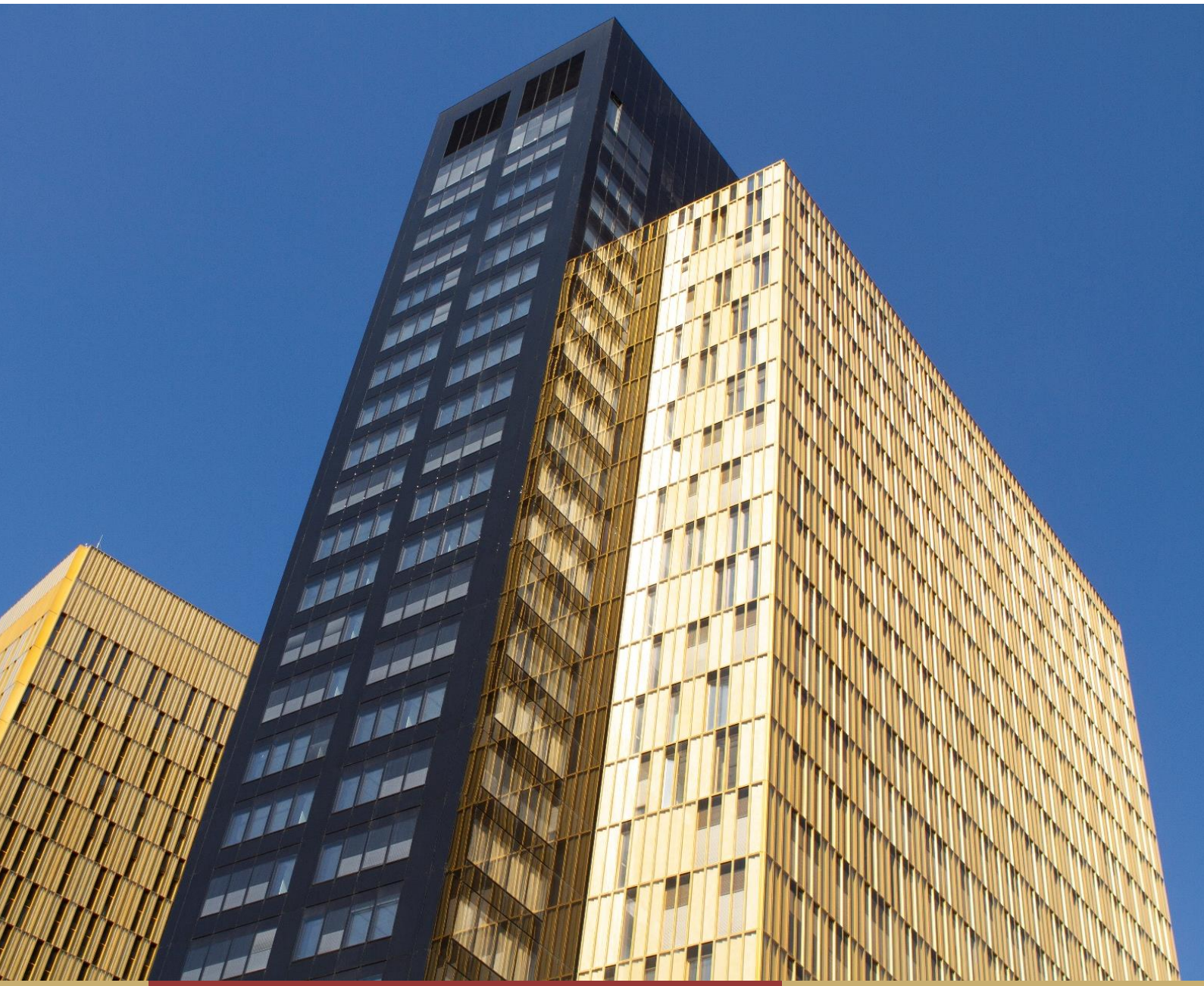
COUR DE JUSTICE
DE L'UNION EUROPÉENNE

FR



Fiche thématique

Protection des données à caractère personnel

Direction de la Recherche et documentation

curia.europa.eu

Avant-propos

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 le droit primaire, notamment par l'article 8 de la charte des droits fondamentaux de l'Union européenne (ci-après la « Charte ») ainsi que par l'article 16, paragraphe 1, du traité sur le fonctionnement de l'Union européenne (TFUE). 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.

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], abrogée depuis 2018, constituait à cet égard le principal acte juridique de l'Union en la matière.

La directive 2002/58/CE [2] est ensuite venue compléter la directive 95/46, 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, afin de tenir compte de nouvelles évolutions technologiques et commerciales, le législateur de l'Union a entamé, depuis 2017, un réexamen de cette directive [4], qui est, à ce jour, toujours en cours [5].

---

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 1995, L 281, p. 31), version consolidée au 20 novembre, abrogée à partir du 25 mai 2018 (voir note 6).

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 2002, L 201, p. 37), version consolidée au 19 décembre 2009.

3 La directive 2002/58 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 2006, L 105, 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 La Commission a présenté, le 10 janvier 2017, une proposition visant à remplacer cette directive par un règlement relatif à la vie privée et aux communications électroniques.

5 Le 10 février 2021, le Conseil de l'Union européenne a approuvé un mandat de négociation en vue de la révision des règles en matière de protection de la vie privée et de la confidentialité dans l'utilisation des services de communications électroniques permettant d'entamer les négociations avec le Parlement européen. Le texte de la proposition de règlement 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 » est disponible sous ce lien : *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6087_2021_INIT&from=EN*.

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 à caractère personnel (ci-après le « RGPD »), qui abroge la directive 95/46 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 dont les dispositions sont applicables depuis le 6 mai 2018.

En ce qui concerne le traitement des données à caractère personnel par les institutions et organes de l'UE, leur protection est notamment assurée, depuis le 11 décembre 2018, par le règlement (UE) 2018/1725 [8]. Dans l'intérêt d'une approche cohérente de la protection des données à caractère personnel dans l'ensemble de l'Union, ce règlement vise à aligner autant que possible les règles en la matière sur le régime établi par le RGPD.

Enfin, afin de faire face aux défis soulevés par les nouvelles technologies, le législateur de l'Union a, depuis 2020, lancé l'adoption de nouvelles mesures législatives [9] qui s'articulent avec les dispositions de droit de l'Union relatives à la protection des données à caractère personnel.

Compte tenu de la riche jurisprudence de la Cour de justice en matière de protection des données à caractère personnel, la présente fiche thématique vise à présenter une sélection d'arrêts fondateurs en la matière ainsi que d'arrêts ayant eu un apport important au développement de cette jurisprudence, avec un intérêt particulier porté sur les arrêts rendus par la grande chambre de la Cour. Plus particulièrement, cette fiche a vocation à couvrir tant la jurisprudence relative à la réglementation générale en matière de protection des données à caractère personnel, issue de l'interprétation de la directive 95/46 et du RGPD, que celle portant sur la réglementation sectorielle visant, notamment, le secteur des communications électroniques et le droit pénal. Par ailleurs, elle aspire à présenter une sélection d'arrêts portant sur des réglementations qui

---

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 2016, L 119, 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 2016, L 119, p. 89).

8 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) n°°45/2001 et la décision n° 1247/2002/CE (JO 2018, L 295, p. 39).

9 Dans ce cadre, il convient notamment de noter trois initiatives législatives : *i)* le règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données) (JO 2022, L 152, p 1) et le règlement (UE) 2023/2854 du Parlement européen et du Conseil du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données et modifiant le règlement (UE) 2017/2394 et la directive (UE) 2020/1828 (règlement sur les données) (JO 2023, L 2854, p. 1) ; *ii)* un paquet législatif sur les services et marchés numériques, composé du règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques) (JO 2022, L 277, p. 1) et du règlement 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828 (règlement sur les marchés numériques) (JO 2022, L 265, p. 1) ; et *iii)* la toute première proposition législative visant la création d'un cadre réglementaire en matière d'intelligence artificielle, qui s'est concrétisée par un règlement relatif à l'intelligence artificielle (JO 2024, L, 1689).

s’appliquent de façon transversale, tout en mettant d’emblée en exergue le rôle déterminant de la Charte dans le développement de la jurisprudence.

Table des matières

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*)

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 [10] et 259/2008 [11], 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 n^{o} 1290/2005 et sur celle du règlement n^{o} 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 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

[10] Règlement (CE) n° 1290/2005 du Conseil, du 21 juin 2005, relatif au financement de la politique agricole commune (JO 2005, L 209, 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 2013, L 347, p. 549).

[11] 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 2008, L 76, 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 2014, L 255, p. 59).

concernés au respect de leur vie privée, en général, et à la protection de leurs données à caractère personnel, en particulier.

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. 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.

Ainsi, la Cour a déclaré invalides certaines dispositions du règlement n° 1290/2005, ainsi que le règlement n° 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. 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.

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)

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 en droit autrichien.

Par leurs demandes de décisions préjudicielles, les juridictions irlandaise et autrichienne ont interrogé la Cour sur la validité de la directive 2006/24 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 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.

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. La directive 2006/24 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. 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. 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.

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 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.

Arrêt du 21 juin 2022 (grande chambre), Ligue des droits humains (C-817/19, EU:C:2022:491)

Les données PNR (Passenger Name Record) sont des informations de réservation stockées par les transporteurs aériens dans leurs systèmes de réservation et de contrôle des départs. La directive PNR [12] oblige ces transporteurs à transférer les données de tout passager empruntant un vol extra-UE, opéré entre un pays tiers et l'Union européenne, à l'unité d'information passagers (ci-après l'« UIP ») de l'État membre de destination ou de départ du vol concerné, afin de lutter contre le terrorisme et les formes graves de criminalité. En effet, les données PNR ainsi transférées font l'objet d'une évaluation préalable par l'UIP [13] et sont ensuite conservées en vue d'une éventuelle évaluation postérieure par les autorités compétentes de l'État membre concerné ou celles d'un autre État membre. Les États membres peuvent décider d'appliquer la directive également aux vols intra-UE [14].

La Cour constitutionnelle (Belgique) a été saisie par la Ligue des droits humains d'un recours en annulation contre la loi belge qui transpose en droit national tant la directive

[12] Directive (UE) 2016/681 du Parlement européen et du Conseil, du 27 avril 2016, relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière (JO 2016, L 119, p. 132) (ci-après la « directive PNR »).

[13] Cette évaluation préalable vise l'identification des personnes pour lesquelles est requis un examen plus approfondi par les autorités compétentes, compte tenu du fait que ces personnes peuvent être impliquées dans une infraction terroriste ou une forme grave de criminalité. Elle est effectuée de manière systématique et par des moyens automatisés, en confrontant les données PNR à des bases de données « utiles » ou en les traitant au regard de critères préétablis à l'article 6, paragraphe 2, sous a), et paragraphe 3, de la directive PNR.

[14] Faisant usage de la possibilité prévue par l'article 2 de la directive PNR.

PNR que la directive API [15]. Selon la requérante, cette loi méconnaît le droit au respect de la vie privée et à la protection des données à caractère personnel. Elle critique, d'une part, le caractère très large des données PNR et, d'autre part, le caractère général de la collecte, du transfert et du traitement de ces données. La loi porterait également atteinte à la libre circulation des personnes en ce qu'elle rétablirait indirectement des contrôles aux frontières en étendant le système PNR aux vols intra-UE et à des transports effectués par d'autres moyens à l'intérieur de l'Union.

Dans ce contexte, la Cour constitutionnelle belge a saisi la Cour à titre préjudiciel en lui posant des questions relatives, notamment, à la validité de la directive PNR.

Par son arrêt, rendu en grande chambre, la Cour confirme la validité de la directive PNR dans la mesure où celle-ci peut être interprétée en conformité avec la Charte.

À cet égard, la Cour juge que, dès lors que l'interprétation dégagée par la Cour des dispositions de la directive PNR à la lumière des droits fondamentaux garantis aux articles 7, 8 et 21 ainsi que de l'article 52, paragraphe 1, de la Charte [16] assure la conformité de cette directive avec ces articles, l'examen des questions posées n'a révélé aucun élément de nature à affecter la validité de ladite directive.

À titre liminaire, elle rappelle qu'un acte de l'Union doit être interprété, dans la mesure du possible, d'une manière qui ne remette pas en cause sa validité et en conformité avec l'ensemble du droit primaire et, notamment, avec les dispositions de la Charte, les États membres devant ainsi veiller à ne pas se fonder sur une interprétation de celle-ci qui entrerait en conflit avec les droits fondamentaux protégés par l'ordre juridique de l'Union ou avec les autres principes généraux reconnus dans cet ordre juridique. S'agissant de la directive PNR, la Cour précise que bon nombre de considérants et dispositions de celle-ci exigent une telle interprétation conforme, en mettant l'accent sur l'importance que le législateur de l'Union accorde, en se référant à un niveau élevé de protection des données, au plein respect des droits fondamentaux consacrés par la Charte.

La Cour constate que la directive PNR comporte des ingérences d'une gravité certaine dans les droits garantis aux articles 7 et 8 de la Charte, dans la mesure notamment où elle vise à instaurer un régime de surveillance continu, non ciblé et systématique, incluant l'évaluation automatisée de données à caractère personnel de l'ensemble des personnes faisant usage de services de transport aérien. Elle rappelle que la possibilité pour les États membres de justifier une telle ingérence doit être appréciée en mesurant

---

15 Directive 2004/82/CE du Conseil, du 29 avril 2004, concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers (JO 2004, L 261, p. 24) (ci-après la « directive API »). Cette directive régit la transmission aux autorités nationales compétentes, par les transporteurs aériens, d'informations préalables relatives aux passagers (telles que le numéro et le type du document de voyage utilisé ainsi que la nationalité), en vue d'améliorer les contrôles aux frontières et de lutter contre l'immigration illégale.

16 Aux termes de cette disposition, toute limitation de l'exercice des droits et des libertés reconnus par la Charte doit être prévue par la loi et respecter leur contenu essentiel. De plus, des limitations ne peuvent être apportées à ces droits et libertés que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et des libertés d'autrui.

sa gravité et en vérifiant que l'importance de l'objectif d'intérêt général poursuivi est en relation avec cette gravité.

La Cour conclut que le transfert, le traitement et la conservation des données PNR prévus par cette directive peuvent être considérés comme étant limités au strict nécessaire aux fins de la lutte contre les infractions terroristes et les formes graves de criminalité, à condition que les pouvoirs prévus par ladite directive fassent l'objet d'une interprétation restrictive. À cet égard, l'arrêt rendu ce jour précise, notamment, que :

- Le système établi par la directive PNR ne doit couvrir que les informations clairement identifiables et circonscrites dans les rubriques figurant dans l'annexe I de celle-ci, lesquelles sont en rapport avec le vol effectué et avec le passager concerné, ce qui implique, pour certaines rubriques figurant dans cette annexe, que seuls les renseignements visés expressément sont couverts [17].
- L'application du système établi par la directive PNR doit être limitée aux infractions terroristes et aux seules formes graves de criminalité présentant un lien objectif, à tout le moins indirect, avec le transport aérien des passagers. S'agissant de ces formes, l'application de ce système ne saurait être étendue à des infractions qui, bien qu'elles remplissent le critère prévu par cette directive relatif au seuil de gravité et qu'elles soient notamment visées à l'annexe II de celle-ci, relèvent de la criminalité ordinaire compte tenu des spécificités du système pénal national.
- L'éventuelle extension de l'application de la directive PNR à tout ou partie des vols intra-UE, qu'un État membre peut décider en faisant usage de la faculté prévue par cette directive, doit être limitée au strict nécessaire. À cet effet, elle doit pouvoir faire l'objet d'un contrôle effectif par une juridiction ou par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant. À cet égard, la Cour précise que :
    - Dans la seule situation où ledit État membre constate l'existence de circonstances suffisamment concrètes pour considérer qu'il fait face à une menace terroriste qui s'avère réelle et actuelle ou prévisible, l'application de cette directive à tous les vols intra-UE en provenance ou à destination dudit État membre, pour une durée limitée au strict nécessaire, mais renouvelable, n'excède pas les limites du strict nécessaire [18].

[17] Ainsi, notamment, « les informations relatives aux modes de paiement » (rubrique 6 de l'annexe) doivent être limitées aux modalités de paiement et à la facturation du billet d'avion, à l'exclusion de toute autre information sans rapport direct avec le vol, et les « remarques générales » (rubrique 12) ne peuvent concerner que les renseignements expressément énumérés dans cette rubrique, relatifs aux passagers mineurs.

[18] En effet, l'existence d'une telle menace est de nature, par elle-même, à établir une relation entre le transfert et le traitement des données concernées et la lutte contre le terrorisme. Dès lors, prévoir l'application de la directive PNR à tous les vols intra-UE en provenance ou à destination de l'État membre concerné, pour une durée limitée, n'excède pas les limites du strict nécessaire, la décision prévoyant cette application devant pouvoir faire l'objet d'un contrôle par une juridiction ou une entité administrative indépendante.

  - En l'absence d'une telle menace terroriste, l'application de ladite directive ne saurait s'étendre à l'ensemble des vols intra-UE, mais doit être limitée aux vols intra-UE relatifs notamment à certaines liaisons aériennes ou à des schémas de voyage ou encore à certains aéroports pour lesquels il existe, selon l'appréciation de l'État membre concerné, des indications de nature à justifier cette application. Le caractère strictement nécessaire de cette application aux vols intra-UE ainsi sélectionnés doit régulièrement être réexaminé, en fonction de l'évolution des conditions ayant justifié leur sélection.

- Aux fins de l'évaluation préalable des données PNR, qui a pour objectif d'identifier les personnes pour lesquelles est requis un examen plus approfondi avant leur arrivée ou leur départ et qui est, dans un premier temps, effectuée au moyen de traitements automatisés, l'UIP ne peut, d'une part, confronter ces données qu'aux seules bases de données concernant les personnes ou les objets recherchés ou faisant l'objet d'un signalement [19]. Ces bases de données doivent être non discriminatoires et exploitées, par les autorités compétentes, en rapport avec la lutte contre des infractions terroristes et des formes graves de criminalité présentant un lien objectif, à tout le moins indirect, avec le transport aérien des passagers. S'agissant, d'autre part, de l'évaluation préalable au regard de critères préétablis, l'UIP ne saurait utiliser des technologies d'intelligence artificielle dans le cadre de systèmes d'autoapprentissage (machine learning), susceptibles de modifier, sans intervention et contrôle humains, le processus d'évaluation et, en particulier, les critères d'évaluation sur lesquels se fonde le résultat de l'application de ce processus ainsi que la pondération de ces critères. Lesdits critères doivent être déterminés de manière à ce que leur application cible, spécifiquement, les individus à l'égard desquels pourrait peser un soupçon raisonnable de participation à des infractions terroristes ou à des formes graves de criminalité et à tenir compte tant des éléments « à charge » que des éléments « à décharge », tout en ne donnant pas lieu à des discriminations directes ou indirectes [20].

