L'APPLICATION DE LA CHARTE À L'ÈRE DU NUMÉRIQUE

JOSÉ LUÍS DA CRUZ VILAÇA[1]
Tribunal de Justicia de la Unión Europea
jlcv@cruzvilaca.eu

Cómo citar/Citation
Da Cruz Vilaça, J. L. (2020).
L'application de la Charte dans l'ère du numérique.
Revista de Derecho Comunitario Europeo, 66, 447-469.
doi: https://doi.org/10.18042/cepc/rdce.66.06

Résumé

Le développement des nouvelles technologies de l'information et de l'Internet a ouvert la porte au risque d'une intrusion excessive dans la vie privée, en permettant un accès sans contrôle à des données à caractère personnel. La Charte a consacré, dans son art. 7, le droit de chaque personne "au respect de sa vie privée et familiale, de son domicile et de ses communications", ainsi que, dans l'art. 8, le "droit à la protection des données à caractère personnel la concernant." Dans ce domaine, le législateur a adopté la directive 95/46 et ensuite, le Règlement 2016/679 (RGPD). Cette contribution offre un tour d'horizon de la jurisprudence récente de Cour de justice concernant l'interprétation et la validité de ces actes de l'Union.

Mots clés

Technologies de l'information; Internet; protection de donnés à caractère personnel; RGPD; vie privée; Cour de Justice de l'Union européenne; droit à l'oubli; transfert de données; Charte des droits fondamentaux de l'UE.

---

[1] Professeur de droit de l'Union européenne et avocat; ancien juge et avocat général à la Cour de justice de l'UE et ancien président du Tribunal de première instance des Communautés européennes.

LA APLICACIÓN DE LA CARTA EN LA ERA DIGITAL

Resumen

El desarrollo de las nuevas tecnologías de la información y de Internet ha traído consigo un riesgo de intrusión excesiva en la vida privada, permitiendo un acceso sin control a los datos personales. La Carta enuncia, en su art. 7, el «derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones» y en su art. 8, el «derecho a la protección de los datos de carácter personal que le conciernan». En este ámbito, el legislador de la UE ha adoptado la Directiva 95/96 y, subsiguientemente, el Reglamento 2016/679 (RGPD). Esta contribución ofrece una vista de pájaro de la jurisprudencia reciente del Tribunal de Justicia sobre la interpretación y la validez de esos actos de la Unión.

Palabras clave

Tecnologías de la información; Internet; protección de datos personales; RGPD; vida privada; Tribunal de Justicia de la Unión Europea; derecho al olvido; transferencia de datos; Carta de los Derechos Fundamentales de la UE.

THE APPLICATION OF THE CHARTER IN THE DIGITAL AGE

Abstract

The development of new information technologies and of the Internet has also brought with it the risk of excessive intrusion into private life by allowing an unlimited access to personal data. The Charter contains, in its Art. 7, 'the right to respect for his or her private and family life, home and communications' and in its Art. 8, 'the right to the protection of personal data concerning him or her'. In this field, the EU legislature has adopted Directive 95/46 and subsequently Regulation 2016/679 (GDPR). This contribution provides an overview of the recent case-law of the Court of Justice concerning the interpretation and validity of those EU acts.

Keywords

Information technologies; Internet; protection of personal data; GDPR; private life; Court of Justice of the European Union; right to be forgotten; data transfers; Charter of fundamental rights of the EU.

SOMMAIRE

I. INTRODUCTION

Le développement exponentiel des nouvelles technologies de l'information, de l'Internet et des réseaux sociaux a eu le grand mérite d'accélérer la diffusion des informations et des connaissances au niveau global, ainsi que le flux transfrontalier des données nécessaires au commerce international.

Pour les entreprises, la disponibilité d'un nombre considérable de données est devenue le moyen par excellence de bien connaître les besoins de leurs clients et des consommateurs, d'accélérer leur croissance et de s'adapter rapidement à un environnement économique et social qui change sans cesse.

En revanche, la généralisation de ces technologies nouvelles, en facilitant la démocratisation du net et en encourageant l'expression de toutes les opinions de façon immédiate et sans intermédiaire, a créé la fausse impression que chacun pouvait, désormais, maîtriser, du jour au lendemain, la connaissance et l'intelligence universelles, et a, finalement, mis en échec la promesse originelle d'un vrai "marché libre des idées".

Par ailleurs, en même temps qu'elle fonctionnait comme un levier au service de transformations sociales importantes, y compris le renversement de régimes politiques autoritaires, le grand univers virtuel d'Internet servait

de véhicule au discours de la haine et du radicalisme, de foyer d'idées extrémistes et d'instrument de préparation d'actes de violence terroriste.

De surcroît, une telle évolution, qui s'est initiée il y a à peine 25 ans, a ouvert la porte au risque d'une intrusion excessive dans la vie privée, en permettant un accès sans contrôle à des données à caractère personnel et en mettant en danger le droit de chacun à sauvegarder le noyau essentiel de son identité personnelle et familiale, à préserver l'intégrité de sa personnalité morale et, en fin de compte, son droit inviolable à la dignité humaine.

C'est dans ce contexte que la Charte des droits fondamentaux de l'Union européenne – à laquelle l'art. 6 TUE, dans la rédaction résultant du traité de Lisbonne, a conféré la même valeur juridique que les traités – a consacré, dans son art. 7, le droit de chaque personne "au respect de sa vie privée et familiale, de son domicile et de ses communications", ainsi que, dans l'art. 8, le "droit à la protection des données à caractère personnel la concernant"[2].

Face à la rapidité avec laquelle le numérique a pris de l'ampleur, le législateur de l'Union s'est senti contraint d'adopter une législation appropriée: c'était le cas, en 1995, de la directive 95/46 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[3]; ensuite, du Règlement 2016/679 (RGPD) du 27 avril 2016[4],

---

[2] Les paragraphes 2 et 3 de ce dernier art. précisent que ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi, que toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification et que le respect de ces règles est soumis au contrôle d'une autorité indépendante.

[3] *JO L 281 du 23/11/1995, p. 31-50.* Modifiée par le Règlement (CE) nº 1882/2003 du Parlement européen e du Conseil, du 29.9.2003, et développée, en ce qui concerne le principe dénommé du *safe harbour*, par la décision 2000/520/CE du 26 juillet 2000, de la Commission, 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 [notifiée sous le numéro C(2000) 2441] (Texte présentant de l'intérêt pour l'EEE) - JO L 215, 25.8.2000, p. 7-47.

[4] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) - JO L 119, 4.5.2016, p. 1-88.

qui est venu révoquer et remplacer la directive et dont plusieurs dispositions sont destinées à mettre en œuvre les principes des traités et, en particulier, les exigences contenues dans les arts. 7 et 8 de la Charte.

