne prévalent pas sur l'objectif légitime du responsable du traitement ou d'un tiers. Or, la Cour considère notamment que, en l'absence d'un consentement de leur part, les intérêts et les droits fondamentaux desdits utilisateurs prévalent sur l'intérêt de l'opérateur d'un réseau social en ligne à la personnalisation de la publicité par laquelle il finance son activité.

Enfin, la Cour précise que le traitement de données en cause est justifié lorsqu'il est effectivement nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis, en vertu d'une disposition du droit de l'Union ou du droit de l'État membre concerné, que cette base juridique répond à un objectif d'intérêt public et est proportionnée à l'objectif légitime poursuivi et que ce traitement est opéré dans les limites du strict nécessaire.

En quatrième et dernier lieu, s'agissant de la validité du consentement des utilisateurs concernés au traitement de leurs données en vertu du RGPD, la Cour considère que la

¹²⁷ Aux termes de l'article 6, paragraphe 1, premier alinéa, sous a), du RGPD.

¹²⁸ Mentionnées à l'article 6, paragraphe 1, premier alinéa, sous b) à f), du RGPD. En vertu de ces dispositions, le traitement n'est licite que si, et dans la mesure où, il est, entre autres, nécessaire à l'exécution d'un contrat auquel la personne concernée est partie [article 6, paragraphe 1, premier alinéa, sous b), du RGPD], au respect d'une obligation légale à laquelle le responsable du traitement est soumis [article 6, paragraphe 1, premier alinéa, sous c), du RGPD] ou aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers [article 6, paragraphe 1, premier alinéa, sous f), du RGPD].

circonstance que l'opérateur d'un réseau social en ligne occupe une position dominante sur le marché des réseaux sociaux en ligne ne fait pas obstacle en tant que telle à ce que les utilisateurs d'un tel réseau puissent valablement consentir au traitement de leurs données à caractère personnel, effectué par cet opérateur. Toutefois, vu qu'une telle position est susceptible d'affecter la liberté de choix de ces utilisateurs et de créer un déséquilibre manifeste entre ceux-ci et ledit opérateur, elle constitue un élément important pour déterminer si le consentement a effectivement été donné valablement et, notamment, librement, ce qu'il incombe à ce même opérateur de prouver¹²⁹.

En particulier, les utilisateurs du réseau social en question doivent disposer de la liberté de refuser individuellement, dans le cadre du processus contractuel, de donner leur consentement à des opérations particulières de traitement de données non nécessaires à l'exécution du contrat sans qu'ils soient pour autant tenus de renoncer intégralement à l'utilisation de ce réseau social en ligne, ce qui implique que lesdits utilisateurs se voient proposer, le cas échéant contre une rémunération appropriée, une alternative équivalente non accompagnée de telles opérations de traitement de données. De plus, un consentement distinct doit pouvoir être donné pour le traitement des données off Facebook.

4. Vente de médicaments et de dispositifs médicaux en ligne

Arrêt du 11 décembre 2003 (grande chambre), Deutscher Apothekerverband (C-322/01, EU:C:2003:664)

L'affaire au principal opposait le Deutscher Apothekerverband eV, une association ayant pour mission de défendre les intérêts économiques et sociaux de la profession de pharmacien, et 0800 DocMorris NV, une pharmacie néerlandaise établie aux Pays-Bas. M. Jacques Waterval était pharmacien et l'un des représentants légaux de DocMorris. Depuis juin 2000, DocMorris et M. Waterval tenaient un site Internet de vente de médicaments sous l'adresse Internet www.0800DocMorris.com. Il s'agissait de médicaments qui étaient autorisés soit en Allemagne, soit aux Pays-Bas. La délivrance de ce type de médicament n'avait lieu que sur présentation de l'ordonnance médicale originale. L'Apothekerverband contestait, devant le Landgericht Frankfurt am Main (tribunal régional de Francfort-sur-le-Main, Allemagne), l'offre de médicaments au moyen d'Internet et la délivrance par voie de vente par correspondance transfrontalière. Selon lui, les dispositions de la loi allemande sur les médicaments ne permettaient pas l'exercice d'une telle activité. Le tribunal régional a demandé à la Cour si de telles interdictions violent le principe de la libre circulation des marchandises. Ensuite, à supposer qu'il y ait violation de l'article 28 CE, la juridiction de renvoi a souhaité savoir si

¹²⁹ En vertu de l'article 7, paragraphe 1, du RGPD.

la réglementation allemande en cause au principal est nécessaire pour protéger efficacement la santé et la vie des personnes, au sens de l'article 30 CE.

La Cour a dit pour droit que l'interdiction nationale constitue une mesure d'effet équivalent au sens de l'article 28 CE. Elle frappe davantage les pharmacies établies en dehors du territoire national et pourrait être de nature à gêner davantage l'accès au marché des produits en provenance d'autres États membres que celui des produits nationaux.

L'article 30 CE peut justifier une telle interdiction nationale, pour autant qu'elle vise les médicaments soumis à prescription médicale. En effet, au vu des risques pouvant s'attacher à l'utilisation de ces médicaments, il est nécessaire de pouvoir vérifier d'une manière efficace et responsable l'authenticité des ordonnances établies par les médecins et d'assurer ainsi la délivrance du médicament soit au client lui-même, soit à une personne chargée par ce dernier de venir le chercher. En revanche, l'article 30 CE ne peut être invoqué pour justifier une interdiction absolue de vente par correspondance des médicaments.

En outre, l'article 88, paragraphe 1, de la directive 2001/83/CE¹³⁰, s'oppose à une interdiction nationale de faire de la publicité pour la vente par correspondance des médicaments dont la délivrance est réservée exclusivement aux pharmacies dans l'État membre concerné, dans la mesure où cette interdiction vise des médicaments qui ne sont pas soumis à prescription médicale.

En effet, l'article 88, paragraphe 2, de la directive 2001/83/CE, qui autorise la publicité auprès du public pour les médicaments qui ne sont pas soumis à prescription médicale, ne saurait être interprété comme excluant la publicité pour la vente par correspondance de médicaments sur le fondement de la prétendue nécessité de la présence physique d'une pharmacie.

Arrêt du 2 décembre 2010, Ker-Optika (C-108/09, EU:C:2010:725)

Selon la législation hongroise, la commercialisation de lentilles de contact requérait un magasin spécialisé d'une superficie minimale de 18 m² ou un local séparé de l'atelier. De plus, dans le cadre de la vente de ces produits, il devait être recouru aux services d'un optométriste ou d'un médecin ophtalmologiste qualifié en matière de lentilles de contact. Toutefois, la société hongroise Ker-Optika commercialisait des lentilles de contact par l'intermédiaire de son site Internet. Les autorités de santé hongroises lui avaient interdit de poursuivre cette activité. Ker-Optika a attaqué en justice cette décision d'interdiction. Le Baranya megyei bíróság (tribunal départemental de Baranya, Hongrie), saisi du litige, a demandé à la Cour de justice si le droit de l'Union s'oppose à la réglementation hongroise.

