COUR DE JUSTICE
DE L'UNION EUROPÉENNE
DIRECTION DE LA RECHERCHE
ET DOCUMENTATION

Fiche thématique

PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

Le droit à la protection des données à caractère personnel est un droit fondamental dont le respect constitue un objectif important pour l'Union européenne.

Il est consacré par la charte des droits fondamentaux de l'Union européenne (ci-après la « Charte ») qui dispose, en son article 8, que :

« 1. Toute personne a droit à la protection des données à caractère personnel la concernant.

2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.

3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante ».

Ce droit fondamental est en outre étroitement lié au droit au respect de la vie privée et familiale consacré à l'article 7 de la Charte.

Le droit à la protection des données à caractère personnel est également prévu à l'article 16, paragraphe 1, du traité sur le fonctionnement de l'Union européenne (TFUE), qui a succédé à ce propos à l'article 286 CE.

S'agissant du droit dérivé, c'est à partir du milieu des années 90 que la Communauté européenne s'est dotée de différents instruments destinés à garantir la protection des données à caractère personnel. La directive 95/46/CE 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[1], adoptée sur la base de l'article 100 A CE, constituait à cet égard le principal acte juridique de l'Union en la matière. Elle établissait des conditions générales de licéité des traitements de ces données ainsi que les droits des personnes concernées et prévoyait notamment l'établissement d'autorités indépendantes de contrôle dans les États membres.

[1] 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 L 281 du 23.11.1995, p. 31), version consolidée au 20.11.2003, abrogée à partir du 25 mai 2018 (voir note 5).

La directive 2002/58/CE[2] est ensuite venue compléter la directive 95/46/CE, en harmonisant les dispositions de la législation des États membres relatives à la protection du droit à la vie privée, en ce qui concerne notamment le traitement des données à caractère personnel dans le secteur des communications électroniques[3]. Il convient de noter que le législateur de l'Union envisage un réexamen de cette directive. À cet égard, la Commission a introduit, le 10 janvier 2017, une proposition visant à remplacer cette directive par un règlement relatif à la vie privée et aux communications électroniques[4].

En outre, dans le champ de l'espace de liberté, de sécurité et de justice (ex-articles 30 et 31 TUE), la décision-cadre 2008/977/JAI[5] a réglementé, jusqu'au mois de mai 2018, la protection des données à caractère personnel dans les domaines de la coopération judiciaire en matière pénale et policière.

En 2016, l'Union européenne a réformé le cadre juridique global en la matière. À cette fin, elle a adopté le règlement (UE) 2016/679[6] sur la protection des données, qui abroge la directive 95/46/CE et qui est applicable depuis le 25 mai 2018, ainsi que la directive (UE) 2016/680[7] visant la protection desdites données en matière pénale, qui abroge la décision-cadre 2008/977/JAI et dont la date de transposition par les États membres a été fixée au 6 mai 2018.

Enfin, dans le cadre de leur traitement par les institutions et organes de l'UE, la protection des données à caractère personnel était, dans un premier temps, assurée par le règlement (CE) nº 45/2001[8]. Ce règlement a notamment permis la création, en 2004, du Contrôleur européen de la protection des données. En 2018, l'Union européenne s'est dotée d'un nouveau cadre juridique en la matière, notamment par l'adoption du règlement (UE) 2018/1725[9], qui abroge le règlement nºº45/2001 et la décision nºº1247/2002/CE[10] et qui est applicable depuis le

---

2 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 L 201 du 31.7.2002, p. 37), version consolidée au 19.12.2009.

3 La directive 2002/58/CE a été modifiée par 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 L 105 du 13.4.2006, p. 54). Cette directive a été invalidée par la Cour, dans l'arrêt du 8 avril 2014, Digital Rights Ireland et Seitlinger e.a. (C-293/12 et C-594/12, EU:C:2014:238), au motif qu'elle portait une atteinte grave aux droits au respect de la vie privée et à la protection des données à caractère personnel (voir rubrique I.1., intitulée « Conformité du droit dérivé de l'Union au droit à la protection des données à caractère personnel » de la présente fiche).

4 Proposition de règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement « vie privée et communications électroniques »), COM/2017/010 final - 2017/03 (COD).

5 Décision-cadre 2008/977/JAI du Conseil, du 27 novembre 2008, relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale (JO L 350 du 30.12.2008, p. 60), abrogée à compter du 6 mai 2018 (voir note 6).

6 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 L 119 du 4.5.2016, p. 1).

7 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 L 119 du 4.5.2016, p. 89).

8 Règlement (CE) nº 45/2001 du Parlement européen et du Conseil, du 18 décembre 2000, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données (JO L 8 du 12.1.2001, p. 1).

9 Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nºº45/2001 et la décision nºº1247/2002/CE.

10 Décision nºº1247/2002/CE du Parlement européen, du Conseil et de la Commission du 1er juillet 2002 relative au statut et aux conditions générales d'exercice des fonctions de Contrôleur européen de la protection des données (JO L 183 du 12.7.2002, p. 1).

11 décembre 2018. Dans l'intérêt d'une approche cohérente de la protection des données à caractère personnel dans l'ensemble de l'Union, ce nouveau règlement vise à aligner autant que possible les règles en la matière sur le régime établi par le règlement (UE) 2016/679.

I. Le droit à la protection des données à caractère personnel reconnu par la charte des droits fondamentaux de l'Union européenne

1. Conformité du droit dérivé de l'Union au droit à la protection des données à caractère personnel

Arrêt du 9 novembre 2010 (grande chambre), Volker und Markus Schecke et Eifert (C-92/09 et C-93/09, EU:C:2010:662)[11]

Dans cette affaire, les litiges au principal opposaient des exploitants agricoles au Land Hessen, au sujet de la publication sur le site Internet de la Bundesanstalt für Landwirtschaft und Ernährung (l'Office fédéral pour l'agriculture et l'alimentation) des données à caractère personnel les concernant en tant que bénéficiaires de fonds provenant du Fonds européen agricole de garantie (FEAGA) et du Fonds européen agricole pour le développement rural (Feader). Lesdits exploitants s'opposaient à cette publication en faisant valoir, en particulier, que celle-ci n'était pas justifiée par un intérêt public prépondérant. Le Land Hessen considérait quant à lui que la publication desdites données découlait des règlements (CE) n^{os} 1290/2005[12] et 259/2008[13], encadrant le financement de la politique agricole commune et imposant une publication d'informations relatives aux personnes physiques bénéficiaires du FEAGA et du Feader.

C'est dans ce contexte que le Verwaltungsgericht Wiesbaden (tribunal administratif de Wiesbaden, Allemagne) a posé à la Cour plusieurs questions portant sur la validité de certaines dispositions du règlement (CE) n° 1290/2005 et sur celle du règlement (CE) n° 259/2008, lesquels imposent la mise à la disposition du public de telles informations, notamment par le biais de sites Internet exploités par les offices nationaux.

La Cour a relevé, s'agissant de l'adéquation entre le droit à la protection des données à caractère personnel reconnu par la Charte et l'obligation de transparence en matière de fonds européens, que la publication sur un site Internet des données nominatives relatives aux

[11] Cet arrêt a été présenté dans le Rapport annuel 2010, p. 11.

[12] Règlement (CE) n° 1290/2005 du Conseil, du 21 juin 2005, relatif au financement de la politique agricole commune (JO L 209 du 11.8.2005, p. 1), abrogé par le règlement (UE) n° 1306/2013 du Parlement européen et du Conseil, du 17 décembre 2013, relatif au financement, à la gestion et au suivi de la politique agricole commune (JO L 347 du 20.12.2013, p. 549).

[13] Règlement (CE) n° 259/2008 de la Commission, du 18 mars 2008, portant modalités d'application du règlement (CE) n° 1290/2005 du Conseil en ce qui concerne la publication des informations relatives aux bénéficiaires de fonds en provenance du FEAGA et du Feader (JO L 76 du 19.3.2008, p. 28), abrogé par le règlement d'exécution (UE) n° 908/2014 de la Commission, du 6 août 2014, portant modalités d'application du règlement (UE) n° 1306/2013 du Parlement européen et du Conseil en ce qui concerne les organismes payeurs et autres entités, la gestion financière, l'apurement des comptes, les règles relatives aux contrôles, les garanties et la transparence (JO L 255 du 28.8.2014, p. 59).

bénéficiaires des fonds et aux montants perçus par ceux-ci constitue, en raison du libre accès par les tiers au site, une atteinte au droit des bénéficiaires concernés au respect de leur vie privée, en général, et à la protection de leurs données à caractère personnel, en particulier (points 56-64).

Pour être justifiée, une telle atteinte doit être prévue par la loi, respecter le contenu essentiel desdits droits et, en application du principe de proportionnalité, être nécessaire et répondre effectivement à des objectifs d'intérêt général reconnus par l'Union, les dérogations et limitations à ces droits devant s'opérer dans les limites du strict nécessaire (point 65). Dans ce contexte, la Cour a estimé que, si, dans une société démocratique, les contribuables ont le droit d'être tenus informés de l'utilisation des fonds publics, il n'en demeure pas moins que le Conseil et la Commission étaient tenus d'effectuer une pondération équilibrée des différents intérêts en cause, ce qui nécessitait, avant l'adoption des dispositions contestées, de vérifier si la publication de ces données au moyen d'un site Internet unique par l'État membre n'allait pas au-delà de ce qui était nécessaire à la réalisation des objectifs légitimes poursuivis (points 77, 79, 85, 86).

Ainsi, la Cour a déclaré invalides certaines dispositions du règlement (CE) nº 1290/2005, ainsi que le règlement (CE) nº 259/2008 dans son ensemble, dans la mesure où, s'agissant des personnes physiques bénéficiaires d'aides du FEAGA et du Feader, ces dispositions imposent la publication de données à caractère personnel relatives à tout bénéficiaire, sans opérer de distinction selon des critères pertinents, tels que les périodes pendant lesquelles elles ont perçu de telles aides, la fréquence ou encore le type et l'importance de celles-ci (point 92, disp. 1). Toutefois, la Cour n'a pas remis en cause les effets de la publication des listes des bénéficiaires de telles aides, effectuée par les autorités nationales pendant la période antérieure à la date du prononcé de l'arrêt (point 94, disp. 2).

Arrêt du 17 octobre 2013, Schwarz (C-291/12, EU:C:2013:670)

M. Schwarz avait sollicité la délivrance d'un passeport auprès de la ville de Bochum (Allemagne), tout en refusant que soient relevées, à cette occasion, ses empreintes digitales. La ville ayant rejeté sa demande, M. Schwarz avait introduit un recours devant le Verwaltungsgericht Gelsenkirchen (tribunal administratif de Gelsenkirchen, Allemagne) pour qu'il soit enjoint à cette commune de lui délivrer un passeport sans relever ses empreintes digitales. Devant cette juridiction, M. Schwarz contestait la validité du règlement (CE) nº 2252/2004[14] qui a introduit l'obligation de relever les empreintes digitales de demandeurs de passeports, en faisant, entre autres, valoir que ce règlement méconnaissait le droit à la protection des données à caractère personnel et le droit au respect de la vie privée.

Dans ce contexte, le Verwaltungsgericht Gelsenkirchen a saisi la Cour à titre préjudiciel afin de savoir si ledit règlement, pour autant qu'il oblige le demandeur d'un passeport à donner ses empreintes digitales et prévoit leur conservation dans le passeport, est valide, notamment au regard de la Charte.

[14] Règlement (CE) nº 2252/2004 du Conseil, du 13 décembre 2004, établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres (JO L 385 du 29.12.2004, p. 1), tel que modifié par le règlement (CE) nº 444/2009 du Parlement européen et du Conseil, du 6 mai 2009 (JO L 142 du 6.6.2009, p. 1).

La Cour a répondu par l'affirmative, en jugeant que, si le prélèvement et la conservation d'empreintes digitales par les autorités nationales, régis par l'article 1er, paragraphe 2, du règlement (CE) nº 2252/2004, constituent une atteinte aux droits au respect de la vie privée et à la protection des données à caractère personnel, cette atteinte est justifiée par le but de protéger les passeports contre toute utilisation frauduleuse.

Tout d'abord, une telle limitation, prévue par la loi, poursuit un objectif d'intérêt général reconnu par l'Union, dans la mesure où elle vise à empêcher, notamment, l'entrée illégale de personnes sur le territoire de l'Union (points 35 à 38). Ensuite, le prélèvement et la conservation des empreintes digitales sont aptes à atteindre cet objectif. En effet, d'une part, bien que la méthode de vérification d'identité au moyen des empreintes digitales ne soit pas totalement fiable, elle réduit considérablement le risque d'acceptation de personnes non autorisées. D'autre part, le défaut de concordance des empreintes digitales du détenteur du passeport avec les données intégrées dans ce document ne signifie pas que la personne concernée se voit automatiquement refuser l'entrée sur le territoire de l'Union, mais aura pour seule conséquence d'entraîner un contrôle approfondi destiné à établir d'une manière définitive l'identité de ladite personne (points 42 à 45).

Enfin, quant au caractère nécessaire d'un tel traitement, il n'a pas été porté à la connaissance de la Cour l'existence de mesures suffisamment efficaces, mais moins attentatoires aux droits reconnus par les articles 7 et 8 de la Charte que celles entraînées par la méthode fondée sur les empreintes digitales (point 53). L'article 1er, paragraphe 2, du règlement (CE) nº 2252/2004 n'implique pas de traitements des empreintes digitales prélevées qui iraient au-delà de ce qui est nécessaire pour la réalisation du but visé. En effet, ledit règlement précise expressément que les empreintes digitales ne peuvent être utilisées que dans le seul but de vérifier l'authenticité du passeport et l'identité de son titulaire. De surcroît, l'article 1er, paragraphe 2, du règlement assure une protection contre le risque de lecture des données contenant des empreintes digitales par des personnes non autorisées et ne prévoit la conservation des empreintes digitales qu'au sein même du passeport, lequel demeure la possession exclusive de son titulaire (points 54 à 57, 60 et 63).

Arrêt du 8 avril 2014 (grande chambre), Digital Rights Ireland et Seitlinger e.a. (affaires jointes C-293/12 et C-594/12, EU:C:2014:238)[15]

Le présent arrêt trouve son origine dans des demandes en appréciation de la validité de la directive 2006/24/CE sur la conservation des données, à l'égard des droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel, soulevées dans le cadre de litiges nationaux devant les juridictions irlandaise et autrichienne. Dans l'affaire C-293/12, la High Court (Haute Cour, Irlande) était saisie d'un litige opposant la société Digital Rights aux autorités irlandaises au sujet de la légalité de mesures nationales portant sur la conservation de données relatives aux communications électroniques. Dans l'affaire C-594/12, le Verfassungsgerichtshof (Cour constitutionnelle, Autriche) était saisi de plusieurs recours en matière constitutionnelle demandant l'annulation de la disposition nationale transposant la directive 2006/24/CE en droit autrichien.

[15] Cet arrêt a été présenté dans le Rapport annuel 2014, p. 60.

Par leurs demandes de décisions préjudicielles, les juridictions irlandaise et autrichienne ont interrogé la Cour sur la validité de la directive 2006/24/CE au regard des articles 7, 8 et 11 de la Charte. Plus précisément, lesdites juridictions ont demandé à la Cour si l'obligation incombant, en vertu de ladite directive, aux fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communication, de conserver pendant une certaine durée des données relatives à la vie privée d'une personne et à ses communications et d'en permettre l'accès aux autorités nationales compétentes, comportait une ingérence injustifiée dans lesdits droits fondamentaux. Les types de données concernées sont, notamment, les données nécessaires pour retrouver et identifier la source d'une communication et la destination de celle-ci, pour déterminer la date, l'heure, la durée et le type d'une communication, le matériel de communication des utilisateurs, ainsi que pour localiser le matériel de communication mobile, données au nombre desquelles figurent, notamment, le nom et l'adresse de l'abonné ou de l'utilisateur inscrit, le numéro de téléphone de l'appelant et le numéro appelé ainsi qu'une adresse IP pour les services Internet. Ces données permettent, notamment, de savoir quelle est la personne avec laquelle un abonné ou un utilisateur inscrit a communiqué et par quel moyen, tout comme de déterminer le temps de la communication ainsi que l'endroit à partir duquel celle-ci a eu lieu. En outre, elles permettent de connaître la fréquence des communications de l'abonné ou de l'utilisateur inscrit avec certaines personnes pendant une période donnée.

La Cour a tout d'abord jugé que, en imposant de telles obligations à ces fournisseurs, les dispositions de la directive 2006/24/CE étaient constitutives d'une ingérence particulièrement grave dans le respect des droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel, garantis par les articles 7 et 8 de la Charte. Dans ce contexte, la Cour a certes constaté que cette ingérence était susceptible d'être justifiée par la poursuite d'un objectif d'intérêt général, tel que la lutte contre la criminalité organisée. À cet égard, la Cour a relevé, en premier lieu, que la conservation des données imposée par la directive n'était pas de nature à porter atteinte au contenu essentiel des droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel, dans la mesure où elle ne permettait pas de prendre connaissance du contenu des communications électroniques en tant que tel et prévoit que les fournisseurs de services ou de réseaux doivent respecter certains principes de protection et de sécurité des données. En second lieu, la Cour a observé que la conservation des données en vue de leur transmission éventuelle aux autorités nationales compétentes répondait effectivement à un objectif d'intérêt général, à savoir la lutte contre la criminalité grave ainsi que, en définitive, la sécurité publique (points 38-44).

Toutefois, la Cour a estimé qu'en adoptant la directive sur la conservation des données, le législateur de l'Union avait excédé les limites qu'impose le respect du principe de proportionnalité. Partant, elle a déclaré la directive invalide en considérant que l'ingérence d'une vaste ampleur et d'une gravité particulière dans les droits fondamentaux qu'elle comportait, n'était pas suffisamment encadrée afin de garantir que cette ingérence soit limitée au strict nécessaire (point 65). La directive 2006/24/CE couvrait en effet de manière généralisée toute personne et tous les moyens de communication électronique ainsi que l'ensemble des données relatives au trafic sans qu'aucune différenciation, limitation ou exception ne soit opérée en fonction de l'objectif de lutte contre les infractions graves (points 57-59). La directive ne prévoyait par ailleurs aucun critère objectif permettant de garantir que les autorités nationales compétentes n'aient accès aux données et ne puissent les utiliser qu'aux seules fins de prévenir, détecter ou poursuivre pénalement des infractions susceptibles d'être considérées comme

suffisamment graves pour justifier une telle ingérence, ni les conditions matérielles et procédurales d'un tel accès ou d'une telle utilisation (points 60-62). S'agissant enfin de la durée de conservation des données, la directive imposait une durée d'au moins six mois sans opérer une quelconque distinction entre les catégories de données en fonction des personnes concernées ou de l'utilité éventuelle des données par rapport à l'objectif poursuivi (points 63, 64).