C'est dans ce contexte que la Cour de justice a jugé[5] que les dispositions de la directive 95/46 [et du RGPD], en ce qu'elles régissent le traitement de données à caractère personnel susceptibles de porter atteinte aux libertés fondamentales, doivent être interprétées à la lumière des principes et des droits fondamentaux qui sont désormais inscrits dans la Charte.

Cela ne s'annonçait pas comme une tâche facile. Ainsi que M. l'avocat général Szpunar l'a fait remarquer au tout début de ses conclusions dans l'affaire G. C. e.a./CNIL[6], "[c]oncilier le droit à la vie privée et à la protection des données à caractère personnel avec le droit à l'information et à la liberté d'expression à l'ère d'Internet est l'un des principaux défis de notre époque".

Dans ces circonstances, il n'est pas étonnant que Cour de justice ait été appelée, à plusieurs reprises, à interpréter ces actes de l'Union ou à apprécier leur validité au regard des traités et de la Charte, suite aux questions préjudicielles posées par des juridictions nationales devant lesquelles les dispositions pertinentes ont été invoquées – ou contestées – par des particuliers (personnes physiques ou morales) en vue de la reconnaissance et la protection de leurs droits.

N'oublions pas qu'en vertu de l'art. 51 de la Charte, les dispositions de cette dernière s'adressent aux institutions, organes et organismes de l'Union, ainsi qu'aux États membres lorsqu'ils mettent en œuvre le droit de l'Union.

Plusieurs juridictions suprêmes ou constitutionnelles de différents États membres (l'Allemagne, l'Espagne, la France, l'Irlande, l'Autriche, la Finlande) se trouvent d'ailleurs parmi celles qui ont été saisies et qui ont demandé l'intervention à titre préjudiciel de la Cour de justice dans ce domaine[7].

---

5 Voir, notamment, arrêts du 6.3.2001, Connolly/Commission, C-274/99 P, EU:C:2001:127, point 37, du 20.5.2003, Österreichischer Rundfunk e.a., EU:C:2003:294, point 68, et du 13.5.2014, Google Spain, C-131/12, EU:C:2014:317, point 68.

6 Conclusions du 10.1.2019, C-136/17, paragraphe 1.

7 D'une façon générale, ces juridictions concourent dans la reconnaissance de l'importance accordée par leurs constitutions nationales à la protection de la vie privée et des communications, ainsi que dans l'exigence que toute ingérence dans ces droits soit proportionnée et respecte scrupuleusement les conditions prévues dans la loi. De même, elles s'opposent à tout accès massif et indiscriminé par des tiers à des données personnelles, ce qui serait contraire au principe de proportionnalité et aux valeurs fondamentales constitutionnellement protégées.

II. PROTECTION DES DROITS DES PARTICULIERS CONTRE LE TRAITEMENT DE LEURS DONNÉES PERSONNELLES SUR INTERNET

1. L'ARRÊT GOOGLE SPAIN ET LE DROIT À L'OUBLI

C'est l'affaire Google Spain[8], qui a porté devant le grand public la jurisprudence de la Cour de justice relative à la protection des données personnelles. Même si l'expression n'a pas été reprise à son compte par la Cour dans l'arrêt, l'affaire est devenue plutôt connue par la locution à laquelle elle est communément associée, à savoir "*le droit à l'oubli*" - "*the right to be forgotten*".

L'arrêt de la Cour peut, à juste titre et à plusieurs égards, être considéré comme un arrêt phare en matière de protection des droits des particuliers sur Internet ainsi que pour la mise en balance entre les différents droits fondamentaux en présence.

Les réponses de la Cour aux questions préjudicielles soumises par la juridiction nationale visant à l'interprétation de la Directive 95/46[9] ont d'ailleurs donné lieu à l'introduction d'une disposition dans le RGPD, l'art. 17, intitulé "droit à l'effacement des données" ou "droit à l'oubli".

Dans cette affaire, M. Costeja González, de nationalité espagnole et domicilié en Espagne, a introduit auprès de l'Agencia Española de Protección de Datos (AEPD) une réclamation à l'encontre du quotidien La Vanguardia, publié en Catalogne, et de Google Spain. Cette réclamation était fondée sur le fait que, lorsqu'un internaute introduisait le nom de M. Costeja dans le moteur de recherche de Google, il obtenait des liens vers deux pages dudit quotidien, datant d'il y avait plus de 16 ans, sur lesquelles figurait une annonce, mentionnant le nom de M. Costeja, pour une vente aux enchères immobilière liée à une saisie pratiquée en recouvrement de dettes de sécurité sociale.

La réclamation a été accueillie par l'AEPD pour autant qu'elle était dirigée contre Google[10]. Les recours que ce dernier a introduits devant

---

8 Arrêt Google Spain, C-131/12, précité.

9 Ces réponses sont applicables, mutatis mutandis, à l'interprétation des dispositions équivalentes du RGPD, qui a succédé à la directive.

10 L'AEPD a considéré que les exploitants de moteurs de recherche réalisent un traitement de données pour lequel ils sont responsables et agissent en tant qu'intermédiaires de la société de l'information. L'Agence a, en particulier, estimé qu'elle était habilitée à ordonner le retrait des données et l'interdiction d'accéder à certaines données par les exploitants de moteurs de recherche lorsqu'elle considérerait que leur localisation et leur diffusion sont susceptibles de porter atteinte au droit fondamental de protection des données et à la dignité des personnes au sens large, ce qui engloberait également la simple volonté de la personne intéressée que ces données ne soient pas connues par

l'Audiencia Nacional ont donné lieu aux questions préjudicielles posées à la Cour de justice.

Google a soutenu devant celle-ci que *l'activité des moteurs de recherche*[11] ne saurait être considérée comme un traitement de données.

Certes, la Cour avait déjà considéré[12] l'opération consistant à faire figurer, sur une *page internet*, des données à caractère personnel comme un "traitement de données", au sens de l'art. 2, alinéa b), de la directive 95/46. Il s'agissait maintenant de savoir si, et dans quelle mesure, l'activité d'un *moteur de recherche* devrait également être qualifiée comme un tel traitement lorsque ce moteur permet l'accès des internautes à des informations, placées sur Internet par des tiers, qui contiennent des données à caractère personnel.

La complexité entourant une telle question peut se comprendre facilement si l'on pense que la réponse à lui apporter reposait sur l'application d'une directive de 1995 à l'activité d'une entreprise, Google, qui n'a été créé qu'en 1998, et que, bien évidemment, ladite directive n'avait pas pu être rédigée en ayant à l'esprit les moteurs de recherche tels qu'ils existent à l'heure actuelle[13]

Néanmoins, la Cour y a répondu par l'affirmative[14].