- Compte tenu du taux d'erreur inhérent à de tels traitements automatisés des données PNR et du nombre assez conséquent de résultats « faux positifs », ayant été obtenus à la suite de leur application au cours des années 2018 et 2019, l'aptitude du système établi par la directive PNR à réaliser les objectifs poursuivis

[19] À savoir les bases de données concernant les personnes ou les objets recherchés ou faisant l'objet d'un signalement au sens de l'article 6, paragraphe 3, sous a), de la directive PNR. En revanche, des analyses à partir de bases de données diverses pourraient prendre la forme d'une exploration de données (data mining) et seraient susceptibles de donner lieu à une utilisation disproportionnée de ces données, fournissant les moyens d'établir le profil précis des personnes concernées pour la seule raison que celles-ci ont l'intention de voyager par avion.

[20] Les critères préétablis doivent être ciblés, proportionnés et spécifiques, et être réexaminés à intervalles réguliers (article 6, paragraphe 4, de la directive PNR). L'évaluation préalable au regard de critères préétablis doit être réalisée de façon non discriminatoire. Selon l'article 6, paragraphe 4, quatrième phrase, de la directive PNR, les critères ne sont en aucun cas fondés sur l'origine raciale ou ethnique d'une personne, ses opinions politiques, sa religion ou ses convictions philosophiques, son appartenance à un syndicat, son état de santé, sa vie sexuelle ou son orientation sexuelle.

dépend essentiellement du bon fonctionnement de la vérification des résultats positifs, obtenus au titre de ces traitements, que l'UIP effectue, dans un deuxième temps, par des moyens non automatisés. À cet égard, les États membres doivent prévoir des règles claires et précises de nature à guider et à encadrer l'analyse effectuée par les agents de l'UIP en charge de ce réexamen individuel aux fins d'assurer le plein respect des droits fondamentaux consacrés aux articles 7, 8 et 21 de la Charte et, notamment, de garantir une pratique administrative cohérente au sein de l'UIP respectant le principe de non-discrimination. En particulier, ils doivent s'assurer que l'UIP établit des critères de réexamen objectifs permettant à ses agents de vérifier, d'une part, si et dans quelle mesure une concordance positive (hit) concerne effectivement un individu qui est susceptible d'être impliqué dans les infractions terroristes ou les formes graves de criminalité, ainsi que, d'autre part, le caractère non discriminatoire des traitements automatisés. Dans ce contexte, la Cour souligne encore que les autorités compétentes doivent s'assurer que l'intéressé peut comprendre le fonctionnement des critères d'évaluation préétablis et des programmes appliquant ces critères, de manière à ce qu'il puisse décider, en pleine connaissance de cause, s'il exerce ou non son droit à un recours juridictionnel. De même, dans le cadre d'un tel recours, le juge chargé du contrôle de la légalité de la décision adoptée par les autorités compétentes ainsi que, hormis les cas de menaces pour la sûreté de l'État, l'intéressé lui-même doivent pouvoir prendre connaissance tant de l'ensemble des motifs que des éléments de preuve sur la base desquels cette décision a été prise, y compris des critères d'évaluation préétablis et du fonctionnement des programmes appliquant ces critères.

- La communication et l'évaluation postérieures des données PNR, c'est-à-dire après l'arrivée ou le départ de la personne concernée, ne peuvent être effectuées que sur la base de circonstances nouvelles et d'éléments objectifs qui soit sont de nature à fonder un soupçon raisonnable d'implication de cette personne dans des formes graves de criminalité présentant un lien objectif, à tout le moins indirect, avec le transport aérien des passagers, soit permettent de considérer que ces données pourraient, dans un cas concret, apporter une contribution effective à la lutte contre des infractions terroristes présentant un tel lien. La communication des données PNR aux fins d'une telle évaluation postérieure doit, en principe, sauf en cas d'urgence dûment justifiée, être subordonnée à un contrôle préalable effectué soit par une juridiction soit par une autorité administrative indépendante, sur demande motivée des autorités compétentes, et ce indépendamment du point de savoir si cette demande a été introduite

avant ou après l'expiration du délai de six mois suivant le transfert de ces données à l'UIP [21].

Arrêt du 22 novembre 2022 (grande chambre), Luxembourg Business Registers (C-37/20 et C-601/20, EU:C:2022:912)

Aux fins de la lutte et de la prévention contre le blanchiment de capitaux et le financement du terrorisme, la directive antiblanchiment [22] impose aux États membres de tenir un registre contenant des informations sur les bénéficiaires effectifs [23] de sociétés et autres entités juridiques constituées sur leur territoire. À la suite d'une modification de cette directive par la directive 2018/843 [24], certaines de ces informations doivent être rendues accessibles dans tous les cas à tout membre du grand public. Conformément à la directive antiblanchiment ainsi modifiée (ci-après la « directive antiblanchiment modifiée »), la législation luxembourgeoise a institué un Registre des bénéficiaires effectifs (ci-après le « RBE ») destiné à conserver et à mettre à disposition une série d'informations sur les bénéficiaires effectifs des entités immatriculées dont l'accès est ouvert à toute personne.

Dans ce contexte, le tribunal d'arrondissement de Luxembourg a été saisi de deux affaires, introduites respectivement par WM et Sovim SA qui contestent le rejet, par Luxembourg Business Registers, gestionnaire du RBE, de leurs demandes visant à empêcher l'accès du grand public aux informations relatives, dans la première affaire, à WM en tant que bénéficiaire effectif d'une société civile immobilière et, dans la seconde affaire, au bénéficiaire effectif de Sovim SA. Dans le cadre de ces deux affaires, éprouvant des doutes notamment quant à la validité des dispositions du droit de l'Union qui instaurent le système d'accès public aux informations relatives aux bénéficiaires effectifs, le tribunal d'arrondissement de Luxembourg a saisi la Cour d'une question préjudicielle en appréciation de validité.

Par son arrêt, la Cour, réunie en grande chambre, déclare invalide la directive 2018/843 en tant qu'elle a modifié la directive antiblanchiment en ce sens que les États membres doivent veiller à ce que les informations sur les bénéficiaires effectifs des sociétés et

---

21 Aux termes de l'article 12, paragraphes 1 et 3, de la directive PNR, un tel contrôle n'est expressément prévu que pour les demandes de communication des données PNR introduites après le délai de six mois suivant le transfert de ces données à l'UIP.

22 Directive (UE) 2015/849 du Parlement européen et du Conseil, du 20 mai 2015, relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) nº 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission (JO 2015, L 141, p. 73, ci-après la « directive antiblanchiment »).

23 Aux termes de l'article 3, point 6, de la directive antiblanchiment, les bénéficiaires effectifs sont les personnes physiques qui, en dernier ressort, possèdent ou contrôlent le client et/ou la ou les personnes physiques pour lesquelles une transaction est exécutée, ou une activité réalisée.

24 Directive (UE) 2018/843 du Parlement européen et du Conseil, du 30 mai 2018, modifiant la directive (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme ainsi que les directives 2009/138/CE et 2013/36/UE (JO 2018, L 156, p. 43).

autres entités juridiques constituées sur leur territoire soient accessibles dans tous les cas à tout membre du grand public [25].

En premier lieu, la Cour constate que l'accès du grand public aux informations sur les bénéficiaires effectifs, prévu par la directive antiblanchiment modifiée, constitue une ingérence grave dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel, respectivement consacrés aux articles 7 et 8 de la Charte.

À cet égard, la Cour observe que, dès lors que les données concernées comportent des informations sur des personnes physiques identifiées, à savoir les bénéficiaires effectifs des sociétés et autres entités juridiques constituées sur le territoire des États membres, l'accès de tout membre du grand public à celles-ci affecte le droit fondamental au respect de la vie privée. En outre, leur mise à la disposition du grand public constitue un traitement de données à caractère personnel. Elle ajoute qu'une telle mise à la disposition du grand public constitue une ingérence dans les deux droits fondamentaux précités, quelle que soit l'utilisation ultérieure des informations communiquées.

S'agissant de la gravité de cette ingérence, la Cour relève que, dans la mesure où les informations mises à la disposition du grand public ont trait à l'identité du bénéficiaire effectif ainsi qu'à la nature et à l'étendue de ses intérêts effectifs détenus dans des sociétés ou d'autres entités juridiques, elles sont susceptibles de permettre de dresser un profil concernant certaines données personnelles d'identification, l'état de fortune de l'intéressé ainsi que les secteurs économiques, les pays et les entreprises spécifiques dans lesquels celui-ci a investi. De plus, ces informations deviennent accessibles à un nombre potentiellement illimité de personnes, de sorte qu'un tel traitement de données à caractère personnel est susceptible de permettre également à des personnes qui, pour des raisons étrangères à l'objectif poursuivi par cette mesure, cherchent à s'informer sur la situation notamment matérielle et financière d'un bénéficiaire effectif, d'accéder librement auxdites informations. Cette possibilité s'avère d'autant plus aisée lorsque les données peuvent être consultées sur Internet. Par ailleurs, les conséquences potentielles pour les personnes concernées résultant d'une éventuelle utilisation abusive de leurs données sont aggravées par le fait que, une fois mises à la disposition du grand public, elles peuvent non seulement être librement consultées, mais également être conservées et diffusées et qu'il devient, ainsi, d'autant plus difficile, voire illusoire, pour ces personnes de se défendre efficacement contre des abus.

En second lieu, au titre de l'examen de la justification de l'ingérence en cause, premièrement, la Cour note que, en l'espèce, le principe de légalité est respecté. En effet, la limitation de l'exercice des droits fondamentaux susmentionnés résultant de l'accès du grand public aux informations sur les bénéficiaires effectifs est prévue par un

[25] Invalidité de l'article 1er, point 15, sous c), de la directive 2018/843, modifiant l'article 30, paragraphe 5, premier alinéa, sous c), de la directive antiblanchiment.

acte législatif, à savoir la directive antiblanchiment modifiée. En outre, d'une part, cette directive précise que ces informations doivent être adéquates, exactes et actuelles, et énumère expressément certaines données auxquelles l'accès public doit être accordé. D'autre part, elle établit les conditions dans lesquelles les États membres peuvent prévoir des dérogations à un tel accès.

Deuxièmement, elle précise que l'ingérence en cause ne porte pas atteinte au contenu essentiel des droits fondamentaux garantis aux articles 7 et 8 de la Charte. S'il est vrai que la directive antiblanchiment modifiée ne contient pas une énumération exhaustive des données auxquelles tout membre du grand public doit être autorisé à accéder et que les États membres sont habilités à donner accès à des informations supplémentaires, il n'en reste pas moins que seules des informations adéquates sur les bénéficiaires effectifs et les intérêts effectifs détenus peuvent être obtenues, conservées et, partant, potentiellement rendues accessibles au public, ce qui exclut notamment des informations n'ayant pas de rapport adéquat avec les finalités de la directive antiblanchiment modifiée. Or, il n'apparaît pas que la mise à disposition du grand public des informations ayant un tel rapport porterait d'une quelconque manière atteinte au contenu essentiel des droits fondamentaux visés.

Troisièmement, la Cour souligne que, en prévoyant l'accès du grand public aux informations sur les bénéficiaires effectifs, le législateur de l'Union vise à prévenir le blanchiment de capitaux et le financement du terrorisme en mettant en place, au moyen d'une transparence accrue, un environnement moins susceptible d'être utilisé à ces fins, ce qui constitue un objectif d'intérêt général susceptible de justifier des ingérences, mêmes graves, dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte.

Quatrièmement, dans le cadre de l'examen du caractère apte, nécessaire et proportionné de l'ingérence en cause, la Cour constate que, certes, l'accès du grand public aux informations sur les bénéficiaires effectifs est apte à contribuer à la réalisation de cet objectif.

Toutefois, elle estime que cette ingérence ne saurait être considérée comme limitée au strict nécessaire. D'une part, la stricte nécessité de ladite ingérence ne peut pas être démontrée en s'appuyant sur le fait que le critère de l'« intérêt légitime » dont, selon la directive antiblanchiment, dans sa version antérieure à sa modification par la directive 2018/843, devait disposer toute personne souhaitant accéder aux informations sur les bénéficiaires effectifs, était difficile à mettre en œuvre et que son application pouvait conduire à des décisions arbitraires. En effet, l'existence éventuelle de difficultés pour définir précisément les hypothèses et les conditions dans lesquelles le public peut accéder aux informations sur les bénéficiaires effectifs ne saurait justifier que le législateur de l'Union prévoie l'accès du grand public à ces informations.

D'autre part, les explications figurant à la directive 2018/843 ne sauraient non plus établir la stricte nécessité de l'ingérence en cause [26]. Dans la mesure où, selon ces explications, l'accès du grand public aux informations sur les bénéficiaires effectifs est censé permettre un contrôle accru des informations par la société civile, notamment la presse ou les organisations de la société civile, la Cour relève que tant la presse que les organisations de la société civile présentant un lien avec la prévention et la lutte contre le blanchiment de capitaux et le financement du terrorisme ont un intérêt légitime à accéder aux informations concernées. Il en va de même des personnes souhaitant connaître l'identité des bénéficiaires effectifs d'une société ou d'une autre entité juridique du fait qu'elles sont susceptibles de conclure des transactions avec celles-ci, ou encore des institutions financières et des autorités impliquées dans la lutte contre des infractions en matière de blanchiment de capitaux ou de financement du terrorisme.

En outre, l'ingérence en cause ne présente pas non plus un caractère proportionné. À cet égard, la Cour constate que les règles matérielles encadrant cette ingérence ne répondent pas à l'exigence de clarté et de précision. En effet, la directive antiblanchiment modifiée prévoit l'accès de tout membre du grand public « au moins » aux données y visées et confère aux États membres la faculté à donner accès à des informations supplémentaires, comprenant, « au moins », la date de naissance ou les coordonnées du bénéficiaire effectif concerné. Or, par l'emploi de l'expression « au moins », cette directive autorise la mise à disposition du public de données qui ne sont pas suffisamment définies ni identifiables.

Par ailleurs, en ce qui concerne la mise en balance de la gravité de cette ingérence avec l'importance de l'objectif d'intérêt général visé, la Cour reconnaît que, compte tenu de son importance, cet objectif est susceptible de justifier des ingérences, mêmes graves, dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte.

Néanmoins, d'une part, la lutte contre le blanchiment de capitaux et le financement du terrorisme incombe prioritairement aux autorités publiques ainsi qu'aux entités, telles que les établissements de crédit ou les établissements financiers, qui, en raison de leurs activités, se voient imposer des obligations spécifiques en la matière. Pour ce motif, la directive antiblanchiment modifiée prévoit que les informations sur les bénéficiaires effectifs doivent être accessibles, dans tous les cas, aux autorités compétentes et aux cellules de renseignement financier, sans aucune restriction, ainsi qu'aux entités assujetties, dans le cadre de la vigilance à l'égard de la clientèle [27].

D'autre part, en comparaison avec le régime antérieur qui prévoyait, outre l'accès des autorités compétentes et de certaines entités aux informations sur les bénéficiaires effectifs, celui de toute personne ou organisation capable de démontrer un intérêt légitime, le régime introduit par la directive 2018/843 représente une atteinte

[26] Sont visées les explications figurant au considérant 30 de la directive 2018/843.
[27] Article 30, paragraphe 5, premier alinéa, sous a) et b), de la directive antiblanchiment modifiée.

considérablement plus grave aux droits fondamentaux garantis aux articles 7 et 8 de la Charte, sans que cette aggravation puisse être compensée par les bénéfices éventuels, qui pourraient résulter de ce dernier régime par rapport au premier, en ce qui concerne la lutte contre le blanchiment de capitaux et le financement du terrorisme.

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)

À la suite de l'arrêt Digital Rights Ireland et Seitlinger e.a. ayant déclaré invalide la directive 2006/24 (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.

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, 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, 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.

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.

La Cour a, en revanche, considéré que l'article 15, paragraphe 1, de la directive 2002/58 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.

II. Le traitement des données à caractère personnel au sens de la réglementation générale en la matière

1. Champ d'application de la réglementation générale

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 [28] 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 [29] 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. Dans ce contexte, elle a constaté qu'il ressortait de la décision

[28] 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 2004, L 235, p. 11).

[29] 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 2004, L 183, p. 83, et rectificatif JO 2005, L 255, p. 168).

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 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.

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.

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, 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.

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.

Dans cet arrêt, la Cour s'est, également, prononcée sur le champ d'application territorial de la directive 95/46.

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, 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.

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.

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, 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.

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, 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. De plus, le libellé même de cette disposition soustrait à l'application de la directive 95/46 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.

Arrêt du 16 janvier 2024 (grande chambre), Österreichische Datenschutzbehörde (C-33/22, EU:C:2024:46)

Afin d'examiner une éventuelle influence politique sur le Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (Office fédéral pour la protection de la Constitution et pour la lutte contre le terrorisme, Autriche) [30], le Nationalrat (Assemblée nationale, Autriche) a constitué une commission d'enquête (ci-après la « commission d'enquête BVT »). Cette commission a entendu WK en tant que témoin. En dépit de sa demande d'anonymisation, le compte rendu de son audition mentionnant ses nom et prénoms complets a été publié sur le site Internet du Parlament Österreich (Parlement autrichien). Faisant valoir qu'une telle divulgation de son identité était contraire au RGPD et à la législation autrichienne, WK a introduit une réclamation auprès de l'Österreichische Datenschutzbehörde (Autorité de la protection des données, Autriche) (ci-après la « Datenschutzbehörde »). Par décision du 18 septembre 2019, la

[30] Le 1er décembre 2021, cette entité est devenue la « Direktion Staatsschutz und Nachrichtendienst » (Direction pour la sécurité de l'État et des services de renseignements, Autriche).

Datenschutzbehörde s'est déclarée incompétente pour statuer sur la réclamation, en expliquant que le principe de la séparation des pouvoirs excluait que, en tant qu'organe du pouvoir exécutif, elle puisse contrôler la commission d'enquête BVT, qui relève du pouvoir législatif.

À la suite de la décision du Bundesverwaltungsgericht (tribunal administratif fédéral, Autriche), qui avait accueilli le recours de WK et avait annulé la décision de la Datenschutzbehörde, cette dernière a saisi la Cour administrative d'un recours en Revision contre la décision du tribunal administratif fédéral.

Dans ce contexte, la juridiction de renvoi a interrogé la Cour sur la question de savoir si les activités d'une commission d'enquête instituée par le parlement d'un État membre relèvent du champ d'application du RGPD et si ce règlement s'applique lorsque ces activités concernent la protection de la sécurité nationale.

En premier lieu, la Cour rappelle que l'article 2, paragraphe 2, sous a), du RGPD, qui prévoit que ce règlement ne s'applique pas au traitement de données à caractère personnel effectué dans le cadre d'une activité ne relevant pas du champ d'application du droit de l'Union, a pour seul objet d'exclure de son champ d'application les traitements effectués par les autorités étatiques dans le cadre d'une activité qui vise à préserver la sécurité nationale ou qui relève de la même catégorie. Ainsi, le seul fait qu'une activité soit propre à l'État ou à une autorité publique ne suffit pas à exclure automatiquement l'application du RGPD à une telle activité.

Cette interprétation, découlant de l'absence de distinction en fonction de l'identité de l'auteur du traitement concerné, est confirmée par l'article 4, point 7, du RGPD [31].