¹³⁰ Directive 2001/83/CE du Parlement européen et du Conseil, du 6 novembre 2001, instituant un code communautaire relatif aux médicaments à usage humain (JO 2001, L 311, p. 67).

La Cour a répondu que des règles nationales relatives à la commercialisation de lentilles de contact relèvent du champ d'application de la directive 2000/31/CE¹³¹ en tant qu'elles concernent l'offre en ligne et la conclusion du contrat par voie électronique. En revanche, des règles nationales relatives à la livraison desdites lentilles ne relèvent pas du champ d'application de cette directive. Les articles 34 TFUE et 36 TFUE ainsi que la directive 2000/31/CE doivent être interprétés en ce sens qu'ils s'opposent à une réglementation nationale qui n'autorise la commercialisation de lentilles de contact que dans des magasins spécialisés en dispositifs médicaux.

En effet, la réglementation constitue une mesure d'effet équivalent à une restriction quantitative interdite par l'article 34 TFUE, dès lors que l'interdiction a pour objet une vente de lentilles de contact par Internet par correspondance et d'une livraison au domicile des consommateurs demeurant sur le territoire national et prive les opérateurs provenant d'autres États membres d'une modalité particulièrement efficace de commercialisation de ces produits, gênant ainsi considérablement l'accès de ces derniers au marché de l'État membre concerné.

Le législateur national a dépassé les limites de la marge d'appréciation dont il jouit pour décider du niveau auquel il entend assurer la protection de la santé publique, et cette réglementation doit être considérée comme allant au-delà de ce qui est nécessaire pour atteindre l'objectif invoqué. L'objectif peut être atteint par des mesures moins restrictives, consistant à ne soumettre à certaines restrictions que la première livraison de lentilles et à imposer aux opérateurs économiques intéressés de mettre à la disposition du client un opticien qualifié. Pour les mêmes motifs, ladite réglementation ne saurait être considérée comme étant proportionnée au regard de l'objectif de protection de la santé publique, au sens de l'article 3, paragraphe 4, de la directive 2000/31/CE.

Arrêt du 19 octobre 2016, Deutsche Parkinson Vereinigung (C-148/15, [EU:C:2016:776](#))

La Deutsche Parkinson Vereinigung, une organisation d'entraide allemande qui cherchait à améliorer les conditions de vie des patients atteints de la maladie de Parkinson, avait convenu d'un système de bonus avec la pharmacie par correspondance néerlandaise DocMorris. Ses membres pouvaient profiter du système de bonus lorsqu'ils achetaient des médicaments, destinés au traitement de la maladie de Parkinson, qui étaient soumis à prescription médicale et ne pouvaient être délivrés qu'en pharmacie. Une association allemande de lutte contre la concurrence déloyale avait considéré que ce système de bonus violait la réglementation allemande, laquelle prévoyait des prix uniformes de délivrance par les pharmacies pour les médicaments soumis à prescription.

¹³¹ 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 (JO 2000, L 178, p. 1).

L'Oberlandesgericht Düsseldorf (tribunal régional supérieur de Düsseldorf, Allemagne) a saisi la Cour pour savoir si cette fixation de prix uniformes est compatible avec la libre circulation des marchandises.

La Cour a jugé que l'article 34 TFUE doit être interprété en ce sens que cette réglementation nationale constitue une mesure d'effet équivalent à une restriction quantitative à l'importation. Cette réglementation affecte davantage la vente de médicaments soumis à prescription par des pharmacies établies dans d'autres États membres que la vente de ces médicaments par des pharmacies établies sur le territoire national.

En effet, les pharmacies traditionnelles sont mieux à même que les pharmacies par correspondance de dispenser aux patients des conseils individuels et d'assurer un approvisionnement en médicaments en cas d'urgence. Il convient de considérer que la concurrence par les prix est susceptible de représenter un paramètre concurrentiel plus important pour ces dernières.

L'article 36 TFUE doit être interprété en ce sens qu'une réglementation nationale ne saurait être justifiée aux fins de la protection de la santé et de la vie des personnes dans la mesure où cette réglementation n'est pas apte à atteindre les objectifs recherchés. L'objectif d'assurer un approvisionnement sûr et de qualité de médicaments sur tout le territoire national relève de l'article 36 TFUE. Mais une telle réglementation ne peut être valablement justifiée que si elle est propre à garantir la réalisation de l'objectif légitime poursuivi et ne va pas au-delà de ce qui est nécessaire pour qu'il soit atteint.

À cet égard, une concurrence accrue par les prix entre les pharmacies serait bénéfique à l'approvisionnement uniforme en médicaments et n'a pas d'influence négative sur l'accomplissement par les pharmacies traditionnelles de certaines activités d'intérêt général, telles que la fabrication de médicaments sur ordonnance ou le maintien d'un certain stock et assortiment de médicaments. Enfin, une concurrence par les prix pourrait être de nature à profiter au patient, dans la mesure où elle permettrait d'offrir les médicaments soumis à prescription à des prix plus favorables.

Arrêt du 29 février 2024, Doctipharma (C-606/21, [EU:C:2024:179](#))

Saisie à titre préjudiciel par la cour d'appel de Paris (France), la Cour précise les contours de la notion de « service de la société de l'information » et donne les éléments d'interprétation qui permettent d'apprécier la conformité avec le droit de l'Union de l'interdiction par un État membre d'un service fourni au moyen d'un site Internet et consistant à mettre en relation des pharmaciens et des clients, pour la vente en ligne de médicaments non soumis à prescription médicale (ci-après le « service fourni »).

Doctipharma a mis en place le site www.doctipharma.fr, sur lequel les internautes pouvaient acheter, à partir des sites d'officines de pharmacies, des produits pharmaceutiques et des médicaments sans ordonnance.

Sur ce site, les pharmaciens souscrivaient à la plateforme de vente en ligne, par le biais d'un abonnement mensuel versé à Doctipharma, et les clients devaient créer un compte client afin d'accéder aux sites des pharmaciens de leur choix.

L'Union des Groupements de pharmaciens d'officine (UDGPO), considérant que cette pratique faisait participer Doctipharma au commerce électronique de médicaments, a assigné celle-ci devant le tribunal de commerce de Nanterre (France), qui a constaté le caractère illicite du site Internet et a enjoint à Doctipharma de cesser son activité. La Cour de cassation (France) a annulé l'arrêt de la cour d'appel de Versailles (France) ayant infirmé le jugement de première instance. Elle a estimé que, en mettant en relation des pharmaciens d'officine et des patients potentiels, Doctipharma avait joué un rôle d'intermédiaire dans la vente de médicaments sans ordonnance et participait au commerce électronique de médicaments, sans, pour autant, avoir la qualité de pharmacien requise par la législation nationale. Elle a renvoyé l'affaire devant la cour d'appel de Paris (France), la juridiction de renvoi en l'espèce.