Par ailleurs, en ce qui concerne les exigences découlant de l'article 8, paragraphe 3, de la Charte, la Cour a constaté que la directive 2006/24/CE ne prévoyait pas de garanties suffisantes permettant d'assurer une protection efficace des données contre les risques d'abus ainsi que contre l'accès et l'utilisation illicites des données, et n'imposait pas non plus une conservation des données sur le territoire de l'Union.

Par conséquent, ladite directive ne garantissait pas pleinement le contrôle du respect des exigences de protection et de sécurité par une autorité indépendante, comme cela est pourtant explicitement requis par la Charte (points 66-68).

2. Respect du droit à la protection des données à caractère personnel dans la mise en œuvre du droit de l'Union

Arrêt du 21 décembre 2016 (grande chambre), Tele2 Sverige (affaires jointes C-203/15 et C-698/15, EU:C:2016:970)[16]

À la suite de l'arrêt Digital Rights Ireland et Seitlinger e.a. ayant déclaré invalide la directive 2006/24/CE (voir supra), la Cour a été saisie de deux affaires portant sur l'obligation générale imposée, en Suède et au Royaume-Uni, aux fournisseurs de services de communications électroniques de conserver les données relatives à ces communications, dont la conservation était prévue par la directive invalidée.

Le lendemain du prononcé de l'arrêt Digital Rights Ireland et Seitlinger e.a., l'entreprise de télécommunications Tele2 Sverige a notifié à l'autorité suédoise de surveillance des postes et télécommunications sa décision de cesser de procéder à la conservation des données ainsi que son intention d'effacer les données déjà enregistrées (affaire C-203/15). Le droit suédois obligeait en effet les fournisseurs de services de communications électroniques à conserver de manière systématique et continue, et ce sans aucune exception, l'ensemble des données relatives au trafic et des données de localisation de tous leurs abonnés et utilisateurs inscrits, concernant tous les moyens de communication électronique. Dans l'affaire C-698/15, trois personnes avaient introduit des recours contre le régime britannique de conservation des données qui permettait au ministre de l'Intérieur d'obliger les opérateurs de télécommunications publiques à conserver toutes les données relatives à des communications pour une durée maximale de douze mois, la conservation du contenu de ces communications étant toutefois exclue.

[16] Cet arrêt a été présenté dans le Rapport annuel 2016, p. 62.

Saisie par le Kammarrätten i Stockholm (cour administrative d'appel de Stockholm, Suède) et la Court of Appeal [(England and Wales) (Civil Division) (chambre civile de la cour d'appel d'Angleterre et du pays de Galles, Royaume-Uni)], la Cour était invitée à se prononcer sur l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58/CE, dite « Vie privée et communications électroniques », qui permet aux États membres d'introduire certaines exceptions à l'obligation, énoncée dans cette directive, d'assurer la confidentialité des communications électroniques et des données relatives au trafic y afférentes.

Dans son arrêt, la Cour a tout d'abord jugé que l'article 15, paragraphe 1, de la directive 2002/58/CE, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, s'oppose à une réglementation nationale, telle que celle de la Suède, prévoyant, à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et aux données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique. Selon la Cour, une telle réglementation excède les limites du strict nécessaire et ne saurait être considérée comme étant justifiée, dans une société démocratique, ainsi que l'exige ledit article 15, paragraphe 1, lu à la lumière des articles précités de la Charte (points 99-105, 107, 112, disp. 1).

Cette même disposition, lue à la lumière des mêmes articles de la Charte, s'oppose également à une réglementation nationale régissant la protection et la sécurité des données relatives au trafic et des données de localisation, en particulier l'accès des autorités nationales compétentes aux données conservées, sans limiter, dans le cadre de la lutte contre la criminalité, cet accès aux seules fins de lutte contre la criminalité grave, sans soumettre ledit accès à un contrôle préalable par une juridiction ou une autorité administrative indépendante, et sans exiger que les données en cause soient conservées sur le territoire de l'Union (points 118-122, 125, disp. 2).

La Cour a, en revanche, considéré que l'article 15, paragraphe 1, de la directive 2002/58/CE ne s'oppose pas à une réglementation qui permet, à titre préventif, à des fins de lutte contre la criminalité grave, la conservation ciblée de données de cette nature, à condition que cette conservation soit limitée au strict nécessaire en ce qui concerne les catégories de données visées, les moyens de communication visés, les personnes concernées ainsi que la durée de conservation retenue. Pour satisfaire à ces exigences, cette réglementation nationale doit, en premier lieu, prévoir des règles claires et précises permettant de protéger efficacement les données contre les risques d'abus. Elle doit en particulier indiquer les circonstances et conditions dans lesquelles une mesure de conservation des données peut, à titre préventif, être prise, garantissant ainsi qu'une telle mesure soit limitée au strict nécessaire. En second lieu, s'agissant des conditions matérielles auxquelles doit satisfaire la réglementation nationale, afin de garantir que celle-ci soit limitée au strict nécessaire, la conservation des données doit toujours répondre à des critères objectifs, établissant un rapport entre les données à conserver et l'objectif poursuivi. En particulier, de telles conditions doivent s'avérer, en pratique, de nature à délimiter effectivement l'ampleur de la mesure et, par suite, le public concerné. S'agissant de cette délimitation, la réglementation nationale doit être fondée sur des éléments objectifs permettant de viser un public dont les données sont susceptibles de révéler un lien, au moins indirect, avec des actes de criminalité grave, de contribuer d'une manière ou d'une autre à la lutte contre la criminalité grave ou de prévenir un risque grave pour la sécurité publique (points 108-111).

II. Le traitement des données à caractère personnel au sens de la directive nº 95/46/CE

1. Traitements de données à caractère personnel exclus du champ d'application de la directive nº 95/46/CE

Arrêt du 30 mai 2006 (grande chambre), Parlement/Conseil (C-317/04 et C-318/04, EU:C:2006:346)

À la suite des attaques terroristes du 11 septembre 2001, les États-Unis avaient adopté une législation disposant que les transporteurs aériens assurant des liaisons à destination, au départ ou à travers le territoire des États-Unis étaient tenus de fournir aux autorités américaines un accès électronique aux données contenues dans leurs systèmes de réservation et de contrôle des départs, dénommées Passenger Name Records (PNR).

Estimant que ces dispositions pouvaient entrer en conflit avec la législation européenne et celle des États membres en matière de protection des données, la Commission avait entamé des négociations avec les autorités américaines. À l'issue de ces négociations, la Commission avait adopté, le 14 mai 2004, la décision 2004/535/CE[17] constatant que le Bureau des douanes et de la protection des frontières des États-Unis (United States Bureau of Customs and Border Protection, ci-après le « CBP ») assure un niveau de protection adéquat des données PNR transférées depuis la Communauté (ci-après la « décision d'adéquation »). Ensuite, le Conseil avait, le 17 mai 2004, adopté la décision 2004/496/CE[18] approuvant la conclusion d'un accord entre la Communauté européenne et les États-Unis sur le traitement et le transfert au CBP de données PNR par des transporteurs aériens établis sur le territoire des États membres de la Communauté.

Le Parlement européen a demandé à la Cour d'annuler les deux décisions susvisées en faisant valoir, notamment, que la décision d'adéquation avait été adoptée ultra vires, que l'article 95 CE (devenu article 114 TFUE) ne constituait pas une base juridique appropriée pour la décision approuvant la conclusion de l'accord et, dans les deux cas, qu'il y avait une violation des droits fondamentaux.

En ce qui concerne la décision d'adéquation, la Cour a examiné, tout d'abord, si la Commission pouvait valablement adopter sa décision sur le fondement de la directive 95/46/CE. Dans ce contexte, elle a constaté qu'il ressortait de la décision d'adéquation que le transfert des données PNR au CBP constitue un traitement ayant pour objet la sécurité publique et les activités de l'État relatives à des domaines du droit pénal. Selon la Cour, si les données PNR étaient initialement collectées par les compagnies aériennes dans le cadre d'une activité qui relève du

[17] Décision 2004/535/CE de la Commission, du 14 mai 2004, relative au niveau de protection adéquat des données à caractère personnel contenues dans les dossiers des passagers aériens transférés au Bureau des douanes et de la protection des frontières des États-Unis d'Amérique (JO L 235 du 6.7.2004, p. 11).

[18] Décision 2004/496/CE du Conseil, du 17 mai 2004, concernant la conclusion d'un accord entre la Communauté européenne et les États-Unis d'Amérique sur le traitement et le transfert de données PNR par des transporteurs aériens au bureau des douanes et de la protection des frontières du ministère américain de la sécurité intérieure (JO L 183 du 20.5.2004, p. 83, et rectificatif JO L 255 du 30.9.2005, p. 168).

droit de l'Union, à savoir la vente d'un billet d'avion qui donnait droit à une prestation de services, le traitement des données qui était pris en compte dans la décision d'adéquation possédait une tout autre nature. En effet, cette décision ne visait pas un traitement de données nécessaire à la réalisation d'une prestation de services, mais un traitement de données considéré comme nécessaire pour sauvegarder la sécurité publique et à des fins répressives (points 56, 57).

À cet égard, la Cour a relevé que le fait que les données PNR avaient été collectées par des opérateurs privés à des fins commerciales et que c'étaient ces derniers qui organisaient leur transfert vers un États tiers ne s'opposait pas à ce que ce transfert fût considéré comme un traitement de données exclu du champ d'application de la directive. En effet, ce transfert s'insérait dans un cadre institué par les pouvoirs publics et visant la sécurité publique. Par conséquent, la Cour a conclu que la décision d'adéquation ne relevait pas du champ d'application de la directive, car elle concernait un traitement de données à caractère personnel qui en est exclu. La Cour a, en conséquence, annulé la décision d'adéquation (points 58, 59).

S'agissant de la décision du Conseil, la Cour a constaté que l'article 95 CE, lu en combinaison avec l'article 25 de la directive 95/46/CE, n'est pas susceptible de fonder la compétence de la Communauté pour conclure l'accord en cause avec les États-Unis. En effet, cet accord visait le même transfert de données que la décision d'adéquation et donc des traitements de données qui étaient exclus du champ d'application de la directive. Par conséquent, la Cour a annulé la décision du Conseil approuvant la conclusion de l'accord (points 67-69).

Arrêt du 11 décembre 2014, Ryneš (C-212/13, EU:C:2014:2428)

En réponse à des agressions répétées, M. Ryneš avait installé sur sa maison une caméra de surveillance. À la suite d'une nouvelle attaque visant sa maison, les enregistrements de ladite caméra avaient permis d'identifier deux suspects, à l'encontre desquels des procédures pénales avaient été engagées. La légalité du traitement des données enregistrées par la caméra de surveillance ayant été contestée par l'un des suspects devant l'Office tchèque pour la protection des données à caractère personnel, ce dernier avait constaté que M. Ryneš avait violé les règles en matière de protection des données à caractère personnel et avait infligé une amende à ce dernier.

Saisi d'un pourvoi formé par M. Ryneš à l'encontre d'une décision du Městský soud v Praze (cour municipale de Prague, République tchèque) qui avait confirmé la décision de l'Office, le Nejvyšší správní soud (Cour suprême administrative) a demandé à la Cour si l'enregistrement réalisé par M. Ryneš en vue de protéger sa vie, sa santé et ses biens constituait un traitement de données non couvert par la directive 95/46/CE, au motif que cet enregistrement avait été effectué par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques, au sens de l'article 3, paragraphe 2, second tiret de ladite directive.

La Cour a jugé que l'exploitation d'un système de caméra, donnant lieu à un enregistrement vidéo de personnes stocké dans un dispositif d'enregistrement continu tel qu'un disque dur, installé par une personne physique sur sa maison familiale afin de protéger les biens, la santé et la vie des propriétaires de la maison, ce système surveillant également l'espace public, ne

constitue pas un traitement de données effectué pour l'exercice d'activités exclusivement personnelles ou domestiques (point 35 et disp.).

À cet égard, elle a rappelé que la protection du droit fondamental à la vie privée, garanti par l'article 7 de la Charte, exige que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci s'opèrent dans les limites du strict nécessaire. Dans la mesure où les dispositions de la directive 95/46/CE, en ce qu'elles régissent le traitement de données à caractère personnel susceptible de porter atteinte aux libertés fondamentales et, en particulier, au droit à la vie privée, doivent nécessairement être interprétées à la lumière des droits fondamentaux qui sont inscrits dans ladite Charte, la dérogation prévue à l'article 3, paragraphe 2, second tiret, de cette directive doit recevoir une interprétation stricte (points 27-29). De plus, le libellé même de cette disposition soustrait à l'application de la directive 95/46/CE le traitement des données effectué pour l'exercice d'activités « exclusivement » personnelles ou domestiques. Or, dans la mesure où une vidéosurveillance s'étend, même partiellement, à l'espace public et, de ce fait, est dirigée vers l'extérieur de la sphère privée de celui qui procède au traitement des données par ce moyen, elle ne saurait être considérée comme une activité exclusivement « personnelle ou domestique », au sens de ladite disposition (points 30, 31, 33).

2. Notion de « données à caractère personnel »

Arrêt du 19 octobre 2016, Breyer (C-582/14, EU:C:2016:779)[19]

M. Breyer avait introduit, devant les juridictions civiles allemandes, un recours visant à ce qu'il fût fait interdiction à la République fédérale d'Allemagne de conserver ou de faire conserver par des tiers des données informatiques qui étaient transmises au terme de chaque consultation des sites Internet des services fédéraux allemands. En effet, afin de se prémunir contre les attaques et de rendre possibles les poursuites pénales contre les « pirates », le fournisseur de services de médias en ligne des services fédéraux allemands enregistrait des données consistant en une adresse IP « dynamique » – une adresse IP qui change à l'occasion de chaque nouvelle connexion à Internet –, ainsi qu'en la date et l'heure de la session de consultation du site. À la différence des adresses IP statiques, les adresses IP dynamiques ne permettaient pas, a priori, de faire le lien, au moyen de fichiers accessibles au public, entre un ordinateur donné et le branchement physique au réseau utilisé par le fournisseur d'accès à Internet. Les données enregistrées n'offraient pas, à elles seules, au fournisseur de services de médias en ligne la possibilité d'identifier l'utilisateur. En revanche, le fournisseur d'accès à Internet disposait, quant à lui, d'informations supplémentaires qui, si elles étaient combinées avec cette adresse IP, permettraient d'identifier ledit utilisateur.

Dans ce contexte, le Bundesgerichtshof (Cour fédérale de justice, Allemagne), saisi d'un recours en « Revision », a interrogé la Cour sur le point de savoir si une adresse IP qui est enregistrée par un fournisseur de services de médias en ligne à l'occasion d'un accès à son site Internet constitue pour celui-ci une donnée à caractère personnel.

[19] Cet arrêt a été présenté dans le Rapport annuel 2016, p. 61.

La Cour a tout d'abord relevé que pour qu'une donnée puisse être qualifiée de « donnée à caractère personnel » au sens de l'article 2, sous a), de la directive 95/46/CE, il n'est pas exigé que toutes les informations permettant d'identifier la personne concernée se trouvent entre les mains d'une seule personne. Le fait que les informations supplémentaires nécessaires pour identifier l'utilisateur d'un site Internet soient détenues non pas par le fournisseur de services de médias en ligne, mais par le fournisseur d'accès à Internet de cet utilisateur, n'apparaît ainsi pas de nature à exclure que les adresses IP dynamiques enregistrées par le fournisseur de services de médias en ligne constituent, pour celui-ci, des données à caractère personnel au sens de l'article 2, sous a), de la directive 95/46/CE (points 43, 44).

Par conséquent, la Cour a constaté qu'une adresse IP dynamique, enregistrée par un fournisseur de services de médias en ligne à l'occasion de la consultation par une personne d'un site Internet que ce fournisseur rend accessible au public, constitue, à l'égard dudit fournisseur, une donnée à caractère personnel au sens de l'article 2, sous a), de la directive 95/46/CE, lorsqu'il dispose de moyens légaux lui permettant de faire identifier la personne concernée grâce aux informations supplémentaires de cette personne dont dispose le fournisseur d'accès à Internet de cette personne (point 49, disp. 1).

Arrêt du 20 décembre 2017, Nowak (C-434/16, ECLI:EU:C:2017:582)

M. Nowak, un expert-comptable stagiaire, avait échoué à l'examen organisé par l'ordre irlandais des experts-comptables. Il avait présenté une demande d'accès, au titre de l'article 4 de la loi sur la protection des données, visant l'ensemble des données à caractère personnel le concernant, détenues par l'ordre des experts-comptables. Ce dernier avait communiqué à M. Nowak certains documents mais avait refusé de lui transmettre sa copie d'examen, au motif que celle-ci ne contenait pas de données à caractère personnel le concernant, au sens de la loi sur la protection des données.

Le commissaire à la protection des données n'ayant pas non plus donné suite à sa demande d'accès pour les mêmes motifs, M. Nowak s'est adressé aux juridictions nationales. La Supreme Court (Cour suprême, Irlande), saisie d'un pourvoi formé par M. Nowak, a interrogé la Cour sur la question de savoir si l'article 2, sous a), de la directive 95/46/CE doit être interprété en ce sens que, dans des conditions telles que celles en cause au principal, les réponses écrites fournies par un candidat lors d'un examen professionnel et les éventuelles annotations de l'examinateur s'y rapportant constituent des données à caractère personnel concernant le candidat, au sens de cette disposition.

En premier lieu, la Cour a relevé que, pour qu'une donnée puisse être qualifiée de « donnée à caractère personnel », au sens de l'article 2, sous a), de la directive 95/46/CE, il n'est pas requis que toutes les informations permettant d'identifier la personne concernée se trouvent entre les mains d'une seule personne. Par ailleurs, dans l'hypothèse où l'examinateur ne connaît pas l'identité du candidat lors de la notation des réponses fournies par celui-ci dans le cadre d'un examen, l'entité organisant l'examen, en l'occurrence l'ordre des experts-comptables, dispose, en revanche, des informations nécessaires lui permettant d'identifier sans difficultés ou doutes ce candidat à partir de son numéro d'identification, apposé sur la copie d'examen ou le feuillet de couverture de cette copie, et ainsi de lui attribuer ses réponses.