La Cour précise que la nature parlementaire de la commission d'enquête BVT n'implique pas que ses activités soient exclues du champ d'application du RGPD. En effet, l'exception prévue à l'article 2, paragraphe 2, sous a), de ce règlement se réfère seulement à des catégories d'activités qui, en raison de leur nature, ne relèvent pas du champ d'application du droit de l'Union et non à des catégories de personnes. Partant, la circonstance que le traitement de données à caractère personnel est effectué par une commission d'enquête mise en place par le parlement d'un État membre dans l'exercice de son pouvoir de contrôle du pouvoir exécutif ne permet pas, en tant que telle, d'établir que ce traitement est effectué dans le cadre d'une activité qui ne relève pas du champ d'application du droit de l'Union.

En second lieu, la Cour relève que, bien qu'il appartienne aux États membres de définir leurs intérêts essentiels de sécurité et d'arrêter les mesures propres à l'assurer [32], le seul fait qu'une mesure nationale a été prise aux fins de la protection de la sécurité nationale

[31] Celui-ci définit la notion de « responsable du traitement » comme se référant à « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ».

[32] Conformément à l'article 4, paragraphe 2, TUE.

ne saurait entraîner l'inapplicabilité du droit de l'Union et dispenser les États membres du respect nécessaire de ce droit. Or, l'exception prévue à l'article 2, paragraphe 2, sous a), du RGPD se réfère seulement à des catégories d'activités qui, en raison de leur nature, ne relèvent pas du champ d'application du droit de l'Union. À cet égard, la circonstance que le responsable du traitement est une autorité publique dont l'activité principale est d'assurer la sécurité nationale ne saurait suffire, en tant que telle, pour exclure du champ d'application du RGPD les traitements de données à caractère personnel qu'elle effectue dans le cadre de ses autres activités.

En l'occurrence, le contrôle politique effectué par la commission d'enquête BVT ne semble pas constituer, en tant que tel, une activité visant à préserver la sécurité nationale ou relevant de la même catégorie. Dès lors, sous réserve de vérification par la juridiction de renvoi, cette activité n'échappe pas au champ d'application du RGPD.

Cela étant, une commission d'enquête parlementaire peut avoir accès à des données à caractère personnel qui, pour des raisons tenant à la sécurité nationale, doivent bénéficier d'une protection particulière. À cet égard, des limitations aux droits et obligations découlant du RGPD peuvent être fixées, par la voie de mesures législatives, pour garantir notamment la sécurité nationale [33]. Pourraient ainsi être justifiées, sur ce fondement, des limitations concernant la collecte des données à caractère personnel, l'information des personnes concernées et leur accès auxdites données ou encore la divulgation de celles-ci, sans le consentement des personnes concernées, à des personnes autres que le responsable du traitement, à condition qu'elles respectent l'essence des libertés et droits fondamentaux des personnes concernées et constituent une mesure nécessaire et proportionnée dans une société démocratique.

La Cour note toutefois qu'il ne ressort pas des informations mises à sa disposition que la commission d'enquête BVT aurait allégué que la divulgation des données à caractère personnel de la personne concernée était nécessaire pour la sauvegarde de la sécurité nationale et fondée sur une mesure législative nationale prévue à cet effet, ce qui reste à vérifier, le cas échéant, par la juridiction de renvoi.

2. Notion de « données à caractère personnel »

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

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

[33] Selon l'article 23 du RGPD.

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.

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, 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.

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, 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.

Arrêt du 20 décembre 2017, Nowak (C-434/16, EU:C:2017:994)

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 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, 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, 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, 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.

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.

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. 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.

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.1., intitulée « Champ d'application de la réglementation générale »), 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.

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. 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.

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

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, 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.

Arrêt du 22 juin 2021 (grande chambre), Latvijas Republikas Saeima (Points de pénalité) (C-439/19, EU:C:2021:504)

B, une personne physique, s'est vu imposer des points de pénalité pour une ou plusieurs infractions routières. Ces points de pénalité ont été inscrits par la Ceļu satiksmes drošības direkcija (direction de la sécurité routière, Lettonie) (ci-après la « CSDD ») au registre national des véhicules et de leurs conducteurs.

En vertu de la réglementation lettonne sur la circulation routière [34], les informations relatives aux points de pénalité imposés aux conducteurs de véhicules inscrits dans ce registre sont accessibles au public et sont communiquées par la CSDD à toute personne qui en fait la demande, sans que celle-ci ait à justifier d'un intérêt spécifique à obtenir ces informations, y compris à des opérateurs économiques à des fins de réutilisation. S'interrogeant sur la légalité de cette réglementation, B a formé un recours constitutionnel devant la Latvijas Republikas Satversmes tiesa (Cour constitutionnelle, Lettonie), afin que celle-ci examine la conformité de cette réglementation avec le droit au respect de la vie privée.

La Cour constitutionnelle a considéré que, dans le cadre de son appréciation de ce droit constitutionnel, elle doit tenir compte du RGPD. Ainsi, elle a demandé à la Cour de clarifier la portée de plusieurs dispositions du RGPD dans le but de déterminer la compatibilité de la réglementation lettonne sur la circulation routière avec ce règlement.

Par son arrêt, prononcé en grande chambre, la Cour juge que le traitement des données à caractère personnel relatives aux points de pénalité constitue un « traitement de données à caractère personnel relatives aux condamnations pénales et aux infractions » [35], pour lequel le RGPD prévoit une protection accrue en raison de la sensibilité particulière des données en cause.

Dans ce cadre, elle observe, à titre liminaire, que les informations relatives aux points de pénalité sont des données à caractère personnel et que leur communication par la

---

34 Article 14[1], paragraphe 2, du Ceļu satiksmes likums (loi sur la circulation routière), du 1er octobre 1997 (Latvijas Vēstnesis, 1997, nº 274/276).

35 Article 10 du RGPD.

CSDD à des tiers constitue un traitement qui relève du champ d'application matériel du RGPD. En effet, ce champ d'application est très large, et ce traitement ne relève pas des exceptions à l'applicabilité de ce règlement.

Ainsi, d'une part, ce traitement n'est pas couvert par l'exception relative à la non-application du RGPD à un traitement effectué dans le cadre d'une activité ne relevant pas du droit de l'Union [36]. Cette exception est à considérer comme ayant pour seul objet d'exclure du champ d'application de ce règlement les traitements de données à caractère personnel effectués par les autorités étatiques dans le cadre d'une activité visant à préserver la sécurité nationale ou d'une activité pouvant être rangée dans la même catégorie. Ces activités couvrent, en particulier, celles visant à protéger les fonctions essentielles de l'État et les intérêts fondamentaux de la société. Or, les activités relatives à la sécurité routière ne poursuivent pas cet objectif et ne sauraient donc être rangées dans la catégorie des activités ayant pour but la préservation de la sécurité nationale.

D'autre part, la communication des données personnelles relatives aux points de pénalité n'est pas non plus un traitement couvert par l'exception prévoyant la non-application du RGPD aux traitements de données personnelles effectués par les autorités compétentes en matière pénale [37]. La Cour constate, en effet, que, dans l'exercice de ladite communication, la CSDD ne peut pas être considérée comme une telle « autorité compétente » [38].

Afin de déterminer si l'accès aux données à caractère personnel relatives aux infractions routières, telles que les points de pénalité, constitue un traitement de données à caractère personnel relatives à des « infractions » [39], qui jouissent d'une protection accrue, la Cour constate, en s'appuyant notamment sur la genèse du RGPD, que cette notion renvoie exclusivement aux infractions pénales. Toutefois, le fait que, dans le système juridique letton, les infractions routières sont qualifiées d'administratives n'est pas déterminant pour apprécier si ces infractions relèvent de la notion d'« infraction pénale » dans la mesure où il s'agit d'une notion autonome du droit de l'Union qui requiert, dans toute l'Union, une interprétation autonome et uniforme. Ainsi, après avoir rappelé les trois critères pertinents pour apprécier le caractère pénal d'une infraction, à savoir la qualification juridique de l'infraction en droit interne, la nature de l'infraction et le degré de sévérité de la sanction encourue, la Cour juge que les infractions routières en cause relèvent de la notion d'« infraction » au sens du RGPD. S'agissant des deux premiers critères, la Cour constate que, même si les infractions ne sont pas qualifiées de

36 Article 2, paragraphe 2, sous a), du RGPD.
37 Article 2, paragraphe 2, sous d), du RGPD.
38 Article 3, paragraphe 7, de la directive (UE) 2016/680 du Parlement européen et du Conseil, du 27 avril 2016, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données et abrogeant la décision-cadre 2008/977/JAI du Conseil (JO 2016, L 119, p. 89).
39 Article 10 du RGPD.

« pénales » en droit national, un tel caractère peut découler de la nature de l'infraction, et notamment de la finalité répressive poursuivie par la sanction que l'infraction est susceptible d'entraîner. Or, en l'espèce, l'attribution de points de pénalité pour des infractions routières, tout comme les autres sanctions que leur commission peut entraîner, poursuivent, entre autres, une telle finalité répressive. Quant au troisième critère, la Cour observe que seules des infractions routières d'une certaine gravité comportent l'imposition de points de pénalité, et que, partant, celles-ci sont susceptibles d'entraîner des sanctions d'une certaine sévérité. De plus, l'imposition de tels points se rajoute généralement à la sanction infligée, et la cumulation de ces points entraîne des conséquences juridiques pouvant même aller jusqu'à l'interdiction de conduire.

Arrêt du 5 décembre 2023 (grande chambre), Nacionalinis visuomenės sveikatos centras (C-683/21,* EU:C:2023:949*)

En 2020, afin de mieux gérer la pandémie de COVID-19, les autorités lituaniennes ont décidé d'organiser l'acquisition d'une application informatique mobile. Cette application devait contribuer à un suivi épidémiologique, en permettant d'enregistrer et de suivre des données des personnes exposées au virus de la COVID-19.

À cette fin, le Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos (Centre national de santé publique auprès du ministère de la Santé, Lituanie, ci-après le « CNSP »), chargé de cette acquisition, a contacté la société UAB « IT sprendimai sėkmei » (ci-après la « société ITSS »), lui demandant de procéder à la création d'une telle application mobile. Par la suite, des courriels portant notamment sur les questions qui devaient figurer dans cette application ont été adressés à cette société par les employés du CNSP.

Durant la période allant d'avril à mai 2020, l'application mobile créée par la société ITSS a été mise à la disposition du public. Par conséquent, 3 802 personnes en ont fait usage et ont fourni différentes données, demandées par cette application, les concernant. Cependant, en raison d'un défaut de financement, le CNSP n'a attribué à la société ITSS aucun marché public visant l'acquisition officielle de son application mobile et a mis fin à la procédure y relative.

Entre-temps, l'autorité nationale de contrôle a entamé une enquête portant sur le traitement des données personnelles résultant de l'utilisation de cette application. Par décision de cette autorité, adoptée à l'issue de l'enquête, les amendes administratives ont été imposées tant au CNSP qu'à la société ITSS considérée comme étant responsable conjoint du traitement.

Le CNSP a contesté cette décision devant le Vilniaus apygardos administracinis teismas (tribunal administratif régional de Vilnius, Lituanie). Nourrissant des doutes sur l'interprétation de plusieurs dispositions du RGPD, cette juridiction a saisi la Cour à titre préjudiciel.

Dans son arrêt, la Cour, réunie en grande chambre, apporte des précisions, entre autres, sur la notion de « traitement ». Elle indique, à cet égard, que l'utilisation de données à caractère personnel à des fins d'essais informatiques d'une application mobile constitue un traitement au sens du RGPD. Cependant, il en va autrement si de telles données avaient été rendues anonymes de telle sorte que la personne concernée par ces données n'est pas ou n'est plus identifiable ou s'il s'agit de données fictives qui ne se rapportent pas à une personne physique existante.

En effet, d'une part, la question de savoir si des données à caractère personnel sont utilisées en vue d'essais informatiques ou à une autre fin est sans incidence sur la qualification de l'opération de « traitement ». D'autre part, seul un traitement qui vise des données à caractère personnel peut être qualifié de « traitement » au sens du RGPD. Or, les données fictives ou anonymes ne constituent pas des données à caractère personnel.

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

Arrêt du 10 juillet 2018 (grande chambre), Jehovan todistajat (C-25/17, 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.

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.

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

Arrêt du 10 juillet 2018 (grande chambre), Jehovan todistajat (C-25/17, 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, 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.

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

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, 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.

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

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. 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).

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, afin que celles-ci soient justifiées dans son chef.

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, 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.

Arrêt du 5 décembre 2023 (grande chambre), Nacionalinis visuomenės sveikatos centras (C-683/21, EU:C:2023:949)

Dans cette affaire (voir également la rubrique II.3, intitulée « Notion de "traitement de données à caractère personnel" »), la Cour relève qu'une entité qui a chargé une entreprise de développer une application informatique mobile et qui a, dans ce contexte, participé à la détermination des finalités et des moyens du traitement des données à caractère personnel réalisé au moyen de cette application peut être considérée comme étant responsable du traitement [40]. Cette considération ne saurait être remise en cause par le fait que cette entité n'a pas procédé, elle-même, à des opérations de traitement de telles données, qu'elle n'a pas donné explicitement son accord pour la réalisation des opérations concrètes d'un tel traitement ou pour la mise à disposition du public de ladite application mobile et qu'elle n'a pas acquis cette même application mobile, à moins que, avant cette mise à disposition du public, ladite entité ne se soit expressément opposée à celle-ci et au traitement des données à caractère personnel qui en a résulté.

6. Notion de « responsable conjoint du traitement »

Arrêt du 5 décembre 2023 (grande chambre), Nacionalinis visuomenės sveikatos centras (C-683/21, EU:C:2023:949)

Dans cette affaire (voir également les rubriques II.3 et II.5, intitulées « Notion de "traitement de données à caractère personnel" » et « Notion de "responsable du traitement de données à caractère personnel" »), la Cour note que la qualification de deux entités comme étant responsables conjoints du traitement ne présuppose ni l'existence d'un accord entre ces entités sur la détermination des finalités et des moyens du traitement des données à caractère personnel ni l'existence d'un accord qui fixe les conditions relatives à la responsabilité conjointe du traitement. Certes, en vertu du RGPD [41], les responsables conjoints du traitement doivent, par voie d'accord entre eux, définir de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences de ce règlement. Toutefois, l'existence d'un tel accord constitue non pas une condition préalable pour que deux entités ou plus soient qualifiées de « responsables conjoints du traitement », mais une obligation que le RGPD impose aux

[40] Au sens de l'article 4, point 7, du RGPD.
[41] Article 26, paragraphe 1, du RGPD, lu à la lumière de son considérant 79.

responsables conjoints du traitement, une fois qualifiés de tels, aux fins d'assurer le respect des exigences de ce règlement pesant sur eux. Ainsi, cette qualification découle du seul fait que plusieurs entités ont participé à la détermination des finalités et des moyens du traitement.

Quant à la détermination conjointe, par les entités concernées, des finalités et des moyens du traitement, la Cour précise que leur participation à cette détermination peut prendre différentes formes et résulter tant de leur décision commune que de leurs décisions convergentes. Or, dans ce dernier cas, ces décisions doivent se compléter, de telle sorte que chacune d'elles ait un effet concret sur la détermination des finalités et des moyens du traitement.

7. Conditions de licéité d'un traitement de données à caractère personnel

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

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 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.

S'agissant de la notion de « nécessité » du traitement au sens de l'article 7, sous e), de la directive 95/46, 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 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, la conservation et le traitement de données à caractère personnel nominatives dans le cadre d'un tel registre à des fins statistiques.

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.

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 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 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, 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.

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 Slovenskej republiky (Cour suprême de la République slovaque) 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 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 soient satisfaites.

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.

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.

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, 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.

Arrêt du 11 novembre 2020, Orange Romania (C-61/19, EU:C:2020:901)

Orange România SA fournit des services de télécommunication mobile sur le marché roumain. Le 28 mars 2018, l'Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) (Autorité nationale de surveillance du traitement des données à caractère personnel, Roumanie) lui a infligé une amende pour avoir collecté et conservé les copies des titres d'identité de ses clients sans le consentement exprès de ces derniers.

D'après l'ANSPDCP, pendant la période allant du 1er au 26 mars 2018, Orange România a conclu des contrats de fourniture de services de télécommunication mobile qui contiennent une clause selon laquelle les clients ont été informés et ont consenti à la collecte et la conservation d'une copie de leur titre d'identité à des fins d'identification.

La case relative à cette clause a été cochée par le responsable du traitement avant la signature du contrat.

C'est dans ce contexte que le Tribunalul București (tribunal de grande instance de Bucarest, Roumanie) a demandé à la Cour de préciser les conditions dans lesquelles le consentement des clients au traitement de données à caractère personnel peut être considéré comme valable.

La Cour, rappelle, tout d'abord, que le droit de l'Union [42] prévoit une liste des cas dans lesquels un traitement de données à caractère personnel peut être considéré comme étant licite. En particulier, le consentement de la personne concernée doit être libre, spécifique, éclairé et univoque [43]. À cet égard, le consentement n'est pas valablement donné en cas de silence, de cases cochées par défaut ou d'inactivité.

De plus, lorsque le consentement de la personne concernée est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions, cette déclaration doit être présentée sous une forme compréhensible et aisément accessible et être formulée en des termes clairs et simples. Pour assurer à la personne concernée une véritable liberté de choix, les stipulations contractuelles ne doivent pas l'induire en erreur quant à la possibilité de conclure le contrat même si elle refuse de consentir au traitement de ses données.

La Cour précise que, Orange România étant le responsable du traitement des données à caractère personnel, elle doit être en mesure de démontrer la licéité du traitement de ces données et, partant, en l'occurrence, l'existence d'un consentement valable de ses clients. À cet égard, étant donné que les clients concernés ne paraissent pas avoir eux-mêmes coché la case relative à la collecte et la conservation des copies de leur titre d'identité, le seul fait que cette case a été cochée n'est pas de nature à établir une manifestation positive de leur consentement. Il appartient à la juridiction nationale d'effectuer les vérifications nécessaires à cette fin.

Il appartient également à la juridiction nationale, selon la Cour, d'apprécier si les stipulations contractuelles en cause étaient ou non susceptibles d'induire les clients concernés en erreur quant à la possibilité de conclure le contrat nonobstant un refus de consentir au traitement de ses données, en l'absence de précisions sur cette possibilité. De plus, en cas de refus d'un client de consentir au traitement de ses données, la Cour observe qu'Orange România exigeait que celui-ci déclare par écrit qu'il ne consentait ni à la collecte ni à la conservation de la copie de son titre d'identité. Selon la Cour, une telle exigence supplémentaire est de nature à affecter indûment le libre choix de s'opposer à cette collecte et à cette conservation. En tout état de cause, ladite société étant tenue d'établir que ses clients ont, par un comportement actif, manifesté leur consentement

[42] Article 7, de la directive 95/46 et article 6, du RGPD.
[43] Article 2, sous h), de la directive 95/46 et article 4, point 11, du RGPD.

au traitement de leurs données à caractère personnel, cette société ne saurait exiger d'eux qu'ils manifestent leur refus activement.