Face aux différentes approches adoptées par les juridictions françaises, la juridiction de renvoi a décidé de saisir la Cour de plusieurs questions préjudiciales. Elle interroge la Cour sur l'interprétation de la directive 98/34¹³², pour déterminer si le service fourni relève de la notion de « service de la société de l'information », et sur celle de l'article 85 quater de la directive 2001/83¹³³, afin de savoir si les États membres peuvent, sur le fondement de cette disposition, interdire la fourniture du service en cause.

En premier lieu, s'agissant des conditions à remplir pour qualifier un service comme relevant de la notion de « service de la société de l'information » aux fins des directives 98/34 et 2015/1535¹³⁴, la Cour estime tout d'abord qu'il serait indifférent, d'une part, que Doctipharma ait été rémunérée par les pharmaciens qui souscrivaient à sa plateforme, sur la base d'un forfait, et, d'autre part, que le service fourni par celle-ci ait fait l'objet d'un abonnement mensuel qui lui était versé par les pharmaciens et d'une rétrocession d'un pourcentage du montant des ventes, prélevé par la plateforme, puisque ces circonstances, si elles étaient avérées, impliquent que le service en cause doit être considéré comme remplissant la condition d'être fourni contre rémunération. Ensuite, la qualification du service en cause de « service de la société de l'information » découle également du fait que celui-ci se fait par l'entremise d'un site Internet qui ne requiert pas la présence simultanée du prestataire de service et du client ou du

¹³² Directive 98/34/CE du Parlement européen et du Conseil, du 22 juin 1998, prévoyant une procédure d'information dans le domaine des normes et réglementations techniques et des règles relatives aux services de la société de l'information (JO 1998, L 204, p. 37), telle que modifiée par la directive 98/48/CE du Parlement européen et du Conseil, du 20 juillet 1998 (JO 1998, L 217, p. 18) (ci-après la « directive 98/34 »).

¹³³ Directive 2001/83/CE du Parlement européen et du Conseil, du 6 novembre 2001, instituant un code communautaire relatif aux médicaments à usage humain (JO 2001, L 311, p. 67), telle que modifiée par la directive 2011/62/UE du Parlement européen et du Conseil, du 8 juin 2011 (JO 2011, L 174, p. 74).

¹³⁴ L'article 1^{er}, point 2, de la directive 98/34 et l'article 1^{er}, paragraphe 1, sous b), de la directive 2015/1535 du Parlement européen et du Conseil, du 9 septembre 2015, prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information (JO 2015, L 241, p. 1), sont libellés de façon identique. Ces articles définissent la notion de « service de la société de l'information » à partir de quatre conditions : « tout service presté normalement contre rémunération, à distance, par voie électronique, et à la demande individuelle d'un destinataire de services ».

pharmacien, ainsi que par le fait que le service est presté à la demande individuelle des pharmaciens et des clients.

La Cour en conclut qu'un service, fourni sur un site Internet, mettant en relation des pharmaciens et des clients pour la vente, à partir des sites d'officines des pharmacies ayant souscrit à ce service, de médicaments non soumis à prescription médicale, relève de la notion de « service de la société de l'information ».

En second lieu, s'agissant de la possibilité pour les États membres d'interdire un tel service d'intermédiation au titre de l'article 85 quater de la directive 2001/83, la Cour rappelle que les États membres sont seuls compétents pour déterminer les personnes physiques ou morales autorisées ou habilitées à délivrer, à distance, au moyen de services de société de l'information, des médicaments au public.

Elle considère que l'article 85 quater, paragraphe 1, sous a), de la directive 2001/83 impose à la juridiction de renvoi de vérifier si le prestataire du service en cause doit être regardé comme se bornant, par une prestation propre et distincte de la vente, à mettre en relation des vendeurs avec des clients, ou si ce prestataire doit être considéré comme étant lui-même prestataire de la vente.

À cet égard, en l'occurrence, si, à l'issue de cette analyse, Doctipharma devait être considérée comme étant elle-même prestataire de la vente, l'article 85 quater, paragraphe 1, sous a), ne s'opposerait pas à l'interdiction de ce service par l'État membre sur le territoire duquel elle est établie. De fait, un État membre peut réserver la vente à distance au public, au moyen de services de la société de l'information, de médicaments sans ordonnance, aux seules personnes ayant la qualité de pharmacien.

À l'inverse, s'il s'avérait que Doctipharma fournit un service propre et distinct de la vente, alors le service fourni ne pourrait pas être interdit sur le fondement de l'article 85, quater, paragraphe 2, de la directive 2001/83 et ne relèverait pas de la notion de « conditions de délivrance au détail » des médicaments offerts à la vente à distance au public. En effet, le service fourni doit être qualifié de « service de la société de l'information ». Or, l'article 85 quater, paragraphe 1, prévoit explicitement que, sans préjudice des législations nationales interdisant l'offre à la vente à distance au public de médicaments soumis à prescription, les États membres veillent à ce que les médicaments soient offerts à la vente à distance au public au moyen de services de la société de l'information. Dès lors, il serait incohérent de considérer que le recours à un tel service puisse être interdit par les États membres.

5. Jeux de hasard

Arrêt du 6 novembre 2003 (grande chambre), Gambelli (C-243/01, EU:C:2003:597)

M. Piergiorgio Gambelli et 137 autres personnes géraient en Italie des centres de transmission de données qui collectaient des paris sportifs sur le territoire italien, pour le compte d'un bookmaker anglais auquel ils étaient reliés par Internet. Le bookmaker, Stanley International Betting Ltd, poursuivait ses activités sur la base d'une licence accordée par la ville de Liverpool en vertu du droit anglais. En Italie, cette activité était réservée à l'État ou à ses concessionnaires. Toute transgression de cette règle pouvait aboutir à une sanction pénale allant jusqu'à un an d'emprisonnement. Des poursuites pénales avaient été diligentées contre M. Gambelli. Celui-ci soutenait que les dispositions italiennes étaient contraires aux principes communautaires de liberté d'établissement et de libre prestation des services. Le Tribunale di Ascoli Piceno (tribunal d'Ascoli Piceno, Italie), saisi de cette affaire, a demandé à la Cour de justice comment interpréter les dispositions du traité CE en la matière.