En deuxième lieu, la Cour a constaté que les réponses écrites fournies par un candidat à un examen professionnel constituent des informations liées à sa personne. En effet, le contenu de ces réponses reflète le niveau de connaissance et de compétence du candidat dans un domaine donné ainsi que, le cas échéant, ses processus de réflexion, son jugement et son esprit critique. En outre, la collecte desdites réponses a pour finalité d'évaluer les capacités professionnelles du candidat et son aptitude à exercer le métier en cause. De plus, l'utilisation de ces informations, qui se traduit, notamment, par le succès ou l'échec du candidat à l'examen concerné, est susceptible d'avoir un effet sur les droits et intérêts de celui-ci, en ce qu'elle peut déterminer ou influencer, par exemple, ses chances d'accéder à la profession ou à l'emploi souhaités. La constatation que les réponses écrites fournies par un candidat à un examen professionnel constituent des informations qui concernent ce candidat en raison de leur contenu, de leur finalité et de leur effet vaut, par ailleurs, également lorsqu'il s'agit d'un examen à livre ouvert.

En troisième lieu, s'agissant des annotations de l'examinateur relatives aux réponses du candidat, la Cour a considéré que celles-ci constituent, tout comme les réponses fournies par le candidat lors de l'examen, des informations concernant ce candidat, étant donné qu'elles reflètent l'avis ou l'appréciation de l'examinateur sur les performances individuelles du candidat lors de l'examen, et notamment sur ses connaissances et ses compétences dans le domaine concerné. Lesdites annotations ont, par ailleurs, précisément pour finalité de documenter l'évaluation par l'examinateur des performances du candidat et sont susceptibles d'avoir des effets pour ce dernier.

En quatrième lieu, la Cour a jugé que les réponses écrites fournies par un candidat lors d'un examen professionnel et les éventuelles annotations de l'examinateur s'y rapportant sont susceptibles d'être soumises à une vérification, notamment, de leur exactitude et de la nécessité de leur conservation, au sens de l'article 6, paragraphe 1, sous d) et e), de la directive 95/46/CE, et peuvent faire l'objet d'une rectification ou d'un effacement, au titre de l'article 12, sous b), de celle-ci. Le fait de donner au candidat un droit d'accès à ces réponses et à ces annotations, en vertu de l'article 12, sous a), de cette directive, sert l'objectif de cette dernière consistant à garantir la protection du droit à la vie privée de ce candidat à l'égard du traitement des données le concernant, et ce indépendamment du point de savoir si ledit candidat dispose ou non d'un tel droit d'accès également en vertu de la réglementation nationale applicable à la procédure d'examen. Cependant, la Cour a souligné que les droits d'accès et de rectification, au titre de l'article 12, sous a) et b), de la directive 95/46/CE, ne s'étendent pas aux questions d'examen, lesquelles ne constituent pas en tant que telles des données à caractère personnel du candidat.

Au vu de ces éléments, la Cour a conclu que, dans des conditions telles que celles en cause au principal, les réponses écrites fournies par un candidat lors d'un examen professionnel et les éventuelles annotations de l'examinateur relatives à ces réponses constituent des données à caractère personnel, au sens de l'article 2, sous a), de la directive 95/46/CE.

3. Notion de « traitement de données à caractère personnel »

Arrêt du 6 novembre 2003 (grande chambre), Lindqvist (C-101/01, EU:C:2003:596)

M^me^ Lindqvist, travailleuse bénévole dans une paroisse de l'Église protestante en Suède, avait créé, depuis son ordinateur personnel, des pages Internet en y publiant des données à

caractère personnel concernant plusieurs personnes qui travaillaient, comme elle, à titre bénévole au sein de ladite paroisse. M^me^ Lindqvist a été condamnée au paiement d'une amende, au motif qu'elle avait utilisé des données personnelles dans le cadre d'un traitement automatisé sans réaliser de déclaration écrite préalable auprès de la Datainspektion suédoise (organisme public pour la protection des données transmises par voie informatique), qu'elle les avait transférées, sans autorisation, vers des pays tiers et qu'elle avait traité des données personnelles sensibles.

Dans le cadre de l'appel formé par M^me^ Lindqvist à l'encontre de cette décision devant le Göta hovrätt (cour d'appel, Suède), ce dernier avait interrogé la Cour à titre préjudiciel aux fins, en particulier, de savoir si M^me^ Lindqvist s'était livrée à un « traitement de données à caractère personnel, automatisé en tout ou en partie », au sens de la directive 95/46/CE.

La Cour a constaté que l'opération consistant à faire référence, sur une page Internet, à diverses personnes et à les identifier soit par leur nom, soit par d'autres moyens, par exemple leur numéro de téléphone ou des informations relatives à leurs conditions de travail et à leurs passe-temps, constitue un « traitement de données à caractère personnel, automatisé en tout ou en partie », au sens de cette directive (point 27, disp. 1). En effet, un tel traitement de données à caractère personnel mis en œuvre pour l'exercice d'activités bénévoles ou religieuses ne relève d'aucune des exceptions au champ d'application de la directive, dans la mesure où il ne rentre ni dans la catégorie d'activités ayant pour objet la sécurité publique ni dans la catégorie d'activités exclusivement personnelles ou domestiques qui sont hors du champ d'application de la directive (points 38, 43-48, disp. 2).

Arrêt du 13 mai 2014 (grande chambre), Google Spain et Google (C-131/12, EU:C:2014:317)

En 2010, un ressortissant espagnol avait introduit auprès de l'Agencia Española de Protección de Datos (Agence espagnole de protection des données, ci-après l'« AEPD ») une réclamation à l'encontre de La Vanguardia Ediciones SL, éditeur d'un quotidien largement diffusé en Espagne, ainsi qu'à l'encontre de Google Spain et de Google. Cette personne faisait valoir que, lorsqu'un internaute introduisait son nom dans le moteur de recherche du groupe Google, la liste de résultats affichait des liens vers deux pages du quotidien de La Vanguardia, datées de 1998, qui annonçaient notamment une vente aux enchères immobilière organisée à la suite d'une saisie destinée à recouvrer ses dettes. Par sa réclamation, cette personne demandait, d'une part, qu'il soit ordonné à La Vanguardia soit de supprimer ou de modifier les pages en cause, soit de recourir à certains outils fournis par les moteurs de recherche pour protéger ces données. D'autre part, elle demandait qu'il soit ordonné à Google Spain ou à Google de supprimer ou d'occulter ses données personnelles afin qu'elles disparaissent des résultats de recherche et des liens de La Vanguardia.

L'AEPD avait rejeté la réclamation dirigée contre La Vanguardia, estimant que les informations en cause avaient été légalement publiées par l'éditeur, mais l'avait, en revanche, accueillie en ce qui concerne Google Spain et Google et avait demandé à ces deux sociétés de prendre les mesures nécessaires pour retirer les données de leur index et pour en rendre l'accès impossible à l'avenir. Lesdites sociétés ayant introduit deux recours devant l'Audiencia Nacional (Audience nationale, Espagne) aux fins d'obtenir l'annulation de la décision de l'AEPD, la juridiction espagnole a déféré une série de questions à la Cour.

Ainsi, la Cour a eu l'occasion de préciser la notion de « traitement de données à caractère personnel » sur Internet au regard de la directive 95/46/CE.

La Cour a ainsi jugé que l'activité d'un moteur de recherche consistant à trouver des informations publiées ou placées sur Internet par des tiers, à les indexer de manière automatique, à les stocker temporairement et, enfin, à les mettre à la disposition des internautes selon un ordre de préférence donné doit être qualifiée de traitement de données à caractère personnel lorsque ces informations contiennent des données à caractère personnel (disp. 1). La Cour a, en outre, rappelé que les opérations visées par la directive doivent être qualifiées de traitement y compris lorsqu'elles concernent exclusivement des informations déjà publiées en l'état dans les médias. Une dérogation générale à l'application de la directive dans une telle hypothèse aurait pour effet de vider largement cette dernière de son sens (points 29 et 30).

Arrêt du 10 juillet 2018 (grande chambre), Jehovan todistajat (C-25/17, ECLI:EU:C:2018:551)[20]

L'autorité finlandaise de protection des données avait adopté une décision interdisant à la communauté des témoins de Jéhovah de collecter ou de traiter des données à caractère personnel dans le cadre de l'activité de prédication de porte-à-porte effectuée par ses membres sans que les conditions de la législation finlandaise relative au traitement de telles données soient respectées. Les membres de cette communauté prennent en effet, dans le cadre de leur activité de prédication de porte-à-porte, des notes sur les visites rendues à des personnes qu'eux-mêmes, ou ladite communauté, ne connaissent pas. Ces données sont collectées à titre d'aide-mémoire, afin de pouvoir être retrouvées pour une éventuelle visite ultérieure, sans que les personnes concernées y aient consenti ni n'en soient informées. À cet égard, la communauté des témoins de Jéhovah a donné à ses membres des lignes directrices relatives à la prise de telles notes, lignes directrices figurant au moins dans une de ses revues consacrées à l'activité de prédication.

La Cour a jugé que la collecte de données à caractère personnel effectuée par des membres d'une communauté religieuse dans le cadre d'une activité de prédication de porte-à-porte et les traitements ultérieurs de ces données ne relèvent pas des exceptions au champ d'application de la directive 95/46/CE, étant donné qu'ils ne constituent ni des traitements de données à caractère personnel mis en œuvre pour l'exercice d'activités visées à l'article 3, paragraphe 2, premier tiret, de cette directive, ni des traitements de données à caractère personnel effectués par des personnes physiques pour l'exercice d'une activité exclusivement personnelle ou domestique, au sens de l'article 3, paragraphe 2, second tiret, de ladite directive (point 51, disp. 1).

Arrêt du 14 février 2019, Buivids (C-345/17, EU:C:2019:122)

Dans cette affaire, la Cour s'est penchée sur l'interprétation, d'une part, du champ d'application

[20] Cet arrêt a été présenté dans le Rapport annuel 2018, pp. 87 et 88.

de la directive 95/46/CE et, d'autre part, sur de la notion de « traitement des données à caractère personnel aux seuls fins de journalisme », visée à l'article 9 de cette directive.

Cet arrêt s'inscrit dans le cadre d'une demande de décision préjudicielle adressée par la Cour suprême de Lettonie, saisie d'un litige opposant M. Buivids (ci-après le « requérant ») à l'autorité nationale de la protection des données, au sujet d'un recours visant à déclarer illégale une décision de cette autorité, selon laquelle cette personne aurait violé la législation nationale en matière de protection des données à caractère personnel en publiant sur un site Internet une vidéo, filmée par lui-même, de la prise de sa déposition par les membres de la police dans les locaux du commissariat de la police nationale, dans le cadre d'une procédure d'infraction administrative. Ainsi, suite au rejet de son recours par deux juridictions inférieures, le requérant a saisi la Cour suprême d'un pourvoi en cassation. Devant cette juridiction, il a invoqué son droit à la liberté d'expression, en faisant valoir que la vidéo en cause montrait des fonctionnaires de la police nationale, qui ont la qualité de personnes publiques, dans un lieu accessible au public et que de ce fait, ces personnes ne bénéficieraient pas de l'application des dispositions de la loi sur la protection des données.

S'agissant, en premier lieu, du champ d'application de la directive 95/46/CE, la Cour a noté que, d'une part, les images des membres de la police enregistrés dans la vidéo en cause constituent des données à caractère personnel et que, d'autre part, l'enregistrement vidéo de ces personnes stocké dans la mémoire de la caméra utilisée par le requérant, constitue un traitement de données à caractère personnel. Ainsi, la Cour a ajouté que le fait de publier un enregistrement vidéo sur lequel figure des données à caractère personnel sur un site Internet de vidéos pouvant être regardées et partagées par les utilisateurs constitue un traitement automatisé, en tout ou en partie de ces données. Par ailleurs, la Cour a souligné que ledit enregistrement et sa publication ne relèvent pas des exceptions prévues au champ d'application de la directive 95/46/CE, concernant notamment les traitements des données à caractère personnel réalisés dans le cadre d'activités qui ne relèvent pas du champ d'application de cette directive et les traitements s'inscrivant dans le cadre de l'exercice des activités exclusivement personnelles ou domestiques. Partant, la Cour a conclu que relèvent du champ d'application de cette directive l'enregistrement vidéo de membres de la police dans un commissariat, lors d'une prise de déposition, et la publication de la vidéo ainsi enregistrée sur un site Internet de vidéos sur lequel les utilisateurs peuvent envoyer, regarder et partager celles-ci (points 31, 32, 35, 39, 42, 43 et disp. 1).

En ce qui concerne, en second lieu, la portée de la notion de « traitement des données à caractère personnel aux seuls fins de journalisme », la Cour a tout d'abord rappelé que, en application d'une interprétation large de la notion de « journalisme », les exemptions et dérogations prévues à l'article 9 de la directive 95/46/CE s'appliquent à toute personne exerçant des activités de journalisme. Ainsi, la Cour a jugé que le fait que le requérant ne soit pas un journaliste de profession n'exclut pas que l'enregistrement de la vidéo en cause et sa transmission puissent être qualifiée de « traitement des données à caractère personnel aux seuls fins de journalisme ». De surcroît, la Cour a souligné que les exemptions et les dérogations prévues à l'article 9 de la directive 95/46/CE ne doivent être appliquées que dans la mesure où elles s'avèrent nécessaires pour concilier deux droits fondamentaux, à savoir le droit à la protection de la vie privée et celui de la liberté d'expression. À cet égard, la Cour a précisé qu'il ne saurait être exclu que l'enregistrement et la publication de la vidéo en cause, qui ont eu lieu

sans que les membres de la police figurant dans cette vidéo soient informés de cet enregistrement et de ses finalités, constitue une ingérence dans le droit fondamental au respect de la vie privée de ces personnes. Partant, elle a conclu que l'enregistrement et la publication sur un site Internet de vidéos de la vidéo en cause peuvent constituer un traitement de données à caractère personnel aux seuls fins du journalisme, pour autant qu'il ressorte de ladite vidéo que ledit enregistrement et ladite publication ont pour seule finalité la divulgation au public d'informations, d'opinions ou d'idées, ce qu'il incombe à la juridiction de renvoi de vérifier (points 51, 52, 55, 63, 67 et disp. 2).

4. Notion de « fichier de données à caractère personnel »

Arrêt du 10 juillet 2018 (grande chambre), Jehovan todistajat (C-25/17, ECLI:EU:C:2018:551)

Dans cet arrêt (voir également la rubrique II.3., intitulée « Notion de "traitement de données à caractère personnel" »), la Cour a précisé la notion de « fichier », visée par l'article 2, sous c), de la directive 94/56/CE.

Ainsi, après avoir rappelé que cette directive ne s'applique aux traitements manuels de données à caractère personnel que lorsque les données traitées sont contenues ou appelées à figurer dans un fichier, la Cour a jugé que ladite notion couvre un ensemble de données à caractère personnel collectées dans le cadre d'une activité de prédication de porte-à-porte, comportant des noms et des adresses ainsi que d'autres informations concernant les personnes démarchées, dès lors que ces données sont structurées selon des critères déterminés permettant, en pratique, de les retrouver aisément aux fins d'une utilisation ultérieure. Pour qu'un tel ensemble relève de cette notion, il n'est pas nécessaire qu'il comprenne des fiches, des listes spécifiques ou d'autres systèmes de recherche (point 62, disp. 2).

5. Notion de « responsable du traitement de données à caractère personnel »

Arrêt du 10 juillet 2018 (grande chambre), Jehovan todistajat (C-25/17, ECLI:EU:C:2018:551)

Dans cette affaire (voir également les rubriques II.3. et II.4., intitulées « Notion de "traitement de données à caractère personnel" et « Notion de "fichier de données à caractère personnel" »), la Cour s'est prononcée sur la responsabilité d'une communauté religieuse à l'égard des traitements de données à caractère personnel effectués dans le cadre d'une activité de prédication de porte-à-porte organisée, coordonnée et encouragée par cette communauté.

Ainsi, la Cour a estimé que l'obligation de toute personne de se conformer aux règles du droit de l'Union relatives à la protection des données à caractère personnel ne peut être considérée comme une ingérence dans l'autonomie organisationnelle des communautés religieuses. À cet égard, elle a conclu que l'article 2, sous d), de la directive 95/46/CE, lu à la lumière de l'article 10, paragraphe 1, de la Charte, doit être interprété en ce sens qu'il permet de considérer une communauté religieuse comme étant responsable, conjointement avec ses membres prédicateurs, des traitements de données à caractère personnel effectués par ces derniers dans le cadre d'une activité de prédication de porte-à-porte organisée, coordonnée et

encouragée par cette communauté, sans qu'il soit nécessaire que ladite communauté ait accès aux données ni qu'il doive être établi qu'elle a donné à ses membres des lignes directrices écrites ou des consignes relativement à ces traitements (points 74, 75 et disp. 3) .

Arrêt du 5 juin 2018 (grande chambre), Wirtschaftsakademie Schleswig Holstein (C-210/16, ECLI:EU:C:2018:388)[21]

L'autorité allemande de protection des données, en sa qualité d'autorité de contrôle, au sens de l'article 28 de la directive 95/46/CE, avait ordonné à une société allemande, spécialisée dans le domaine de l'éducation et offrant des services de formation au moyen d'une page fan hébergée sur le site du réseau social Facebook, de désactiver sa page fan. En effet, selon ladite autorité, ni cette société ni Facebook n'avaient informé les visiteurs de la page fan que cette dernière collectait, à l'aide de cookies, des informations à caractère personnel les concernant et que ladite société et Facebook traitaient ensuite ces données.

Dans ce contexte, la Cour a précisé la notion de « responsable du traitement » de données à caractère personnel. À cet égard, elle a considéré que l'administrateur d'une page fan hébergée sur Facebook, tel que la société en cause au principal, participe, par son action de paramétrage (en fonction, notamment, de son audience cible ainsi que d'objectifs de gestion ou de promotion de ses activités), à la détermination des finalités et des moyens du traitement des données personnelles des visiteurs de sa page fan. De ce fait, selon la Cour, cet administrateur doit être qualifié de responsable au sein de l'Union, conjointement avec Facebook Ireland (la filiale au sein de l'Union de la société américaine Facebook), de ce traitement au sens de l'article 2, sous d), de la directive 95/46/CE (point 39).

Arrêt du 29 juillet 2019, Fashion ID (C-40/17, EU:C:2019:629)

Dans cette affaire, la Cour a eu l'occasion de développer la notion de « responsable du traitement » au regard de l'intégration d'un « plugiciel » dans une page web.

En l'espèce, Fashion ID, une entreprise allemande de vente de vêtements de mode en ligne, avait inséré sur son site Internet le module social « j'aime » du réseau social Facebook. Cette insertion semble avoir pour conséquence que, lorsqu'un visiteur consulte le site Internet de Fashion ID, des données à caractère personnel de ce visiteur sont transmises à Facebook Ireland. Il apparaît que cette transmission s'effectue sans que ledit visiteur en soit conscient et indépendamment du fait qu'il soit membre du réseau social Facebook ou qu'il ait cliqué sur le bouton « j'aime » de Facebook.