La Cour conclut donc qu'un contrat relatif à la fourniture de services de télécommunication qui contient une clause selon laquelle la personne concernée a été informée et a consenti à la collecte et à la conservation d'une copie de son titre d'identité à des fins d'identification n'est pas de nature à démontrer que cette personne a valablement donné son consentement à cette collecte et à cette conservation, lorsque la case se référant à cette clause a été cochée par le responsable du traitement des données avant la signature de ce contrat, lorsque les stipulations contractuelles de ce contrat sont susceptibles d'induire la personne concernée en erreur quant à la possibilité de conclure le contrat en question même si elle refuse de consentir au traitement de ses données, ou lorsque le libre choix de s'opposer à cette collecte et à cette conservation est affecté indûment par ce responsable, en ce qu'il exige de la personne concernée qu'elle remplisse, afin d'exprimer son refus de donner son consentement à ces traitements, un formulaire supplémentaire faisant état d'un tel refus.

Arrêt du 22 juin 2021 (grande chambre), Latvijas Republikas Saeima (Points de pénalité) (C-439/19, EU:C:2021:504)

Dans cet arrêt (voir également la rubrique II.3., intitulée « Notion de "traitement des données à caractère personnel" »), la Cour juge que le RGPD s'oppose à la réglementation faisant obligation à la Ceļu satiksmes drošības direkcija (direction de la sécurité routière, Lettonie) (ci-après la « CSDD ») de rendre accessibles au public les données relatives aux points de pénalité imposés aux conducteurs de véhicules pour des infractions routières, sans que la personne demandant l'accès ait à justifier d'un intérêt spécifique à les obtenir. Elle constate que la nécessité, notamment au regard de l'objectif d'amélioration de la sécurité routière invoqué par le gouvernement letton, d'une communication de données à caractère personnel relatives aux points de pénalité imposés pour des infractions routières n'est pas établie. En outre, selon la Cour, ni le droit du public d'accéder aux documents officiels ni le droit à la liberté d'information ne justifient une telle réglementation.

Dans ce contexte, la Cour souligne que l'amélioration de la sécurité routière, visée par la réglementation lettonne, constitue un objectif d'intérêt général reconnu par l'Union et que, partant, les États membres peuvent qualifier la sécurité routière de « mission d'intérêt public » [44]. Cependant, la nécessité du régime letton de communication de données à caractère personnel relatives aux points de pénalité pour assurer l'objectif visé n'est pas établie. En effet, d'une part, le législateur letton dispose d'une multitude de

[44] En vertu de l'article 6, paragraphe 1, sous e), du RGPD, un traitement des données à caractère personnel est licite lorsqu'il est « nécessaire à l'exécution d'une mission d'intérêt public [...] ».

voies d'actions qui lui auraient permis d'atteindre cet objectif par d'autres moyens moins attentatoires aux droits fondamentaux des personnes concernées. D'autre part, il convient de tenir compte de la sensibilité des données relatives aux points de pénalité et du fait que leur communication au public est susceptible de constituer une ingérence grave dans les droits au respect de la vie privée et à la protection des données à caractère personnel, dès lors qu'elle peut provoquer la désapprobation de la société et entraîner la stigmatisation de la personne concernée.

En outre, la Cour considère que, compte tenu de la sensibilité de ces données et de la gravité de cette ingérence dans ces deux droits fondamentaux, ces droits prévalent tant sur l'intérêt du public à avoir accès à des documents officiels, tels que le registre national des véhicules et de leurs conducteurs, que sur le droit à la liberté d'information.

Par ailleurs, pour des raisons identiques, la Cour juge que le RGPD s'oppose également à la réglementation lettonne dans la mesure où elle autorise la CSDD à communiquer les données relatives aux points de pénalité imposés aux conducteurs de véhicules pour des infractions routières à des opérateurs économiques afin que ces derniers puissent les réutiliser et les communiquer au public.

Enfin, la Cour précise que le principe de primauté du droit de l'Union s'oppose à ce que la juridiction de renvoi, saisie du recours contre la réglementation lettonne, qualifiée par la Cour d'incompatible avec le droit de l'Union, décide de maintenir les effets juridiques de cette réglementation jusqu'à la date de prononcé de son arrêt définitif.

III. Traitements des données à caractère personnel au sens de la réglementation sectorielle

1. Traitement des données à caractère personnel dans le secteur des communications électroniques

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

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 n'étaient pas 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.

Dans ce contexte, la Cour a précisé que si, dans son arrêt *Tele2 Sverige et Watson e.a.* [45], 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.

[45] 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).

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 ».

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

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

C'est sur cette toile de fond que l'Investigatory Powers Tribunal (tribunal chargé des pouvoirs d'enquête, Royaume-Uni) (Privacy International, C-623/17), le Conseil d'État (France) (La Quadrature du Net e.a., affaires jointes C-511/18 et C-512/18), ainsi que la Cour constitutionnelle (Belgique) (Ordre des barreaux francophones et germanophone e.a., C-520/18) ont été saisis de litiges concernant la légalité des réglementations adoptées par certains États membres dans ces domaines, prévoyant en particulier une obligation pour les fournisseurs de services de communications électroniques de transmettre à une autorité publique ou de conserver de manière généralisée ou indifférenciée les données des utilisateurs relatives au trafic et à la localisation.

Par deux arrêts prononcés en grande chambre, le 6 octobre 2020, la Cour juge, tout d'abord, que des réglementations nationales imposant aux fournisseurs de services de communications électroniques de conserver des données relatives au trafic et à la localisation ou encore de transmettre ces données aux autorités nationales de sécurité et de renseignement à cette fin relèvent du champ d'application de la directive 2002/58.

Ensuite, la Cour rappelle que la directive 2002/58 [46] ne permet pas que la dérogation à l'obligation de principe de garantir la confidentialité des communications électroniques et des données y afférentes et à l'interdiction de stocker ces données devienne la règle. Ceci implique que cette directive n'autorise les États membres à adopter, entre autres à

[46] Article 15, paragraphes 1 et 3, de la directive 2002/58.

des fins de sécurité nationale, des mesures législatives visant à limiter la portée des droits et des obligations prévus par cette directive, notamment l'obligation de garantir la confidentialité des communications et des données relatives au trafic [47], que dans le respect des principes généraux du droit de l'Union, parmi lesquels figure le principe de proportionnalité, et des droits fondamentaux garantis par la Charte [48].

Dans ce cadre, la Cour considère, d'une part, dans l'affaire Privacy International, que la directive 2002/58, lue à la lumière de la Charte, s'oppose à une réglementation nationale, imposant aux fournisseurs de services de communications électroniques, en vue de la sauvegarde de la sécurité nationale, la transmission généralisée et indifférenciée aux services de sécurité et de renseignement des données relatives au trafic et à la localisation. D'autre part, dans les affaires jointes La Quadrature du Net e.a., ainsi que dans l'affaire Ordre des barreaux francophones et germanophone e.a., la Cour estime que cette même directive s'oppose à des mesures législatives imposant aux fournisseurs de services de communications électroniques, à titre préventif, une conservation généralisée et indifférenciée des données relatives au trafic et à la localisation.

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

En revanche, la Cour estime que, dans des situations où l'État membre concerné fait face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, la directive 2002/58, lue à la lumière de la Charte, ne s'oppose pas au fait d'enjoindre aux fournisseurs de services de communications électroniques de conserver de manière généralisée et indifférenciée des données relatives au trafic et à la localisation. Dans ce contexte, la Cour précise que la décision prévoyant cette injonction, pour une période temporellement limitée au strict nécessaire, doit faire l'objet d'un contrôle effectif, soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, afin de vérifier l'existence d'une de ces situations ainsi que le respect des conditions et des garanties prévues. Dans ces mêmes conditions, ladite directive ne s'oppose pas non plus à l'analyse automatisée des données, notamment

47 Article 5, paragraphe 1, de la directive 2002/58.
48 En particulier, les articles 7, 8 et 11 ainsi que l'article 52, paragraphe 1, de la Charte.

celles relatives au trafic et à la localisation, de l'ensemble des utilisateurs de moyens de communications électroniques.

La Cour ajoute que la directive 2002/58, lue à la lumière de la Charte, ne s'oppose pas à des mesures législatives permettant le recours à une conservation ciblée, temporellement limitée au strict nécessaire, des données relatives au trafic et à la localisation, qui soit délimitée, sur la base d'éléments objectifs et non discriminatoires, en fonction de catégories de personnes concernées ou au moyen d'un critère géographique. De même, cette directive ne s'oppose pas à de telles mesures prévoyant une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une communication, pour autant que la durée de conservation est limitée au strict nécessaire, ni à celles prévoyant une telle conservation des données relatives à l'identité civile des utilisateurs des moyens de communications électroniques, les États membres n'étant dans ce dernier cas pas tenus de limiter temporellement la conservation. Au surplus, ladite directive ne s'oppose pas à une mesure législative permettant le recours à une conservation rapide des données dont disposent les fournisseurs de services dès lors que se présentent des situations dans lesquelles survient la nécessité de conserver lesdites données au-delà des délais légaux de conservation des données aux fins de l'élucidation d'infractions pénales graves ou d'atteintes à la sécurité nationale, lorsque ces infractions ou atteintes ont déjà été constatées ou lorsque leur existence peut être raisonnablement soupçonnée.

En outre, la Cour juge que la directive 2002/58, lue à la lumière de la Charte, ne s'oppose pas à une réglementation nationale imposant aux fournisseurs de services de communications électroniques de recourir au recueil en temps réel, notamment, des données relatives au trafic et à la localisation, lorsque ce recueil est limité aux personnes à l'égard desquelles il existe une raison valable de soupçonner qu'elles sont impliquées, d'une manière ou d'une autre, dans des activités de terrorisme et est soumis à un contrôle préalable, effectué soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, s'assurant qu'un tel recueil en temps réel n'est autorisé que dans la limite de ce qui est strictement nécessaire. En cas d'urgence, le contrôle doit intervenir dans de brefs délais.

Enfin, la Cour aborde la question du maintien des effets dans le temps d'une réglementation nationale jugée incompatible avec le droit de l'Union. À cet égard, elle juge qu'une juridiction nationale ne peut faire application d'une disposition de son droit national qui l'habilite à limiter dans le temps les effets d'une déclaration d'illégalité lui incombant, à l'égard d'une réglementation nationale imposant aux fournisseurs de services de communications électroniques une conservation généralisée et indifférenciée des données relatives au trafic et à la localisation, jugée incompatible avec la directive 2002/58, lue à la lumière de la Charte.

Ceci étant dit, afin de donner une réponse utile à la juridiction nationale, la Cour rappelle que l'admissibilité et l'appréciation d'éléments de preuve qui ont été obtenus par une conservation de données contraire au droit de l'Union, dans le cadre d'une

procédure pénale ouverte à l'encontre de personnes soupçonnées d'actes de criminalité grave, relèvent, en l'état actuel du droit de l'Union, du seul droit national. Toutefois, la Cour précise que la directive 2002/58, interprétée à la lumière du principe d'effectivité, exige que le juge pénal national écarte des éléments de preuve qui ont été obtenus par une conservation généralisée et indifférenciée des données relatives au trafic et à la localisation incompatible avec le droit de l'Union, dans le cadre d'une telle procédure pénale, si les personnes soupçonnées d'actes de criminalité ne sont pas en mesure de prendre efficacement position sur ces éléments de preuve.

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

Une procédure pénale a été engagée en Estonie contre H. K. des chefs de vol, d'utilisation de la carte bancaire d'un tiers et de violence à l'égard de personnes participant à une procédure en justice. H. K. a été condamnée pour ces infractions par un tribunal de première instance à une peine privative de liberté de deux ans. Cette décision a ensuite été confirmée en appel. Les procès-verbaux sur lesquels s'appuie la constatation de ces infractions ont été établis, notamment, sur la base de données à caractère personnel générées dans le cadre de la fourniture de services de communications électroniques. La Riigikohus (Cour suprême, Estonie), devant laquelle un pourvoi en cassation a été introduit par H. K., a émis des doutes quant à la compatibilité avec le droit de l'Union [49] des conditions dans lesquelles les services d'enquête ont eu accès à ces données.

Ces doutes concernent, en premier lieu, la question de savoir si la durée de la période pour laquelle les services d'enquête ont eu accès aux données constitue un critère permettant d'évaluer la gravité de l'ingérence que constitue cet accès dans les droits fondamentaux des personnes concernées. Ainsi, lorsque cette période est très brève ou que la quantité de données recueillies est très limitée, la juridiction de renvoi s'est interrogée sur le fait de savoir si l'objectif de lutte contre la criminalité en général, et pas seulement de lutte contre la criminalité grave, est susceptible de justifier une telle ingérence. En second lieu, la juridiction de renvoi a nourri des doutes quant à la possibilité de considérer le ministère public estonien, compte tenu des différentes missions qui lui sont confiées par la réglementation nationale, comme une autorité administrative « indépendante » au sens de l'arrêt Tele2 Sverige et Watson e.a. [50], susceptible d'autoriser l'accès de l'autorité chargée de l'enquête aux données concernées.

[49] Plus précisément, avec l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte.

[50] Arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a. (C-203/15 et C-698/15, EU:C:2016:970, point 120).

Par son arrêt, prononcé en grande chambre, la Cour juge que la directive 2002/58, lue à la lumière de la Charte, s'oppose à une réglementation nationale permettant l'accès des autorités publiques à des données relatives au trafic ou à des données de localisation, susceptibles de fournir des informations sur les communications effectuées par un utilisateur d'un moyen de communication électronique ou sur la localisation des équipements terminaux qu'il utilise et de permettre de tirer des conclusions précises sur sa vie privée, à des fins de prévention, de recherche, de détection et de poursuite d'infractions pénales, sans que cet accès soit circonscrit à des procédures visant à la lutte contre la criminalité grave ou à la prévention de menaces graves contre la sécurité publique. Selon la Cour, la durée de la période pour laquelle l'accès à ces données est sollicité et la quantité ou la nature des données disponibles pour une telle période n'a pas d'incidence à cet égard. En outre, la Cour considère que cette même directive, lue à la lumière de la Charte, s'oppose à une réglementation nationale donnant compétence au ministère public pour autoriser l'accès d'une autorité publique aux données relatives au trafic et aux données de localisation afin de mener une instruction pénale.

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

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

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

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

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

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

Dans la présente affaire, la demande de décision préjudicielle a été présentée par la Supreme Court (Cour suprême, Irlande) dans le cadre d'une procédure civile engagée par une personne condamnée à la réclusion à perpétuité pour un meurtre commis en Irlande. Cette dernière contestait la compatibilité avec le droit de l'Union de certaines dispositions de la loi nationale relative à la conservation des données générées dans le cadre des communications électroniques. En vertu de cette loi, des données relatives au trafic et des données de localisation afférentes à des appels téléphoniques de l'inculpé

avaient été conservées par les fournisseurs de services de communications électroniques et rendues accessibles aux autorités de police. Les doutes émis par la juridiction de renvoi portaient notamment sur la compatibilité avec la directive 2002/58, lue à la lumière de la Charte, d'un régime de conservation généralisée et indifférenciée de ces données, en lien avec la lutte contre la criminalité grave.

Par son arrêt, prononcé en grande chambre, la Cour confirme, tout en précisant sa portée, la jurisprudence issue de l'arrêt La Quadrature du Net e.a. [51], en rappelant que la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation afférentes aux communications électroniques n'est pas autorisée aux fins de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique. Elle confirme également la jurisprudence issue de l'arrêt Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques) [52], notamment quant à l'obligation de subordonner l'accès des autorités nationales compétentes auxdites données conservées à un contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante, à l'égard d'un fonctionnaire de police.

La Cour juge, en premier lieu, que la directive 2002/58, lue à la lumière de la Charte, s'oppose à des mesures législatives prévoyant, à titre préventif, aux fins de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation. En effet, compte tenu, d'une part, des effets dissuasifs sur l'exercice des droits fondamentaux [53] que cette conservation est susceptible d'entraîner et, d'autre part, de la gravité de l'ingérence qu'elle comporte, une telle conservation doit constituer l'exception et non la règle au système mis en place par cette directive, de manière à ce que ces données ne puissent faire l'objet d'une conservation systématique et continue. La criminalité, même particulièrement grave, ne peut être assimilée à une menace pour la sécurité nationale, dans la mesure où une telle assimilation serait susceptible d'introduire une catégorie intermédiaire entre la sécurité nationale et la sécurité publique, aux fins d'appliquer à la seconde les exigences inhérentes à la première.

En revanche, la directive 2002/58, lue à la lumière de la Charte, ne s'oppose pas à des mesures législatives prévoyant, aux fins de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation ciblée des données relatives au trafic et des données de localisation qui soit délimitée, sur la base d'éléments objectifs et non discriminatoires, en fonction de catégories de personnes concernées ou au moyen d'un critère géographique, pour une période temporellement

[51] Arrêt du 6 octobre 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 et C-520/18, EU:C:2020:791).
[52] Arrêt du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques) (C-746/18, EU:C:2021:152).
[53] Consacrés aux articles 7 à 11 de la Charte.

limitée au strict nécessaire, mais renouvelable. Elle ajoute qu'une telle mesure de conservation visant des lieux ou des infrastructures fréquentés régulièrement par un nombre très élevé de personnes ou des lieux stratégiques, tels que des aéroports, des gares, des ports maritimes ou des zones de péages, est susceptible de permettre aux autorités compétentes d'obtenir des informations sur la présence, dans ces lieux ou zones géographiques, des personnes y utilisant un moyen de communication électronique et d'en tirer des conclusions sur leur présence et leur activité dans lesdits lieux ou zones géographiques aux fins de la lutte contre la criminalité grave. En tout état de cause, l'existence éventuelle de difficultés pour définir précisément les hypothèses et les conditions dans lesquelles une conservation ciblée peut être effectuée ne saurait justifier que des États membres prévoient une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation.

Cette directive, lue à la lumière de la Charte, ne s'oppose pas non plus à des mesures législatives prévoyant, aux mêmes fins, une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion, pour une période temporellement limitée au strict nécessaire, ainsi que des données relatives à l'identité civile des utilisateurs de communications électroniques. S'agissant de ce dernier aspect, la Cour précise plus particulièrement que ni la directive 2002/58 ni aucun autre acte du droit de l'Union ne s'opposent à une législation nationale, ayant pour objet la lutte contre la criminalité grave, en vertu de laquelle l'acquisition d'un moyen de communication électronique, tel qu'une carte SIM prépayée, est subordonnée à la vérification de documents officiels établissant l'identité civile de l'acheteur et à l'enregistrement, par le vendeur, des informations en résultant, le vendeur étant le cas échéant tenu de donner accès à ces informations aux autorités nationales compétentes.

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

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

En outre, la Cour précise qu'autoriser, aux fins de la lutte contre la criminalité grave, un accès à des telles données conservées de manière généralisée et indifférenciée, pour faire face à une menace grave pour la sécurité nationale, serait contraire à la hiérarchie des objectifs d'intérêt général pouvant justifier une mesure prise au titre de la directive 2002/58. En effet, ceci reviendrait à permettre que l'accès puisse être justifié par un objectif d'une importance moindre que celui ayant justifié la conservation, à savoir la sauvegarde de la sécurité nationale, risquant ainsi de priver de tout effet utile l'interdiction de procéder à une conservation généralisée et indifférenciée aux fins de la lutte contre la criminalité grave.