La Cour a dit pour droit qu'une telle réglementation nationale constitue une restriction à la liberté d'établissement et à la libre prestation des services prévues respectivement aux articles 43 CE et 49 CE. Pour être justifiée, elle doit se fonder sur des raisons impérieuses d'intérêt général, être propre à garantir la réalisation de l'objectif poursuivi, ne pas aller au-delà de ce qui est nécessaire pour atteindre cet objectif et être appliquée de manière non discriminatoire.

Il appartient, à cet égard, aux juridictions nationales de vérifier si une telle réglementation, au regard de ses modalités concrètes d'application, répond véritablement aux objectifs susceptibles de la justifier et si les restrictions qu'elle impose n'apparaissent pas disproportionnées au regard de ces objectifs.

La Cour a également décidé que dans la mesure où les autorités d'un État membre incitent et encouragent les consommateurs à participer aux loteries, aux jeux de hasard ou aux jeux de paris afin que le trésor public en retire des bénéfices sur le plan financier, les autorités de cet État ne sauraient invoquer l'ordre public social tenant à la nécessité de réduire les occasions de jeu pour justifier des mesures telles que celles en cause au principal.

Arrêt du 8 septembre 2009 (grande chambre), Liga Portuguesa et Bwin International (C-42/07, EU:C:2009:519)

Bwin, une entreprise de jeux en ligne dont le siège est à Gibraltar (Royaume-Uni) et qui n'a aucun établissement au Portugal, proposait des jeux de hasard sur un site Internet. Ses serveurs étaient situés à Gibraltar et en Autriche. La Liga, une personne morale de droit privé, regroupant tous les clubs qui disputent des compétitions de football au niveau professionnel au Portugal, avait changé son nom pour devenir la Bwin Liga, car

ladite entreprise devenait le principal parraineur institutionnel de la première division de football au Portugal. Le site Internet de la Liga avait été pourvu des références du site Internet de Bwin et d'un lien vers celui-ci.

La direction du département des jeux de Santa Casa a par la suite adopté des décisions infligeant des amendes à la Liga et à Bwin pour le développement de jeux sociaux, d'une part, et, d'autre part, en raison de la publicité faite pour ces jeux. La Liga et Bwin ont introduit des recours devant le Tribunal de Pequena Instância Criminal do Porto (tribunal pénal de Porto, Portugal) pour demander l'annulation desdites décisions en invoquant, notamment, les articles 43 CE, 49 CE et 56 CE.

La Cour a jugé que lorsqu'une mesure nationale se rattache simultanément à plusieurs libertés fondamentales, la Cour l'examine, en principe, au regard d'une seule de ces libertés s'il s'avère que, dans les circonstances de l'espèce, les autres sont tout à fait secondaires par rapport à la première et peuvent lui être rattachées.

À la suite, elle constate qu'une telle réglementation donne lieu à une restriction à la libre prestation des services garantie par l'article 49 CE, en imposant en outre une restriction à la liberté des résidents de l'État membre concerné de bénéficier, par Internet, de services offerts dans d'autres États membres. Toutefois, la restriction en cause peut être considérée comme justifiée par l'objectif de lutte contre la fraude et la criminalité.

Le secteur des jeux de hasard offerts par Internet ne fait pas l'objet d'une harmonisation communautaire. Un État membre est donc en droit de considérer que le seul fait qu'un opérateur privé propose légalement des services par Internet dans un autre État membre, où il est établi, ne saurait être considéré comme une garantie suffisante de protection des consommateurs nationaux. En outre, en raison du manque de contact direct entre le consommateur et l'opérateur, les jeux de hasard accessibles par Internet comportent des risques de nature différente en ce qui concerne d'éventuelles fraudes. Par ailleurs, ne saurait être exclue la possibilité qu'un opérateur qui parraine certaines des compétitions sportives sur lesquelles il prend des paris pourrait se trouver dans une situation qui lui permette d'influencer le résultat de celles-ci et d'augmenter ainsi ses profits. L'article 49 CE ne s'oppose pas à une réglementation d'un État membre qui interdit à des opérateurs privés établis dans d'autres États membres, où ils fournissent légalement des services analogues, de proposer des jeux de hasard par Internet sur le territoire dudit État membre.

Arrêt du 22 juin 2017, Unibet International (C-49/16, [EU:C:2017:491](#))

La société maltaise Unibet International organisait des jeux de hasard en ligne. En 2014, Unibet, qui était titulaire d'autorisations délivrées par plusieurs États membres, avait fourni sur des sites Internet en langue hongroise des services de jeux de hasard, alors qu'elle ne disposait pas de l'autorisation requise en Hongrie. Les autorités hongroises avaient, d'une part, ordonné la fermeture temporaire de l'accès depuis la Hongrie aux sites Internet d'Unibet et, d'autre part, infligé une amende à Unibet. Les opérateurs

établis dans d'autres États membres auraient pu, en théorie, se voir octroyer une autorisation permettant l'organisation de jeux de hasard en ligne dans la mesure où la fourniture de tels services n'avait pas été réservée à un monopole étatique. Néanmoins, ils étaient en pratique dans l'impossibilité de se procurer une telle autorisation. Dans ce contexte, la Fővárosi Közigazgatási és Munkaügyi Bíróság (tribunal administratif et du travail de Budapest, Hongrie) a demandé à la Cour de justice si la réglementation hongroise en cause est compatible avec le principe de la libre prestation des services.

La Cour a jugé que l'article 56 TFUE doit être interprété en ce sens qu'il s'oppose à une législation nationale qui instaure un régime de concessions pour l'organisation de jeux de hasard en ligne, lorsque celle-ci contient des règles discriminatoires à l'égard des opérateurs établis dans d'autres États membres ou dès lors qu'elle prévoit des règles non discriminatoires, mais qui sont appliquées de façon non transparente de manière à empêcher ou à rendre plus difficile la candidature de soumissionnaires établis dans d'autres États membres.

Une règle selon laquelle les opérateurs fiables devraient avoir exercé, pendant une période de dix ans au moins, une activité d'organisation de jeux de hasard sur le territoire de cet État membre, désavantage les opérateurs établis dans d'autres États membres. La seule invocation d'un objectif d'intérêt général ne saurait suffire à justifier une telle différence de traitement.

L'obligation nationale d'avoir exercé pendant trois ans dans un État membre une activité d'organisation de jeux de hasard ne crée pas d'avantage en faveur des opérateurs établis dans l'État membre d'accueil et pourrait être justifiée par un objectif d'intérêt général. Il importe toutefois que les règles en cause soient appliquées de manière transparente à l'égard de tous les soumissionnaires. Ne remplit pas cette exigence une réglementation nationale dont les conditions d'exercice des pouvoirs du ministre de l'Économie qu'elle fixe lors d'une telle procédure, ainsi que les conditions techniques devant être remplies par les opérateurs de jeux de hasard lors de la présentation de leur offre, ne sont pas définies avec suffisamment de précision.