---

des tiers. L'AEPD a considéré que cette obligation peut incomber directement aux exploitants de moteurs de recherche, sans qu'il soit nécessaire d'effacer les données ou les informations du site web où elles figurent, notamment lorsque le maintien de ces informations sur ce site est justifié par une disposition légale.

11 L'activité d'un moteur de recherche en tant que fournisseur de contenus consiste 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 (voir point 21 de l'arrêt).

12 Arrêt du 6.11.2003, Lindqvist, C-101/01, EU:C:2003:596.

13 Voir, en ce sens, les paragraphes 2 et 44 des conclusions de l'avocat général Macej Szpunar dans l'affaire GC/CNIL.

14 Selon la Cour (point 28 de l'arrêt), en explorant de manière automatisée, constante et systématique Internet à la recherche des informations qui y sont publiées, l'exploitant d'un moteur de recherche "collecte" de telles données qu'il "extrait", "enregistre" et "organise" par la suite dans le cadre de ses programmes d'indexation, "conserve" sur ses serveurs et, le cas échéant, "communique à" et "met à disposition de" ses utilisateurs sous forme de listes des résultats de leurs recherches. Ces opérations étant visées de manière explicite et inconditionnelle à [l'art. 4, sous 7) du RGPD], elles doivent être qualifiées de "traitement" au sens de cette disposition, sans qu'il importe que l'exploitant du moteur de recherche applique les mêmes opérations également à d'autres types d'information et ne distingue pas entre celles-ci et les données à caractère personnel. Au point 57 de l'arrêt, la Cour a encore précisé que cet affichage de

Elle a précisé que l'exploitant de ce moteur de recherche, en tant que personne déterminant les finalités et les moyens de cette activité, doit être considéré, *dans les limites de ses responsabilités, de ses compétences et de ses possibilités*, comme "responsable" de ce traitement, même lorsque ce dernier vise des informations qui ont déjà été publiées telles quelles dans les médias et qu'il ne les modifie aucunement et cela sans préjudice de la responsabilité propre des éditeurs de sites web[15].

---

données à caractère personnel sur une page de résultats d'une recherche constituant un traitement de telles données et étant, en plus, accompagné, sur la même page, de celui de publicités liées aux termes de recherche, il s'imposait de constater que le traitement de données à caractère personnel en question était effectué dans le cadre de l'activité publicitaire et commerciale de l'établissement du responsable du traitement sur le territoire d'un État membre, en l'occurrence le territoire espagnol.

15 Voir points 29 et 30 de l'arrêt. À cet égard, la Cour a précisé (points 35 à 37) que le traitement de données à caractère personnel effectué dans le cadre de l'activité d'un moteur de recherche se distingue de et s'ajoute à celui effectué par les éditeurs de sites web, consistant à faire figurer ces données sur une page internet. La Cour a encore souligné que cette activité des moteurs de recherche joue un rôle décisif dans la diffusion globale desdites données en ce qu'elle rend celles-ci accessibles à tout internaute effectuant une recherche à partir du nom de la personne concernée, y compris aux internautes qui, autrement, n'auraient pas trouvé la page web sur laquelle ces mêmes données sont publiées. De plus, l'organisation et l'agrégation des informations publiées sur Internet effectuées par les moteurs de recherche dans le but de faciliter à leurs utilisateurs l'accès à celles-ci peut conduire, lorsque la recherche de ces derniers est effectuée à partir du nom d'une personne physique, à ce que ceux-ci obtiennent par la liste de résultats un aperçu structuré des informations relatives à cette personne trouvables sur Internet leur permettant d'établir un profil plus ou moins détaillé de la personne concernée. La Cour a encore précisé, à cet égard (points 39 et 40 de l'arrêt), que la circonstance que les éditeurs de sites web ont la faculté d'indiquer aux exploitants de moteurs de recherche, à l'aide notamment de protocoles d'exclusion comme "robot.txt" ou de codes comme "noindex" ou "noarchive", qu'ils souhaitent qu'une information déterminée, publiée sur leur site, soit exclue en totalité ou partiellement des index automatiques de ces moteurs ne signifie pas que l'absence d'une telle indication de la part de ces éditeurs libérerait l'exploitant d'un moteur de recherche de sa responsabilité pour le traitement des données à caractère personnel qu'il effectue dans le cadre de l'activité de ce moteur. En effet, cette circonstance ne change pas le fait que les finalités et les moyens de ce traitement sont déterminés par cet exploitant. En outre, à supposer même que ladite faculté des éditeurs de sites web signifie que ceux-ci déterminent conjointement avec ledit exploitant les moyens dudit traitement, cette constatation n'enlèverait rien à la responsabilité de ce dernier, [l'art. 4, sous 7), du RGPD] prévoyant expressément que cette détermination peut être effectuée "seul ou conjointement avec d'autres".

La Cour a donc voulu consacrer une définition large de la notion de "responsable", afin d'assurer une protection efficace et complète des personnes concernées, de manière que les garanties prévues par le RGDP puissent développer leur plein effet[16] [17].

Sur la question centrale de l'étendue des droits des personnes concernées et des correspondantes obligations du responsable du traitement, la Cour a relevé (points 80 et 81) qu'au vu de la gravité potentielle de l'ingérence dans les droits fondamentaux représentée par ce traitement[18], ce dernier ne saurait être justifié par le seul intérêt économique de l'exploitant du moteur de recherche, et qu'il y a lieu de rechercher, par ailleurs, un juste équilibre entre l'éventuel intérêt légitime des internautes à avoir accès à l'information en cause et les droits fondamentaux du titulaire des données.

La Cour a toutefois ajouté (point 81) que les droits de la personne concernée prévalent, en règle générale, sur l'intérêt (*a fortiori*, la simple curiosité) des internautes, mais que cet équilibre peut dépendre, dans des cas particuliers, de la nature de l'information en question, de son ancienneté (16 ans, dans le cas d'espèce) 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.

Dans ce contexte, la Cour a encore renchéri (points 80 et 87) : en rendant des informations relatives à une personne contenues dans une page web plus

---

16 Voir points 34 et 38 de l'arrêt.

17 Cette même approche préside à la détermination du *champ d'application territorial* de la directive (et du RGPD). C'est ainsi que la Cour a précisé qu'une entreprise comme Google (ou Facebook) ayant son siège social dans un État tiers est soumise au RGPD, sans que ce soit nécessaire que l'opération de traitement soit effectuée par une filiale dans un État membre, dès lors qu'une telle opération a lieu "dans le cadre des activités" de cette dernière, notamment, comme dans le cas d'espèce, lorsque ces activités sont destinées à assurer, dans cet État membre (l'Espagne), la promotion et la vente des espaces publicitaires proposés par le moteur de recherche et servent à rentabiliser le service offert par ce moteur (points 52, 55 et 57).