En deuxième lieu, la Cour décide que la directive 2002/58, lue à la lumière de la Charte, s'oppose à une réglementation nationale, en vertu de laquelle le traitement centralisé des demandes d'accès à des données conservées par les fournisseurs de services de communications électroniques, émanant de la police dans le cadre de la recherche et de la poursuite d'infractions pénales graves, incombe à un fonctionnaire de police, même lorsque celui-ci est assisté par une unité instituée au sein de la police jouissant d'un certain degré d'autonomie dans l'exercice de sa mission et dont les décisions peuvent faire ultérieurement l'objet d'un contrôle juridictionnel. En effet, d'une part, un tel fonctionnaire ne remplit pas les exigences d'indépendance et d'impartialité qui s'imposent à une autorité administrative exerçant le contrôle préalable des demandes d'accès aux données émanant des autorités nationales compétentes, dans la mesure où il n'a pas la qualité de tiers par rapport à ces autorités. D'autre part, si la décision d'un tel fonctionnaire peut faire l'objet d'un contrôle juridictionnel exercé a posteriori, ce contrôle ne peut pas se substituer à un contrôle indépendant et, sauf cas d'urgence dûment justifiée, préalable.

En troisième lieu, enfin, la Cour confirme sa jurisprudence selon laquelle le droit de l'Union s'oppose à ce qu'une juridiction nationale limite dans le temps les effets d'une déclaration d'invalidité qui lui incombe, en vertu du droit national, à l'égard d'une législation nationale imposant aux fournisseurs de services de communications électroniques une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, en raison de l'incompatibilité de cette législation avec la directive 2002/58. Cela étant, la Cour rappelle que l'admissibilité des éléments de preuve obtenus au moyen d'une telle conservation relève, conformément au principe

d'autonomie procédurale des États membres, du droit national, sous réserve du respect notamment des principes d'équivalence et d'effectivité.

Arrêt du 20 septembre 2022 (grande chambre), VD et SR (C-339/20 et C-397/20, EU:C:2022:703)

À la suite d'une enquête de l'Autorité des marchés financiers (AMF, France), des procédures pénales ont été engagées contre VD et SR, deux personnes physiques accusées de délits d'initiés, de recel de délits d'initiés, de complicité, de corruption et de blanchiment. Dans le cadre de cette enquête, l'AMF avait utilisé des données à caractère personnel issues d'appels téléphoniques de VD et SR, générées sur le fondement du code des postes et des communications électroniques français, dans le cadre de la fourniture de services de communications électroniques.

Dans la mesure où leur mise en examen respective était fondée sur les données de trafic fournies par l'AMF, VD et SR ont chacun saisi la cour d'appel de Paris (France) d'un recours, en invoquant, notamment, un moyen tiré de la violation de l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte. Plus particulièrement, s'appuyant sur la jurisprudence issue de l'arrêt Tele2 Sverige et Watson e.a. [54], VD et SR contestaient le fait que l'AMF se soit fondée, pour procéder à la collecte desdites données, sur les dispositions nationales en cause, alors que, selon eux, ces dispositions, d'une part, n'étaient pas conformes au droit de l'Union, pour autant qu'elles prévoyaient une conservation généralisée et indifférenciée des données de connexion et, d'autre part, ne fixaient aucune limite au pouvoir pour les enquêteurs de l'AMF de se faire communiquer les données conservées.

Par deux arrêts du 20 décembre 2018 et du 7 mars 2019, la cour d'appel de Paris a rejeté les recours de VD et SR. Pour écarter le moyen susmentionné, les juges de fond ont pris appui, notamment, sur le fait que le règlement relatif aux abus de marché [55] permet aux autorités compétentes de se faire remettre, dans la mesure où le droit national l'autorise, les enregistrements existants des données relatives au trafic détenus par les opérateurs de services de communications électroniques, lorsqu'il existe des raisons de suspecter une violation de l'interdiction des opérations d'initiés et que de tels enregistrements peuvent se révéler pertinents pour l'enquête relative à cette violation.

VD et SR ont alors formé un pourvoi devant la Cour de cassation (France), la juridiction de renvoi dans les présentes affaires.

---

54 Arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a. (C-203/15 et C-698/15, EU:C:2016:970).

55 Règlement (UE) nº 596/2014 du Parlement européen et du Conseil, du 16 avril 2014, sur les abus de marché (règlement relatif aux abus de marché) et abrogeant la directive 2003/6/CE du Parlement européen et du Conseil et les directives 2003/124/CE, 2003/125/CE et 2004/72/CE de la Commission (JO 2014, L 173, p. 1).

Dans ce contexte, cette juridiction s'interroge sur la conciliation de l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière de la Charte, avec les exigences ressortant de l'article 12, paragraphe 2, sous a) et d), de la directive « abus de marché » [56] et de l'article 23, paragraphe 2, sous g) et h), du règlement relatif aux abus de marché. Cette interrogation trouve son origine dans les mesures législatives en cause au principal, lesquelles prévoient à titre préventif, dans le chef des opérateurs de services de communications électroniques, une conservation généralisée et indifférenciée des données relatives au trafic pendant un an à partir du jour de l'enregistrement, aux fins de la lutte contre les infractions d'abus de marché, dont font partie les opérations d'initiés. Dans l'hypothèse où la Cour devrait considérer que la législation portant sur la conservation des données de connexion en cause au principal n'est pas conforme au droit de l'Union, la juridiction de renvoi se pose la question du maintien provisoire des effets de cette législation, en vue d'éviter une insécurité juridique et de permettre que les données précédemment collectées et conservées soient utilisées aux fins de la détection et de la poursuite des opérations d'initiés.

Par son arrêt, la Cour, réunie en grande chambre, juge que la conservation généralisée et indifférenciée des données de trafic pendant un an à compter du jour de l'enregistrement par les opérateurs de services de communications électroniques n'est pas autorisée, à titre préventif, aux fins de la lutte contre les infractions d'abus de marché. Par ailleurs, elle confirme sa jurisprudence selon laquelle le droit de l'Union s'oppose à ce qu'une juridiction nationale limite dans le temps les effets d'une déclaration d'invalidité qui lui incombe concernant des dispositions législatives nationales incompatibles avec le droit de l'Union.

La Cour rappelle tout d'abord que, afin d'interpréter une disposition du droit de l'Union, il convient non seulement de se référer aux termes de celle-ci, mais également de tenir compte de son contexte et des objectifs poursuivis par la réglementation dont elle fait partie.

S'agissant du libellé des dispositions visées par les questions préjudicielles, la Cour constate que, tandis que l'article 12, paragraphe 2, sous d), de la directive « abus de marché » se réfère au pouvoir de l'AMF « d'exiger des enregistrements téléphoniques et des données échangées existants », l'article 23, paragraphe 2, sous g) et h), du règlement relatif aux abus de marché renvoie au pouvoir de cette autorité de se faire remettre, d'une part, les « enregistrements […] de données relatives au trafic détenus par des entreprises d'investissement, des établissements de crédit ou des institutions financières » et, d'autre part, « dans la mesure où le droit national l'autorise, les enregistrements existants de données relatives au trafic détenus par un opérateur de télécommunications ». Selon la Cour, il ressort sans ambigüité du libellé de ces

[56] Directive 2003/6/CE du Parlement européen et du Conseil, du 28 janvier 2003, sur les opérations d'initiés et les manipulations de marché (abus de marché) (JO 2003, L 96, p. 16).

dispositions que celles-ci se bornent à encadrer le pouvoir de l'AMF d'« exiger », ou encore, de « se faire remettre » les données dont disposent ces opérateurs, ce qui correspond à un accès à ces données. En outre, la référence faite aux enregistrements « existants », tels que « détenus » par lesdits opérateurs, laisse entendre que le législateur de l'Union n'a pas entendu régir la possibilité, pour le législateur national, d'instaurer une obligation de conservation de tels enregistrements. Selon la Cour, cette interprétation serait, par ailleurs, corroborée tant par le contexte dans lequel s'inscrivent lesdites dispositions, que par les objectifs poursuivis par la réglementation dont ces mêmes dispositions font partie.

En ce qui concerne le contexte dans lequel s'inscrivent les dispositions visées par les questions préjudicielles, la Cour observe que, si, aux termes des dispositions pertinentes de la directive « abus de marché » et du règlement relatif aux abus de marché [57], le législateur de l'Union a entendu imposer aux États membres de prendre les mesures requises pour que les autorités compétentes en matière financière disposent d'un ensemble d'outils, de compétences et de ressources adéquates, ainsi que des pouvoirs de surveillance et d'enquête nécessaires pour assurer l'efficacité de leurs missions, ces dispositions ne se prononcent ni sur l'éventuelle possibilité pour les États membres d'instituer, à ces fins, à la charge des opérateurs de services de communications électroniques, une obligation de conservation généralisée et indifférenciée des données de trafic ni sur les conditions dans lesquelles ces données doivent être conservées par lesdits opérateurs aux fins de leur remise, le cas échéant, aux autorités compétentes.

Quant aux objectifs poursuivis par la réglementation en cause, la Cour relève qu'il ressort tant de la directive « abus de marché » que du règlement relatif aux abus de marché [58], que ces instruments ont pour finalité d'assurer l'intégrité des marchés financiers de l'Union et de renforcer la confiance des investisseurs en ces marchés, confiance qui repose, notamment, sur le fait qu'ils seront placés sur un pied d'égalité et protégés contre l'utilisation illicite d'informations privilégiées. L'interdiction des opérations d'initiés énoncée par lesdits instruments [59] vise ainsi à garantir l'égalité des cocontractants dans une transaction boursière en évitant que l'un d'eux, qui détient une information privilégiée et se trouve, de ce fait, dans une position avantageuse par rapport aux autres investisseurs, en tire profit au détriment de ceux qui l'ignorent. Si, aux termes du règlement relatif aux abus de marché [60], les enregistrements des données de connexion constituent une preuve essentielle et parfois la seule permettant de détecter et de démontrer l'existence d'une opération d'initié ou d'une manipulation de marché, il n'en reste pas moins que ce règlement ne se réfère qu'aux enregistrements « détenus » par les opérateurs de services de communications

57 Respectivement, article 12, paragraphe 1, de la directive « abus de marché » et article 23, paragraphe 3, du règlement relatif aux abus de marché, lu à la lumière du considérant 62 de celui-ci.

58 Respectivement, considérants 2 et 12 de la directive « abus de marché » et article 1er du règlement relatif aux abus de marché, lu à la lumière des considérants 2 et 24 de celui-ci.

59 Article 2, paragraphe 1, de la directive « abus de marché » et article 8, paragraphe 1, du règlement relatif aux abus de marché.

60 Considérant 62 du règlement relatif aux abus de marché.

électroniques, ainsi qu'au pouvoir de l'autorité compétente en matière financière d'« exiger », auprès de ces opérateurs, la communication des données « existantes ». Ainsi, il ne ressort nullement de ce texte que le législateur de l'Union a entendu, par ce biais, reconnaître aux États membres le pouvoir d'imposer aux opérateurs de services de communications électroniques une obligation générale de conservation des données. Il s'ensuit que ni la directive « abus de marché » ni le règlement relatif aux abus de marché ne peuvent constituer le fondement juridique d'une obligation générale de conservation des enregistrements de données relatives au trafic détenus par les opérateurs de services de communications électroniques aux fins de l'exercice des pouvoirs conférés à l'autorité compétente en matière financière au titre de ces actes.

Ensuite, la Cour rappelle que la directive 2002/58 constitue l'acte de référence en matière de conservation et, de manière plus générale, de traitement des données à caractère personnel dans le secteur des communications électroniques, de sorte que son interprétation, telle qu'effectuée au regard de cette directive, régit également les enregistrements des données de trafic détenus par les opérateurs de services de communications électroniques que les autorités compétentes en matière financière, au sens de la directive « abus de marché » et du règlement relatif aux abus de marché [61], peuvent se faire remettre par ceux-ci. L'appréciation de la licéité du traitement des enregistrements détenus par les opérateurs de services de communications électroniques [62] doit, dès lors, s'effectuer à la lumière des conditions prévues par la directive 2002/58, ainsi que de l'interprétation de cette directive par la Cour, dans sa jurisprudence.

Ainsi, la Cour juge que la directive « abus de marché » et le règlement relatif aux abus de marché, lus en combinaison avec la directive 2002/58 et à la lumière de la Charte, s'opposent à des mesures législatives prévoyant, à titre préventif, aux fins de la lutte contre les infractions d'abus de marché, dont font partie les opérations d'initiés, une conservation temporaire, à savoir d'un an à compter du jour de l'enregistrement, mais généralisée et indifférenciée des données relatives au trafic, par les opérateurs de services de communications électroniques.

Enfin, la Cour confirme sa jurisprudence selon laquelle le droit de l'Union s'oppose à ce qu'une juridiction nationale limite dans le temps les effets d'une déclaration d'invalidité qui lui incombe, en vertu du droit national, à l'égard des dispositions nationales qui, d'une part, imposent aux opérateurs de services de communications électroniques une conservation généralisée et indifférenciée des données relatives au trafic et, d'autre part, permettent la communication de telles données à l'autorité compétente en matière financière, sans autorisation préalable d'une juridiction ou d'une autorité administrative indépendante, en raison de l'incompatibilité de ces dispositions avec la

61 Respectivement, article 11 de la directive « abus de marché » et article 22 du règlement relatif aux abus de marché.

62 Au sens de l'article 12, paragraphe 2, sous d), de la directive « abus de marché » et de l'article 23, paragraphe 2, sous g) et h), du règlement relatif aux abus de marché.

directive 2002/58, lue à la lumière de la Charte. Cela étant, la Cour rappelle que l'admissibilité des éléments de preuve obtenus au moyen d'une telle conservation relève, conformément au principe d'autonomie procédurale des États membres, du droit national, sous réserve du respect notamment des principes d'équivalence et d'effectivité. Ce dernier principe requiert du juge pénal national qu'il écarte des informations et des éléments de preuve qui ont été obtenus au moyen d'une conservation généralisée et indifférenciée incompatible avec le droit de l'Union si les personnes concernées ne sont pas en mesure de commenter efficacement ces informations et ces éléments de preuve, provenant d'un domaine échappant à la connaissance des juges et qui sont susceptibles d'influencer de manière prépondérante l'appréciation des faits.

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

Saisie à titre préjudiciel par le Conseil d'État (France), l'assemblée plénière de la Cour développe sa jurisprudence sur la directive 2002/58 en apportant des précisions concernant, d'une part, les conditions dans lesquelles une conservation généralisée d'adresses IP par des fournisseurs de services de communications électroniques peut ne pas être regardée comme entraînant une ingérence grave dans les droits au respect de la vie privée, à la protection des données à caractère personnel ainsi qu'à la liberté d'expression garantis par la Charte [63], ainsi que, d'autre part, la possibilité, pour une autorité publique, d'accéder à certaines données à caractère personnel conservées dans le respect de telles conditions, dans le cadre de la lutte contre les infractions aux droits de propriété intellectuelle commises en ligne.

En l'occurrence, quatre associations ont présenté au Premier ministre (France) une demande d'abrogation du décret relatif au traitement automatisé de données à caractère personnel [64]. Cette demande n'ayant pas été suivie d'effet, ces associations ont saisi le Conseil d'État d'un recours tendant à l'annulation de cette décision implicite de rejet. Selon elles, ce décret ainsi que les dispositions qui en constituent la base légale [65] méconnaissent le droit de l'Union.

En vertu de la législation française, la Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet (Hadopi), afin de pouvoir identifier les responsables d'atteintes aux droits d'auteur ou aux droits voisins commises en ligne, est autorisée à accéder à certaines données que les fournisseurs de services de communications

63 Articles 7, 8 et 11 de la Charte.

64 Décret nº 2010-236, du 5 mars 2010, relatif au traitement automatisé de données à caractère personnel autorisé par l'article L. 331-29 du code de la propriété intellectuelle dénommé « Système de gestion des mesures pour la protection des œuvres sur internet » (JORF nº 56 du 7 mars 2010, texte nº 19), tel que modifié par le décret nº 2017-924, du 6 mai 2017, relatif à la gestion des droits d'auteur et des droits voisins par un organisme de gestion de droits et modifiant le code de la propriété intellectuelle (JORF nº 109 du 10 mai 2017, texte nº 176).

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

électroniques sont tenus de conserver. Ces données portent sur l'identité civile d'une personne concernée correspondant à son adresse IP collectée préalablement par des organismes d'ayants droit. Une fois que le titulaire de l'adresse IP utilisée pour des activités portant une telle atteinte est identifié, la Hadopi suit la procédure dite de « réponse graduée ». Concrètement, elle est habilitée à envoyer, à cette personne, deux recommandations qui s'apparentent à des avertissements et, si les activités persistent, une lettre lui notifiant que ses activités sont susceptibles de poursuites pénales. Enfin, elle est en droit de saisir le ministère public en vue de la poursuite de ladite personne [66].

Dans ce contexte, le Conseil d'État a interrogé la Cour sur l'interprétation de la directive 2002/58, lue à la lumière de la Charte [67].

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

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

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

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

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

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

doivent permettre une telle mise en relation que par l'usage d'un procédé technique performant ne remettant pas en cause l'efficacité de la séparation étanche de ces catégories de données. La fiabilité de cette séparation doit faire l'objet d'un contrôle régulier par une autorité publique tierce. Pour autant que la législation nationale applicable prévoit de telles exigences strictes, l'ingérence résultant de cette conservation des adresses IP ne saurait être qualifiée de « grave ».

Dès lors, la Cour conclut que, en présence d'un dispositif législatif garantissant qu'aucune combinaison de données ne permettra de tirer des conclusions précises sur la vie privée des personnes dont les données sont conservées, la directive 2002/58, lue à la lumière de la Charte, ne s'oppose pas à ce qu'un État membre impose une obligation de conservation généralisée et indifférenciée des adresses IP, pour une durée ne dépassant pas le strict nécessaire, aux fins d'un objectif de lutte contre les infractions pénales en général.

En deuxième lieu, en ce qui concerne l'accès à des données relatives à l'identité civile correspondant à des adresses IP, la Cour dit pour droit que la directive 2002/58, lue à la lumière de la Charte, ne s'oppose pas, en principe, à une réglementation nationale permettant l'accès, par une autorité publique, à ces données conservées par les fournisseurs de services de communications électroniques de manière séparée et effectivement étanche, à la seule fin que cette autorité puisse identifier les titulaires de ces adresses soupçonnés d'être responsables d'atteintes aux droits d'auteur et aux droits voisins sur Internet et prendre des mesures à leur égard. Dans un tel cas, la réglementation nationale doit interdire aux agents disposant d'un tel accès, premièrement, de divulguer sous quelque forme que ce soit des informations sur le contenu des fichiers consultés par ces titulaires, sauf aux seules fins de saisir le ministère public, deuxièmement, d'effectuer tout traçage du parcours de navigation de ces titulaires et, troisièmement, d'utiliser ces adresses IP à des fins autres que celle de l'adoption de ces mesures.