L'article 56 TFUE doit être interprété en ce sens qu'il s'oppose à des sanctions infligées en raison de la violation de la législation nationale instaurant un régime de concessions et d'autorisations pour l'organisation de jeux de hasard, dans l'hypothèse où une telle législation nationale s'avère être contraire à cet article.

6. Économie du partage

Arrêt du 20 décembre 2017 (grande chambre), Asociación Profesional Élite Taxi (C-434/15, EU:C:2017:981)

La plateforme électronique Uber fournissait, au moyen d'une application, un service rémunéré de mise en relation de chauffeurs non professionnels utilisant leur propre véhicule. En 2014, une association professionnelle de chauffeurs de taxi de la ville de Barcelone (Espagne) avait formé un recours devant le Juzgado de lo Mercantil n° 3 de Barcelona (tribunal de commerce n° 3 de Barcelone, Espagne). Selon elle, les activités d'Uber constituaient des pratiques trompeuses et des actes de concurrence déloyale. Le tribunal de commerce a estimé nécessaire de vérifier si Uber doit disposer d'une autorisation administrative préalable. Si le service relevait de la directive relative aux services dans le marché intérieur¹³⁵ ou de la directive 98/34/CE¹³⁶, les pratiques d'Uber ne pourraient pas être considérées comme déloyales.

La Cour a dit pour droit que les questions de la juridiction de renvoi portent sur la qualification juridique du service en cause et qu'elle est donc compétente pour connaître de ces questions.

Ainsi, un tel service pourrait être qualifié de « service de la société de l'information », au sens de l'article 1^{er}, point 2, de la directive 98/34/CE, auquel renvoie l'article 2, sous a), de la directive 2000/31/CE. Ce service constitue un « service presté normalement contre rémunération, à distance par voie électronique et à la demande individuelle d'un destinataire de services ».

Un tel service ne se résume pas à un service d'intermédiation consistant à mettre en relation, au moyen d'une application pour téléphone intelligent, un chauffeur non professionnel utilisant son propre véhicule et une personne qui souhaite effectuer un déplacement urbain. En effet, dans une situation telle que celle visée par la juridiction de renvoi, le fournisseur crée en même temps une offre de services de transport urbain, qu'il rend accessible par l'application et dont il organise le fonctionnement général.

Les chauffeurs ne seraient pas amenés à fournir des services de transport sans l'application et les passagers n'auraient pas recours aux services desdits chauffeurs. De surcroît, Uber exerce une influence décisive sur les conditions de la prestation de tels chauffeurs et établit, au moyen de l'application éponyme, à tout le moins le prix maximum de la course, elle collecte ce prix auprès du client avant d'en reverser une partie au chauffeur non professionnel du véhicule. En outre, elle exerce un certain contrôle sur la qualité des véhicules et de leurs chauffeurs ainsi que sur le

¹³⁵ Directive 2006/123/CE du Parlement européen et du Conseil, du 12 décembre 2006, relative aux services dans le marché intérieur (JO 2006, L 376, p. 36).

¹³⁶ Directive 98/34/CE du Parlement européen et du Conseil, du 22 juin 1998, prévoyant une procédure d'information dans le domaine des normes et réglementations techniques et des règles relatives aux services de la société de l'information (JO 1998, L 204, p. 37).

comportement de ces derniers, pouvant entraîner, le cas échéant, leur exclusion. Ce service d'intermédiation doit donc être considéré comme « service dans le domaine des transports », au sens de l'article 2, paragraphe 2, sous d), de la directive 2006/123/CE, et est donc exclu du champ d'application de ladite directive.

Arrêt du 10 avril 2018 (grande chambre), Uber France (C-320/16, [EU:C:2018:221](#))

La société française Uber France qui exploitait un service dénommé Uber Pop, par lequel elle mettait en relation des chauffeurs non professionnels utilisant leur propre véhicule avec des personnes souhaitant effectuer des déplacements urbains, au moyen d'une application pour téléphone intelligent, était poursuivie au pénal pour avoir organisé ce service. Elle soutenait que la législation française sur la base de laquelle elle était poursuivie constituait une règle technique concernant un service de la société de l'information au sens de la directive relative aux normes et réglementations techniques¹³⁷. Cette directive requiert des États membres qu'ils notifient à la Commission tout projet de loi ou de réglementation édictant des règles techniques relatives aux produits et services de la société de l'information. Or, en l'occurrence, les autorités françaises n'avaient pas notifié à la Commission la législation pénale en cause avant sa promulgation. Saisi de l'affaire, le tribunal de grande instance de Lille (France) a demandé à la Cour de justice si les autorités françaises étaient tenues ou non de notifier préalablement le projet de loi à la Commission.

La Cour a jugé que l'article 1^{er} de la directive 98/34/CE, modifiée par la directive 98/48/CE, et l'article 2, paragraphe 2, sous d), de la directive 2006/123/CE doivent être interprétés en ce sens qu'une réglementation nationale qui sanctionne pénalement le fait d'organiser un tel système porte sur un « service dans le domaine des transports », en tant qu'elle s'applique à un service d'intermédiation fourni au moyen d'une application pour téléphone intelligent et qui fait partie intégrante d'un service global dont l'élément principal est le service de transport. Un tel service est exclu du champ d'application de ces directives.

La Cour a rappelé qu'elle a jugé, dans l'affaire Asociación Profesional Élite Taxi, C-434/15 (voir ci-dessus), que le service UberPop relevait du domaine du transport et ne constituait pas un service de la société de l'information au sens de la directive 98/34. Selon la Cour, le service UberPop proposé en France est substantiellement identique à celui fourni en Espagne. Il s'ensuit que les autorités françaises n'étaient pas tenues de notifier préalablement le projet de loi pénale en cause à la Commission.

¹³⁷ Directive 98/34/CE du Parlement européen et du Conseil, du 22 juin 1998, prévoyant une procédure d'information dans le domaine des normes et réglementations techniques et des règles relatives aux services de la société de l'information (JO 1998, L 204, p. 37).

Arrêt du 19 décembre 2019 (grande chambre), Airbnb Ireland (C-390/18, EU:C:2019:1112)

Par son arrêt du 19 décembre 2019, Airbnb Ireland (C-390/18), la grande chambre de la Cour a jugé, d'une part, qu'un service d'intermédiation qui a pour objet, au moyen d'une plateforme électronique, de mettre en relation, contre rémunération, des locataires potentiels avec des loueurs professionnels ou non professionnels proposant des prestations d'hébergement de courte durée, tout en fournissant également un certain nombre de prestations accessoires à ce service d'intermédiation, doit être qualifié de « service de la société de l'information » relevant de la directive 2000/31 sur le commerce électronique¹³⁸. D'autre part, la Cour a considéré qu'un particulier peut s'opposer à ce que lui soient appliquées, dans le cadre d'une procédure pénale avec constitution de partie civile, des mesures d'un État membre restreignant la libre circulation d'un tel service, qu'il fournit à partir d'un autre État membre, lorsque lesdites mesures n'ont pas été notifiées conformément à l'article 3, paragraphe 4, sous b), second tiret, de la même directive.