18 La Cour (point 80) a souligné, à cet égard, qu'une recherche effectuée à l'aide d'un moteur de recherche, à partir du nom d'une personne physique, permet à tout internaute d'obtenir par la liste de résultats un aperçu structuré des informations relatives à la personne trouvables sur Internet, qui touchent potentiellement à une multitude d'aspects de sa vie privée et qui, sans ledit moteur, n'auraient pas ou seulement que très difficilement pu être interconnectées, et ainsi d'établir un profil plus ou moins détaillé de celle-ci.

facilement accessibles par un internaute, à partir de la liste de résultats affichée lors d'une recherche menée, en ligne, à partir du nom de cette personne, le traitement de données effectué par l'exploitant d'un moteur de recherche contribue à démultiplier de façon ubiquitaire la diffusion desdites informations et est, donc, susceptible de constituer une ingérence dans le droit fondamental au respect de la vie privée bien plus importante que la "simple" publication par l'éditeur de la page web (points 80 et 87)[19].

En plus, compte tenu de la facilité avec laquelle des informations publiées sur un site web peuvent être répliquées sur d'autres sites et du fait que les responsables de leur publication ne sont pas toujours soumis à la législation de l'Union, une protection efficace et complète des personnes concernées ne pourrait être réalisée si celles-ci devaient d'abord ou en parallèle obtenir l'effacement des informations les concernant auprès des éditeurs de sites web.

La Cour en a conclu (points 88 et 98) que, dès lors que les conditions établies dans la directive ou le RGPD sont vérifiées, la personne concernée justifie d'un droit à exiger la suppression des liens avec ces informations à partir de son nom dans la liste de résultats, en tout état de cause dans la mesure où il n'existe pas de raisons particulières justifiant un intérêt prépondérant du public à avoir accès à ces informations.

Une telle demande peut être adressée directement à l'exploitant du moteur de recherche, en tant que responsable du traitement, qui doit dûment examiner le bien-fondé de cette demande et, le cas échéant, y faire droit, même lorsque la publication des informations en question sur les pages web de tiers est en elle-même licite et sans que la personne concernée ait à démontrer que l'inclusion de ces informations dans la liste de résultats, associées au nom de cette personne, lui cause un préjudice (point 96).

Lorsque le responsable du traitement ne donne pas suite à ces demandes, la personne concernée peut saisir l'autorité de contrôle ou l'autorité judiciaire pour que celles-ci effectuent les vérifications nécessaires et ordonnent à ce responsable des mesures appropriées (point 77).

---

[19] Voir également, en ce sens, arrêt du 5.10.2011, eDate Advertising e.a., C-509/09 et C-161/10, EU:C:2011:685, point 45. Ainsi que la Cour l'a expliqué, « la mise en ligne de contenus sur un site Internet se distingue de la diffusion territorialisée d'un média tel un imprimé en ce qu'elle vise, dans son principe, à l'ubiquité desdits contenus. Ceux-ci peuvent être consultés instantanément par un nombre indéfini d'internautes partout dans le monde, indépendamment de toute intention de leur émetteur visant à leur consultation au-delà de son État membre d'établissement et en dehors de son contrôle.»

2. LA JURISPRUDENCE POSTERIEURE À L'ARRÊT GOOGLE SPAIN

Comme on pouvait s'y attendre, l'arrêt Google Spain a ouvert la porte à de nombreuses demandes de citoyens intéressés à voir leurs noms et les informations y associées éliminées des listes de résultats affichés dans les recherches Google.

Certes, l'arrêt Google Spain a contribué à clarifier bon nombre de concepts liés à la protection de la vie privée et des données personnelles dans l'ère du numérique.

Mais, bien évidemment, les questions posées à la Cour étaient loin de permettre un éclaircissement complet de tous les doutes soulevés par la législation pertinente dans ce nouveau contexte.

Trois arrêts postérieurs permettent d'exemplifier cette activité de la Cour dans l'interprétation des notions contenues aujourd'hui dans le RGPD.

2.1. L'arrêt Wirtschaftsakademie Schleswig-Holstein

Considérons, tout d'abord, l'arrêt de juin 2018[20], ayant son origine dans un renvoi préjudiciel d'une juridiction allemande (le *Bundesverwaltungsgericht*), dans une affaire opposant l'Autorité régionale indépendante de protection des données du Schleswig-Holstein à une société de droit privée (ci-après, la *Wirtschaftsakademie*), spécialisée dans le domaine de l'éducation et de la formation, au sujet de la légalité d'une injonction faite par ladite autorité à cette société de désactiver sa page fan (*fan page*) hébergée sur Facebook.

Il s'agissait, en substance, de savoir si et dans quelle mesure l'administrateur d'une telle page fan doit être considéré comme étant *responsable du traitement* relativement aux données personnelles des visiteurs de ladite page.

À cet égard, la Cour (point 30) a constaté que, en l'occurrence, Facebook détermine, à titre principal, les finalités et les moyens du traitement des données à caractère personnel des utilisateurs de son réseau ainsi que des personnes ayant visité les pages fan hébergées sur ce dernier, et relève ainsi de la notion de "responsable du traitement".

Cependant, étant donné que, selon l'art. 2, sous d), de la directive [art. 4, sous 7) du RGPD], la notion de "responsable du traitement" vise l'organisme qui, "*seul ou conjointement avec d'autres*", détermine les finalités et les moyens du traitement de données, cette notion ne renvoie pas nécessairement

[20] Arrêt du 5.6.2018, C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein contre Wirtschaftsakademie Schleswig-Holstein GmbH, EU:C:2018:388.

à un organisme unique et peut concerner plusieurs acteurs participant à ce traitement (point 29).

Dans ces circonstances, l'administrateur d'une page fan hébergée sur Facebook, tel que la *Wirtschaftsakademie*, doit être qualifié de responsable au sein de l'Union, conjointement avec Facebook Ireland, de ce traitement, dans la mesure où il participe, par une action de paramétrage, en fonction de son audience cible et d'objectifs de gestion ou de promotion, à la détermination des finalités et des moyens du traitement des données personnelles des visiteurs de sa page fan (point 39)[21]. Et ceci, même si l'existence d'une responsabilité conjointe n'implique pas qu'elle soit équivalente pour les différents opérateurs concernés (point 43).

Cette notion de "responsabilité conjointe" a été densifié dans les arrêts Témoins de Jeovah[22] et Fashion ID[23], comme visant toute personne physique ou morale qui influe, à des fins qui lui sont propres, sur le traitement de données à caractère personnel et participe de ce fait à la détermination des finalités et des moyens de ce traitement selon différents degrés, compte tenu du niveau de responsabilité de chacun, même si chacun d'eux n'a eu accès à l'ensemble des données en question.