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

Dans ce même contexte, la Cour se réfère également à sa jurisprudence selon laquelle, s'agissant de la lutte contre les infractions pénales portant atteinte aux droits d'auteur ou aux droits voisins commises en ligne, la circonstance que l'accès aux adresses IP peut

constituer le seul moyen d'investigation permettant l'identification de la personne concernée tend à établir que la conservation de ces adresses et l'accès à celles-ci sont strictement nécessaires à la réalisation de l'objectif poursuivi et répondent donc à l'exigence de proportionnalité. Ne pas permettre un tel accès comporterait d'ailleurs un réel risque d'impunité systémique d'infractions pénales commises en ligne ou dont la commission ou la préparation est facilitée par les caractéristiques propres à Internet. Or, l'existence d'un tel risque constitue une circonstance pertinente afin d'apprécier, dans le cadre d'une mise en balance des différents droits et intérêts en présence, si une ingérence dans les droits au respect de la vie privée, à la protection des données personnelles ainsi qu'à la liberté d'expression est une mesure proportionnée au regard de l'objectif de lutte contre les infractions pénales.

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

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

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

En l'occurrence, un titulaire d'une adresse IP peut être particulièrement exposé à un tel risque lorsque l'autorité publique est appelée à décider de saisir ou non le ministère public en vue de sa poursuite. En effet, l'intensité de l'atteinte au droit au respect de la vie privée est susceptible de croître au fur et à mesure que la procédure de réponse graduée, qui opère selon un processus séquentiel, parcourt les différentes étapes qui la

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

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

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

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

telle mise en relation, susceptible dans de telles hypothèses de permettre que soient tirées des conclusions précises sur la vie privée de ladite personne dont l'adresse IP a été utilisée pour des activités pouvant porter atteinte aux droits d'auteur ou aux droits voisins.

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

Dans ce cadre, la Cour observe que, en l'occurrence, le traitement automatisé des données à caractère personnel effectué par l'autorité publique sur la base des informations relatives aux contrefaçons constatées par les organismes d'ayants droit est susceptible de comporter un certain nombre de faux cas positifs et surtout le risque qu'un nombre de données potentiellement très élevé soit détourné par des tiers à des fins abusives ou illicites, ce qui explique la nécessité d'un tel contrôle. En outre, elle ajoute que ce traitement doit respecter les règles spécifiques de protection des données à caractère personnel prévues par la directive 2016/680. En effet, en l'espèce, même si l'autorité publique ne dispose pas de pouvoirs décisionnels propres dans le cadre de la procédure dite de réponse graduée, elle doit être qualifiée d'« autorité publique » impliquée dans la prévention et la détection des infractions pénales, et relève donc de son champ d'application. Ainsi, les personnes impliquées dans une telle procédure doivent bénéficier d'un ensemble de garanties matérielles et procédurales prescrit par la directive 2016/680, dont il appartient à la juridiction de renvoi de vérifier qu'elles sont prévues par la législation nationale.

2. Traitement des données à caractère personnel en matière pénale

Arrêt du 12 mai 2021 (grande chambre), Bundesrepublik Deutschland (Notice rouge d'Interpol) (C-505/19, EU:C:2021:376***)***

En 2012, l'Organisation internationale de police criminelle (ci-après « Interpol ») a publié, à la demande des États-Unis et sur la base d'un mandat d'arrêt émis par les autorités de ce pays, une notice rouge visant WS, un ressortissant allemand, en vue de son extradition éventuelle. Lorsqu'une personne faisant l'objet d'une telle notice est localisée dans un État membre d'Interpol, celui-ci doit, en principe, procéder à son arrestation provisoire ou bien surveiller ou restreindre ses déplacements.

Toutefois, avant même la publication de cette notice rouge, une procédure d'enquête portant, selon la juridiction de renvoi, sur les mêmes faits que ceux à l'origine de cette

notice avait été engagée contre WS en Allemagne. Cette procédure a été définitivement clôturée en 2010, après le paiement d'une somme d'argent par WS, et ce conformément à une procédure spécifique de transaction prévue en droit pénal allemand. Par la suite, le Bundeskriminalamt (Office fédéral de la police criminelle, Allemagne) a informé Interpol qu'il considérait que, en raison de cette procédure antérieure, le principe ne bis in idem était applicable en l'espèce. Ce principe, consacré tant à l'article 54 de la Convention d'application de l'accord de Schengen [68] qu'à l'article 50 de la Charte, interdit notamment qu'une personne ayant déjà été définitivement jugée soit poursuivie de nouveau pour la même infraction.

En 2017, WS a introduit un recours contre la République fédérale d'Allemagne devant le Verwaltungsgericht Wiesbaden (tribunal administratif de Wiesbaden, Allemagne), pour qu'il lui soit ordonné de prendre les mesures nécessaires au retrait de cette notice rouge. À cet égard, WS invoque, outre une violation du principe ne bis in idem, une violation de son droit à la libre circulation, garanti par l'article 21 TFUE, dans la mesure où il ne peut pas se rendre dans un État partie à l'accord de Schengen ou dans un État membre sans risquer d'être arrêté. Il estime également que, en raison de ces violations, le traitement de ses données à caractère personnel, figurant dans la notice rouge, est contraire à la directive 2016/680, relative à la protection des données à caractère personnel en matière pénale [69].

C'est dans ce contexte que le tribunal administratif de Wiesbaden a décidé d'interroger la Cour sur l'application du principe ne bis in idem et, plus précisément, sur la possibilité de procéder à l'arrestation provisoire d'une personne faisant l'objet d'une notice rouge dans une situation telle que celle en cause. De plus, en cas d'applicabilité de ce principe, cette juridiction cherche à savoir quelles sont les conséquences sur le traitement, par les États membres, des données à caractère personnel contenues dans une telle notice.

Dans son arrêt de grande chambre, la Cour juge, *inter alia*, que les dispositions de la directive 2016/680, lues à la lumière de l'article 54 de la CAAS et de l'article 50 de la Charte, doivent être interprétées en ce sens qu'elles ne s'opposent pas au traitement des données à caractère personnel figurant dans une notice rouge émise par Interpol, tant qu'il n'a pas été établi, par la voie d'une telle décision judiciaire, que le principe ne bis in idem s'applique s'agissant des faits sur lesquels cette notice est fondée, pour autant qu'un tel traitement satisfait aux conditions prévues par cette directive.

S'agissant de la question relative aux données à caractère personnel figurant dans une notice rouge d'Interpol, la Cour indique que toute opération appliquée à ces données,

---

[68] Convention d'application de l'accord de Schengen, du 14 juin 1985, entre les gouvernements des États de l'Union économique Benelux, de la République fédérale d'Allemagne et de la République française relatif à la suppression graduelle des contrôles aux frontières communes (JO 2000, L 239, p. 19) (ci-après la « CAAS »).

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

telle que leur enregistrement dans les fichiers de recherche d'un État membre, constitue un « traitement » relevant de la directive 2016/680 [70]. En outre, elle considère, d'une part, que ce traitement poursuit une finalité légitime et, d'autre part, qu'il ne saurait être considéré comme illicite au seul motif que le principe ne bis in idem pourrait s'appliquer aux faits sur lesquels la notice rouge est fondée [71]. Ce traitement, par les autorités des États membres, peut d'ailleurs s'avérer indispensable, précisément afin de vérifier si ledit principe s'applique.

Dans ces conditions, la Cour juge, de même, que la directive 2016/680, lue à la lumière de l'article 54 de la CAAS et de l'article 50 de la Charte, ne s'oppose pas au traitement des données à caractère personnel figurant dans une notice rouge, tant qu'une décision judiciaire définitive n'a pas établi que le principe ne bis in idem s'applique en l'espèce. Toutefois, un tel traitement doit respecter les conditions prévues par cette directive. Dans cette perspective, il doit notamment être nécessaire à l'exécution d'une mission, effectuée par une autorité nationale compétente, à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites ou d'exécution de sanctions pénales [72].

En revanche, lorsque le principe ne bis in idem s'applique, l'enregistrement, dans les fichiers de recherche des États membres, des données à caractère personnel figurant dans une notice rouge d'Interpol n'est plus nécessaire, étant donné que la personne en cause ne peut plus faire l'objet de poursuites pénales pour les faits couverts par ladite notice et, par conséquent, être arrêtée pour ces mêmes faits. Il s'ensuit que la personne concernée doit pouvoir demander l'effacement de ses données. Si cet enregistrement est néanmoins maintenu, il doit être accompagné par l'indication que la personne en cause ne peut plus être poursuivie dans un État membre ou un État contractant pour les mêmes faits, en raison du principe ne bis in idem.

Arrêt du 21 juin 2022 (grande chambre), Ligue des droits humains (C-817/19, EU:C:2022:491)

Dans cette affaire (voir également la rubrique I.1., intitulée « Conformité du droit dérivé de l'Union au droit à la protection des données à caractère personnel »), après avoir constaté la validité de la directive PNR, la Cour apporte des précisions quant à l'interprétation de certaines de ses dispositions [73].

Premièrement, elle relève que la directive énumère les objectifs poursuivis par le traitement des données PNR de manière exhaustive. Dès lors, cette directive s'oppose à une législation nationale qui autorise le traitement de données PNR à d'autres fins que

[70] Voir article 2, paragraphe 1, et article 3, point 2, de la directive 2016/680.
[71] Voir article 4, paragraphe 1, sous b), et article 8, paragraphe 1, de la directive 2016/680.
[72] Voir article 1er, paragraphe 1, et article 8, paragraphe 1, de la directive 2016/680.
[73] En particulier, l'article 2 (« Application de la [directive] aux vols intra-UE »), l'article 6 (« Traitement des données PNR »), et l'article 12 (« Période de conservation et dépersonnalisation des données »), de la directive PNR.

la lutte contre les infractions terroristes et les formes graves de criminalité. Ainsi, une législation nationale admettant de surcroît, comme finalité du traitement des données PNR, le suivi des activités visées par les services de renseignement et de sécurité est susceptible de méconnaître le caractère exhaustif de cette énumération. De même, le système établi par la directive PNR ne peut être prévu aux fins de l'amélioration des contrôles aux frontières et de la lutte contre l'immigration clandestine. Il s'ensuit également que les données PNR ne sauraient être conservées dans une base de données unique pouvant être consultée aux fins de la poursuite tant des finalités de la directive PNR que d'autres finalités.

Deuxièmement, la Cour explicite la notion d'autorité nationale indépendante, compétente pour vérifier si les conditions de communication des données PNR, aux fins de leur évaluation postérieure, sont remplies et pour approuver une telle communication. En particulier, l'autorité mise en place en tant qu'UIP ne peut être qualifiée comme telle puisqu'elle n'a pas la qualité de tiers par rapport à l'autorité qui demande l'accès aux données. En effet, les membres de son personnel pouvant être des agents détachés par les autorités habilitées à demander un tel accès, l'UIP apparaît nécessairement liée à ces autorités. Dès lors, la directive PNR s'oppose à une législation nationale selon laquelle l'autorité mise en place en tant qu'UIP a également la qualité d'autorité nationale compétente, habilitée à approuver la communication des données PNR à l'expiration des six mois suivant le transfert de ces données à l'UIP.

Troisièmement, s'agissant du délai de conservation des données PNR, la Cour juge que l'article 12 de la directive PNR, lu à la lumière des articles 7 et 8 ainsi que de l'article 52, paragraphe 1, de la Charte, s'oppose à une législation nationale qui prévoit une durée générale de conservation de ces données de cinq ans, applicable indifféremment à tous les passagers aériens.

En effet, selon la Cour, après l'expiration de la période de conservation initiale de six mois, la conservation des données PNR n'apparaît pas limitée au strict nécessaire en ce qui concerne les passagers aériens pour lesquels ni l'évaluation préalable, ni les éventuelles vérifications effectuées au cours de la période de conservation initiale de six mois, ni aucune autre circonstance n'ont révélé l'existence d'éléments objectifs – tels que le fait que les données PNR des passagers concernés ont donné lieu à une concordance positive vérifiée dans le cadre de l'évaluation préalable – de nature à établir un risque en matière d'infractions terroristes ou de formes graves de criminalité présentant un lien objectif, à tout le moins indirect, avec le voyage aérien effectué par ces passagers. En revanche, elle estime que, au cours de la période initiale de six mois, la conservation des données PNR de l'ensemble des passagers aériens soumis au système instauré par cette directive ne paraît pas, par principe, excéder les limites du strict nécessaire.

Quatrièmement, la Cour fournit des indications concernant une éventuelle application de la directive PNR, aux fins de la lutte contre les infractions terroristes et les formes graves de criminalité, à d'autres modes de transport acheminant des passagers dans l'Union. Or, la directive, lue à la lumière de l'article 3, paragraphe 2, TUE, de l'article 67,

paragraphe 2, TFUE et de l'article 45 de la Charte, s'oppose à un système de transfert et de traitement des données PNR de l'ensemble des transports effectués par d'autres moyens à l'intérieur de l'Union en l'absence de menace terroriste réelle et actuelle ou prévisible à laquelle fait face l'État membre concerné. Dans une telle situation, comme pour les vols intra-UE, l'application du système établi par la directive PNR doit être limitée aux données PNR des transports relatifs notamment à certaines liaisons ou à des schémas de voyage ou encore à certaines gares ou certains ports maritimes pour lesquels il existe des indications de nature à justifier cette application. Il appartient à l'État membre concerné de sélectionner les transports pour lesquels de telles indications existent et de réexaminer régulièrement cette application en fonction de l'évolution des conditions ayant justifié leur sélection.

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

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

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, 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.

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 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.

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

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 2000/520/CE [74], la Commission avait considéré que, dans le cadre du régime dit de la « sphère de sécurité » (en anglais, « safe harbour ») [75], les États-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, 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 adoptée par la Commission sur le fondement dudit article 25, paragraphe 6, de la directive 95/46.

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, 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, 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 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

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

[75] 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.

ingérences dans ces droits et sans faire état de l'existence d'une protection juridique efficace contre des ingérences de cette nature.

En outre, la Cour a déclaré invalide l'article 3 de la décision 2000/520, 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, 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. La Cour a conclu que l'invalidité des articles 1er et 3 de la décision 2000/520 avait pour effet d'affecter la validité de cette décision dans son ensemble.

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.

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. 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. 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.

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, 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.

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.).

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.

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.

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, 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.

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

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 [76]. 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 [77]. Par ailleurs, le RGPD établit, de manière précise, les conditions dans lesquelles un tel transfert peut avoir lieu en l'absence d'une décision d'adéquation ou de garanties appropriées [78].

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

[76] Article 45 du RGPD.
[77] Article 46, paragraphes 1 et 2, sous c), du RGPD.
[78] Article 49 du RGPD.

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 [79], 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 ») [80].

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/UE [81]. 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 [82]).

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 ne révèle aucun élément de nature à affecter sa validité. En revanche, elle déclare la décision 2016/1250 invalide.

---

79 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).

80 Arrêt de la Cour du 6 octobre 2015, Schrems, C-362/14, EU:C:2015:650.

81 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).

82 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).

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.

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

S'agissant des obligations incombant aux autorités de contrôle dans le contexte d'un tel transfert, la Cour juge que, à moins qu'il existe une décision d'adéquation valablement adoptée par la Commission, ces autorités sont notamment obligées de suspendre ou d'interdire un transfert de données à caractère personnel vers un pays tiers lorsqu'elles estiment, au regard des circonstances propres à ce transfert, que les clauses types de protection des données ne sont pas ou ne peuvent pas être respectées dans ce pays et que la protection des données transférées, requise par le droit de l'Union, ne peut pas être assurée par d'autres moyens, à défaut pour l'exportateur établi dans l'Union d'avoir lui-même suspendu ou mis fin à un tel transfert

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

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.

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.

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.

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 les rubriques II.1. et II.3., intitulées « Champ d'application de la réglementation générale » et « 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.

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, 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.

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. 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. 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.

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.

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)

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 ») [83], 2001/29/CE, sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information [84], 2004/48/CE, relative au respect des droits de propriété intellectuelle [85], et 2002/58 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.

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 et 2004/48, 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

[83] Directive 2000/31/CE du Parlement européen et du Conseil, du 8 juin 2000, relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« directive sur le commerce électronique ») (JO 2000, L 178, p. 1).

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

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

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, 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, lu en combinaison avec l'article 15, paragraphe 1, de la directive 2002/58, 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.

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.

En conséquence, la Cour a conclu que les directives 2002/58 et 2004/48 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.

3. Déréférencement de données à caractère personnel

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

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 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.

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 [86], 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 [87].

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.

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

[86] Article 8, paragraphe 1, de la directive 95/46 et article 9, paragraphe 1, du règlement 2016/679.
[87] Article 8, paragraphe 5, de la directive 95/46 et article 10 du règlement 2016/679.

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.

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 [88], 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 [89].

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 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.

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

88 Article 8, paragraphe 2, sous e), de la directive 95/46 et article 9, paragraphe 2, sous e), du règlement 2016/679.
89 Article 14, premier alinéa, sous a), de la directive 95/46 et article 21, paragraphe 1, du règlement 2016/679.

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.

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

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.

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, 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 [90].

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 [91] 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

[90] Article 4, paragraphe 1, sous a), de la directive 95/46, et article 3, paragraphe 1, du règlement 2016/679.
[91] Articles 12, sous b), et 14, premier alinéa, sous a), de la directive 95/46, et article 17, paragraphe 1, du règlement 2016/679.

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.

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.

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.

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

Les requérants au principal, TU, qui occupe des postes à responsabilité et détient des participations dans différentes sociétés, et RE, qui était sa compagne et, jusqu'en mai 2015, fondée de pouvoir d'une de ces sociétés, ont fait l'objet de trois articles publiés sur un site Internet en 2015 par G LLC, exploitant de ce site Internet. Ces articles, dont l'un était illustré de quatre photographies représentant les requérants et suggérant que ces derniers menaient une vie luxueuse, présentaient de manière critique le modèle d'investissement de plusieurs de leurs sociétés. L'accès à ces articles était possible par la saisie, dans le moteur de recherche exploité par Google LLC (ci-après « Google »), des noms et prénoms des requérants, tant isolément qu'en combinaison avec certains noms de sociétés. La liste de résultats renvoyait à ces articles au moyen d'un lien, ainsi qu'aux photographies affichées sous la forme de vignettes (« thumbnails »).

Les requérants au principal ont demandé à Google, en tant que responsable du traitement des données à caractère personnel effectué par son moteur de recherche,

d'une part, de déréférencer de la liste de résultats de recherche les liens vers les articles en cause, au motif que ceux-ci contiendraient des allégations inexactes et des opinions diffamatoires, et, d'autre part, de retirer les vignettes de la liste des résultats de recherche. Google a refusé de faire droit à cette demande.

Ayant été déboutés tant en première instance qu'en appel, les requérants au principal ont saisi le Bundesgerichtshof (Cour fédérale de justice, Allemagne) d'un recours en Revision, dans le cadre duquel le Bundesgerichtshof a saisi la Cour à titre préjudiciel quant à l'interprétation du RGPD et de la directive 95/46 [92].