La Verbraucherzentrale NRW, association allemande d'utilité publique de défense des intérêts des consommateurs, reproche à Fashion ID d'avoir transmis à Facebook Ireland des données à caractère personnel appartenant aux visiteurs de son site Internet, d'une part, sans le consentement de ces derniers et, d'autre part, en violation des obligations d'information prévues par les dispositions relatives à la protection des données personnelles. Saisi du litige,

[21] Cet arrêt a été présenté dans le Rapport annuel 2018, pp. 86 et 87.

l'Oberlandesgericht Düsseldorf (tribunal régional supérieur de Düsseldorf, Allemagne) a demandé à la Cour d'interpréter plusieurs dispositions de la directive 95/46/CE.

La Cour a, tout d'abord, constaté que le gestionnaire d'un site Internet, tel que Fashion ID, peut être considéré comme étant responsable du traitement, au sens de l'article 2, sous d), de la directive 95/46/CE. Cette responsabilité est cependant limitée à l'opération ou à l'ensemble des opérations de traitement des données à caractère personnel dont il détermine effectivement les finalités et les moyens, à savoir la collecte et la communication par transmission des données en cause. En revanche, selon la Cour, il apparaît, de prime abord, exclu que Fashion ID détermine les finalités et les moyens des opérations de traitement de données à caractère personnel ultérieures, effectuées par Facebook Ireland après leur transmission à cette dernière, de sorte que Fashion ID ne saurait être considérée comme étant responsable de ces opérations, au sens de cet article 2, sous d) (points 76, 85 et disp. 2).

En outre, la Cour a souligné qu'il est nécessaire que le gestionnaire d'un site Internet et le fournisseur d'un module social, tel que Facebook Ireland, poursuivent chacun, avec ces opérations de traitement, un intérêt légitime, au sens de l'article 7, sous f), de la directive 95/46/CE, afin que celles-ci soient justifiées dans son chef (point 97 et disp. 3).

Enfin, la Cour a précisé que le consentement de la personne concernée, visé à l'article 2, sous h), et l'article 7, sous a), de la directive 95/46/CE, doit être recueilli par le gestionnaire d'un site Internet uniquement en ce qui concerne les opérations de traitement des données à caractère personnel dont ce gestionnaire détermine les finalités et les moyens. Dans une telle situation, l'obligation d'information prévue par l'article 10 de cette directive pèse également sur ledit gestionnaire, l'information que ce dernier doit fournir à la personne concernée ne devant toutefois porter que sur l'opération ou l'ensemble des opérations de traitement des données à caractère personnel dont il détermine les finalités et les moyens (point 106 et disp. 4).

6. Conditions de licéité d'un traitement de données à caractère personnel au regard de l'article 7 de la directive nº 95/46/CE

Arrêt du 16 décembre 2008 (grande chambre), Huber (C-524/06, EU:C:2008:724)[22]

L'office fédéral de la migration et des réfugiés (Bundesamt für Migration und Flüchtlinge, Allemagne), assurait la gestion d'un registre central des étrangers qui rassemblait certaines données à caractère personnel relatives aux étrangers séjournant sur le territoire allemand pour une période supérieure à trois mois. Le registre était utilisé à des fins statistiques et lors de l'exercice, par les services de sécurité et de police ainsi que les autorités judiciaires, de leurs compétences en matière de poursuites et de recherches relatives à des agissements criminels ou mettant en danger la sécurité publique.

M. Huber, ressortissant autrichien, s'est installé en Allemagne en 1996 pour y exercer la profession d'agent d'assurance indépendant. S'estimant discriminé du fait du traitement dont

[22] Cet arrêt a été présenté dans le Rapport annuel 2008, p. 45.

faisaient l'objet les données le concernant contenues dans le registre en cause, une telle base de données n'existant pas pour les ressortissants allemands, M. Huber a demandé la suppression de ces données.

Dans ce contexte, l'Oberverwaltungsgericht für das Land Nordrhein-Westfalen (tribunal administratif supérieur du Land de Rhénanie-du-Nord-Westphalie, Allemagne), saisi du litige, a interrogé la Cour sur la compatibilité avec le droit de l'Union du traitement de données à caractère personnel auquel il était procédé dans le registre en cause.

La Cour a rappelé, tout d'abord, que le droit de séjour d'un citoyen de l'Union sur le territoire d'un État membre dont il n'est pas ressortissant n'est pas inconditionnel, mais peut être assorti de limitations. Ainsi, l'utilisation d'un tel registre dans un but de soutien aux autorités en charge de l'application de la réglementation sur le droit de séjour est, en principe, légitime et, au vu de sa nature, compatible avec l'interdiction de discrimination exercée en raison de la nationalité contenue à l'article 12, paragraphe 1, CE (devenu article 18, premier alinéa, TFUE). Cependant, un tel registre ne peut contenir d'autres informations que celles qui sont nécessaires à cette fin au sens de la directive sur la protection des données à caractère personnel (points 54, 58, 59).

S'agissant de la notion de nécessité du traitement au sens de l'article 7, sous e), de la directive 95/46/CE, la Cour a tout d'abord rappelé qu'il s'agissait d'une notion autonome du droit de l'Union devant recevoir une interprétation de nature à répondre pleinement à l'objet de la directive 95/46/CE tel que défini à son article 1er, paragraphe 1. Elle a ensuite constaté qu'un système de traitement de données à caractère personnel est conforme au droit de l'Union s'il contient uniquement les données nécessaires à l'application par lesdites autorités de cette réglementation, et si son caractère centralisé permet une application plus efficace de cette réglementation en ce qui concerne le droit de séjour des citoyens de l'Union non-ressortissants de cet État membre.

En tout état de cause, ne sauraient être considérés comme nécessaires au sens de l'article 7, sous e), de la directive 95/46/CE, la conservation et le traitement de données à caractère personnel nominatives dans le cadre d'un tel registre à des fins statistiques (points 52, 66, 68).

Par ailleurs, concernant la question de l'utilisation des données contenues dans le registre à des fins de lutte contre la criminalité, la Cour a relevé notamment que cet objectif vise la poursuite des crimes et des délits commis, indépendamment de la nationalité de leurs auteurs. Partant, pour un État membre, la situation de ses ressortissants ne saurait être différente de celle des citoyens de l'Union non-ressortissants de cet État membre séjournant sur son territoire au regard de l'objectif de lutte contre la criminalité. Par conséquent, la différence de traitement entre ces ressortissants et ces citoyens de l'Union induite par le traitement systématique des données à caractère personnel relatives aux seuls citoyens de l'Union non-ressortissants de l'État membre concerné dans un objectif de lutte contre la criminalité constitue une discrimination prohibée par l'article 12, paragraphe 1, CE (points 78-80).

Arrêt du 24 novembre 2011, ASNEF et FECEMD (C-468/10 et C-469/10, EU:C:2011:777)

L'Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF), d'une part, et la Federación de Comercio Electrónico y Marketing Directo (FECEMD), d'autre part, avaient formé,

auprès du Tribunal Supremo (Espagne), un recours contentieux administratif contre plusieurs articles de l'arrêté royal 1720/2007 qui avait mis en œuvre la loi organique 15/1999 transposant la directive 95/46/CE.

En particulier, l'ASNEF et la FECEMD considéraient que le droit espagnol, pour permettre le traitement des données à caractère personnel, en l'absence du consentement de la personne concernée, ajoutait une condition qui n'existe pas dans la directive 95/46/CE, exigeant que lesdites données figurent dans des « sources accessibles au public », telles qu'énumérées à l'article 3, sous j), de la loi organique 15/1999. À cet égard, ils avaient fait valoir que cette loi et l'arrêté royal 1720/2007 restreignaient la portée de l'article 7, sous f), de la directive 95/46/CE, qui soumet le traitement de données à caractère personnel, en l'absence de consentement de la personne concernée, à une condition tenant uniquement à l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées.

À cet égard, la Cour a tout d'abord relevé que l'article 7 de la directive 95/46/CE prévoit une liste exhaustive et limitative des cas dans lesquels un traitement de données à caractère personnel peut être considéré comme étant licite en l'absence de consentement de la personne concernée. Les États membres ne sauraient, par conséquent, introduire, au titre de l'article 5 de ladite directive, d'autres principes relatifs à la légitimation des traitements de données à caractère personnel que ceux énoncés à l'article 7, ni modifier, par des exigences supplémentaires, la portée des principes prévus audit article 7. En effet, l'article 5 n'autorise les États membres qu'à préciser, dans les limites du chapitre II de ladite directive et, partant, de l'article 7 de celle-ci, les conditions dans lesquelles les traitements de données à caractère personnel sont licites (points 30, 32, 33).

En particulier, pour effectuer la pondération nécessaire des droits et intérêts opposés en cause, prévue à l'article 7, sous f), de ladite directive, les États membres peuvent établir des principes directeurs. Ils peuvent également prendre en considération le fait que la gravité de l'atteinte aux droits fondamentaux de la personne concernée par ledit traitement peut varier en fonction du fait de savoir si les données en cause figurent déjà, ou non, dans des sources accessibles au public (points 44 et 46).

Toutefois, la Cour a considéré que si une réglementation nationale exclut, pour certaines catégories de données à caractère personnel, la possibilité d'être traitées en prescrivant, pour ces catégories, de manière définitive, le résultat de la pondération des droits et intérêts opposés, sans permettre un résultat différent en raison de circonstances particulières d'un cas concret, il ne s'agit plus d'une précision au sens de l'article 5 de la directive 95/46/CE. En conséquence, la Cour a conclu que l'article 7, sous f), de la directive 95/46/CE s'oppose à ce qu'un État membre exclue de façon catégorique et généralisée la possibilité pour certaines catégories de données à caractère personnel d'être traitées, sans permettre une pondération des droits et intérêts opposés en cause dans un cas particulier (points 47, 48).

Arrêt du 19 octobre 2016, Breyer (C-582/14, EU:C:2016:779)

Dans cet arrêt (voir également la rubrique II.2., intitulée « Notion de "données à caractère personnel" »), la Cour s'est, également, prononcée sur le point de savoir si l'article 7, sous f), de la directive 95/46/CE s'oppose à une disposition de droit national en vertu de laquelle le

fournisseur de services de médias en ligne ne peut collecter et utiliser des données à caractère personnel afférentes à un utilisateur sans le consentement de celui-ci que dans la mesure où cela est nécessaire pour permettre et facturer l'utilisation concrète du média en ligne par l'utilisateur en question et en vertu de laquelle la finalité consistant à garantir la capacité générale de fonctionnement du média en ligne ne peut pas justifier l'utilisation des données après la fin de la session de consultation en cours.

La Cour a jugé que l'article 7, sous f), de la directive 95/46/CE s'oppose à la réglementation en cause. En effet, en vertu de cette disposition, le traitement de données à caractère personnel au sens de cette disposition est licite s'il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée. Or, en l'espèce, la réglementation allemande avait exclu de façon catégorique et généralisée la possibilité pour certaines catégories de données à caractère personnel d'être traitées, sans permettre une pondération des droits et des intérêts opposés en cause dans un cas particulier. Ce faisant, elle avait illicitement réduit la portée de ce principe prévu à l'article 7, sous f), de la directive 95/46/CE, en excluant que l'objectif de garantir la capacité générale de fonctionnement des sites du média en ligne puisse faire l'objet d'une pondération avec l'intérêt ou les droits et libertés fondamentaux des utilisateurs (points 62-64, disp. 2).

Arrêt du 4 mai 2017, Rīgas satiksme (C-13/16, EU:C:2017:336)

Cette affaire s'inscrivait dans le cadre d'un litige opposant la police nationale lettonne à Rīgas satiksme, société de trolleybus de la ville de Riga, relatif à une demande de communication des données d'identification de l'auteur d'un accident. En l'espèce, lors d'un accident de la circulation routière, un chauffeur de taxi avait garé son véhicule sur le bord de la route. Alors que le trolleybus de Rīgas satiksme passait à côté de ce taxi, le passager occupant le siège arrière dudit taxi avait ouvert la portière qui avait heurté et endommagé le trolleybus. Aux fins de l'introduction d'un recours en droit civil, Rīgas satiksme avait, entre autres, demandé à la police nationale la communication des données d'identification de l'auteur de l'accident. La police avait refusé de communiquer le numéro d'identification et l'adresse du passager et les documents relatifs aux explications des personnes impliquées dans l'accident au motif que les documents relatifs à une procédure administrative aboutissant à des sanctions pouvaient être communiqués uniquement aux parties à cette affaire, et, pour ce qui concernait le numéro d'identification et l'adresse, la loi relative à la protection des données des personnes physiques interdisait la divulgation de telles informations concernant les personnes privées.

Dans ces conditions, l'Augstākās tiesas Administratīvo lietu departaments (Cour suprême, département des affaires administratives, Lettonie) a décidé de poser à la Cour la question de savoir si l'article 7, sous f), de la directive 95/46/CE impose l'obligation de communiquer des données à caractère personnel à un tiers afin de permettre à ce dernier d'introduire un recours en indemnisation devant une juridiction civile pour un dommage causé par la personne concernée par la protection de ces données et si le fait que cette personne soit mineure peut avoir une incidence sur l'interprétation de cette disposition.

La Cour a jugé que l'article 7, sous f), de la directive 95/46/CE doit être interprété en ce sens qu'il n'impose pas l'obligation de communiquer des données à caractère personnel à un tiers afin de lui permettre d'introduire un recours en indemnisation devant une juridiction civile pour un dommage causé par la personne concernée par la protection de ces données. Toutefois, ladite disposition ne s'opposerait pas à une telle communication, dans l'hypothèse où celle-ci serait effectuée sur la base du droit national, en respectant les conditions prévues par cette disposition (points 27, 34 et disp.).

Dans ce contexte, la Cour a relevé que, sous réserve des vérifications à effectuer à cet égard par le juge national, il n'apparaît pas justifié, dans des conditions telles que celles en cause au principal, de refuser à une partie lésée la communication des données à caractère personnel nécessaire pour l'introduction d'un recours en indemnisation contre l'auteur du dommage, ou, le cas échéant, les personnes exerçant l'autorité parentale, au motif que cet auteur serait mineur (point 33).

Arrêt du 27 septembre 2017, Puškár (C-73/16, EU:C:2017:725)

Dans le litige au principal, M. Puškár avait introduit un recours auprès du Najvyšší súd Slovenskej republiky (Cour suprême de la République slovaque) visant à ordonner au Finančné riaditel'stvo (direction des finances), à tous les bureaux des impôts subordonnés à celui-ci et au Kriminálny úrad finančnej správy (bureau de lutte contre la criminalité financière) de ne pas inscrire son nom sur la liste de personnes considérées par la direction des finances comme des prête-noms, établie par celle-ci dans le cadre de la perception de l'impôt et dont la mise à jour était assurée par la direction des finances, ainsi que le bureau de lutte contre la criminalité financière (ci-après la « liste litigieuse »). En outre, il avait demandé de supprimer toute mention le concernant de ces listes et du système informatique de l'administration financière.

Dans ces conditions, le Najvyšší súd a saisi la Cour, notamment, de la question de savoir si le droit au respect de la vie privée et familiale, du domicile et des communications, consacré à l'article 7, et le droit à la protection des données à caractère personnel, consacré à l'article 8 de la Charte, pouvaient être interprétés en ce sens qu'ils ne permettent pas à un État membre de créer, sans le consentement de la personne concernée, des listes de données à caractère personnel aux fins de la perception de l'impôt, si bien que l'obtention de données à caractère personnel par les autorités publiques en vue de la répression de la fraude fiscale présenterait un risque en soi.

La Cour a conclu que l'article 7, sous e), de la directive 95/46/CE ne s'oppose pas à un traitement de données à caractère personnel par les autorités d'un État membre aux fins de la perception de l'impôt et de la lutte contre la fraude fiscale tel que celui auquel il est procédé par l'établissement d'une liste de personnes telle que celle en cause dans l'affaire au principal, sans le consentement des personnes concernées, à condition, d'une part, que ces autorités aient été investies par la législation nationale de missions d'intérêt public au sens de cette disposition, que l'établissement de cette liste et l'inscription sur celle-ci du nom des personnes concernées soient effectivement aptes et nécessaires aux fins de la réalisation des objectifs poursuivis et qu'il existe des indices suffisants pour présumer que les personnes concernées figurent à juste titre sur ladite liste et, d'autre part, que toutes les conditions de licéité de ce traitement de

données à caractère personnel imposées par la directive 95/46/CE soient satisfaites (point 117, disp. 3).

À cet égard, la Cour a relevé qu'il incombe à la juridiction nationale de vérifier si l'établissement de la liste litigieuse est nécessaire à l'exécution des missions d'intérêt public en cause au principal, en tenant compte, notamment, de la finalité exacte de l'établissement de la liste litigieuse, des effets juridiques auxquels sont soumises les personnes figurant sur celle-ci et du caractère public ou non de cette liste. De plus, au regard du principe de proportionnalité, il appartient à la juridiction nationale de vérifier si l'établissement de la liste litigieuse et l'inscription sur celle-ci du nom des personnes concernées sont propres à réaliser les objectifs poursuivis par ceux-ci et s'il n'existe pas d'autres moyens moins contraignants afin d'atteindre ces objectifs (points 111, 112, 113).

En outre, la Cour a constaté que le fait pour une personne d'être inscrite sur la liste litigieuse est susceptible de porter atteinte à certains de ses droits. En effet, une inscription sur cette liste pourrait nuire à sa réputation et affecter ses relations avec les autorités fiscales. De même, cette inscription pourrait affecter la présomption d'innocence de cette personne, consacrée à l'article 48, paragraphe 1, de la Charte, ainsi que la liberté d'entreprise, inscrite à l'article 16 de la Charte, des personnes morales associées aux personnes physiques inscrites sur la liste litigieuse. Par conséquent, une telle atteinte ne peut être appropriée que s'il existe des indices suffisants permettant de soupçonner la personne concernée d'occuper de manière fictive des fonctions de direction au sein des personnes morales qui lui sont associées et de porter ainsi atteinte à la perception de l'impôt et à la lutte contre la fraude fiscale (point 114).

Par ailleurs, la Cour a estimé que s'il existait des raisons de limiter, en vertu de l'article 13 de la directive 95/46/CE, certains des droits prévus aux articles 6 et 10 à 12 de celle-ci, tels que le droit d'information de la personne concernée, une telle limitation devait être nécessaire à la sauvegarde d'un intérêt mentionné au paragraphe 1 dudit article 13, tel que, notamment, un intérêt économique et financier important dans le domaine fiscal, et être fondée sur des mesures législatives (point 116).