2.2. L'arrêt Google LLC/CNIL

Prenons ensuite un autre exemple, celui de la *portée territoriale* de l'obligation de l'exploitant d'un moteur de recherche de supprimer les liens

[21] La Cour a précisé, à cet égard, que l'administrateur d'une page fan peut, à l'aide de filtres mis à sa disposition par Facebook, définir les critères à partir desquels doivent être établies des statistiques à partir des visites de la page fan et même désigner les catégories de personnes qui vont faire l'objet de l'exploitation de leurs données par Facebook (point 36). Dans ces conditions, le fait pour un administrateur d'une page fan d'utiliser la plateforme mise en place par Facebook, afin de bénéficier des services y afférents, ne saurait l'exonérer du respect de ses obligations en matière de protection des données à caractère personnel (point 40). De surcroît, il importe de noter que les pages fan hébergées sur Facebook peuvent être visitées également par des personnes qui ne sont pas utilisateurs de Facebook et qui ne disposent donc pas d'un compte utilisateur sur ce réseau social. Dans ce cas, la responsabilité de l'administrateur de la page fan à l'égard du traitement des données de ces personnes apparaît encore plus importante, en vue d'une protection complète des droits de ces personnes, car la simple consultation de la page fan par des visiteurs déclenche automatiquement le traitement de leurs données à caractère personnel (points 41 et 42).

[22] Arrêt du 10.7.2018, Témoins de Jeovah, C-25/17, EU:C:2018:551, points 66-68.

[23] Arrêt du 29.7.2019, Fashion ID, C-40/17, EU:C:2019:629, points 68-70.

vers des pages web contenant certaines informations le concernant, question qui a fait l'objet de l'arrêt Google LLC/CNIL – Commission nationale de l'informatique et des libertés, suite à un renvoi préjudiciel du Conseil d'État français[24].

Dans la procédure nationale qui était à l'origine de cette affaire devant la Cour, Google a refusé de donner suite à une injonction de la CNIL visant à ce qu'il supprime lesdits liens *sur toutes les extensions de nom de domaine de son moteur de recherche*[25].

Dans ses conclusions (paragraphe 36), l'avocat général Szpunar a rejeté, pour séduisante qu'elle puisse paraître, au vu de sa radicalité, sa clarté, sa simplicité et son efficacité, l'idée d'un déréférencement (effacement) mondial, car elle tient compte d'un seul côté de la médaille, à savoir la protection des données d'un individu.

À son avis (paragraphe 46), une différenciation s'imposerait donc selon le lieu à partir duquel la recherche est effectuée.

Dans son arrêt, la Cour (points 56 à 58) ne manqua pas de souligner le caractère mondial et sans frontières du réseau d'Internet, ce qu'elle considéra de nature à justifier l'existence d'une compétence du législateur de l'Union pour prévoir une obligation, imposée à l'exploitant d'un moteur de recherche, de procéder, le cas échéant, à un déréférencement sur l'ensemble des versions de son moteur de recherche.

Elle souligna, toutefois (points 59 et 60), non seulement que de nombreux États tiers ne connaissaient pas le droit à l'effacement ou adoptaient une approche différente, mais aussi que, conformément au principe de proportionnalité, le droit à la protection des données à caractère personnel n'est pas un droit absolu, devant être considéré par rapport à sa fonction dans la société et mis en balance avec d'autres droits fondamentaux, comme la liberté d'information des internautes, ce qui est susceptible de varier de manière importante à travers le monde.

La Cour conclut alors (points 64, 65 et 72) que, même s'il *ne l'interdit pas*, le droit de l'Union *n'impose pas*, non plus, en l'état actuel, que le déréférencement auquel il serait fait droit porte sur l'ensemble des versions du moteur de recherche en cause.

Est-ce alors qu'un tel déréférencement doit s'effectuer sur les versions du moteur de recherche correspondant aux États membres ou sur la seule version

[24] Arrêt du 24.9.2019, C-507/17, Google LLC/CNIL, EU:C:2019:772.

[25] Google était d'avis que cette suppression ne se justifiait qu'à l'égard des seuls résultats affichés en réponse à des recherches effectuées depuis les noms de domaine correspondant aux déclinaisons de son moteur dans les seuls États membres.

de ce moteur correspondant à *l'État membre de résidence* du bénéficiaire de la mesure?

À cette question, la Cour répond (point 66) que, puisque le législateur de l'Union a désormais choisi de fixer les règles en matière de protection des données par la voie d'un règlement (le RGPD), qui est directement applicable dans tous les États membres, afin d'assurer un niveau cohérent et élevé de protection dans l'ensemble de l'Union et de lever les obstacles aux flux de données au sein de celle-ci, le droit à l'effacement est, en principe, censé opérer pour l'ensemble des États membres.

Elle relève, néanmoins (point 67), que la perception de l'intérêt du public à accéder à une information peut, même au sein de l'Union, varier d'un État membre à l'autre, de sorte que le résultat de la mise en balance à effectuer entre les différentes exigences de protection n'est pas forcément le même pour tous les États membres[26].

2.3. *L'arrêt GC e.a./CNIL et le droit à l'oubli*

Enfin, une autre affaire (GC e.a./CNIL, C-136/17) a permis à la Cour de se prononcer, par arrêt de la même date du précédent[27], sur la portée du fameux "droit à l'oubli" lorsque sont en cause certaines catégories de *données personnelles particulièrement sensibles*.

L'art. 9, paragraphe 1, du RGPD (ancien art. 8, paragraphe 1, de la directive) dispose que – sous réserve des exceptions prévues au paragraphe 2 – le 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 ou des données biométriques aux fins d'identifier une personne physique de manière unique, ou encore le traitement des données concernant

[26] À cet égard, la Cour souligne (point 68) l'importance des mécanismes de coopération entre les autorités nationales compétentes, prévus dans le RGPD afin de parvenir à un consensus et à une décision unique qui puisse lier l'ensemble de ces autorités et dont le responsable du traitement doit assurer le respect dans le cadre de tous ses établissements dans l'Union. Il incombe, en outre, à l'exploitant du moteur de recherche de prendre, si nécessaire au moyen de la technologie du "géo-blocage", des mesures suffisamment efficaces pour assurer une protection effective des droits fondamentaux de la personne concernée.

[27] Arrêt du 24.9.2019, GC e.a./CNIL - Commission nationale de l'informatique et des libertés, C-136/17, EU:C:2019:773.

la santé ou la vie ou l'orientation sexuelle d'une personne physique *sont interdits*[28].

Les interdictions et restrictions imposées par ces dispositions, s'appliquent-elles également à l'exploitant du moteur de recherche et pas seulement au responsable du site web qui héberge les informations auxquelles ce moteur renvoie? Telle était la première question à laquelle la Cour était appelée à répondre.