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

En premier lieu, la Cour dit pour droit que, dans le cadre de la mise en balance entre, d'une part, les droits au respect de la vie privée et à la protection des données à caractère personnel, et, d'autre part, le droit à la liberté d'expression et d'information [93], aux fins de l'examen d'une demande de déréférencement adressée à l'exploitant d'un moteur de recherche et visant à la suppression de la liste de résultats d'une recherche d'un lien qui mène vers un contenu comportant des informations prétendument inexactes, ce déréférencement n'est pas soumis à la condition que la question de l'exactitude du contenu référencé ait été résolue, au moins à titre provisoire, dans le cadre d'un recours intenté par le demandeur contre le fournisseur de contenu.

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

---

92 Respectivement, l'article 17, paragraphe 3, sous a), du RGPD et l'article 12, sous b), et l'article 14, premier alinéa, sous a), de la directive 95/46.

93 Droits fondamentaux garantis respectivement par les articles 7, 8 et 11 de la Charte.

• dans la mesure où l'activité d'un moteur de recherche est susceptible d'affecter significativement et de manière additionnelle par rapport à celle des éditeurs de sites Internet les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel, l'exploitant de ce moteur, en tant que personne déterminant les finalités et les moyens de cette activité, doit assurer, dans le cadre de ses responsabilités, de ses compétences et de ses possibilités, que les garanties prévues par la directive 95/46 et le RGPD puissent développer leur plein effet et qu'une protection efficace et complète des personnes concernées puisse effectivement être réalisée ;

• lorsqu'il est saisi d'une demande de déréférencement, l'exploitant d'un moteur de recherche doit vérifier si l'inclusion du lien vers la page Internet en question dans la liste des résultats est nécessaire à l'exercice du droit à la liberté d'information des internautes potentiellement intéressés à avoir accès à cette page Internet au moyen d'une telle recherche, protégée par le droit à la liberté d'expression et d'information ;

• le RGPD consacre explicitement l'exigence d'une mise en balance entre, d'une part, les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel et, d'autre part, le droit fondamental à la liberté d'information.

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

La question du caractère exact ou non du contenu référencé constitue également un élément pertinent dans le cadre de cette appréciation. C'est ainsi que, dans certaines circonstances, le droit à l'information des internautes et la liberté d'expression du fournisseur de contenu peuvent prévaloir sur les droits à la protection de la vie privée et à la protection des données à caractère personnel, notamment lorsque la personne concernée joue un rôle dans la vie publique. Cependant, ce rapport s'inverse lorsque, à tout le moins, une partie des informations visées par la demande de déréférencement ne présentant pas un caractère mineur au regard de l'ensemble du contenu se révèlent inexactes. Dans une telle hypothèse, le droit d'informer et le droit d'être informé ne sauraient être pris en compte, car ils ne peuvent inclure le droit de diffuser de telles informations et d'y avoir accès.

Ensuite, s'agissant, d'une part, des obligations relatives à l'établissement du caractère exact ou non des informations figurant dans le contenu référencé, la Cour précise que la personne qui demande le déréférencement, en raison de l'inexactitude de telles informations, est tenue d'établir l'inexactitude manifeste de ces informations ou, à tout

le moins, d'une partie de ces informations ne présentant pas un caractère mineur au regard de l'ensemble de ce contenu. Toutefois, afin d'éviter de faire peser sur cette personne une charge excessive susceptible de nuire à l'effet utile du droit au déréférencement, il lui incombe uniquement de fournir les éléments de preuve qu'il peut être, compte tenu des circonstances du cas d'espèce, raisonnablement exigé de rechercher de sa part. En principe, cette personne ne saurait être tenue de produire, dès le stade précontentieux, à l'appui de sa demande de déréférencement, une décision juridictionnelle obtenue contre l'éditeur du site Internet, même sous la forme d'une décision prise en référé.

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

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

l'ensemble des circonstances du cas d'espèce, d'accorder une importance particulière au droit à la liberté d'expression et d'information.

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

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

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

Partant, lorsque l'exploitant d'un moteur de recherche est saisi d'une demande de déréférencement tendant à ce que soient supprimées des résultats d'une recherche d'images effectuée à partir du nom d'une personne des photographies affichées sous la forme de vignettes qui représentent cette personne, il doit vérifier si l'affichage des photographies en question est nécessaire à l'exercice du droit à la liberté d'information des internautes potentiellement intéressés à avoir accès à ces photographies au moyen d'une telle recherche.

Or, dans la mesure où le moteur de recherche affiche des photographies de la personne concernée en dehors du contexte dans lequel celles-ci sont publiées sur la page Internet référencée, le plus souvent en vue d'illustrer les éléments textuels que contient cette page, il y a lieu de déterminer si ce contexte doit néanmoins être pris en considération lors de la mise en balance des droits et des intérêts concurrents à effectuer. Dans ce

cadre, la question de savoir si ladite appréciation doit également inclure le contenu de la page Internet dans laquelle figure la photographie dont la suppression de l'affichage sous la forme d'une vignette est demandée dépend de l'objet et de la nature du traitement en cause.

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

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

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

Par conséquent, une appréciation autonome de l'activité de l'exploitant du moteur de recherche, consistant en l'affichage des résultats d'une recherche d'images, sous la forme de vignettes, s'impose, car l'atteinte additionnelle aux droits fondamentaux qui résulte d'une telle activité peut être particulièrement intense du fait de l'agrégation, lors

d'une recherche par nom, de toutes les informations relatives à la personne concernée qui se trouvent sur Internet. Dans le cadre de cette appréciation autonome, il y a lieu de tenir compte du fait que cet affichage constitue en soi le résultat recherché par l'internaute, indépendamment de sa décision ultérieure d'accéder ou non à la page Internet d'origine.

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

4. Consentement de l'utilisateur d'un site Internet au stockage d'informations

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

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 2002/58 [94], lue en combinaison avec la directive 95/46/CE [95], ainsi qu'avec le RGPD [96].

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 2002/58, 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 directive2002/58, qui prévoit depuis sa modification par la directive 2009/136 que l'utilisateur doit avoir « donné son accord » au placement de cookies, tend à indiquer que le consentement de l'utilisateur ne peut dorénavant plus être présumé et doit résulter d'un comportement actif de ce dernier. Enfin, un consentement actif est désormais prévu par le RGPD [97] dont l'article 4, point 11, requiert une manifestation de volonté prenant la forme, notamment, d'un « acte positif clair » et dont le considérant 32 exclut expressément qu'il y ait un consentement « en cas de silence, de cases cochées par défaut ou d'inactivité ».

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

Deuxièmement, la Cour a constaté que l'article 5, paragraphe 3, de la directive 2002/58 vise à protéger l'utilisateur de toute ingérence dans sa vie privée, indépendamment du point de savoir si cette ingérence concerne ou non des données à caractère personnel. Il en résulte que la notion de « consentement » ne doit pas être interprétée différemment selon que les informations stockées ou consultées dans l'équipement terminal de l'utilisateur d'un site Internet constituent ou non des données à caractère personnel.

Troisièmement, la Cour a relevé que l'article 5, paragraphe 3, de la directive 2002/58 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

---

94 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).

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

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

97 IDEM.

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.

5. Traitement des données à caractère personnel sur les réseaux sociaux en ligne

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

La société Meta Platforms est propriétaire du réseau social en ligne « Facebook », qui est gratuit pour les utilisateurs privés. Le modèle économique de ce réseau social se fonde sur le financement par la publicité en ligne, qui est faite sur mesure pour ses utilisateurs individuels. Une telle publicité est techniquement rendue possible par l'établissement automatisé de profils détaillés des utilisateurs du réseau et des services en ligne proposés au niveau du groupe Meta. Ainsi, afin de pouvoir utiliser ledit réseau social, les utilisateurs doivent, au moment de leur inscription, accepter les conditions générales établies par Meta Platforms, qui renvoient aux politiques d'utilisation des données et des cookies fixées par cette société. En vertu de ces dernières, outre les données que ces utilisateurs fournissent directement lors de leur inscription, Meta Platforms collecte également des données relatives aux activités desdits utilisateurs à l'intérieur et à l'extérieur du réseau social et les met en relation avec les comptes Facebook des utilisateurs concernés. Quant à ces dernières données, également désignées comme des « données *off* Facebook », il s'agit, d'une part, des données concernant la consultation de pages Internet et d'applications tierces et, d'autre part, des données relatives à l'utilisation d'autres services en ligne appartenant au groupe Meta (dont Instagram et WhatsApp). L'aperçu global des données ainsi collectées permet de tirer des conclusions détaillées sur les préférences et les intérêts de ces mêmes utilisateurs.

Par décision du 6 février 2019, le Bundeskartellamt (autorité fédérale de la concurrence, Allemagne) a interdit à Meta Platforms, d'une part, de subordonner, dans les conditions générales alors en vigueur, l'utilisation du réseau social Facebook par des utilisateurs privés résidant en Allemagne au traitement de leurs données off Facebook et, d'autre part, de procéder, sans leur consentement, au traitement de ces données. En outre, l'autorité fédérale de la concurrence lui a imposé d'adapter ces conditions générales, de sorte qu'il en ressorte clairement que lesdites données ne seront pas collectées, mises en relation avec les comptes d'utilisateurs Facebook et utilisées sans le consentement des utilisateurs concernés. Enfin, cette autorité a souligné qu'un tel consentement n'était

pas valide lorsqu'il constituait une condition pour l'utilisation du réseau social. Elle a motivé sa décision par le fait que le traitement des données en cause, qui ne serait pas conforme au RGPD, constituerait une exploitation abusive de la position dominante de Meta Platforms sur le marché des réseaux sociaux en ligne.

Meta Platforms a introduit un recours contre cette décision devant l'Oberlandesgericht Düsseldorf (tribunal régional supérieur de Düsseldorf, Allemagne). Nourrissant des doutes, entre autres, sur l'interprétation et l'application de certaines dispositions du RGPD, le tribunal régional supérieur de Düsseldorf a saisi la Cour à titre préjudiciel.

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

S'agissant du traitement de catégories particulières de données à caractère personnel [98], la Cour estime que, dans le cas où un utilisateur d'un réseau social en ligne consulte des sites Internet ou des applications en rapport avec une ou plusieurs de ces catégories et, le cas échéant, y insère des données en s'inscrivant ou en effectuant des commandes en ligne, le traitement de données à caractère personnel par l'opérateur de ce réseau social en ligne [99] doit être considéré comme un « traitement portant sur des catégories particulières de données à caractère personnel », au sens de l'article 9, paragraphe 1, du RGPD, lorsqu'il permet de révéler des informations relevant d'une de ces catégories particulières, que ces informations concernent un utilisateur de ce réseau ou toute autre personne physique. Un tel traitement de données est en principe interdit, sous réserve de certaines dérogations [100].

À ce dernier égard, la Cour précise que, lorsqu'un utilisateur d'un réseau social en ligne consulte des sites Internet ou des applications en rapport avec une ou plusieurs desdites catégories particulières de données, il ne rend pas manifestement publiques [101]

---

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

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

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

a) la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques, sauf lorsque le droit de l'Union ou le droit de l'État membre prévoit que l'interdiction visée au paragraphe 1 ne peut pas être levée par la personne concernée ; […]

e) le traitement porte sur des données à caractère personnel qui sont manifestement rendues publiques par la personne concernée ;

f) le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ou chaque fois que des juridictions agissent dans le cadre de leur fonction juridictionnelle ;

[…] ».

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

les données relatives à cette consultation, collectées par l'opérateur de ce réseau social en ligne à travers des cookies ou des technologies d'enregistrement similaires. Par ailleurs, lorsqu'il insère des données dans de tels sites Internet ou dans de telles applications ou lorsqu'il active des boutons de sélection intégrés à ces sites et à ces applications, tels que les boutons « j'aime » ou « partager », ou les boutons permettant à l'utilisateur de s'identifier sur ces sites ou applications en utilisant les identifiants de connexion liés à son compte d'utilisateur du réseau social, son numéro de téléphone ou son adresse électronique, un tel utilisateur ne rend manifestement publiques les données ainsi insérées ou résultant de l'activation de ces boutons que dans le cas où il a explicitement exprimé son choix au préalable, le cas échéant sur la base d'un paramétrage individuel effectué en toute connaissance de cause, de rendre les données le concernant publiquement accessibles à un nombre illimité de personnes.

En ce qui concerne plus généralement les conditions de licéité d'un traitement de données à caractère personnel, la Cour rappelle que, en vertu du RGPD, le traitement de données est licite si, et dans la mesure où, la personne concernée y a consenti pour une ou plusieurs finalités spécifiques [102]. En l'absence d'un tel consentement, ou lorsque ce consentement n'a pas été donné de manière libre, spécifique, éclairée et univoque, un tel traitement est néanmoins justifié lorsqu'il répond à l'une des exigences de nécessité [103], qui doivent être interprétées strictement. Or, le traitement de données à caractère personnel de ses utilisateurs effectué par un opérateur d'un réseau social en ligne ne peut être considéré comme étant nécessaire à l'exécution du contrat auquel ces utilisateurs sont parties qu'à la condition que ce traitement soit objectivement indispensable pour réaliser une finalité faisant partie intégrante de la prestation contractuelle destinée auxdits utilisateurs, de telle sorte que l'objet principal du contrat ne pourrait être atteint en l'absence de ce traitement.

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

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

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

fondamentaux desdits utilisateurs prévalent sur l'intérêt de l'opérateur d'un réseau social en ligne à la personnalisation de la publicité par laquelle il finance son activité.

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

S'agissant de la validité du consentement des utilisateurs concernés au traitement de leurs données en vertu du RGPD, la Cour considère que la circonstance que l'opérateur d'un réseau social en ligne occupe une position dominante sur le marché des réseaux sociaux en ligne ne fait pas obstacle en tant que telle à ce que les utilisateurs d'un tel réseau puissent valablement consentir au traitement de leurs données à caractère personnel, effectué par cet opérateur. Toutefois, vu qu'une telle position est susceptible d'affecter la liberté de choix de ces utilisateurs et de créer un déséquilibre manifeste entre ceux-ci et ledit opérateur, elle constitue un élément important pour déterminer si le consentement a effectivement été donné valablement et, notamment, librement, ce qu'il incombe à ce même opérateur de prouver [104].

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

[104] En vertu de l'article 7, paragraphe 1, du RGPD.

VI. Autorités nationales de contrôle

1. Portée de l'exigence d'indépendance

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

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, en soumettant à la tutelle de l'État les 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 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.

La Cour a jugé que la garantie d'indépendance des autorités nationales de contrôle prévue par la directive 95/46 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.

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.

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.

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, 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.

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, 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.

La Cour a précisé que, afin de pouvoir satisfaire au critère d'indépendance énoncé à la disposition précitée de la directive 95/46, 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 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 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.

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

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.

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.

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.

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.

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)

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.

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. 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 permet l'application de la législation relative à la protection des données à caractère personnel d'un État membre autre que celui dans lequel le responsable du traitement de ces données est immatriculé, pour autant que celui-ci exerce, au moyen d'une installation stable sur le territoire de cet État membre, une activité effective et réelle, 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

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, 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.

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.

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 IV, 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, 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.

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 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.

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, 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.

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

Dans cet arrêt (voir également la rubrique II.5., 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, 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).

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 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.

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

Le 11 septembre 2015, le président de la Commission belge de la protection de la vie privée, (ci-après la « CPVP ») a saisi le Nederlandstalige rechtbank van eerste aanleg Brussel (tribunal de première instance néerlandophone de Bruxelles, Belgique), d'une action en cessation à l'encontre de Facebook Ireland, Facebook Inc. et Facebook Belgium, visant à mettre un terme à des violations, prétendument commises par

Facebook, de la législation relative à la protection des données. Ces violations consistaient notamment en la collecte et l'utilisation d'informations sur le comportement de navigation des internautes belges, détenteurs ou non d'un compte Facebook, au moyen de différentes technologies, telles les cookies, les modules sociaux [105] ou les pixels.

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

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

La juridiction de renvoi a éprouvé des doutes au sujet de l'incidence de l'application du mécanisme de « guichet unique » prévu par le RGPD [106] sur les compétences de l'APD et s'est posé, plus particulièrement, la question de savoir si, pour les faits postérieurs à l'entrée en vigueur du RGPD, à savoir le 25 mai 2018, l'APD peut agir contre Facebook Belgium, dès lors que c'est Facebook Ireland qui a été identifié comme responsable du traitement des données concernées. En effet, depuis cette date et notamment en application du principe de « guichet unique » prévu par le RGPD, seul le Commissaire irlandais à la protection des données serait compétent pour intenter une action en cessation, sous le contrôle des juridictions irlandaises.

Dans son arrêt, rendu en grande chambre, la Cour précise les pouvoirs des autorités nationales de contrôle dans le cadre du RGPD. Ainsi, elle juge notamment que ce règlement autorise, sous certaines conditions, une autorité de contrôle d'un État membre à exercer son pouvoir de porter toute prétendue violation du RGPD devant une juridiction de cet État et d'ester en justice en ce qui concerne un traitement de données transfrontalier [107], alors qu'elle n'est pas l'autorité chef de file pour ce traitement.

En premier lieu, la Cour précise les conditions dans lesquelles une autorité nationale de contrôle, n'ayant pas la qualité d'autorité chef de file en ce qui concerne un traitement transfrontalier, doit exercer son pouvoir de porter toute prétendue violation du RGPD devant une juridiction d'un État membre et, le cas échéant, d'ester en justice afin

[105] Par exemple, les boutons « J'aime » ou « Partager ».

[106] Aux termes de l'article 56, paragraphe 1, du RGPD : « Sans préjudice de l'article 55, l'autorité de contrôle de l'établissement principal ou de l'établissement unique du responsable du traitement ou du sous-traitant est compétente pour agir en tant qu'autorité de contrôle chef de file concernant le traitement transfrontalier effectué par ce responsable du traitement ou ce sous-traitant ».

[107] Au sens de l'article 4, point 23, du RGPD.

d'assurer l'application de ce règlement. Ainsi, d'une part, le RGPD doit conférer à cette autorité de contrôle une compétence pour adopter une décision constatant que ce traitement méconnaît les règles prévues par ce règlement et, d'autre part, ce pouvoir doit être exercé dans le respect des procédures de coopération et de contrôle de la cohérence prévues par ce règlement [108].

En effet, pour les traitements transfrontaliers, le RGPD prévoit le mécanisme du « guichet unique » [109], qui est fondé sur une répartition des compétences entre une « autorité de contrôle chef de file » et les autres autorités nationales de contrôle concernées. Ce mécanisme exige une coopération étroite, loyale et efficace entre ces autorités, afin d'assurer une protection cohérente et homogène des règles relatives à la protection des données à caractère personnel et ainsi préserver son effet utile. Le RGPD consacre à cet égard la compétence de principe de l'autorité de contrôle chef de file pour adopter une décision constatant qu'un traitement transfrontalier méconnaît les règles prévues par ce règlement [110], tandis que la compétence des autres autorités nationales de contrôle pour adopter une telle décision, même à titre provisoire, constitue l'exception [111]. Cependant, dans l'exercice de ses compétences, l'autorité de contrôle chef de file ne saurait s'affranchir d'un dialogue indispensable ainsi que d'une coopération loyale et efficace avec les autres autorités de contrôle concernées. De ce fait, dans le cadre de cette coopération, l'autorité de contrôle chef de file ne peut ignorer les points de vue des autres autorités de contrôle concernées et toute objection pertinente et motivée formulée par l'une de ces dernières autorités a pour effet de bloquer, à tout le moins temporairement, l'adoption du projet de décision de l'autorité de contrôle chef de file.