III. Traitements des données à caractère personnel au sens de la directive 2002/58/CE

Arrêt du 2 octobre 2018 (grande chambre), Ministerio Fiscal (C-207/16, ECLI:EU:C:2018:788)[23]

Dans la présente affaire était en cause le rejet, par un juge d'instruction espagnol, d'une demande introduite dans le cadre d'une enquête sur un vol avec violence d'un portefeuille et d'un téléphone mobile. Plus particulièrement, la police judiciaire avait demandé audit juge de lui accorder l'accès aux données d'identification des utilisateurs des numéros de téléphone activés depuis le téléphone volé durant une période de douze jours à compter de la date du vol. Le rejet avait été fondé sur une motivation selon laquelle les faits à l'origine de l'enquête pénale

[23] Cet arrêt a été présenté au Rapport annuel 2018, pp. 88 et 89.

n'étaient pas été constitutifs d'une infraction « grave » – c'est à dire, selon le droit espagnol, une infraction sanctionnée d'une peine de prison supérieure à cinq ans – l'accès aux données d'identification n'étant en effet possible que pour ce type d'infraction.

Après avoir rappelé que l'accès d'autorités publiques à des données à caractère personnel conservées par les fournisseurs de services de communications électroniques, dans le cadre d'une procédure d'instruction pénale, relève du champ d'application de la directive 2002/58, la Cour a jugé que l'accès aux données visant à l'identification des titulaires des cartes SIM activées avec un téléphone mobile volé, telles que les noms, prénoms et, le cas échéant, adresses de ces titulaires, constitue une ingérence dans les droits fondamentaux au respect de la vie privée et à la protection des données, consacrés par la Charte, même en l'absence de circonstances permettant de qualifier cette ingérence de « grave » et sans qu'il importe que les informations relatives à la vie privée concernées présentent ou non un caractère sensible ou que les intéressés aient ou non subi d'éventuels inconvénients en raison de ladite ingérence. Toutefois, la Cour a souligné que cette ingérence ne présente pas une gravité telle que cet accès devrait être limité, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, à la lutte contre la criminalité grave. En effet, si la directive 2002/58 énumère de manière exhaustive les objectifs susceptibles de justifier une réglementation nationale régissant l'accès des autorités publiques aux données concernées et dérogeant, ainsi, au principe de confidentialité des communications électroniques, cet accès devant répondre effectivement et strictement à l'un de ces objectifs, la Cour observe que, s'agissant de l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales, le libellé de la directive 2002/58 ne limite pas cet objectif à la lutte contre les seules infractions graves, mais vise les « infractions pénales » en général (points 38, 42, 59 à 63, et disp.).

Dans ce contexte, la Cour a précisé que si, dans son arrêt *Tele2 Sverige et Watson e.a.*[24], elle avait jugé que seule la lutte contre la criminalité grave est susceptible de justifier un accès des autorités publiques à des données à caractère personnel conservées par les fournisseurs de services de communications qui, prises dans leur ensemble, permettent de tirer des conclusions précises concernant la vie privée des personnes dont les données sont concernées, une telle interprétation était motivée par le fait que l'objectif poursuivi par une réglementation régissant cet accès doit être en relation avec la gravité de l'ingérence dans les droits fondamentaux en cause que cette opération entraîne. Ainsi, conformément au principe de proportionnalité, une ingérence grave ne peut être justifiée dans ce domaine que par un objectif de lutte contre la criminalité devant également être qualifiée de « grave ». En revanche, lorsque l'ingérence n'est pas grave, ledit accès est susceptible d'être justifié par un objectif de prévention, de recherche, de détection et de poursuite d'« infractions pénales » en général (points 54 à 57) .

S'agissant du cas d'espèce, la Cour a estimé que l'accès aux seules données visées par la demande en cause ne saurait être qualifié d'ingérence « grave » dans les droits fondamentaux des personnes dont les données sont concernées, puisque ces données ne permettent pas de tirer de conclusions précises concernant leur vie privée. La Cour en a conclu que l'ingérence que comporterait un accès à de telles données est donc susceptible d'être justifiée par l'objectif de prévention, de recherche, de détection et de poursuite d'« infractions pénales » en général, sans qu'il soit nécessaire que ces infractions soient qualifiées de « graves » (points 61, 62).

---

[24] Arrêt de la Cour du 21 décembre 2016, *Tele2 Sverige et Watson e.a.* (C-203/15 et C-698/15, EU:C:2016:970).

IV. Transfert de données à caractère personnel vers des pays tiers

Arrêt du 6 novembre 2003 (grande chambre), Lindqvist (C-101/01, EU:C:2003:596)[25]

Dans cette affaire (voir également la rubrique II.3., intitulée « Notion de "traitement de données à caractère personnel" »), la juridiction de renvoi souhaitait, en particulier, savoir si M^me^ Lindqvist s'était livrée à un transfert de données vers un pays tiers au sens de ladite directive.

La Cour a jugé qu'il n'existe pas de « transfert vers un pays tiers de données », au sens de l'article 25 de la directive 95/46/CE, lorsqu'une personne qui se trouve dans un État membre inscrit sur une page Internet, stockée auprès d'une personne physique ou morale qui héberge le site Internet sur lequel la page peut être consultée et qui est établie dans ce même État ou un autre État membre, des données à caractère personnel, les rendant ainsi accessibles à toute personne qui se connecte à Internet, y compris des personnes se trouvant dans des pays tiers (point 71, disp. 4).

En effet, eu égard, d'une part, à l'état du développement d'Internet à l'époque de l'élaboration de la directive 95/46/CE et, d'autre part, à l'absence de critères applicables à l'utilisation d'Internet dans son chapitre IV, lequel comprend ledit article 25, visant à assurer un contrôle par les États membres des transferts de données à caractère personnel vers les pays tiers et à interdire ces transferts lorsque ceux-ci n'offrent pas un niveau de protection adéquat, on ne saurait présumer que le législateur communautaire avait l'intention d'inclure prospectivement dans la notion de « transfert vers un pays tiers de données » une telle inscription de données sur une page Internet, même si celles-ci sont ainsi rendues accessibles aux personnes de pays tiers possédant les moyens techniques d'y accéder (points 63, 64, 68).

Arrêt du 6 octobre 2015 (grande chambre), Schrems (C-362/14, EU:C:2015:650)[26]

M. Schrems, citoyen autrichien et utilisateur du réseau social Facebook, avait déposé plainte auprès du Data Protection Commissioner (commissaire à la protection des données, Irlande), en raison du fait que Facebook Ireland transférait aux États-Unis les données à caractère personnel de ses utilisateurs et les conservait sur des serveurs situés dans ce pays, où elles faisaient l'objet d'un traitement. Selon M. Schrems, 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. Le Data Protection Commissioner avait refusé d'enquêter sur cette plainte, au motif, notamment, que dans sa décision 2000/520CE[27], la Commission avait considéré que, dans le cadre du régime dit de la « sphère de sécurité » (en anglais, « safe harbour »)[28], les États-

[25] Cet arrêt a été présenté dans le Rapport annuel 2003, p. 67.
[26] Cet arrêt a été présenté dans le Rapport annuel 2015, p. 53.
[27] 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 L 215 du 25.8.2000, p. 7).
[28] Le régime de la sphère de sécurité comprend une série de principes relatifs à la protection des données à caractère personnel auxquels les entreprises américaines peuvent souscrire volontairement.

Unis assuraient un niveau adéquat de protection aux données à caractère personnel transférées.

C'est dans ce contexte que la Cour a été saisie par la High Court (Haute Cour, Irlande) d'une demande en interprétation de l'article 25, paragraphe 6, de la directive 95/46/CE, en vertu duquel la Commission peut constater qu'un pays tiers assure un niveau de protection adéquat aux données transférées, ainsi que, en substance, d'une demande visant à établir la validité de la décision 2000/520/CE adoptée par la Commission sur le fondement dudit article 25, paragraphe 6, de la directive 95/46/CE.

La Cour a déclaré invalide la décision de la Commission dans son ensemble, en soulignant, tout d'abord, que son adoption exigeait la constatation dûment motivée par la Commission que le pays tiers concerné assure effectivement un niveau de protection des droits fondamentaux substantiellement équivalent à celui garanti dans l'ordre juridique de l'Union. Or, dans la mesure où la Commission, dans sa décision 2000/520/CE, n'en a pas fait état, l'article 1er de cette décision méconnaît les exigences fixées à l'article 25, paragraphe 6, de la directive 95/46/CE, lu à la lumière de la Charte, et est de ce fait invalide. 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 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 (points 82, 87-89, 96-98, disp. 2).

En outre, la Cour a déclaré invalide l'article 3 de la décision 2000/520/CE, dans la mesure où celui-ci prive les autorités nationales de contrôle des pouvoirs qu'elles tirent de l'article 28 de la directive 95/46/CE, dans le cas où une personne avance des éléments susceptibles de remettre en cause la compatibilité avec la protection de la vie privée et des libertés et droits fondamentaux des personnes d'une décision de la Commission ayant constaté qu'un pays tiers assure un niveau de protection adéquat (points 102-104). La Cour a conclu que l'invalidité des articles 1er et 3 de la décision 2000/520/CE avait pour effet d'affecter la validité de cette décision dans son ensemble (points 105, 106).

S'agissant de l'impossibilité de justifier une telle ingérence, la Cour a, tout d'abord, observé qu'une réglementation de l'Union comportant une ingérence dans les droits fondamentaux garantis par les articles 7 et 8 de la Charte doit prévoir des règles claires et précises régissant la portée et l'application d'une mesure et imposant un minimum d'exigences, de sorte que les personnes dont les données à caractère personnel sont concernées disposent de garanties suffisantes permettant de protéger efficacement leurs données contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données. La nécessité de disposer de telles garanties est d'autant plus importante lorsque les données à caractère personnel sont soumises à un traitement automatique et qu'il existe un risque important d'accès illicite à ces données (point 91).

En outre et surtout, la protection du droit fondamental au respect de la vie privée au niveau de l'Union exige que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci s'opèrent dans les limites du strict nécessaire (point 92). Ainsi, n'est pas limitée au strict nécessaire une réglementation qui autorise de manière généralisée la conservation de l'intégralité des données à caractère personnel de toutes les personnes dont les données ont été transférées depuis l'Union sans qu'aucune différenciation, limitation ou exception soit opérée en fonction de l'objectif poursuivi et sans que soit prévu un critère objectif permettant de délimiter l'accès des autorités publiques aux données et leur utilisation ultérieure à des fins précises, strictement restreintes et susceptibles de justifier l'ingérence que comportent tant l'accès que l'utilisation de ces données (point 93). En particulier, une réglementation permettant aux autorités publiques d'accéder de manière généralisée au contenu de communications électroniques porte atteinte au contenu essentiel du droit fondamental au respect de la vie privée. De même, une réglementation ne prévoyant aucune possibilité pour le justiciable d'exercer des voies de droit afin d'avoir accès à des données à caractère personnel le concernant, ou d'obtenir la rectification ou la suppression de telles données, ne respecte pas le contenu essentiel du droit fondamental à une protection juridictionnelle effective, tel que consacré à l'article 47 de la Charte (points 94, 95).

Avis 1/15 (Accord PNR UE-Canada) du 26 juillet 2017 (grande chambre) (EU:C:2017:592)

Le 26 juillet 2017, la Cour s'est prononcée pour la première fois sur la compatibilité d'un projet d'accord international avec la charte des droits fondamentaux de l'Union européenne, et, en particulier, avec les dispositions relatives au respect de la vie privée ainsi qu'à la protection des données à caractère personnel.

L'Union européenne et le Canada ont négocié un accord sur le transfert et le traitement des données des dossiers passagers (accord PNR) qui a été signé en 2014. Le Conseil de l'Union européenne ayant demandé au Parlement européen de l'approuver, ce dernier a décidé de saisir la Cour pour savoir si l'accord envisagé était conforme au droit de l'Union.

L'accord envisagé permet le transfert systématique et continu des données PNR de l'ensemble des passagers aériens à une autorité canadienne en vue de leur utilisation et de leur conservation, ainsi que de leur éventuel transfert ultérieur à d'autres autorités et à d'autres pays tiers, dans le but de lutter contre le terrorisme et les formes graves de criminalité transnationale. À cet effet, l'accord envisagé prévoit, entre autres, une durée de stockage des données de cinq ans et pose des exigences particulières en matière de sécurité et d'intégrité des PNR, tel qu'un masquage immédiat des données sensibles, de même qu'il prévoit des droits d'accès aux données, de rectification et d'effacement et la possibilité d'introduire des recours administratifs ou judiciaires.

Les données PNR visées par l'accord envisagé comprennent, notamment, outre le nom et les coordonnées du ou des passagers aériens, des informations nécessaires à la réservation, telles que les dates prévues du voyage et l'itinéraire de voyage, des informations relatives aux billets, les groupes de personnes enregistrées sous le même numéro de réservation, des informations relatives aux moyens de paiement ou à la facturation, des informations concernant les bagages ainsi que des remarques générales à l'égard des passagers.

Dans son avis, la Cour a jugé que l'accord PNR ne peut pas être conclu sous sa forme actuelle en raison de l'incompatibilité de plusieurs de ses dispositions avec les droits fondamentaux reconnus par l'Union.

La Cour a constaté, en premier lieu, que tant le transfert des données PNR depuis l'Union vers l'autorité canadienne compétente que l'encadrement négocié par l'Union avec le Canada des conditions tenant à la conservation de ces données, à leur utilisation ainsi qu'à leur transfert éventuel ultérieur à d'autres autorités canadiennes, à Europol, à Eurojust, aux autorités judiciaires ou de police des États membres ou encore à des autorités d'autres pays tiers, constituent des ingérences dans le droit garanti à l'article 7 de la Charte. Ces opérations sont également constitutives d'une ingérence dans le droit fondamental à la protection des données à caractère personnel garanti à l'article 8 de la Charte, puisqu'elles constituent des traitements des données à caractère personnel (points 125, 126).

De surcroît, elle a souligné que même si certaines des données PNR, prises isolément, ne paraissent pas pouvoir révéler des informations importantes sur la vie privée des personnes concernées, il n'en demeure pas moins que, prises ensemble, lesdites données peuvent, entre autres, révéler un itinéraire de voyage complet, des habitudes de voyage, des relations existant entre deux ou plusieurs personnes ainsi que des informations sur la situation financière des passagers aériens, leurs habitudes alimentaires ou leur état de santé, et pourraient même fournir des informations sensibles sur ces passagers, telles que définies à l'article 2, sous e), de l'accord envisagé (informations révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses, etc.) (point 128).

À cet égard, la Cour a considéré que, bien que les ingérences en cause puissent être justifiées par la poursuite d'un objectif d'intérêt général (garantie de la sécurité publique dans le cadre de la lutte contre des infractions terroristes et la criminalité transnationale grave), plusieurs dispositions de l'accord ne sont pas limitées au strict nécessaire et ne prévoient pas des règles claires et précises.

En particulier, la Cour a relevé que, compte tenu du risque d'un traitement contraire au principe de non-discrimination, un transfert des données sensibles vers le Canada nécessiterait une justification précise et particulièrement solide, tirée de motifs autres que la protection de la sécurité publique contre le terrorisme et la criminalité transnationale grave. Or, en l'occurrence, une telle justification fait défaut. La Cour en a conclu que les dispositions de l'accord sur le transfert des données sensibles vers le Canada ainsi que sur le traitement et la conservation de ces données sont incompatibles avec les droits fondamentaux (points 165, 232).

En deuxième lieu, la Cour a estimé qu'après le départ des passagers aériens du Canada, le stockage continu des données PNR de l'ensemble des passagers aériens que l'accord envisagé permet n'est pas limité au strict nécessaire. En effet, s'agissant des passagers aériens pour lesquels un risque en matière de terrorisme ou de criminalité transnationale grave n'a pas été identifié à leur arrivée au Canada et jusqu'à leur départ de ce pays, il n'apparaît pas exister, une fois qu'ils sont repartis, de rapport, ne serait-ce qu'indirect, entre leurs données PNR et l'objectif poursuivi par l'accord envisagé, qui justifierait la conservation de ces données. En revanche, un stockage des données PNR des passagers aériens pour lesquels sont identifiés des éléments objectifs permettant de considérer qu'ils pourraient, même après leur départ du Canada, présenter un risque en termes de lutte contre le terrorisme et la criminalité transnationale grave

est admissible au-delà de leur séjour dans ce pays, même pour une durée de cinq ans (points 205-207, 209).

En troisième lieu, la Cour a constaté que le droit fondamental au respect de la vie privée, consacré à l'article 7 de la charte des droits fondamentaux de l'Union européenne, implique que la personne concernée puisse s'assurer que ses données à caractère personnel sont traitées de manière exacte et licite. Afin de pouvoir effectuer les vérifications nécessaires, cette personne doit disposer d'un droit d'accès aux données la concernant qui font l'objet d'un traitement.

À cet égard, elle a souligné que, dans l'accord envisagé, il importe que les passagers aériens soient informés du transfert de leurs données des dossiers passagers vers le pays tiers concerné et de l'utilisation de ces données dès le moment où cette communication n'est pas susceptible de compromettre les enquêtes conduites par les autorités publiques visées par l'accord envisagé. En effet, une telle information s'avère, de fait, nécessaire pour permettre aux passagers aériens d'exercer leurs droits de demander l'accès aux données les concernant et, le cas échéant, la rectification de celles-ci ainsi que d'introduire, conformément à l'article 47, premier alinéa, de la Charte, un recours effectif devant un tribunal.

Ainsi, dans les hypothèses dans lesquelles se présentent des éléments objectifs justifiant l'utilisation des données des dossiers passagers afin de lutter contre le terrorisme et la criminalité transnationale grave et nécessitant une autorisation préalable d'une autorité judiciaire ou d'une entité administrative indépendante, une information individuelle des passagers aériens s'avère nécessaire. Il en va de même dans les cas où les données des dossiers des passagers aériens sont communiquées à d'autres autorités publiques ou à des particuliers. Cependant, une telle information ne doit intervenir qu'à partir du moment où elle n'est pas susceptible de compromettre les enquêtes conduites par les autorités publiques visées par l'accord envisagé (points 219, 220, 223, 224).

Arrêt du 16 juillet 2020 (grande chambre), Facebook Ireland et Schrems (C-311/18, ECLI:EU:C:2015:650)

Le règlement général relatif à la protection des données[29] (ci-après le « 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 législation interne ou de ses engagements internationaux, un niveau de protection adéquat[30]. 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 effectives[31]. Par

[29] 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).
[30] Article 45 du RGPD.
[31] Article 46, paragraphes 1 et 2, sous c), du RGPD.

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 appropriées[32].

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 2000/520[33], 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 »)[34] (points 52, 53).

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 2010/87[35]. 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 aux fins que celle-ci soumette à la Cour une demande de décision préjudicielle. Après l'ouverture de cette procédure, la Commission a adopté la décision (UE) 2016/1250 relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis[36] (points 54, 55, 57).