Dans son arrêt, au terme d'une analyse qui suivit sa méthode traditionnelle d'interprétation (texte, contexte et objectifs), la Cour réaffirma le principe selon lequel l'exploitant d'un moteur de recherche doit, à l'instar de tout autre responsable, assurer, dans le cadre de ses responsabilités, de ses compétences et de ses possibilités, que le traitement des données à caractère personnel sensibles qu'il effectue satisfait aux exigences, selon le cas, de la directive ou du RGPD. Ceci est d'autant plus nécessaire qu'il s'agit de catégories de données à l'égard desquelles une protection accrue s'impose.

Cela dit, et à l'instar de ce qu'avait également indiqué l'avocat général Szpunar dans ses conclusions, la Cour déclara qu'il n'est pas possible d'appliquer à un exploitant d'un moteur de recherche les interdictions et restrictions édictées à l'art. 9 du RGPD *comme si cet exploitant avait lui-même fait figurer les données sensibles dans les pages Internet référencées*.

En effet[29], l'exploitant d'un moteur de recherche n'est responsable que du référencement d'une page web publiée par un tiers et, tout particulièrement, de l'affichage du lien vers celle-ci dans la liste des résultats présentée aux internautes à la suite d'une recherche effectuée à partir du nom d'une personne.

Ainsi, les interdictions et restrictions prévues pour les données sensibles ne peuvent s'appliquer à un moteur de recherche que par l'intermédiaire d'une vérification à effectuer ex post par l'exploitant de ce moteur, sous le contrôle des autorités nationales compétentes, sur la base d'une demande formée par la personne concernée (arrêt, points 41-48; conclusions, paragraphes 49-57).

Cela étant, est-ce que l'exploitant d'un moteur de recherche est obligé, sous réserve des exceptions prévues, de faire droit à toute demande d'effacement relatives à des données à caractère personnel relevant des catégories

[28] L'art. 10 du RGPD prévoit, pour sa part, les conditions dans lesquelles le traitement des données à caractère personnel relatives aux condamnations pénales ou mesures connexes peut être effectué. De même, l'art. 18 prévoit les circonstances dans lesquelles la personne concernée a le droit d'obtenir du responsable du traitement la limitation de ce dernier.

[29] Ainsi que la Commission l'a souligné elle-même (voir point 46 de l'arrêt).

particulièrement sensibles, ou a-t-il la possibilité de refuser de faire droit à une telle demande ?

À ces questions la Cour a répondu (points 55-58), en substance, que, même si, en vertu du paragraphe 1 de l'art. 17 du RGPD, l'exploitant d'un moteur de recherche est en principe obligé de faire droit aux demandes d'effacement lorsque l'un des motifs énumérés dans cette disposition s'applique, l'imposition d'exceptions[30] ou de limitations au droit à l'effacement (parmi lesquelles figurent les nécessaires à l'exercice du droit à la liberté d'expression et d'information – art. 17, paragraphe 3, sous a)) constitue une expression du fait que le droit à la protection des données à caractère personnel n'est pas un droit absolu, mais doit être considéré par rapport à sa fonction dans la société et être mis en balance avec d'autres droits fondamentaux.

Au surplus, toute restriction à l'exercice des droits consacrés aux arts. 7 et 8 de la Charte doit respecter les conditions établies dans l'art. 52, paragraphe 1, de la Charte, à savoir, que ces restrictions sont prévues par la loi, respectent le contenu essentiel desdits droits et libertés et, dans le respect du principe de proportionnalité, sont nécessaires et répondent effectivement à des objectifs

[30] Notamment, lorsque la personne concernée donne son consentement explicite. Il résulte de la définition de la notion de "consentement" fournie à l'art. 4, point 11, du RGPD que ce consentement doit être "spécifique" et, donc, porter spécifiquement sur le traitement effectué dans le cadre de l'activité du moteur de recherche et ainsi sur le fait que ce traitement permet à des tiers d'obtenir, au moyen d'une recherche à partir du nom de cette personne, une liste de résultats incluant des liens menant vers des pages web qui contiennent des données sensibles la concernant. Or, il est, en pratique, difficilement envisageable que l'exploitant d'un moteur de recherche sollicite le consentement explicite des personnes concernées avant de procéder, pour les besoins de son activité de référencement, au traitement des données à caractère personnel les concernant. En tout état de cause, le fait même qu'une personne formule une demande de déréférencement signifie, en principe, que, à tout le moins à la date de cette demande, elle ne consent plus au traitement effectué par l'exploitant du moteur de recherche. Dans ce contexte, il convient également de rappeler que l'art. 17, paragraphe 1, sous b), dudit règlement vise, parmi les motifs justifiant le "droit à l'oubli", la circonstance que la personne concernée retire le consentement sur lequel est fondé le traitement, conformément à l'art. 9, paragraphe 2, sous a), du même règlement, et qu'il n'existe pas d'autre fondement juridique au traitement (point 62). En revanche (point 63), lorsque les données en cause ont manifestement été rendues publiques par la personne concernée, l'art. 9, paragraphe 2, sous e), du RGPD a vocation à s'appliquer tout autant à l'exploitant du moteur de recherche qu'à l'éditeur de la page web en question.

d'intérêt général reconnus par l'Union ou au besoin de protection des droits et des libertés d'autrui.

De même, l'exploitant d'un moteur de recherche est tenu de faire droit à une demande de déréférencement portant sur des liens vers des pages web, sur lesquelles figurent des informations relatives à une procédure judiciaire dont une personne physique a été l'objet ainsi que, le cas échéant, celles relatives à la condamnation qui en a découlé, lorsque ces informations se rapportent à une étape antérieure de la procédure judiciaire en cause et ne correspondent plus à la situation actuelle, dans la mesure où il est constaté que, eu égard à l'ensemble des circonstances de l'espèce, les droits fondamentaux de la personne concernée, garantis par les arts. 7 et 8 de la Charte, prévalent sur ceux des internautes potentiellement intéressés, protégés par l'art. 11 de cette Charte (points 77-79).

III. LA PROTECTION DES LIBERTÉS PUBLIQUES CONTRE LES AGISSEMENTS DES POUVOIRS PUBLICS

Jusqu'à présent, je me suis penché sur la réponse donnée par la Cour de justice aux délicates questions posées par la protection des droits des particuliers contre le traitement de ses données personnelles par des opérateurs de l'ère digitale sur Internet.

J'aimerais maintenant, pour terminer, consacrer quelques lignes à une autre dimension du problème: la protection des libertés publiques contre les agissements des pouvoirs publics et leur interaction avec les droits fondamentaux.

1. L'ARRÊT DIGITAL RIGHTS IRELAND

Tout d'abord, je voudrais me référer à l'arrêt de la Cour dans les affaires Digital Rights Ireland et Sitlinger[31].