La Cour précise par ailleurs que la circonstance qu'une autorité de contrôle d'un État membre qui n'est pas l'autorité de contrôle chef de file s'agissant d'un traitement de données transfrontalier ne puisse exercer le pouvoir de porter toute prétendue violation du RGPD devant une juridiction de cet État et d'ester en justice que dans le respect des règles de répartition des compétences décisionnelles entre l'autorité de contrôle chef de file et les autres autorités de contrôle [112] est conforme aux articles 7, 8 et 47 de la Charte, garantissant à la personne concernée, respectivement, le droit à la protection de ses données à caractère personnel et le droit à un recours effectif.

En deuxième lieu, la Cour juge que, en cas de traitement de données transfrontalier, l'exercice du pouvoir d'une autorité de contrôle d'un État membre, autre que l'autorité de contrôle chef de file, d'intenter une action en justice [113] ne requiert pas que le

[108] Prévues aux articles 56 et 60 du RGPD.
[109] Article 56, paragraphe 1, du RGPD.
[110] Article 60 paragraphe 7, RGPD.
[111] L'article 56, paragraphe 2, et l'article 66 du RGPD consacrent les exceptions au principe de la compétence décisionnelle de l'autorité de contrôle chef de file.
[112] Prévues aux articles 55 et 56, lus conjointement avec l'article 60 du RGPD.
[113] En vertu de l'article 58, paragraphe 5, du RGPD.

responsable du traitement ou le sous-traitant pour le traitement transfrontalier de données à caractère personnel visé par cette action dispose d'un établissement principal ou d'un autre établissement sur le territoire de cet État membre. Cependant, l'exercice de ce pouvoir doit relever du champ d'application territoriale du RGPD [114], ce qui suppose que le responsable du traitement ou le sous-traitant pour le traitement transfrontalier dispose d'un établissement sur le territoire de l'Union.

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

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

En quatrième lieu, la Cour juge que, lorsqu'une autorité de contrôle d'un État membre qui n'est pas l'« autorité de contrôle chef de file » a intenté, avant la date d'entrée en vigueur du RGPD, une action en justice visant un traitement transfrontalier de données à caractère personnel, cette action peut être maintenue, en vertu du droit de l'Union, sur le fondement des dispositions de la directive 95/46 laquelle demeure applicable en ce qui concerne les infractions aux règles qu'elle prévoit commises jusqu'à la date à laquelle cette directive a été abrogée. En outre, cette action peut être intentée par cette autorité pour des infractions commises après la date d'entrée en vigueur du RGPD, pour autant que ce soit dans l'une des situations où, à titre d'exception, ce règlement confère à cette même autorité une compétence pour adopter une décision constatant que le traitement de données concerné méconnaît les règles prévues par ce règlement et dans le respect des procédures de coopération et de contrôle de la cohérence que ce dernier prévoit.

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

En cinquième et dernier lieu, la Cour reconnaît l'effet direct de la disposition du RGPD en vertu de laquelle chaque État membre prévoit, par la loi, que son autorité de contrôle a le pouvoir de porter toute violation de ce règlement à l'attention des autorités judiciaires et, le cas échéant, d'ester en justice. Par conséquent, une telle autorité peut invoquer cette disposition pour intenter ou reprendre une action contre des particuliers, même si elle n'a pas été spécifiquement mise en œuvre dans la législation de l'État membre concerné.

Arrêt du 16 janvier 2024 (grande chambre), Österreichische Datenschutzbehörde (C-33/22, EU:C:2024:46)

Dans cette affaire (voir également la rubrique II.1., intitulée « Champ d'application de la réglementation générale »), la Cour relève que les dispositions du RGPD relatives à la compétence des autorités de contrôle nationales et au droit de réclamation [115] ne nécessitent pas l'adoption de mesures nationales d'application et sont suffisamment claires, précises et inconditionnelles pour produire un effet direct. Il s'ensuit que, si le RGPD laisse une marge d'appréciation aux États membres quant au nombre d'autorités de contrôle à instituer [116], il fixe en revanche l'étendue de leurs compétences pour surveiller l'application du RGPD. Ainsi, dans le cas où un État membre décide d'instituer une seule autorité de contrôle nationale, celle-ci est nécessairement dotée de l'intégralité des compétences prévues par ce règlement. Toute autre interprétation remettrait en cause l'effet utile de ces dispositions et risquerait d'affaiblir l'effet utile de toutes les autres dispositions du RGPD susceptibles d'être concernées par une réclamation.

En ce qui concerne la circonstance que les dispositions nationales d'ordre constitutionnel excluent la possibilité pour une autorité de contrôle qui dépend du pouvoir exécutif de surveiller l'application du RGPD par un organe relevant du pouvoir législatif, la Cour souligne que c'est précisément dans le respect de la structure constitutionnelle des États membres que le RGPD se borne à exiger de ces derniers qu'ils établissent au moins une autorité de contrôle, tout en leur offrant la possibilité d'en instituer plusieurs. Ce règlement reconnaît ainsi à chaque État membre une marge d'appréciation lui permettant de mettre en place autant d'autorités de contrôle que le requièrent, notamment, les exigences tenant à sa structure constitutionnelle.

En outre, l'invocation de dispositions de droit national par un État membre ne saurait porter atteinte à l'unité et à l'efficacité du droit de l'Union. En effet, les effets s'attachant au principe de primauté du droit de l'Union s'imposent à l'ensemble des organes d'un État membre, sans, notamment, que les dispositions internes, y compris d'ordre constitutionnel, puissent y faire obstacle.

---

115 Respectivement, l'article 55, paragraphe 1, et l'article 77, paragraphe 1, du RGPD.
116 Conformément à l'article 51, paragraphe 1, du RGPD.

Ainsi, dès lors qu'un État membre a choisi d'instaurer une seule autorité de contrôle, il ne saurait invoquer des dispositions de droit national, fussent-elles d'ordre constitutionnel, afin de soustraire des traitements de données à caractère personnel qui relèvent du champ d'application du RGPD à la surveillance de cette autorité.

4. Conditions d'imposition d'amendes administratives

Arrêt du 5 décembre 2023 (grande chambre), Nacionalinis visuomenės sveikatos centras (C-683/21, EU:C:2023:949)

Dans cette affaire (voir également les rubriques II.3., II.5. et II.6., intitulées « Notion de "traitement de données à caractère personnel" », « Notion de "responsable du traitement de données à caractère personnel" » et « Notion de "responsable conjoint du traitement de données à caractère personnel" »), la Cour constate que, en vertu de l'article 83 du RGPD, une amende administrative peut être imposée à un responsable du traitement uniquement s'il est établi qu'il a commis, délibérément ou par négligence, une violation des règles contenues dans ce règlement [117].

À cet égard, elle précise que le législateur de l'Union n'a pas laissé aux États membres une marge d'appréciation en ce qui concerne les conditions de fond devant être respectées par une autorité de contrôle lorsque celle-ci décide d'imposer une amende administrative à un responsable du traitement en vertu de cette disposition. Le fait que le RGPD donne aux États membres la possibilité de prévoir des exceptions par rapport aux autorités publiques et aux organismes publics établis sur leur territoire [118] ainsi que des exigences concernant la procédure à suivre par les autorités de contrôle pour imposer une amende administrative [119] ne signifie nullement qu'ils seraient également habilités à prévoir de telles conditions de fond.

En ce qui concerne ces conditions, la Cour note que parmi les éléments énumérés dans le RGPD au vu desquels l'autorité de contrôle impose au responsable du traitement une amende administrative figure « le fait que la violation a été commise délibérément ou par négligence » [120]. En revanche, aucun de ces éléments ne fait état d'une quelconque possibilité d'engager la responsabilité du responsable du traitement en l'absence d'un comportement fautif de sa part. Ainsi, seules les violations des dispositions du RGPD commises par le responsable du traitement délibérément ou par négligence peuvent

117 Violation visée à l'article 83, paragraphes 4 à 6.

118 En vertu de l'article 83, paragraphe 7, du RGPD qui prévoit que « […] chaque État membre peut établir les règles déterminant si et dans quelle mesure des amendes administratives peuvent être imposées à des autorités publiques et à des organismes publics établis sur son territoire ».

119 En vertu de l'article 83, paragraphe 8, du RGPD, lu à la lumière de son considérant 129.

120 Article 83, paragraphe 2, sous b), du RGPD.

conduire à l'imposition d'une amende administrative à ce dernier en application de l'article 83 de ce règlement.

La Cour ajoute que cette interprétation est corroborée par l'économie générale et la finalité du RGPD. Dans ce contexte, elle précise que l'existence d'un système de sanctions en vertu du RGPD permettant d'imposer, lorsque les circonstances spécifiques de chaque cas d'espèce le justifient, une amende administrative crée, pour les responsables du traitement et les sous-traitants, une incitation à se conformer à ce règlement et que, par leur effet dissuasif, les amendes administratives contribuent au renforcement de la protection des personnes concernées. Cependant, le législateur de l'Union n'a pas jugé nécessaire de prévoir l'imposition d'amendes administratives en l'absence de faute. Compte tenu du fait que le RGPD vise un niveau de protection à la fois équivalent et homogène et qu'il doit, à cette fin, être appliqué de manière cohérente dans l'ensemble de l'Union, il serait contraire à cette finalité de permettre aux États membres de prévoir un tel régime pour l'imposition d'une amende.

En outre, la Cour conclut qu'une telle amende peut être imposée à un responsable du traitement au regard des opérations de traitement de données à caractère personnel effectuées par un sous-traitant pour le compte de celui-ci, sauf si, dans le cadre de ces opérations, ce sous-traitant a effectué des traitements pour des finalités qui lui sont propres ou a traité ces données de manière incompatible avec le cadre ou les modalités du traitement tels qu'ils avaient été déterminés par le responsable du traitement ou d'une façon telle qu'il ne saurait être raisonnablement considéré que ce responsable y aurait consenti. Dans cette hypothèse, le sous-traitant doit être considéré comme étant responsable d'un tel traitement.

Arrêt du 5 décembre 2023 (grande chambre), Deutsche Wohnen (C-807/21, EU:C:2023:950)

Deutsche Wohnen SE (ci-après « DW ») est une société immobilière qui détient indirectement, par le biais de participations dans différentes sociétés, de nombreuses unités commerciales et de logement. Elle traite, dans le cadre de ses activités commerciales, des données à caractère personnel des locataires de ces unités.

À la suite de deux contrôles réalisés en 2017 et en 2019, le Berliner Beauftragte für den Datenschutz (autorité de contrôle de Berlin, Allemagne) a constaté une série de violations du RGPD commises par DW. Par décision du 30 octobre 2019, cette autorité de contrôle lui a, à ce titre, imposé des amendes administratives.

DW a formé un recours contre cette décision devant le Landgericht Berlin (tribunal régional de Berlin, Allemagne), qui a classé la procédure sans suite. Ce tribunal a relevé que, en vertu de la loi allemande [121], une infraction administrative ne pourrait être

[121] Gesetz über Ordnungswidrigkeiten (loi relative aux infractions administratives), du 24 mai 1968 (BGBl. 1968 I, p. 481), dans la version de la communication du 19 février 1987 (BGBl. 1987 I, p. 602), telle qu'adaptée par la loi du 19 juin 2020 (BGBl. 2020 I, p. 1350).

constatée qu'à l'encontre d'une personne physique et non pas à l'encontre d'une personne morale. En outre, dans le cas d'un engagement de la responsabilité d'une personne morale, seuls les actes des membres de ses organes ou de ses représentants pourraient lui être imputés. La Staatsanwaltschaft Berlin (parquet de Berlin, Allemagne) a introduit un recours contre cette décision devant le Kammergericht Berlin (tribunal régional supérieur de Berlin, Allemagne). Dans ce contexte, cette juridiction a saisi la Cour à titre préjudiciel sur l'interprétation du RGPD.

Dans son arrêt, la Cour, réunie en grande chambre, se prononce sur les conditions d'imposition d'amendes administratives au titre du RGPD. En premier lieu, elle examine la question de savoir si les États membres peuvent soumettre l'imposition d'une amende administrative à une personne morale à la condition que la violation de ce règlement soit imputée au préalable à une personne physique identifiée. En second lieu, elle se penche également, à l'instar de l'arrêt Nacionalinis visuomenės sveikatos centras (voir supra) sur la question de savoir si la violation sanctionnée des dispositions du RGPD doit être commise délibérément ou par négligence.

En ce qui concerne l'imposition d'une amende administrative en vertu du RGPD à une personne morale, la Cour relève, tout d'abord, que les principes, interdictions et obligations prévus par le RGPD s'adressent, en particulier, aux « responsables du traitement », dont la responsabilité s'étend à tout traitement de données à caractère personnel qu'ils effectuent eux-mêmes ou qui est réalisé pour leur compte. C'est cette responsabilité qui constitue, en cas de violation des dispositions du RGPD, le fondement pour l'imposition d'une amende administrative au responsable du traitement en application de l'article 83 de ce règlement. Cependant, le législateur de l'Union n'a pas opéré, aux fins de la détermination d'une telle responsabilité, une distinction entre les personnes physiques et les personnes morales, cette responsabilité étant soumise à la seule condition que celles-ci, seules ou conjointement avec d'autres, déterminent les finalités et les moyens du traitement de données à caractère personnel [122.] Partant, en principe, toute personne répondant à cette condition est notamment responsable pour toute violation du RGPD, commise par elle-même ou pour son compte. Cela implique, d'une part, que les personnes morales sont responsables non seulement des violations commises par leurs représentants, directeurs ou gestionnaires, mais également par toute autre personne qui agit dans le cadre de l'activité commerciale de ces personnes morales et pour leur compte. D'autre part, les amendes administratives prévues par le RGPD en cas de telles violations doivent pouvoir être infligées directement à des personnes morales lorsque celles-ci peuvent être qualifiées de responsables du traitement.

Ensuite, la Cour observe qu'aucune disposition du RGPD ne permet de considérer que l'infliction d'une amende administrative à une personne morale en tant que responsable

[122] Selon l'article 4, point 7, du RGPD.

du traitement serait soumise à la constatation préalable que cette violation a été commise par une personne physique identifiée. En outre, le législateur de l'Union n'a pas laissé aux États membres une marge d'appréciation à cet égard. Le fait que le RGPD donne à ceux-ci la possibilité de prévoir des exigences concernant la procédure à suivre par les autorités de contrôle pour imposer une amende administrative [123] ne signifie nullement qu'ils seraient également habilités à prévoir des conditions de fond supplémentaires à celles fixées par le RGPD.

Dans ce contexte, la Cour précise que permettre aux États membres d'exiger, de manière unilatérale et en tant que condition nécessaire à l'imposition d'une amende administrative en application de l'article 83 du RGPD à un responsable du traitement qui est une personne morale, que la violation en cause soit imputée ou imputable, au préalable, à une personne physique identifiée serait contraire à la finalité du RGPD. En outre, une telle exigence supplémentaire risquerait, en définitive, d'affaiblir l'effectivité et l'effet dissuasif des amendes administratives imposées à des personnes morales en tant que responsables du traitement.

Enfin, la Cour souligne que la notion d'« entreprise », au sens des articles 101 et 102 TFUE [124], n'a pas d'incidence sur le point de savoir si et dans quelles conditions une amende administrative peut être imposée en vertu du RGPD à un responsable du traitement qui est une personne morale et n'est pertinente que pour déterminer le montant d'une telle amende.

Ainsi, la Cour conclut que le RGPD [125] s'oppose à une réglementation nationale en vertu de laquelle une amende administrative ne peut être infligée à une personne morale en sa qualité de responsable du traitement pour une violation de ce règlement [126] que pour autant que cette violation a été imputée préalablement à une personne physique identifiée.

S'agissant de la question de savoir si les États membres peuvent prévoir l'imposition d'une amende administrative même lorsque la violation sanctionnée n'a pas été commise délibérément ou par négligence, la Cour rappelle, tout d'abord, que les conditions de fond qu'une autorité de contrôle doit respecter lorsqu'elle impose une telle amende à un responsable du traitement relèvent uniquement du droit de l'Union et que les États membres ne disposent d'aucune marge de manœuvre à cet égard. En suivant un raisonnement identique à celui adopté dans l'arrêt Nacionalinis visuomenės sveikatos centras précité, la Cour constate que, en vertu de l'article 83 du RGPD, une amende administrative ne peut être imposée que s'il est établi que le responsable du traitement, qui est à la fois une personne morale et une entreprise, a commis, délibérément ou par négligence, une violation des règles contenues dans ce règlement.

---

123 Comme cela ressort de l'article 58, paragraphe 4, et de l'article 83, paragraphe 8, du RGPD, lus à la lumière de son considérant 129.
124 À laquelle le renvoi est effectué au considérant 150 du RGPD.
125 Article 58, paragraphe 2, sous i), et article 83, paragraphes 1 à 6, du RGPD.
126 Visée à l'article 83, paragraphes 4 à 6, du RGPD.

5. Articulation des compétences des autorités nationales de contrôle avec les compétences des autres autorités nationales

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

Dans cette affaire (voir également la rubrique V.5., intitulée « Traitement des données à caractère personnel sur les réseaux sociaux en ligne »), en se prononçant sur la compétence d'une autorité de la concurrence pour constater la non-conformité avec le RGPD d'un traitement de données à caractère personnel, la Cour relève que, sous réserve du respect de son obligation de coopération loyale [127] avec les autorités de contrôle de la protection des données, une telle autorité peut constater, dans le cadre de l'examen d'un abus de position dominante de la part d'une entreprise [128], que les conditions générales d'utilisation fixées par cette entreprise en matière de traitement des données à caractère personnel et leur mise en œuvre ne sont pas conformes à ce règlement, lorsque ce constat est nécessaire pour établir l'existence d'un tel abus. Cependant, lorsqu'une autorité de la concurrence relève une violation du RGPD dans le cadre du constat d'un abus de position dominante, elle ne se substitue pas aux autorités de contrôle.

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

---

127 Consacrée à l'article 4, paragraphe 3, TUE.
128 Au sens de l'article 102 TFUE.

Lorsqu'elle nourrit des doutes sur la portée de l'appréciation effectuée par l'autorité de contrôle nationale compétente ou l'autorité de contrôle chef de file, lorsque le comportement en cause ou un comportement similaire fait, en même temps, l'objet d'un examen de la part de ces autorités, ou encore lorsque, en l'absence d'enquête desdites autorités, elle considère qu'un comportement d'une entreprise n'est pas conforme aux dispositions du RGPD, l'autorité de la concurrence doit consulter ces autorités et solliciter leur coopération, afin de lever ses doutes ou de déterminer s'il y a lieu d'attendre l'adoption d'une décision par l'autorité de contrôle concernée avant d'entamer sa propre appréciation. En l'absence d'objection de leur part ou de réponse dans un délai raisonnable, l'autorité de la concurrence peut poursuivre sa propre enquête.

COUR DE JUSTICE
DE L'UNION EUROPÉENNE

Direction de la recherche et documentation

Juillet 2024