Par sa demande de décision préjudicielle, 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.

La Cour constate que l'examen de la décision 2010/87 au regard de la charte des droits fondamentaux de l'Union européenne (ci-après la « Charte ») ne révèle aucun élément de

[32] Article 49 du RGPD.
[33] 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 d'Amérique (JO 2000, L 215, p. 7).
[34] Arrêt de la Cour du 6 octobre 2015, Schrems, C-362/14, EU:C:2015:650 (voir également CP n° 117/15).
[35] 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).
[36] Décision d'exécution 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).

nature à affecter sa validité. En revanche, elle déclare la décision 2016/1250 invalide (disp. 4 et 5).

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 RGPD (points 86, 88, 89 et disp. 1).

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 (point 105 et disp. 2).

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 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 (point 121 et disp. 3).

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 donnés et le destinataire du transfert de vérifier, au préalable, que ce niveau de protection est 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 (points 132, 136, 137, 142, 148 et disp. 4).

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 d'une 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 (points 164, 165, 180-182, 184, 185).

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 (points 195-197, 201 et disp. 5).

V. La protection des données à caractère personnel sur Internet

1. Droit d'opposition au traitement des données à caractère personnel (« droit à l'oubli »)

Arrêt du 13 mai 2014 (grande chambre), Google Spain et Google (C-131/12, EU:C:2014:317)

Dans cet arrêt (voir également la rubrique II.3., intitulée « Notion de "traitement de données à caractère personnel" »), la Cour a précisé la portée des droits d'accès et d'opposition au traitement des données à caractère personnel sur Internet, prévus par la directive 95/46/CE.

Ainsi, lorsqu'elle s'est prononcée sur la question de l'étendue de la responsabilité de l'exploitant d'un moteur de recherche sur Internet, la Cour a, en substance, jugé que pour respecter les droits d'accès et d'opposition garantis par les articles 12, sous b), et 14, premier alinéa, sous a), de la directive 95/46/CE, et pour autant que les conditions prévues à ces articles sont satisfaites, celui-ci est, dans certaines conditions, obligé de supprimer de la liste de résultats, affichée à la suite d'une recherche effectuée à partir du nom d'une personne, des liens vers des pages web, publiées par des tiers et contenant des informations relatives à cette personne. La Cour a précisé qu'une telle obligation peut exister également dans l'hypothèse où ce nom ou ces informations ne sont pas effacés préalablement ou simultanément de ces pages web, et ce, le cas échéant, même lorsque leur publication en elle-même sur lesdites pages est licite (point 88, disp. 3).

Par ailleurs, interrogée sur la question de savoir si la directive permet à la personne concernée de demander que des liens vers des pages web soient supprimés d'une telle liste de résultats au motif qu'elle souhaiterait que les informations y figurant relatives à sa personne soient « oubliées » après un certain temps, la Cour relève, tout d'abord, que même un traitement initialement licite de données exactes peut devenir, avec le temps, incompatible avec cette directive lorsque ces données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées, notamment lorsque ces données apparaissent inadéquates, qu'elles ne sont pas ou plus pertinentes, ou encore qu'elles apparaissent excessives au regard de ces finalités ou du temps qui s'est écoulé (point 93). Dès lors, s'il est constaté, à la suite d'une demande de la personne concernée, que l'inclusion de ces liens dans la liste est, au stade actuel, incompatible avec la directive, les informations et liens figurant dans cette liste doivent être effacés (point 94). Dans ce contexte, la constatation d'un droit de la personne concernée à ce que l'information relative à sa personne ne soit plus liée à son nom par une liste de résultats ne présuppose pas que l'inclusion de l'information en question dans la liste de résultats cause un préjudice à la personne concernée (point 96, disp. 4).

Enfin, la Cour a précisé que la personne concernée pouvant, eu égard à ses droits fondamentaux au titre des articles 7 et 8 de la Charte, demander à ce que l'information en question ne soit plus mise à la disposition du grand public par son inclusion dans une telle liste de résultats, ces droits prévalent, en principe, non seulement sur l'intérêt économique de l'exploitant du moteur de recherche, mais également sur l'intérêt de ce public à trouver ladite information lors d'une recherche portant sur le nom de cette personne. Cependant, tel ne serait pas le cas s'il apparaissait, pour des raisons particulières, telles que le rôle joué par ladite

personne dans la vie publique, que l'ingérence dans ses droits fondamentaux est justifiée par l'intérêt prépondérant dudit public à avoir, du fait de cette inclusion, accès à l'information en question (point 97, disp. 4).

2. Traitement des données à caractère personnel et droits de propriété intellectuelle

Arrêt du 29 janvier 2008 (grande chambre), Promusicae (C-275/06, EU:C:2008:54)[37]

Promusicae, une association espagnole sans but lucratif regroupant des producteurs et des éditeurs d'enregistrements musicaux et audiovisuels, avait saisi les tribunaux espagnols afin d'ordonner à Telefónica de España SAU (société commerciale ayant pour activité, notamment, la fourniture de services d'accès à l'Internet) de révéler l'identité et l'adresse physique de certaines personnes auxquelles cette dernière fournissait un service d'accès à l'Internet et dont l'adresse IP ainsi que la date et l'heure de connexion étaient connues. Selon Promusicae, ces personnes utilisaient le programme d'échange d'archives dit « peer-to-peer » ou « P2P » (moyen transparent de partage de contenu, indépendant, décentralisé et muni de fonctions de recherche et de téléchargement avancées) et permettaient l'accès, dans le répertoire partagé de leur ordinateur personnel, à des phonogrammes dont les droits patrimoniaux d'exploitation appartenaient aux associés de Promusicae. Elle avait donc demandé la communication de ces informations pour pouvoir engager des procédures civiles contre les intéressés.

Dans ces conditions, le Juzgado de lo Mercantil nº 5 de Madrid (tribunal de commerce nº 5 de Madrid, Espagne) a interrogé la Cour sur la question de savoir si la législation européenne impose aux États membres de prévoir, en vue d'assurer la protection effective du droit d'auteur, l'obligation de communiquer des données à caractère personnel dans le cadre d'une procédure civile.

Selon la Cour, ladite demande de décision préjudicielle a soulevé la question de la conciliation nécessaire des exigences liées à la protection de différents droits fondamentaux, à savoir, d'une part, le droit au respect de la vie privée et, d'autre part, les droits à la protection de la propriété et à un recours effectif.

À cet égard, la Cour a conclu que les directives 2000/31/CE, 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 »)[38], 2001/29/CE, sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information[39], 2004/48/CE, relative au respect des droits de propriété intellectuelle[40], et 2002/58/CE, concernant le traitement des données à caractère personnel et la protection de la vie privée

37 Cet arrêt a été présenté dans le Rapport annuel 2008, p. 46.

38 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 L 178 du 17.7.2000, p. 1).

39 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 L 167 du 22.6.2001, p. 10).

40 Directive 2004/48/CE du Parlement européen et du Conseil, du 29 avril 2004, relative au respect des droits de propriété intellectuelle (JO L 157 du 30.4.2004, p. 45, et rectificatif JO L 195 du 2.6.2004, p. 16).

dans le secteur des communications électroniques (directive vie privée et communications électroniques) n'imposent pas aux États membres de prévoir, dans une situation telle que celle de l'affaire au principal, l'obligation de communiquer des données à caractère personnel en vue d'assurer la protection effective du droit d'auteur dans le cadre d'une procédure civile. Toutefois, le droit de l'Union exige desdits États que, lors de la transposition de ces directives, ils veillent à se fonder sur une interprétation de celles-ci qui permette d'assurer un juste équilibre entre les différents droits fondamentaux protégés par l'ordre juridique communautaire. Ensuite, lors de la mise en œuvre des mesures de transposition desdites directives, il incombe aux autorités et aux juridictions des États membres non seulement d'interpréter leur droit national d'une manière conforme à ces mêmes directives, mais également de ne pas se fonder sur une interprétation de celles-ci qui entrerait en conflit avec lesdits droits fondamentaux ou avec les autres principes généraux du droit communautaire, tels que le principe de proportionnalité (point 70 et disp.).

Arrêt du 24 novembre 2011, Scarlet Extended (C-70/10, EU:C:2011:771)[41]

La société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) avait constaté que des internautes utilisant les services de Scarlet Extended SA, fournisseur d'accès à Internet (ci-après « Scarlet »), téléchargeaient sur Internet, sans autorisation et sans paiement de droits, des œuvres reprises dans son catalogue au moyen de réseaux « peer-to-peer ». La SABAM avait saisi le juge national et obtenu, en première instance, qu'il prononce, à l'encontre de Scarlet, une injonction de faire cesser ces atteintes au droit d'auteur en rendant impossible, au moyen d'un logiciel « peer-to-peer », toute forme d'envoi ou de réception par ses clients de fichiers électroniques reprenant une œuvre musicale du répertoire de la SABAM.

Saisie par Scarlet, la cour d'appel de Bruxelles (Belgique) a sursis à statuer afin de demander à la Cour, à titre préjudiciel, si une telle injonction était compatible avec le droit européen.

La Cour a jugé que les directives 95/46/CE, 2000/31/CE, 2001/29/CE, 2002/58/CE et 2004/48/CE, lues ensemble et interprétées au regard des exigences résultant de la protection des droits fondamentaux applicables, doivent être interprétées en ce sens qu'elles s'opposent à une injonction faite à Scarlet de mettre en place un système de filtrage de toutes les communications électroniques transitant par ses services, notamment par l'emploi de logiciels « peer-to-peer », qui s'applique indistinctement à l'égard de toute sa clientèle, à titre préventif, à ses frais exclusifs, et sans limitation dans le temps, et qui soit capable d'identifier sur le réseau de ce fournisseur la circulation de fichiers électroniques contenant une œuvre musicale, cinématographique ou audiovisuelle sur laquelle le demandeur prétend détenir des droits de propriété intellectuelle, en vue de bloquer le transfert de fichiers dont l'échange porte atteinte au droit d'auteur (point 54 et disp.).

En effet, selon la Cour, une telle injonction ne respecte pas l'interdiction, posée par l'article 15, paragraphe 1, de la directive 2000/31/CE, d'imposer à un tel prestataire une obligation générale de surveillance, ni l'exigence d'assurer le juste équilibre entre, d'une part, le droit de propriété intellectuelle et, d'autre part, la liberté d'entreprise et le droit à la protection des données à

[41] Cet arrêt a été présenté dans le Rapport annuel 2011, p. 37.

caractère personnel et la liberté de recevoir ou de communiquer des informations (points 40, 49).

Dans ce contexte, la Cour a relevé que, d'une part, l'injonction de mettre en place le système de filtrage litigieux impliquerait une analyse systématique de tous les contenus ainsi que la collecte et l'identification des adresses IP des utilisateurs qui sont à l'origine de l'envoi des contenus illicites sur le réseau, ces adresses étant des données protégées à caractère personnel, car elles permettent l'identification précise desdits utilisateurs (point 51). D'autre part, ladite injonction risquerait de porter atteinte à la liberté d'information puisque ce système risquerait de ne pas suffisamment distinguer entre un contenu illicite et un contenu licite, de sorte que son déploiement pourrait avoir pour effet d'entraîner le blocage de communications à contenu licite. En effet, il n'est pas contesté que la réponse à la question de la licéité d'une transmission dépende également de l'application d'exceptions légales au droit d'auteur qui varient d'un État membre à l'autre. En outre, certaines œuvres peuvent relever, dans certains États membres, du domaine public ou elles peuvent faire l'objet d'une mise en ligne à titre gratuit de la part des auteurs concernés (point 52).

Par conséquent, la Cour a constaté que, en adoptant l'injonction obligeant Scarlet à mettre en place le système de filtrage litigieux, la juridiction nationale concernée ne respecterait pas l'exigence d'assurer un juste équilibre entre le droit de propriété intellectuelle, d'une part, et la liberté d'entreprise, le droit à la protection des données à caractère personnel et la liberté de recevoir ou de communiquer des informations, d'autre part (point 53).

Arrêt du 19 avril 2012, Bonnier Audio e.a. (C-461/10, EU:C:2012:219)

Le Högsta domstolen (Cour suprême, Suède) a saisi la Cour à titre préjudiciel afin d'interpréter les directives 2002/58/CE et 2004/48/CE, dans le cadre d'un litige opposant Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB et Storyside AB (ci-après « Bonnier Audio e.a. ») à Perfect Communication Sweden AB (ci-après « ePhone ») au sujet de l'opposition de cette dernière à une demande d'injonction de communication de données formulée par Bonnier Audio e.a.

En l'espèce, Bonnier Audio e.a. étaient des sociétés d'édition, titulaires notamment de droits exclusifs de reproduction, d'édition et de mise à disposition du public de 27 ouvrages se présentant sous la forme de livres audio. Elles estimaient qu'il aurait été porté atteinte à leurs droits exclusifs, en raison de la diffusion au public de ces 27 œuvres, sans leur consentement, au moyen d'un serveur FTP (« file transfer protocol ») qui permettait le partage de fichiers et le transfert de données entre ordinateurs connectés à Internet. Dès lors, elles avaient saisi les tribunaux suédois d'une demande d'injonction aux fins de communication des nom et adresse de la personne faisant usage de l'adresse IP à partir de laquelle il est présumé que les fichiers en question auraient été transmis.

Dans ce contexte, le Högsta domstolen, saisi d'un pourvoi en cassation, a interrogé la Cour sur le point de savoir si le droit de l'Union s'oppose à l'application d'une disposition de droit national, instituée sur la base de l'article 8 de la directive 2004/48/CE, qui, aux fins d'identification d'un abonné, permettait d'enjoindre à un fournisseur d'accès Internet de communiquer au titulaire d'un droit d'auteur ou à son ayant droit, dans une procédure civile, l'identité de l'abonné à qui

une adresse IP, qui aurait servi à l'atteinte audit droit, avait été attribuée. Il était présumé, d'une part, que le demandeur de l'injonction avait réuni des indices réels de l'atteinte à un droit d'auteur et, d'autre part, que la mesure demandée était proportionnée.

La Cour a tout d'abord rappelé que l'article 8, paragraphe 3, de la directive 2004/48/CE, lu en combinaison avec l'article 15, paragraphe 1, de la directive 2002/58/CE, ne s'oppose pas à ce que les États membres établissent une obligation de transmission à des personnes privées de données à caractère personnel pour permettre d'engager, devant les juridictions civiles, des poursuites contre les atteintes au droit d'auteur, mais n'oblige pas non plus ces États à prévoir une telle obligation. Cependant, il incombe aux autorités et aux juridictions des États membres non seulement d'interpréter leur droit national d'une manière conforme à ces mêmes directives, mais également de veiller à ne pas se fonder sur une interprétation de celles-ci qui entrerait en conflit avec lesdits droits fondamentaux ou avec les autres principes généraux du droit de l'Union, tels que le principe de proportionnalité (points 55 et 56).

À cet égard, elle a constaté que la législation nationale en question exigeait, notamment, que pour qu'une injonction de communiquer les données en cause pût être ordonnée, des indices réels d'atteinte à un droit de propriété intellectuelle sur une œuvre existaient, que les informations demandées fussent susceptibles de faciliter l'enquête sur la violation du droit d'auteur ou l'atteinte à un tel droit et que les raisons motivant cette injonction fussent d'un intérêt supérieur aux inconvénients ou aux autres préjudices qu'elle pouvait entraîner pour son destinataire ou à tout intérêt qui s'y opposait (point 58).

En conséquence, la Cour a conclu que les directives 2002/58/CE et 2004/48/CE ne s'opposent pas à une législation nationale, telle que celle en cause au principal, dans la mesure où cette législation permet, à la juridiction nationale saisie d'une demande d'injonction de communiquer des données à caractère personnel, introduite par une personne ayant qualité pour agir, de pondérer, en fonction des circonstances de chaque espèce et en tenant dûment compte des exigences résultant du principe de proportionnalité, les intérêts opposés en présence (point 61 et disp.).

3. Déréférencement de données à caractère personnel

Arrêt du 24 septembre 2019 (grande chambre), GC e.a. (Déréférencement de données sensibles) (C-136/17, ECLI:EU:C:2019:773)[42]

Dans cet arrêt, la Cour, réunie en grande chambre, a précisé les obligations de l'exploitant d'un moteur de recherche dans le cadre d'une demande de déréférencement portant sur des données sensibles.

Google avait refusé de faire droit aux demandes de quatre personnes de déréférencer, dans la liste de résultats affichée par le moteur de recherche en réponse à une recherche effectuée à partir de leur nom respectif, divers liens menant vers des pages web publiées par des tiers, notamment des articles de presse. Suite aux plaintes de ces quatre personnes, la Commission

[42] Cet arrêt a été présenté dans le Rapport annuel 2019, pp. 117 et 118.

nationale de l'informatique et des libertés (CNIL) (France) a refusé de mettre en demeure Google de procéder aux déréférencements demandés. Le Conseil d'État (France), saisi de l'affaire, a demandé à la Cour de préciser les obligations incombant à l'exploitant d'un moteur de recherche lors du traitement d'une demande de déréférencement en vertu de la directive 95/46/CE.

Premièrement, la Cour a rappelé que le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle, est interdit[43], sous réserve de certaines exceptions et dérogations. S'agissant du traitement de données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté, il ne peut en principe être effectué que sous le contrôle de l'autorité publique ou si des garanties appropriées et spécifiques sont prévues par le droit national[44] (points 39 et 40).

La Cour a jugé que l'interdiction et les restrictions relatives au traitement de ces catégories particulières de données s'appliquent à l'exploitant d'un moteur de recherche, à l'instar de tout autre responsable du traitement de données à caractère personnel. En effet, la finalité de ces interdictions et restrictions consiste à assurer une protection accrue à l'encontre de tels traitements qui, en raison de la sensibilité particulière de ces données, sont susceptibles de constituer une ingérence particulièrement grave dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel (points 42 à 44).

Toutefois, l'exploitant d'un moteur de recherche est responsable non pas du fait que des données à caractère personnel figurent sur une page web publiée par un tiers, mais du référencement de cette page. Dans ces conditions, l'interdiction et les restrictions relatives au traitement de données sensibles ne s'appliquent à cet exploitant qu'en raison de ce référencement et, donc, par l'intermédiaire d'une vérification à effectuer, sous le contrôle des autorités nationales compétentes, sur la base d'une demande formée par la personne concernée (points 46 et 47).