Considéré comme une "première juridictionnelle mondiale"[32] sur la conservation des données et les libertés publiques, cet arrêt témoigne de la volonté de la Cour d'exercer un contrôle approfondi de la marge d'appréciation du législateur de l'Union en matière de droits fondamentaux dans l'ère digitale.

[31] Arrêt du 8.4.2014, Digital Rights Ireland et Sitlinger, C-293/12 et C -594/12, EU:C:2014:238.

[32] Jean-Claude Bonichot (2016). La Cour de justice de l'Union européenne et les nouvelles technologies de l'information: vers une Cour 2.0?. *Petites affiches*, 53, 8-22.

À la suite des attentats terroristes de Madrid et de Londres en 2004 et 2005, et afin de promouvoir le rapprochement des législations nationales approuvées par différents États membres "en ordre dispersé", l'Union a adopté la directive 2006/24[33], mettant en place un dispositif commun de conservation des données générées ou traitées par les fournisseurs des services de communications électroniques, en vue de garantir la disponibilité de ces données à des fins de recherche, de détection et de poursuite d'infractions graves, liées notamment à la criminalité organisée et au terrorisme.

Dans un arrêt qui a fait l'objet de nombreux commentaires dans la doctrine, la Cour a déclaré l'invalidité de la directive dans son entièreté, sans même admettre, contrairement à ce que lui suggérait, prudemment, M. l'avocat général Pedro Cruz-Villalón dans ses conclusions, un aménagement des effets de l'arrêt dans le temps, notamment afin de permettre l'adoption, par le législateur de l'Union, dans un délai raisonnable, les mesures appropriées à remédier à l'invalidité constatée.

S'écartant d'une jurisprudence traditionnelle selon laquelle le contrôle juridictionnel des actes législatifs dans des domaines impliquant des choix de nature politique, économique ou sociale est, par définition, limité, la Cour a déclaré qu'en matière de droits fondamentaux, ce contrôle se doit d'être "strict" ou "étroit", dès lors que, comme dans le cas d'espèce, le pouvoir d'appréciation du législateur de l'Union s'avère réduit en raison de la gravité de l'ingérence dans les droits fondamentaux au respect de la vie privée et des données personnelles.

En effet, la Cour a estimé que, même si les données à conserver excluaient le contenu des communications[34], ces données, prises dans leur ensemble, étaient susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales et les milieux sociaux fréquentés par ces personnes (point 27).

Elle a donc considéré que la réglementation de l'Union devrait prévoir des règles claires et précises imposant un minimum de garanties contre les

[33] Directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE – JO L 105/54, 13.4.2006.

[34] Elles ne concernaient que des catégories de données telles que l'identification de la source et de la destination de la communication, la date, l'heure et la durée de la communication, ainsi que le type de communication, le matériel utilisé et sa localisation.

risques d'abus ainsi que contre tout accès ou utilisation illicite[35]. Or, la directive ne prévoyait aucun contrôle préalable par une autorité judiciaire ou administrative indépendante ; de surcroît, elle instituait un mécanisme de rétention et de conservation des données portant, sans limitations assurant une relation entre ces données et une menace pour la sécurité publique, sur toutes les données relatives au trafic concernant la téléphonie fixe, la téléphonie mobile, l'accès à l'internet, le courrier électronique ainsi que la téléphonie par Internet.

La Cour a ainsi soumis le système de la directive 2006/24 à un contrôle de proportionnalité, à la suite duquel elle a conclu que ladite directive ne prévoyait pas de garanties suffisantes contre les abus et les utilisation illicites, d'autant plus que la durée de conservation des données (entre six mois et deux ans) pouvait s'avérer excessive, qu'il n'était pas imposé que les données en cause soient conservées sur le territoire de l'Union et, par-dessus tout, que le système en cause comportait une ingérence dans les droits fondamentaux de la quasi-totalité de la population européenne.

Bref, l'on peut conclure que, par son arrêt Digital Rights, la Cour a condamné tout système qui conduise à instituer, pour des raisons de prévention et de poursuite de la criminalité organisée et du terrorisme, une "conservation préventive de masse" des données des communications électroniques[36].

---

[35] La Commission a ignoré, dans sa proposition de directive, un certain nombre de recommandations en ce sens formulées par le Comité des Libertés civiles, Justice et Affaires intérieures du Parlement européen.

[36] À la suite de l'invalidation de la directive 2006/24 par l'arrêt Digital Rights, la Cour de justice a été saisie de renvois préjudiciels en provenance de deux juridictions, l'une suédoise, l'autre britannique, concernant l'incidence dudit arrêt sur les réglementations nationales imposant aux opérateurs de télécommunications de conserver les données relatives aux communications électroniques. Dans son arrêt du 21.12.2016, Tele2 Sverige et Tom Watson, C-203/15 et C-698/15, EU:C:2016:970, la Cour a statué que l'art. 15, paragraphe 1, de la directive 2002/58 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), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009, lu à la lumière de la charte des droits fondamentaux de l'Union européenne, devait être interprété en ce sens qu'il s'opposait à une réglementation nationale prévoyant, à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique ainsi qu'à une réglementation

Au législateur de l'Union d'assurer la suite à donner à la déclaration d'invalidité de la directive 2006/24, en prévoyant un régime qui, sans préjudice de l'efficacité dans la poursuite des objectifs impératifs de sécurité publique qui étaient les siens, satisfasse les exigences de protection des droits fondamentaux de l'ensemble des citoyens.

2. JURISPRUDENCE DE LA COUR SUR DES ACTES DES POUVOIRS PUBLICS RELATIFS À LA DIFFUSION DES DONNÉES : L'ARRÊT VOLKER UND MARKUS SCHENKER

Pour terminer, j'aimerais faire une brève référence à deux arrêts de la Cour qui concernent également la protection des personnes contre des actes des pouvoirs publics, relatifs non pas à la rétention des données mais à leur diffusion ou leur transfert en dehors de l'Union.

Le premier de ces arrêts, dans l'affaire Volker und Markus Schenker[37], permet d'illustrer les difficultés de concilier le *principe de la transparence* avec le *respect de la vie privée et des données personnelles*.

Afin d'accroître la transparence de l'utilisation des fonds communautaires dans le cadre de la politique agricole commune (PAC) et de renforcer le contrôle public de l'utilisation des sommes concernées, le Conseil et la Commission ont adopté des règlements prévoyant la publication sur un site web des noms des bénéficiaires ainsi que du montant des aides accordées aux agriculteurs.

Un certain nombre de bénéficiaires en Allemagne se sont plaints que la publication de leurs noms, lieu d'établissement, code postal, ainsi que des montants reçus dans le site web de l'Office fédéral pour l'agriculture et l'alimentation, auquel l'on pouvait accéder à l'aide d'un moteur de recherche, les rendait la cible de la curiosité et des remarques désobligeantes de leurs concitoyens, leur causant de sérieux désagréments.