Le litige au principal s'inscrit dans le cadre d'une procédure pénale introduite en France, faisant suite à une plainte avec constitution de partie civile déposée contre Airbnb Ireland par l'Association pour un hébergement et un tourisme professionnels. Airbnb Ireland est une société irlandaise qui administre une plateforme électronique permettant, moyennant le paiement d'une commission, la mise en relation, notamment en France, de loueurs professionnels ainsi que particuliers proposant des prestations d'hébergement de courte durée et de personnes recherchant ce type d'hébergement. En outre, Airbnb Ireland propose auxdits loueurs des prestations accessoires, comme un canevas définissant le contenu de leur offre, une assurance responsabilité civile, un outil d'estimation du prix de leur location ou encore des services de paiement relatifs à ces prestations.

L'association ayant porté plainte contre Airbnb Ireland soutenait que cette société ne se contentait pas de mettre en relation deux parties grâce à la plateforme éponyme, mais qu'elle exerçait une activité d'agent immobilier sans détenir de carte professionnelle, violant ainsi la loi dite Hoguet, applicable en France aux activités des professionnels de l'immobilier. Pour sa part, Airbnb Ireland faisait valoir que la directive 2000/31 s'opposait, en tout état de cause, à cette réglementation.

Interrogée en premier lieu sur la qualification du service d'intermédiation fourni par Airbnb Ireland, la Cour a rappelé, en se référant à l'arrêt Asociación Profesional Elite Taxi¹³⁹, que, si un service d'intermédiation satisfait aux conditions visées à l'article 1^{er}, paragraphe 1, sous b), de la directive 2015/1535¹⁴⁰, auquel renvoie l'article 2, sous a), de

¹³⁸ 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 (« directive sur le commerce électronique ») (JO 2000, L 178, p. 1).

¹³⁹ Arrêt du 20 décembre 2017, Asociación Profesional Elite Taxi (C-434/15, [EU:C:2017:981](#)), point 40.

¹⁴⁰ Directive (UE) 2015/1535 du Parlement européen et du Conseil, du 9 septembre 2015, prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information (JO 2015, L 241, p. 1).

la directive 2000/31, il constitue en principe un « service de la société de l'information », distinct du service subséquent auquel il se rapporte. Toutefois, il doit en aller autrement s'il apparaît que ce service d'intermédiation fait partie intégrante d'un service global dont l'élément principal est un service relevant d'une autre qualification juridique.

En l'espèce, la Cour a considéré qu'un service d'intermédiation tel que celui fourni par Airbnb Ireland remplissait ces conditions sans que la nature des liens existant entre le service d'intermédiation et la prestation d'hébergement ne justifiât d'écartier la qualification de « service de la société de l'information » dudit service d'intermédiation et, partant, l'application à celui-ci de la directive 2000/31.

Pour souligner le caractère dissociable que présente un tel service d'intermédiation par rapport aux prestations d'hébergement auxquelles il se rapporte, la Cour a relevé, en premier lieu, que ce service ne tend pas uniquement à la réalisation immédiate de telles prestations, mais consiste pour l'essentiel en la fourniture d'un instrument de présentation et de recherche des logements mis à la location, facilitant la conclusion de futurs contrats de location. Dès lors, ce type de service ne saurait être considéré comme constituant le simple accessoire d'un service global d'hébergement. En deuxième lieu, la Cour a souligné qu'un service d'intermédiation tel que celui fourni par Airbnb Ireland n'est aucunement indispensable à la réalisation de prestations d'hébergement, les locataires et les loueurs disposant de nombreux autres canaux à cet effet, dont certains existent de longue date. En troisième lieu, enfin, la Cour a relevé qu'aucun élément du dossier n'indiquait qu'Airbnb fixerait ou plafonnerait le montant des loyers réclamés par les loueurs ayant recours à sa plateforme.

La Cour a encore précisé que les autres prestations proposées par Airbnb Ireland ne permettent pas de remettre en cause ce constat, ces diverses prestations étant simplement accessoires au service d'intermédiation fourni par cette société. En outre, elle a indiqué que, à la différence des services d'intermédiation en cause dans les arrêts *Asociación Profesional Elite Taxi* et *Uber France*¹⁴¹, ni ce service d'intermédiation ni les prestations accessoires proposés par Airbnb Ireland ne permettent d'établir l'existence d'une influence décisive exercée par cette société sur les services d'hébergement auxquels se rapporte son activité, s'agissant tant de la détermination des prix des loyers réclamés que de la sélection des loueurs ou des logements mis en location sur sa plateforme.

En second lieu, la Cour a examiné si Airbnb Ireland peut, dans le litige au principal, s'opposer à ce que lui soit appliquée une loi restreignant la libre prestation des services de la société de l'information fournis par un opérateur à partir d'un autre État membre, telle que la loi Hoguet, au motif que cette loi n'a pas été notifiée par la France, conformément à l'article 3, paragraphe 4, sous b), second tiret, de la directive 2000/31. À cet égard, la Cour a relevé que le fait que ladite loi soit antérieure à l'entrée en vigueur

¹⁴¹ Arrêt du 10 avril 2018, *Uber France* (C-320/16, [EU:C:2018:221](#)).

de la directive 2000/31 ne saurait avoir eu pour conséquence de libérer la République française de son obligation de notification. Ensuite, s'inspirant du raisonnement suivi dans l'arrêt CIA Security International¹⁴², elle a considéré que ladite obligation, qui constitue une exigence procédurale de nature substantielle, doit se voir reconnaître un effet direct. Elle en a déduit que la méconnaissance, par un État membre, de son obligation de notification d'une telle mesure peut être invoquée par un particulier dans le cadre non seulement de poursuites pénales dirigées contre lui mais également d'une demande indemnitaire formée par un autre particulier s'étant constitué partie civile.

Arrêt du 9 novembre 2023, Google Ireland e.a. (C-376/22, EU:C:2023:835)

Google Ireland Limited, Meta Platforms Ireland Limited et Tik Tok Technology Limited sont des sociétés établies en Irlande qui fournissent, notamment en Autriche, des services de plateformes de communication.

Par ses décisions, adoptées en 2021, la Kommunikationsbehörde Austria (KommAustria) (autorité autrichienne de régulation en matière de communication) a déclaré que les trois sociétés susvisées étaient soumises à la loi autrichienne¹⁴³.