Deuxièmement, la Cour a considéré que, lorsque l'exploitant est saisi d'une demande de déréférencement relative à des données sensibles, il est en principe obligé, sous réserve de certaines exceptions, de faire droit à cette demande. S'agissant de ces exceptions, l'exploitant peut notamment refuser de faire droit à une telle demande lorsqu'il constate que les liens mènent vers des données manifestement rendues publiques par la personne concernée[45], à condition que le référencement de tels liens réponde aux autres conditions de licéité d'un traitement de données à caractère personnel et à moins que cette personne n'ait le droit de s'opposer audit référencement pour des raisons tenant à sa situation particulière[46] (points 65 et 69).

En tout état de cause, lorsqu'il est saisi d'une demande de déréférencement, l'exploitant d'un moteur de recherche doit vérifier si l'inclusion dans la liste de résultats du lien vers une page

43 Article 8, paragraphe 1, de la directive 95/46/CE et article 9, paragraphe 1, du règlement 2016/679.
44 Article 8, paragraphe 5, de la directive 95/46/CE et article 10 du règlement 2016/679.
45 Article 8, paragraphe 2, sous e), de la directive 95/46/CE et article 9, paragraphe 2, sous e), du règlement 2016/679.
46 Article 14, premier alinéa, sous a), de la directive 95/46/CE et article 21, paragraphe 1, du règlement 2016/679.

web sur laquelle des données sensibles sont publiées, qui est affichée à la suite d'une recherche effectuée à partir du nom de cette personne, s'avère strictement nécessaire pour protéger la liberté d'information des internautes potentiellement intéressés à avoir accès à cette page web au moyen d'une telle recherche. À cet égard, la Cour a souligné que, si les droits au respect de la vie privée et à la protection des données à caractère personnel prévalent, en règle générale, sur la liberté d'information des internautes, cet équilibre peut toutefois dépendre, dans des cas particuliers, de la nature de l'information en question et de sa sensibilité pour la vie privée de la personne concernée ainsi que de l'intérêt du public à disposer de cette information, lequel peut varier, notamment, en fonction du rôle joué par cette personne dans la vie publique (points 66 et 68).

Troisièmement, la Cour a jugé que, dans le cadre d'une demande de déréférencement portant sur des données relatives à une procédure judiciaire en matière pénale menée contre la personne concernée, qui se rapportent à une étape antérieure de cette procédure et ne correspondent plus à la situation actuelle, il appartient à l'exploitant d'un moteur de recherche d'apprécier si, eu égard à l'ensemble des circonstances de l'espèce, ladite personne a droit à ce que les informations en question ne soient plus, au stade actuel, liées à son nom par une liste de résultats, affichée à la suite d'une recherche effectuée à partir de ce nom. Cependant, même si tel n'est pas le cas en raison du fait que l'inclusion du lien en cause s'avère strictement nécessaire pour concilier les droits au respect de la vie privée et à la protection des données de la personne concernée avec la liberté d'information des internautes potentiellement intéressés, l'exploitant est tenu, au plus tard à l'occasion de la demande de déréférencement, d'aménager la liste de résultats de telle sorte que l'image globale qui en résulte pour l'internaute reflète la situation judiciaire actuelle, ce qui nécessite notamment que des liens vers des pages web comportant des informations à ce sujet apparaissent en premier lieu sur cette liste (points 77 et 78).

Arrêt du 24 septembre 2019 (grande chambre), Google (Portée territoriale du déréférencement) (C-507/17, ECLI:EU:C:2019:772)[47]

La Commission nationale de l'informatique et des libertés (CNIL) (France) a mis Google en demeure, lorsque cette société fait droit à une demande de déréférencement, de procéder à la suppression de la liste de résultats, affichée à la suite d'une recherche effectuée à partir du nom de la personne concernée, de liens menant vers des pages web comportant des données personnelles concernant cette dernière, sur toutes les extensions de nom du domaine de son moteur de recherche. À la suite du refus de Google de se conformer à cette mise en demeure, la CNIL a prononcé à l'encontre de cette société une sanction de 100 000 euros. Le Conseil d'État, saisi par Google, a demandé à la Cour de préciser la portée territoriale de l'obligation, pour l'exploitant d'un moteur de recherche, de mettre en œuvre le droit au déréférencement en application de la directive 95/46/CE.

Tout d'abord, la Cour a rappelé la possibilité pour les personnes physiques de faire valoir, sur le fondement du droit de l'Union, leur droit au déréférencement à l'encontre de l'exploitant d'un moteur de recherche disposant d'un ou de plusieurs établissements sur le territoire de l'Union,

[47] Cet arrêt a été présenté dans le Rapport annuel 2019, pp. 118 et 119.

indépendamment du fait que le traitement de données à caractère personnel (en l'occurrence, le référencement de liens vers des pages web sur lesquelles figurent des données personnelles concernant la personne qui se prévaut de ce droit) ait lieu ou non dans l'Union[48].

S'agissant de la portée du droit au déréférencement, la Cour a considéré que l'exploitant d'un moteur de recherche est tenu d'opérer le déréférencement non pas sur l'ensemble des versions de son moteur mais sur les versions de celui-ci correspondant à l'ensemble des États membres. Elle a relevé à cet égard que, si un déréférencement universel serait, compte tenu des caractéristiques d'Internet et des moteurs de recherche, de nature à rencontrer pleinement l'objectif du législateur de l'Union consistant à garantir un niveau élevé de protection des données personnelles dans l'ensemble de l'Union, il ne ressort toutefois aucunement du droit de l'Union[49] que, aux fins de la réalisation d'un tel objectif, le législateur aurait fait le choix de conférer au droit au déréférencement une portée qui dépasserait le territoire des États membres. En particulier, alors que le droit de l'Union institue des mécanismes de coopération entre autorités de contrôle des États membres pour parvenir à une décision commune, fondée sur une mise en balance entre le droit à la protection de la vie privée et des données personnelles, d'une part, et l'intérêt du public des différents États membres à accéder à une information, d'autre part, de tels mécanismes ne sont, actuellement, pas prévus pour ce qui concerne la portée d'un déréférencement en dehors de l'Union (points 62 et 73).

En l'état actuel du droit de l'Union, il incombe à l'exploitant d'un moteur de recherche de procéder au déréférencement demandé, non pas sur la seule version du moteur correspondant à l'État membre de résidence du bénéficiaire de ce déréférencement, mais sur les versions du moteur correspondant aux États membres, et ce, afin, notamment, d'assurer un niveau cohérent et élevé de protection dans l'ensemble de l'Union. Par ailleurs, il incombe à un tel exploitant de prendre, si nécessaire, des mesures suffisamment efficaces pour empêcher ou, à tout le moins, sérieusement décourager les internautes de l'Union d'avoir accès, le cas échéant à partir d'une version du moteur correspondant à un État tiers, aux liens faisant l'objet du déréférencement, et il appartient à la juridiction nationale de vérifier si les mesures adoptées par l'exploitant satisfont à cette exigence (point 70).

Enfin, la Cour a souligné que, si le droit de l'Union n'impose pas à l'exploitant d'un moteur de recherche d'opérer un déréférencement sur l'ensemble des versions de son moteur, il ne l'interdit pas non plus. Partant, une autorité de contrôle ou une autorité judiciaire d'un État membre reste compétente pour effectuer, à l'aune des standards nationaux de protection des droits fondamentaux, une mise en balance entre le droit de la personne concernée au respect de sa vie privée et à la protection de ses données personnelles, d'un côté, et le droit à la liberté d'information, de l'autre côté, et, au terme de cette mise en balance, pour enjoindre, le cas échéant, à l'exploitant de ce moteur de recherche de procéder à un déréférencement portant sur l'ensemble des versions dudit moteur (points 65 et 72).

---

48 Article 4, paragraphe 1, sous a), de la directive 95/46/CE, et article 3, paragraphe 1, du règlement 2016/679.

49 Articles 12, sous b), et 14, premier alinéa, sous a), de la directive 95/46/CE, et article 17, paragraphe 1, du règlement 2016/679.

4. Consentement de l'utilisateur d'un site Internet au stockage d'informations ou à l'accès à des informations par l'intermédiaire de cookies

Arrêt du 1er octobre 2019 (grande chambre), Planet49 (C-673/17, ECLI:EU:C:2019:801)[50]

Par cet arrêt, la Cour a jugé que le consentement au stockage d'informations ou à l'accès à des informations par l'intermédiaire de cookies installés sur l'équipement terminal de l'utilisateur d'un site Internet n'est pas valablement donné lorsque l'autorisation résulte d'une case cochée par défaut, et ce indépendamment du fait que les informations en cause constituent ou non des données à caractère personnel. En outre, la Cour a précisé que le fournisseur de services doit indiquer à l'utilisateur d'un site Internet la durée de fonctionnement des cookies ainsi que la possibilité ou non pour des tiers d'avoir accès à ces cookies.

Le litige au principal portait sur l'organisation d'un jeu promotionnel par Planet49 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[51], lue en combinaison avec la directive 95/46/CE[52], ainsi qu'avec le règlement général sur la protection des données[53]

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

---

50 Cet arrêt a été présenté dans le Rapport annuel 2019, pp. 120 et 121.

51 Articles 2, sous f), et 5, paragraphe 3, de la directive 2002/58, 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).

52 Article 2, sous h), de la directive 95/46/CE.

53 Article 6, paragraphe 1, sous a), du règlement 2016/679.

est désormais prévu par le règlement général sur la protection des données[54] 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 » (points 49, 52, 56 et 62).

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. Elle a ajouté que le fait pour un tel utilisateur d'activer le bouton de participation au jeu promotionnel en cause ne saurait suffire à considérer qu'il a valablement donné son consentement au placement de cookies (point 63).

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 (points 69 et 71).

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 (points 73 à 75 et 81).

VI. Autorités nationales de contrôle

1. Portée de l'exigence d'indépendance

Arrêt du 9 mars 2010 (grande chambre), Commission/Allemagne (C-518/07, ECLI:EU:C:2010:125) [55]

Par sa requête, la Commission avait demandé à la Cour de constater que la République fédérale d'Allemagne avait manqué aux obligations qui lui incombaient en vertu de l'article 28, paragraphe 1, second alinéa, de la directive 95/46/CE, en soumettant à la tutelle de l'État les

[54] IDEM.

[55] Cet arrêt a été présenté dans le Rapport annuel 2010, p. 34.

autorités de contrôle compétentes pour la surveillance du traitement des données à caractère personnel dans le secteur non public dans les différents Länder et en transposant ainsi de façon erronée l'exigence de « totale indépendance » des autorités chargées de garantir la protection de ces données.

La République fédérale d'Allemagne estimait, pour sa part, que l'article 28, paragraphe 1, second alinéa, de la directive 95/46/CE exige une indépendance fonctionnelle des autorités de contrôle, en ce sens que ces autorités doivent être indépendantes du secteur non public soumis à leur contrôle et qu'elles ne doivent pas être exposées à des influences extérieures. Or, selon elle, la tutelle de l'État exercée dans les Länder allemands constituait non pas une telle influence extérieure, mais un mécanisme de surveillance interne à l'administration, mis en œuvre par des autorités relevant du même appareil administratif que les autorités de contrôle et tenues, tout comme ces dernières, de remplir les objectifs de la directive 95/46/CE.

La Cour a jugé que la garantie d'indépendance des autorités nationales de contrôle prévue par la directive 95/46/CE vise à assurer l'efficacité et la fiabilité du contrôle du respect des dispositions en matière de protection des personnes physiques à l'égard du traitement des données à caractère personnel et doit être interprétée à la lumière de cet objectif. Elle n'a pas été établie afin de conférer un statut particulier à ces autorités elles-mêmes ainsi qu'à leurs agents mais en vue de renforcer la protection des personnes et des organismes concernés par leurs décisions, les autorités de contrôle devant en conséquence, lors de l'exercice de leurs missions, agir de manière objective et impartiale (point 25).

La Cour a considéré que ces autorités de contrôle compétentes pour la surveillance du traitement des données à caractère personnel dans le secteur non public doivent jouir d'une indépendance leur permettant d'exercer leurs missions sans influence extérieure. Cette indépendance exclut non seulement toute influence exercée par les organismes contrôlés, mais aussi toute injonction et toute autre influence extérieure, que cette dernière soit directe ou indirecte, qui pourraient remettre en cause l'accomplissement, par lesdites autorités, de leur tâche consistant à établir un juste équilibre entre la protection du droit à la vie privée et la libre circulation des données à caractère personnel. Le seul risque que les autorités de tutelle puissent exercer une influence politique sur les décisions des autorités de contrôle compétentes suffit pour entraver l'exercice indépendant de leurs missions. D'une part, il pourrait y avoir une « obéissance anticipée » de ces autorités eu égard à la pratique décisionnelle de l'autorité de tutelle. D'autre part, le rôle de gardiennes du droit à la vie privée qu'assument lesdites autorités de contrôle exige que leurs décisions, et donc elles-mêmes, soient au-dessus de tout soupçon de partialité. Selon la Cour, la tutelle de l'État exercée sur les autorités nationales de contrôle n'est donc pas compatible avec l'exigence d'indépendance (points 30, 36, 37 et disp.).

Arrêt du 16 octobre 2012 (grande chambre), Commission/Autriche (C-614/10, EU:C:2012:631)

Par sa requête, la Commission avait demandé à la Cour de constater que, en ne prenant pas toutes les dispositions nécessaires pour que la législation en vigueur en Autriche satisfasse au critère d'indépendance concernant la Datenschutzkommission (commission de protection des données) instituée en tant qu'autorité de contrôle de la protection des données à caractère

personnel, l'Autriche avait manqué aux obligations lui incombant en vertu de l'article 28, paragraphe 1, second alinéa, de la directive 95/46/CE.

La Cour a constaté un manquement de la part de l'Autriche, en considérant, en substance, que ne satisfait pas au critère d'indépendance de l'autorité de contrôle, posé par la directive 95/46/CE, l'État membre qui institue un cadre réglementaire en vertu duquel le membre administrateur de ladite autorité est un fonctionnaire de l'État assujetti à une tutelle de service, dont le bureau est intégré aux services du gouvernement national, et sur laquelle le chef du gouvernement national dispose d'un droit inconditionnel à l'information sur tous les aspects de la gestion de ladite autorité (point 66 et disp.).

La Cour a, tout d'abord, rappelé que les termes « en toute indépendance » figurant à l'article 28, paragraphe 1, second alinéa, de la directive 95/46/CE, impliquent que les autorités de contrôle doivent jouir d'une indépendance qui leur permette d'exercer leurs missions sans influence extérieure. À cet égard, le fait qu'une telle autorité dispose d'une indépendance fonctionnelle, en ce que ses membres sont indépendants et ne sont liés par aucune instruction dans l'exercice de leur fonction, ne suffit pas, à lui seul, à préserver l'autorité de contrôle de toute influence extérieure. Or, l'indépendance requise dans ce cadre vise à exclure non seulement l'influence directe, sous forme d'instructions, mais également toute forme d'influence indirecte susceptible d'orienter les décisions de l'autorité de contrôle. Par ailleurs, eu égard au rôle de gardiennes du droit à la vie privée qu'assument les autorités de contrôle, leurs décisions, et donc elles-mêmes, doivent être au-dessus de tout soupçon de partialité (points 41-43, 52).

La Cour a précisé que, afin de pouvoir satisfaire au critère d'indépendance énoncé à la disposition précitée de la directive 95/46/CE, une autorité nationale de contrôle ne doit pas disposer d'une ligne budgétaire autonome, à l'instar de celle prévue à l'article 43, paragraphe 3, du règlement (CE) n° 45/2001. Les États membres ne sont, en effet, pas obligés de reprendre dans leur législation nationale des dispositions analogues à celles du chapitre V du règlement (CE) n° 45/2001 afin de garantir une totale indépendance à leur(s) autorité(s) de contrôle et peuvent ainsi prévoir que, du point de vue du droit budgétaire, l'autorité de contrôle dépend d'un département ministériel déterminé. Cependant, l'attribution des moyens humains et matériels nécessaires à une telle autorité ne doit pas l'empêcher d'exercer ses missions « en toute indépendance » au sens de l'article 28, paragraphe 1, second alinéa, de la directive 95/46/CE (point 58).

Arrêt du 8 avril 2014 (grande chambre), Commission/Hongrie (C-288/12, EU:C:2014:237)[56]

Dans cette affaire, la Commission avait demandé à la Cour de constater que, en mettant fin de manière anticipée au mandat de l'autorité de contrôle de la protection des données à caractère personnel, la Hongrie avait manqué aux obligations lui incombant en vertu de la directive 95/46/CE.

[56] Cet arrêt a été présenté dans le Rapport annuel 2014, p. 62.

La Cour a jugé que manque aux obligations qui lui incombent en vertu de la directive 95/46/CE, un État membre qui met fin de manière anticipée au mandat de l'autorité de contrôle de la protection des données à caractère personnel (point 62, disp. 1).

En effet, selon la Cour, l'indépendance dont doivent jouir les autorités de contrôle compétentes pour la surveillance du traitement desdites données exclut notamment toute injonction et toute autre influence extérieure sous quelque forme que ce soit, qu'elle soit directe ou indirecte, qui seraient susceptibles d'orienter leurs décisions et qui pourraient ainsi remettre en cause l'accomplissement, par lesdites autorités, de leur tâche consistant à établir un juste équilibre entre la protection du droit à la vie privée et la libre circulation des données à caractère personnel (point 51).

La Cour a, en outre, rappelé que l'indépendance fonctionnelle ne suffisant pas, à elle seule, à préserver les autorités de contrôle de toute influence extérieure, le seul risque que les autorités de tutelle d'un État puissent exercer une influence politique sur les décisions des autorités de contrôle suffit pour entraver l'exercice indépendant des missions de celles-ci. Or, s'il était loisible à chaque État membre de mettre fin au mandat d'une autorité de contrôle avant le terme initialement prévu de celui-ci sans respecter les règles et les garanties préétablies à cette fin par la législation applicable, la menace d'une telle cessation anticipée qui planerait sur cette autorité tout au long de l'exercice de son mandat pourrait conduire à une forme d'obéissance de celle-ci au pouvoir politique, incompatible avec ladite exigence d'indépendance. De plus, dans une telle situation, l'autorité de contrôle ne pourrait être considérée comme pouvant opérer, en toute circonstance, au-dessus de tout soupçon de partialité (points 52-55).

2. Détermination du droit applicable et de l'autorité de contrôle compétente

Arrêt du 1er octobre 2015, Weltimmo (C-230/14, EU:C:2015:639)[57]

La Nemzeti Adatvédelmi és Információszabadság Hatóság (autorité nationale chargée de la protection des données et de la liberté de l'information, Hongrie) avait infligé une amende à la société Weltimmo, immatriculée en Slovaquie et exploitant des sites Internet d'annonces immobilières concernant des biens situés en Hongrie, au motif que celle-ci n'avait pas procédé à l'effacement des données à caractère personnel des annonceurs de ces sites, malgré leur demande en ce sens, et avait communiqué ces données à des agences de recouvrement afin d'obtenir le règlement de factures impayées. Selon l'autorité de contrôle hongroise, la société Weltimmo avait, ce faisant, violé la loi hongroise transposant la directive 95/46/CE.