Saisie par une juridiction allemande, la Cour a considéré que, s'agissant des personnes physiques, une telle publication – qui n'opérait aucune distinction selon des critères pertinents, tels que les périodes pendant lesquelles les aides

prévoyant 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.

37 Arrêt du 9.11.2010, Volker und Markus Schenker et Eifert, C-92/09 et C-93/09, EU:C:2010:662.

ont été perçues, la fréquence ou encore le type et l'importance de celles-ci – constituait une atteinte excessive aux droits reconnus à ces personnes par les arts. 7 et 8 de la Charte, qui ne pouvait se justifier par les objectifs légitimes visés par le législateur[38].

En revanche, pour ce qui concerne les personnes morales, la Cour a indiqué que celles-ci ne pouvaient se prévaloir de la protection des arts. 7 et 8 de la Charte que dans la mesure où le nom légal de la personne morale identifiait une ou plusieurs personnes physiques, comme c'était le cas de la société Volker und Markus Schecke.

À la suite de cet arrêt, et dans l'attente de l'adoption de nouvelles règles, la Commission a modifié son règlement afin d'établir clairement que l'obligation de publier des informations sur les bénéficiaires ne s'appliquait pas aux personnes physiques.

Plus tard, le règlement 1306/2013 du Parlement et du Conseil[39] a réintroduit l'obligation de publication pour tous les bénéficiaires, dont les modalités ont été modifiées dans le but de les rendre compatibles avec le principe de proportionnalité, tel qu'interprété par la Cour dans son arrêt (p. ex., par l'introduction de seuils en dessous desquels une telle obligation ne s'applique pas).

3. JURISPRUDENCE DE LA COUR SUR DES ACTES DES POUVOIRS PUBLICS RELATIFS AU TRANSFERT DES DONNÉES EN DEHORS DE L'UNION: L'ARRÊT SCHREMS

Enfin, dans l'arrêt Schrems[40], de 2015, la Cour s'est prononcée sur la légitimité du transfert de données personnelles vers les États Unis.

L'affaire a eu son origine dans un recours introduit en Irlande, siège européen de Facebook, par M. Schrems, citoyen autrichien client de Facebook, qui s'opposait, devant le Data Protection Commissioner, à ce que ses données personnelles soient envoyées sur des serveurs aux États Unis, au motif que les

[38] La Cour a précisé, par ailleurs, qu'une simple information préalable selon laquelle les données étaient susceptibles d'être publiés ne pouvait être considérée comme un consentement des personnes concernées.

[39] 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 et abrogeant les règlements (CEE) n° 352/78, (CE) n° 165/94, (CE) n° 2799/98, (CE) n° 814/2000, (CE) n° 1200/2005 et n° 485/2008 du Conseil - OJ L 347, 20.12.2013, p. 549-607.

[40] Arrêt du 6 octobre 2015, Maximillian Schrems / Data Protection Commissioner, C-362/14,EU:C:2015:650.

autorités américaines y avaient accès, comme le prouveraient les révélations d'Edward Snowden, sur les pratiques de la NSA et du FBI.

Sa demande d'une injonction a été rejetée par le Commissioner au motif que la Commission européenne avait déjà pris une décision, en 2000, constatant, sur la base de l'art. 25, paragraphe 1, de la directive 95/46 (aujourd'hui ce serait l'art. 44 du RGPD), que les États-Unis offraient une protection adéquate aux données transférées vers les serveurs internet d'une organisation située aux États Unis (Facebook, dans le cas d'espèce) qui s'était engagée à respecter un certain nombre de "directives" du ministère du Commerce des États Unis, accompagnées de "frequently asked questions".

La Cour, après avoir précisé les pouvoirs respectifs des autorités nationales et de la Commission et souligné qu'il est essentiel de pouvoir soumettre toute décision prise, tant au niveau national qu'à celui de l'Union, au contrôle des juridictions compétentes, a interprété la notion de "niveau de protection adéquat" figurant à l'art. 25, paragraphe 6, de la directive 95/46, comme exigeant d'un pays tiers qu'il assure, certes, non pas un niveau de protection "identique", mais, du moins, "un niveau de protection des libertés et droits fondamentaux substantiellement équivalent à celui garanti au sein de l'Union" (point 73). Ce niveau étant susceptible d'évoluer dans l'État tiers concerné, la Commission doit évaluer périodiquement la situation et il appartient à la Cour de constater, le cas échéant, que la décision de la Commission est devenue illégale du fait du changement des circonstances de droit ou de fait.

Au terme d'une analyse approfondie des caractéristiques propres du système américain et de son application, la Cour est parvenue à la conclusion que ce système n'offrait pas de garanties suffisantes de protection, notamment en ce qu'il autorisait la conservation généralisée de l'intégralité des données transférées, sans qu'aucune différentiation, limitation ou exception soit opérée en fonction des objectifs poursuivis, qu'il comportait un système d'auto-certification s'appliquant aux entreprises mais pas aux autorités publiques, qui pouvaient accéder de manière généralisée au contenu des communications électroniques, et qu'en plus il reconnaissait la primauté des principes de la sécurité nationale des États Unis sur le droit de la personne concernée à la protection de ses données qui ont été transférées, sans que des voies de droit, administratives ou judiciaires, n'existent afin de permettre la rectification ou la suppression de certaines de ces données.

La décision 2000/520 de la Commission a donc été déclarée invalide dans sa totalité, puisque, de surcroît, elle conduisait à priver les autorités nationales de contrôle des pouvoirs qui leur étaient conférés par la directive.

IV. CONCLUSIONS

Au terme de ce tour d'horizon sur la jurisprudence, il me paraît pertinent de tirer une conclusion importante, à savoir que la Cour de justice en sort renforcée dans son rôle de garant des libertés et des droits fondamentaux dans l'ordre juridique de l'Union, dans un domaine nouveau, qui a fait naître des défis d'une ampleur et d'une complexité difficiles à imaginer il y a quelques années.

Cependant, de nouvelles étapes de ce parcours – qui semblerait ne connaître de limites qu'à l'infini ! – se dessinent déjà à l'horizon du contentieux. En effet, la Cour devrait être appelée, plus tôt ou plus tard, à se prononcer sur les implications juridiques en droit européen d'innovations technologiques plus révolutionnaires telles que l'intelligence artificielle, la robotisation et les voitures sans conducteur, sans oublier d'autres déjà établies mais dont les développements conduisent de plus en plus les législateurs nationaux à vouloir intervenir par le biais de réglementations diverses. Ce dernier est le cas de la dénommée "économie de partage" (*sharing economy*) – Uber, *airbnb*, etc.

À côté du changement climatique, ces nouvelles étapes du développement humain devraient marquer, du point de vue de la protection des droits fondamentaux, les années à venir.