Considérant que cette loi autrichienne, qui impose aux fournisseurs de services de plateformes de communication, qu'ils soient établis en Autriche ou ailleurs, un ensemble d'obligations en matière de contrôle et de notification des contenus prétendument illicites, ne devrait pas leur être appliquée, ces sociétés ont intenté des recours contre les décisions de la KommAustria. Ces recours ont été rejetés en première instance.

À la suite de ce rejet, lesdites sociétés ont introduit des pourvois en Revision devant le Verwaltungsgerichtshof (Cour administrative, Autriche). Au soutien de ces pourvois, elles font notamment valoir que les obligations instaurées par la loi autrichienne seraient disproportionnées et incompatibles avec la libre circulation des services de la société de l'information et avec le principe du contrôle de ces services par l'État membre d'origine, autrement dit, par l'État sur le territoire duquel le prestataire de services est établi, prévu par la directive sur le commerce électronique¹⁴⁴.

Nourrissant des doutes quant à la compatibilité de loi autrichienne et des obligations qu'elle impose aux fournisseurs de services avec la directive sur le commerce électronique, qui prévoit la faculté pour un État membre autre que celui d'origine de déroger, sous certaines conditions, au principe de libre circulation des services de la société de l'information, la Cour administrative a saisi la Cour à titre préjudiciel sur l'interprétation de cette directive.

¹⁴² Arrêt du 30 avril 1996, CIA Security International (C-194/94, EU:C:1996:172).

¹⁴³ À savoir, au Bundesgesetz über Maßnahmen zum Schutz der Nutzer auf Kommunikationsplattformen (Kommunikationsplattformen-Gesetz) (loi fédérale portant mesures de protection des utilisateurs de plateformes de communication) (BGBI. I, 151/2020).

¹⁴⁴ 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 (JO 2000, L 178, p. 1) (ci-après la « directive sur le commerce électronique »).

Dans son arrêt, la Cour se prononce sur la question de savoir si un État membre de destination de services de la société de l'information peut déroger à la libre circulation de ces services en prenant non seulement des mesures individuelles et concrètes, mais également des mesures générales et abstraites visant une catégorie de services donnés et concrètement, si ces mesures sont susceptibles de relever de la notion de « mesures prises à l'encontre d'un service donné de la société de l'information » au sens de la directive sur le commerce électronique¹⁴⁵.

Tout d'abord, la Cour relève que la possibilité de déroger au principe de libre circulation des services de la société de l'information concerne, selon les termes de la directive sur le commerce électronique, un « service donné de la société de l'information ». Dans ce cadre, l'emploi du mot « donné » tend à indiquer que le service ainsi visé doit être entendu comme un service individualisé. Par conséquent, les États membres ne sauraient adopter des mesures générales et abstraites visant une catégorie de services donnés de la société de l'information décrite en des termes généraux et s'appliquant indistinctement à tout prestataire de cette catégorie de services.

Cette appréciation n'est pas remise en cause par le fait que la directive sur le commerce électronique emploie la notion de « mesures ». En effet, en ayant recours à un tel terme large et général, le législateur de l'Union européenne a laissé à la discrétion des États membres la nature et la forme des mesures qu'ils peuvent adopter pour déroger au principe de libre circulation des services de la société de l'information. En revanche, le recours à ce terme ne préjuge en rien de la substance et du contenu matériel de ces mesures.

Ensuite, la Cour note que cette interprétation littérale est corroborée par l'analyse contextuelle de la directive sur le commerce électronique.

En effet, la possibilité de déroger au principe de libre circulation des services de la société de l'information est soumise à la condition selon laquelle l'État membre de destination de ces services doit préalablement demander à l'État membre de leur origine de prendre des mesures¹⁴⁶, ce qui presuppose la possibilité d'identifier les prestataires et, par conséquent, les États membres concernés. Or, si les États membres étaient autorisés à restreindre la libre circulation de tels services au moyen de mesures à caractère général et abstrait s'appliquant indistinctement à tout prestataire d'une catégorie de ces services, une telle identification serait, si ce n'est impossible, à tout le moins excessivement difficile, de telle sorte que les États membres ne seraient pas en mesure de respecter une telle condition.

Enfin, la Cour souligne que la directive sur le commerce électronique repose sur l'application des principes du contrôle dans l'État membre d'origine et de la

¹⁴⁵ Article 3, paragraphe 4, de la directive sur le commerce électronique.

¹⁴⁶ Article 3, paragraphe 4, sous b), de la directive sur le commerce électronique.

reconnaissance mutuelle, de telle sorte que, dans le cadre du domaine coordonné¹⁴⁷, les services de la société de l'information sont réglementés dans le seul État membre sur le territoire duquel les prestataires de ces services sont établis. Or, si les États membres de destination étaient autorisés à adopter des mesures à caractère général et abstrait s'appliquant indistinctement à tout prestataire d'une catégorie de ces services, qu'il soit établi ou non dans ce dernier État membre, le principe du contrôle dans l'État membre d'origine serait remis en cause. En effet, ce principe engendre une répartition de la compétence réglementaire entre l'État membre d'origine et l'État membre de destination. Or, autoriser ce dernier État à adopter de telles mesures empièterait sur la compétence réglementaire de l'État membre d'origine et aurait pour effet de soumettre ces prestataires tant à la législation de cet État qu'à celle du ou des États membres de destination. La remise en cause de ce principe porterait atteinte au système et aux objectifs de la directive sur le commerce électronique. Par ailleurs, permettre à l'État membre de destination d'adopter de telles mesures saperait la confiance mutuelle entre les États membres et serait en contradiction avec le principe de reconnaissance mutuelle.

En outre, la Cour indique que la directive sur le commerce électronique vise à supprimer les obstacles juridiques au bon fonctionnement du marché intérieur résidant dans la divergence des législations ainsi que dans l'insécurité juridique des régimes nationaux applicables à ces services. Or, la possibilité d'adopter les mesures susvisées reviendrait in fine à soumettre les prestataires de services concernés à des législations différentes et, partant, à réintroduire les obstacles juridiques à la libre prestation que cette directive vise à supprimer.

Ainsi, la Cour conclut que des mesures générales et abstraites visant une catégorie de services donnés de la société de l'information décrite en des termes généraux et s'appliquant indistinctement à tout prestataire de cette catégorie de services ne relèvent pas de la notion de « mesures prises à l'encontre d'un service donné de la société de l'information » au sens de la directive sur le commerce électronique.

7. TVA

Arrêts du 5 mars 2015, Commission/France (C-479/13, [EU:C:2015:141](#)) et Commission/Luxembourg (C-502/13, [EU:C:2015:143](#))

En France et au Luxembourg, la fourniture de livres électroniques était soumise à un taux réduit de taxe sur la valeur ajoutée (TVA). Ainsi, depuis le 1^{er} janvier 2012, la France

¹⁴⁷ Au sens de l'article 2, sous h), de la directive sur le commerce électronique.

et le Luxembourg appliquaient respectivement un taux de TVA de 5,5 % et de 3 % à la fourniture de livres électroniques (ou numériques).