Saisie d'un pourvoi en cassation, la Kúria (Cour suprême, Hongrie) a exprimé des doutes quant à la détermination du droit applicable et quant aux pouvoirs dont dispose l'autorité de contrôle hongroise au regard des articles 4, paragraphe 1, et 28 de la directive 95/46/CE. Elle a, en conséquence, adressé à la Cour plusieurs questions préjudicielles.

S'agissant du droit national applicable, la Cour a jugé que l'article 4, paragraphe 1, sous a), de la directive 95/46/CE permet l'application de la législation relative à la protection des données à

[57] Cet arrêt a été présenté dans le Rapport annuel 2015, p. 55.

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, même minime, dans le cadre de laquelle ce traitement est effectué. Afin de déterminer si tel est le cas, la juridiction de renvoi peut, notamment, tenir compte du fait, d'une part, que l'activité du responsable dudit traitement, dans le cadre de laquelle ce dernier a lieu, consiste dans l'exploitation de sites Internet d'annonces immobilières concernant des biens immobiliers situés sur le territoire de cet État membre et rédigés dans la langue de celui-ci et qu'elle est, par conséquent, principalement, voire entièrement, tournée vers ledit État membre. La juridiction de renvoi peut, d'autre part, également tenir compte du fait que ce responsable dispose d'un représentant dans ledit État membre, qui est chargé de recouvrer les créances résultant de cette activité ainsi que de le représenter dans des procédures administrative et judiciaire relatives au traitement des données concernées. La Cour a, en revanche, précisé qu'est dénuée de pertinence la question de la nationalité des personnes concernées par ce traitement de données (point 41, disp. 1).

S'agissant de la compétence et des pouvoirs de l'autorité de contrôle saisie de plaintes, conformément à l'article 28, paragraphe 4, de la directive 95/46/CE, la Cour a considéré que cette autorité peut examiner ces plaintes indépendamment du droit applicable et avant même de savoir quel est le droit national qui est applicable au traitement en cause (point 54). Cependant, si elle parvient à la conclusion que le droit d'un autre État membre est applicable, elle ne saurait imposer des sanctions en dehors du territoire de l'État membre dont elle relève. Dans une telle situation, il lui appartient, en exécution de l'obligation de coopération que prévoit l'article 28, paragraphe 6, de cette directive, de demander à l'autorité de contrôle de cet autre État membre de constater une éventuelle infraction à ce droit et d'imposer des sanctions si ce dernier le permet, en s'appuyant, le cas échéant, sur les informations qu'elle lui aura transmises (points 57, 60, disp. 2).

3. Pouvoirs des autorités nationales de contrôle

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

Dans cette affaire (voir également la rubrique III, intitulée « Transfert de données à caractère personnel vers des pays tiers »), la Cour a, notamment, jugé que les autorités nationales de contrôle sont compétentes pour contrôler les transferts de données à caractère personnel vers des pays tiers.

À cet égard, la Cour a tout d'abord constaté que les autorités nationales de contrôle disposent d'un large éventail de pouvoirs et que ceux-ci, énumérés de façon non exhaustive à l'article 28, paragraphe 3, de la directive 95/46/CE, constituent autant de moyens nécessaires à l'exécution de leurs tâches. Ainsi, lesdites autorités jouissent, notamment, de pouvoirs d'investigation, tels que celui de recueillir toutes les informations nécessaires à l'accomplissement de leur mission de contrôle, de pouvoirs effectifs d'intervention, tels que celui d'interdire temporairement ou définitivement un traitement de données, ou encore du pouvoir d'ester en justice (point 43).

S'agissant du pouvoir de contrôler les transferts de données à caractère personnel vers les pays tiers, la Cour a jugé qu'il ressort, certes, de l'article 28, paragraphes 1 et 6, de la directive 95/46/CE que les pouvoirs des autorités nationales de contrôle concernent les traitements de

données à caractère personnel effectués sur le territoire de l'État membre dont ces autorités relèvent, de sorte qu'elles ne disposent pas de pouvoirs, sur le fondement de cet article 28, à l'égard des traitements de telles données effectués sur le territoire d'un pays tiers (point 44).

Toutefois, 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 effectué sur le territoire d'un État membre. Par conséquent, les autorités nationales de contrôle étant, conformément à l'article 8, paragraphe 3, de la Charte et à l'article 28 de la directive 95/46/CE, chargées du contrôle du respect des règles de l'Union relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, chacune d'entre elles est investie de la compétence de vérifier si un transfert de ces données depuis l'État membre dont elle relève vers un pays tiers respecte les exigences posées par cette directive (points 45 et 47).

Arrêt du 5 juin 2018 (grande chambre), Wirtschaftsakademie Schleswig-Holstein (C-210/16, ECLI:EU:C:2018:388)

Dans cet arrêt (voir également la rubrique II.4., intitulée « Notion de "responsable du traitement des données à caractère personnel" ») portant, entre autres, sur l'interprétation des articles 4 et 28 de la directive 95/46/CE, la Cour s'est prononcée sur l'étendue des pouvoirs d'intervention dont disposent les autorités de contrôle à l'égard d'un traitement de données à caractère personnel qui implique la participation de plusieurs acteurs.

Ainsi, la Cour a jugé que lorsqu'une entreprise établie en dehors de l'Union européenne (telle que la société américaine Facebook) dispose de plusieurs établissements dans différents États membres, l'autorité de contrôle d'un État membre est habilitée à exercer les pouvoirs que lui confère l'article 28, paragraphe 3, de cette directive à l'égard d'un établissement de cette entreprise situé sur le territoire de cet État membre (en l'espèce Facebook Germany), alors même que, en vertu de la répartition des missions au sein du groupe, d'une part, cet établissement est chargé uniquement de la vente d'espaces publicitaires et d'autres activités de marketing sur le territoire dudit État membre et, d'autre part, la responsabilité exclusive de la collecte et du traitement des données à caractère personnel incombe, pour l'ensemble du territoire de l'Union européenne, à un établissement situé dans un autre État membre (en l'espèce Facebook Ireland) (point 64, disp. 2).

En outre, la Cour a précisé que lorsque l'autorité de contrôle d'un État membre entend exercer à l'égard d'un organisme établi sur le territoire de cet État membre les pouvoirs d'intervention visés à l'article 28, paragraphe 3, de la directive 95/46/CE en raison d'atteintes aux règles relatives à la protection des données à caractère personnel, commises par un tiers responsable du traitement de ces données et ayant son siège dans un autre État membre (en l'espèce Facebook Ireland), cette autorité de contrôle est compétente pour apprécier, de manière autonome par rapport à l'autorité de contrôle de ce dernier État membre (Irlande), la légalité d'un tel traitement de données et peut exercer ses pouvoirs d'intervention à l'égard de l'organisme établi sur son territoire sans préalablement appeler l'autorité de contrôle de l'autre État membre à intervenir (point 74, disp. 3).

VII. Application territoriale de la législation européenne

Arrêt du 13 mai 2014 (grande chambre), Google Spain et Google (C-131/12, EU:C:2014:317)

Dans cet arrêt (voir également les rubriques II.3., intitulée « Notion de "traitement de données à caractère personnel" », et IV.1., intitulée « Droit d'opposition au traitement des données à caractère personnel ("droit à l'oubli") »), la Cour s'est, également, prononcée sur le champ d'application territorial de la directive 95/46/CE.

Ainsi, la Cour a jugé qu'un traitement de données à caractère personnel est effectué dans le cadre des activités d'un établissement du responsable de ce traitement sur le territoire d'un État membre, au sens de la directive 95/46/CE, lorsque l'exploitant d'un moteur de recherche, bien qu'ayant son siège dans un État tiers, crée dans un État membre une succursale ou une filiale destinée à assurer la promotion et la vente des espaces publicitaires proposés par ce moteur et dont l'activité vise les habitants de cet État membre (points 55, 60, disp. 2).

En effet, dans de telles circonstances, les activités de l'exploitant du moteur de recherche et celles de son établissement situé dans un État membre, bien que distinctes, sont indissociablement liées dès lors que les activités relatives aux espaces publicitaires constituent le moyen pour rendre le moteur de recherche en cause économiquement rentable et que ce moteur est, en même temps, le moyen permettant l'accomplissement de ces activités (point 56).

VIII. Droit d'accès du public aux documents des institutions de l'Union européenne et protection des données à caractère personnel

Arrêt du 29 juin 2010 (grande chambre), Commission/Bavarian Lager (C-28/08 P, EU:C:2010:378)

Bavarian Lager, une société créée en vue d'importer de la bière allemande destinée aux débits de boissons du Royaume-Uni, n'avait pu vendre son produit, dans la mesure où un grand nombre d'exploitants de débits de boissons du Royaume-Uni étaient liés par des contrats d'achat exclusif qui les obligeaient à s'approvisionner en bière auprès de certaines brasseries.

En vertu de la réglementation du Royaume-Uni relative à la fourniture de bière (ci-après la « GBP »), les brasseries britanniques étaient tenues d'accorder aux gérants des pubs la possibilité d'acheter une bière provenant d'une autre brasserie à la condition qu'elle eût été conditionnée en baril. Or, la plupart des bières produites en dehors du Royaume-Uni ne pouvait être considérées comme des « bières conditionnées en baril », au sens de la GBP, et n'entrait donc pas dans le champ d'application de cette dernière. Estimant que ladite réglementation constituait une mesure d'effet équivalent à une restriction quantitative aux importations, Bavarian Lager avait déposé une plainte auprès de la Commission.

Au cours de la procédure en manquement engagée par la Commission à l'encontre du Royaume-Uni, des représentants des administrations communautaire et britannique, ainsi que des représentants de la confédération des brasseurs du marché commun (CBMC) avaient participé à une réunion qui s'était tenue le 11 octobre 1996. Après avoir été avertie par les autorités britanniques de la modification de la réglementation en cause visant à permettre la vente de bière embouteillée en tant que bière d'une provenance différente à l'instar de la bière conditionnée en baril, la Commission avait informé Bavarian Lager de la suspension de la procédure en manquement.

Bavarian Lager ayant déposé une demande en vue d'obtenir le procès-verbal complet de la réunion d'octobre 1996, avec la mention du nom de tous les participants, la Commission avait, par la suite, rejeté cette demande, par décision du 18 mars 2004, en invoquant notamment la protection de la vie privée de ces personnes, telle que garantie par le règlement relatif à la protection des données personnelles.

Bavarian Lager a ensuite introduit un recours auprès du Tribunal en demandant l'annulation de cette décision de la Commission. Par l'arrêt du 8 novembre 2007, le Tribunal a annulé la décision de la Commission, en estimant notamment que la seule inscription du nom des intéressés sur la liste des personnes ayant participé à une réunion au nom de l'entité qu'elles représentaient ne constituait pas une atteinte et ne mettait pas en danger la vie privée de ces personnes. La Commission, soutenue par le Royaume-Uni et le Conseil, a alors saisi la Cour d'un pourvoi contre cet arrêt du Tribunal.

La Cour a tout d'abord relevé que, lorsqu'une demande fondée sur le règlement (CE) nº 1049/2001[58], relatif à l'accès aux documents, vise à obtenir l'accès à des documents comprenant des données à caractère personnel, les dispositions du règlement (CE) nº 45/2001 deviennent intégralement applicables, y compris la disposition qui impose au destinataire du transfert de données à caractère personnel l'obligation de démontrer la nécessité de la divulgation de celles-ci ainsi que la disposition qui confère à la personne concernée la possibilité de s'opposer à tout moment, pour des raisons impérieuses et légitimes tenant à sa situation particulière, à ce que des données la concernant fassent l'objet d'un traitement (point 63).

Par la suite, la Cour a constaté que la liste des participants à une réunion tenue dans le cadre d'une procédure en manquement figurant dans le procès-verbal de ladite réunion contenait des données à caractère personnel, au sens de l'article 2, sous a), du règlement (CE) nº 45/2001, car les personnes qui ont pu participer à cette réunion pouvaient être identifiées (point 70).

Enfin, elle a conclu qu'en exigeant que, pour les personnes n'ayant pas donné leur consentement exprès à la diffusion des données personnelles les concernant contenues dans ce procès-verbal, soit établie la nécessité du transfert de ces données personnelles, la Commission s'était conformée aux dispositions de l'article 8, sous b), dudit règlement (point 77).

En effet, lorsque, dans le cadre d'une demande d'accès audit procès-verbal au titre du règlement (CE) nº 1049/2001, aucune justification expresse et légitime ni aucun argument

[58] Règlement (CE) nº 1049/2001 du Parlement européen et du Conseil, du 30 mai 2001, relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission (JO L 145 du 31.5.2001, p. 43).

convaincant n'est fourni afin de démontrer la nécessité du transfert de ces données personnelles, la Commission ne peut pas mettre en balance les différents intérêts des parties en cause. Elle ne peut pas non plus vérifier s'il existe des raisons de penser que ce transfert pourrait porter atteinte aux intérêts légitimes des personnes concernées, comme le prescrit l'article 8, sous b), du règlement (CE) nº 45/2001 (point 78)[59].

Arrêt du 16 juillet 2015, ClientEarth et PAN Europe/EFSA (C-615/13 P, EU:C:2015:489)

L'Autorité européenne de sécurité des aliments (EFSA) avait constitué un groupe de travail afin d'élaborer l'orientation pour indiquer la manière de mettre en œuvre l'article 8, paragraphe 5, du règlement (CE) nº 1107/2009[60], au sens duquel l'auteur d'une demande d'autorisation de mise sur le marché d'un produit phytopharmaceutique joint au dossier la documentation scientifique accessible, telle que déterminée par l'EFSA, validée par la communauté scientifique, concernant les effets secondaires sur la santé, sur l'environnement et sur les espèces non visées de la substance active et de ses métabolites pertinents.

Le projet d'orientation ayant été soumis à consultation publique, ClientEarth et Pesticide Action Network Europe (PAN Europe) avaient présenté des observations sur ce projet. Dans ce contexte, ils avaient adressé conjointement à l'EFSA une demande d'accès à plusieurs documents relatifs à la préparation du projet d'orientation, y compris les observations des experts externes.

L'EFSA a autorisé ClientEarth et PAN Europe à accéder, notamment, aux observations individuelles des experts externes sur le projet d'orientation. Elle a, toutefois, indiqué qu'elle avait occulté le nom de ces experts, conformément à l'article 4, paragraphe 1, sous b), du règlement (CE) nº 1049/2001 ainsi qu'à la législation de l'Union concernant la protection des données à caractère personnel, notamment le règlement (CE) nº 45/2001. Elle a fait valoir, à cet égard, que la divulgation du nom de ces experts correspondait à un transfert de données à caractère personnel, au sens de l'article 8 du règlement (CE) nº 45/2001, et que les conditions d'un tel transfert énoncées à cet article n'étaient pas réunies en l'espèce.

Dès lors, ClientEarth et PAN Europe ont introduit devant le Tribunal un recours tendant à l'annulation de ladite décision de l'EFSA. Le Tribunal ayant rejeté ce recours, ClientEarth et PAN Europe ont alors formé un pourvoi contre l'arrêt[61] du Tribunal devant la Cour.

En premier lieu, la Cour a relevé que du fait que l'information demandée permettrait de rattacher à tel ou tel expert déterminé une observation donnée, elle concernait des personnes physiques identifiées et, partant, constituaient un ensemble de données à caractère personnel, au sens de l'article 2, sous a), du règlement (CE) nº 45/2001. Les notions de « données à caractère personnel », au sens de l'article 2, sous a), du règlement (CE) nº 45/2001, et de « données relatives à la vie privée » ne se confondant pas, la Cour a considéré, en outre, que

59 Cet arrêt a été présenté dans le Rapport annuel 2010, p. 14.
60 Règlement (CE) nº 1107/2009 du Parlement européen et du Conseil, du 21 octobre 2009, concernant la mise sur le marché des produits phytopharmaceutiques et abrogeant les directives 79/117/CEE et 91/414/CEE du Conseil (JO L 309 du 24.11.2009, p. 1).
61 Arrêt du Tribunal du 13 septembre 2013, ClientEarth et PAN Europe/EFSA (T-214/11, EU:T:2013:483).

l'allégation de ClientEarth et de PAN Europe selon laquelle l'information litigieuse ne relevait pas de la vie privée des experts concernés, était inopérante (points 29, 32).

La Cour a examiné, en second lieu, l'argument de ClientEarth et de PAN Europe fondé sur l'existence d'un climat de méfiance envers l'EFSA, souvent accusée de partialité en raison du recours par celle-ci à des experts ayant des intérêts personnels dictés par leurs liens avec les milieux industriels, ainsi que sur la nécessité d'assurer la transparence du processus décisionnel de cette autorité. Cet argument était étayé par une étude faisant état des liens entretenus par la majorité des experts membres d'un groupe de travail de l'EFSA avec des groupes de pression industriels. À cet égard, la Cour a jugé que l'obtention de l'information litigieuse s'avérait nécessaire pour permettre de vérifier concrètement l'impartialité de chacun de ces experts dans l'accomplissement de sa mission scientifique au service de l'EFSA. La Cour a annulé en conséquence l'arrêt du Tribunal, en constatant que c'était à tort que le Tribunal avait jugé que l'argument susvisé de ClientEarth et de PAN Europe ne suffisait pas à démontrer la nécessité du transfert de l'information litigieuse (points 57-59).

En troisième lieu, aux fins d'apprécier la légalité de la décision litigieuse de l'EFSA, la Cour a examiné s'il existait, ou non, une raison de penser que le transfert aurait pu porter atteinte aux intérêts légitimes des personnes concernées. À cet égard, elle a constaté que l'allégation de l'EFSA selon laquelle la divulgation de l'information litigieuse aurait risqué de porter atteinte à la vie privée et à l'intégrité desdits experts relevait d'une considération générale non autrement étayée par un quelconque élément propre à l'espèce. La Cour a considéré, au contraire, qu'une telle divulgation aurait permis, par elle-même, de dissiper les soupçons de partialité en cause ou aurait offert aux experts éventuellement concernés l'occasion de contester, le cas échéant par les voies de recours disponibles, le bien-fondé de ces allégations de partialité. Au vu de ces éléments, la Cour a également annulé la décision de l'EFSA (points 69, 73).

* * *

Les arrêts figurant dans cette fiche sont indexés dans le Répertoire de jurisprudence sous les rubriques 1.04.03.07, 1.04.03.08, 1.04.03.10, 1.04.03.11, 2.04, 2.05.00, 4.11.01, 4.11.07., 4.11.11.01.