Les livres électroniques en cause en l'espèce recouvriraient les livres au format électronique fournis à titre onéreux par voie de téléchargement ou de diffusion en flux (streaming) à partir d'un site Internet pour être consultés sur un ordinateur, sur un téléphone intelligent, sur un lecteur de livres électroniques ou sur tout autre système de lecture. La Commission européenne a demandé à la Cour de justice de constater qu'en appliquant un taux réduit de TVA à la fourniture de livres électroniques, la France et le Luxembourg ont manqué aux obligations qui leur incombent en vertu de la directive TVA¹⁴⁸.

La Cour a jugé qu'un État membre qui applique un taux réduit de TVA à la fourniture de livres numériques ou électroniques manque aux obligations qui lui incombent en vertu des articles 96 et 98 de la directive 2006/112/CE et du règlement (UE) n° 282/2011¹⁴⁹.

En effet, il ressort des termes du point 6 de l'annexe III de la directive 2006/112/CE que le taux réduit de TVA est applicable à l'opération qui consiste à fournir un livre se trouvant sur un support physique. Si, certes, le livre électronique nécessite, aux fins d'être lu, un support physique, tel qu'un ordinateur, un tel support n'est cependant pas compris dans la fourniture de livres électroniques. En outre, ainsi qu'il ressort de l'article 98, paragraphe 2, second alinéa, de ladite directive, le législateur de l'Union a décidé d'exclure toute possibilité d'appliquer un taux réduit de TVA aux services fournis par voie électronique. Or, la fourniture de livres électroniques constitue un tel service, dès lors qu'elle ne saurait être considérée comme étant une livraison de biens, au sens de l'article 14, paragraphe 1, de cette directive, à défaut pour les livres électroniques de pouvoir être qualifiés de biens corporels. De même, la fourniture de livres électroniques répond à la définition de services fournis par voie électronique figurant à l'article 7, paragraphe 1, du règlement (UE) n° 282/2011.

Cette interprétation ne saurait être remise en cause par le principe de neutralité fiscale, dès lors que ce principe ne permet pas d'étendre le champ d'application d'un taux réduit de TVA en l'absence d'une disposition non équivoque.

Arrêt du 7 mars 2017 (grande chambre), RPO (C-390/15, [EU:C:2017:174](#))

Conformément à la directive TVA¹⁵⁰, les États membres pouvaient appliquer un taux réduit de TVA aux publications imprimées telles que les livres, les journaux et les périodiques. En revanche, les publications numériques devaient être soumises au taux

¹⁴⁸ Directive 2006/112/CE du Conseil, du 28 novembre 2006, relative au système commun de taxe sur la valeur ajoutée (JO 2006, L 347, p. 1).

¹⁴⁹ Règlement d'exécution (UE) n° 282/2011 du Conseil, du 15 mars 2011, portant mesures d'exécution de la directive 2006/112/CE relative au système commun de taxe sur la valeur ajoutée (JO 2011, L 77, p. 1).

¹⁵⁰ Directive 2006/112/CE du Conseil, du 28 novembre 2006, relative au système commun de taxe sur la valeur ajoutée (JO 2006, L 347, p. 1), dans sa version résultant de la directive 2009/47/CE du Conseil, du 5 mai 2009, modifiant la directive 2006/112/CE en ce qui concerne les taux réduits de taxe sur la valeur ajoutée (JO 2009, L 116, p. 18).

normal de TVA, à l'exception des livres numériques fournis sur un support physique (CD-ROM par exemple). Le Trybunał Konstytucyjny (Cour constitutionnelle, Pologne), saisi par le médiateur polonais, doutait de la validité de cette différence d'imposition. Il a demandé à la Cour de justice, d'une part, si celle-ci est compatible avec le principe d'égalité de traitement et, d'autre part, si le Parlement européen a été suffisamment impliqué dans la procédure législative.

Selon la Cour, l'obligation de consulter le Parlement, au cours de la procédure législative, dans les cas prévus par le traité, implique que celui-ci soit de nouveau consulté à chaque fois que le texte finalement adopté, considéré dans son ensemble, s'écarte, dans sa substance même, de celui sur lequel le Parlement a déjà été consulté, à l'exception des cas où les amendements correspondent, pour l'essentiel, à un souhait exprimé par le Parlement lui-même.

Il y a lieu de constater que le texte du point 6 de l'annexe III de la directive 2006/112/CE modifiée n'est autre qu'une simplification rédactionnelle du texte qui figurait dans la proposition de directive et dont la substance a été entièrement maintenue.

En outre, l'examen des questions préjudiciales n'a révélé aucun élément de nature à affecter la validité du point 6 de l'annexe III de la directive 2006/112/CE ou de l'article 98, paragraphe 2, de cette directive, lu conjointement avec le point 6 de l'annexe III de celle-ci.

Il y a lieu de constater que la fourniture de livres numériques sur tout type de support physique, d'une part, et la fourniture de livres numériques par voie électronique, d'autre part, constituent des situations comparables. Ces dispositions doivent être regardées comme instaurant une différence de traitement entre deux situations pourtant comparables au regard de l'objectif poursuivi par le législateur de l'Union. Lorsqu'une telle différence est constatée, le principe d'égalité de traitement n'est pas violé pour autant que cette différence soit dûment justifiée. Tel est le cas lorsque la différence de traitement est en rapport avec un objectif légalement admissible poursuivi par la mesure ayant pour effet d'instaurer une telle différence et qu'elle est proportionnée à cet objectif.

Dans ce contexte, il est entendu que le législateur de l'Union est appelé, lorsqu'il adopte une mesure de nature fiscale, à procéder à des choix de nature politique, économique ainsi que sociale et à hiérarchiser des intérêts divergents ou à effectuer des appréciations complexes. Par conséquent, il y a lieu de lui reconnaître, dans ce cadre, un large pouvoir d'appréciation, de telle sorte que le contrôle juridictionnel doit se limiter à celui de l'erreur manifeste. Il résulte, en effet, des explications du Conseil et de la Commission qu'il a été jugé nécessaire de soumettre les services fournis par voie électronique à des règles claires, simples et uniformes afin que le taux de TVA applicable à ces services puisse être établi avec certitude et que soit ainsi facilitée la gestion de cette taxe par les assujettis et les administrations fiscales nationales. À cet égard, la possibilité d'appliquer un taux réduit de TVA à la fourniture de livres numériques par

voie électronique reviendrait à porter atteinte à la cohérence d'ensemble de la mesure voulue par le législateur de l'Union.



COUR DE JUSTICE
DE L'UNION EUROPÉENNE

Direction de la recherche et documentation

Juillet 2024