Guide de la jurisprudence européenne en matière de protection des données à caractère personnel

Cour Européenne des Droits de l'Homme et Cour de Justice de l'Union Européenne

Version 0.9.18
14 juin 2018

Julien Rossi
julien.rossi@utc.fr
www.julienrossi.com
Twitter : @julienrossi

Table des matières

Introduction....5
1. Champ d'application de la directive 95/46/CE....6
1.A. Absence de nécessité d'un élément transfrontalier et de lien avec la libre-circulation....6
1.B. La relation entre l'art. 8 CEDH et la directive 95/46/CE....7
1.C. Directive 95/46/CE : une directive d'harmonisation complète....8
1.D. Notion de donnée à caractère personnel....9
1.E. Catégories de traitements de données couvertes par la directive 95/46/CE....12
1.E.a. Données personnelles traitées à des fins « exlusivement personnelles ou domestiques » 12
1.E.b. L'application de la directive 95/46/CE aux établissements de droit public et ses limites 12
1.F. Sur la notion de traitement de données....14
1.F.a. Définition de la notion de traitement....14
1.F.b. Traitement automatisé en tout ou partie....14
1.G. Sur les notions de responsable de traitement et de sous-traitant....15
1.G.a. Définitions....15
1.G.b. Le cas particulier de la sous-traitance de la facturation d'une prestation de services de télécommunications à une agence de recouvrement (impliquant tant les directives 95/46/CE que 2002/58/CE)....15
1.H. Champ d'application territorial de la directive 95/46/CE et notion d'établissement au sens de cette directive....17
1.I. Détermination du droit national applicable....19
2. Principe de légalités : les bases légales des traitements....21
2.A. Consentement....21
2.A.a. Consentement libre et éclairé....22
2.A.b. Cas particulier du croisement avec l'article 12 de la directive ePrivacy (2002/58/CE) et l'article 25 de la directive service universel (2002/22/CE)....22
2.A.c. Le statut des fichiers « robots.txt »....22
2.B. Les traitements de données nécessaires à l'exécution d'une mission de service public ou relevant de l'autorité publique (art. 7 sous e) de la directive 95/46/CE)....23
2.C. Les traitements fondés sur l'intérêt légitime du responsable de traitement (art. 7 sous f) de la directive 95/46/CE)....23
3. Principe de loyauté et droits des personnes concernées....26
3.A. Test de proportionnalité, ingérence et notion de mise en balance des intérêts....26
3.B. La limite de la durée de conservation des données....31
3.C. L'information des personnes concernées (et la possibilité de la restreindre)....33
3.D. Droit d'opposition....34
3.E. Droit d'accès et de rectification des personnes concernées....35
3.F. Droit au déréférencement (droit à l'oubli ?)....36
3.F.a. Présentation du droit au déréférencement....37
3.F.b. Les limites du droit au déréférencement....37
3.G. Droit à la suppression de données personnelles collectées dans le cadre d'une procédure

pénale....38
3.H. Recevabilité de données à caractère personnel dans le cadre d'une procédure judiciaire....38
4. Surveillance d'État (dont la question des fichiers de police)....40
4.A. Cadre général....40
4.B. La surveillance d'État dans la jurisprudence de la CJUE....44
4.C. Surveillance par géolocalisation....46
4.D. Question de l'accès aux données personnelles par les autorités publiques autre que des autorités de police, et de sa communication....47
4.E. La question des procédures d'habilitation au secret de la défense....48
5. Surveillance sur le lieu de travail....50
5.A. Principes généraux....50
5.B. Activités de détective privé dans le cadre d'une enquête disciplinaire....52
6. Protection des données personnelles dans le cadre de la liberté de l'information et de l'Open Data 54
7. Le principe de sécurisation des données....57
8. Transfert de données personnelles vers des pays tiers....59
9. Les autorités de protection des données personnelles (APDP) prévues à l'article 28 de la directive 95/46/CE....61
9.A. L'indépendance des autorités de protection des données....61
9.C. Autres éléments de jurisprudence sur les autorités de protection des données....63
9.C.1. Faut-il avoir saisi l'autorité de protection des données pour pouvoir saisir un juge ?....64
9.C.2. Dans le cadre de la directive 95/46/CE, quelle est l'autorité compétente ?....64
10. Lutte contre le téléchargement illégal....68
11. Les régimes particuliers....70
11.A. Détectives privés....70
11.B. Journalisme....70
11.C. Données de santé....71
11.D. Fins statistiques, historiques ou scientifiques....72
11.E. Le cas où la personne concernée est mineure....73
11.F. Données biométriques....74
ANNEXE : Liste des arrêts étudiés....76
ANNEXE : Liste des abréviations....79

Introduction

Le droit de la protection des données à caractère personnel est en Europe un droit qui, relativement à d'autres domaines, se caractérise par un fort niveau d'harmonisation, tant par le droit issu de la Convention européenne des droits de l'Homme que par le droit de l'Union européenne. Une jurisprudence assez extensive s'est donc développée, qui précise les différentes normes supranationales applicables, comme l'article 8 de la Convention européenne des droits de l'Homme, la convention 108 du Conseil de l'Europe, la directive 95/46/CE ou encore la directive 2002/58/CE. De nombreux arrêts montrent que l'ignorance du droit européen en matière de protection des données peut amener à des surprises : dans « ASNEF et FECEMD contre Administracion del Estado »[1], deux organisations professionnelles ont obtenu qu'une disposition nationale interdisant leurs traitements de données soit déclarée contraire au droit de l'Union. Dans « Commission contre Hongrie »[2], un arrêt du 8 avril 2014, la CJUE a réaffirmé son attachement à l'indépendance des autorités de protection des données, et constaté la violation par la Hongrie du droit de l'Union pour une affaire qui eût été évitée si le gouvernement de cet Etat avait mieux suivi la jurisprudence de la Cour de Luxembourg. Enfin, l'arrêt « Google contre Espagne »[3], qui consacre le droit au déréférencement, a également montré qu'une lecture attentive du droit de l'Union en matière de protection des données peut aboutir à des surprises qui méritent toute l'attention du chercheur ou du professionnel de la protection des données.

Inspiré d'un travail similaire effectué en 2014 lors d'un stage à la Commission nationale informatique et libertés (CNIL), ce guide, qui se veut le plus complet possible et a vocation à être régulièrement actualisé, s'inscrit dans un projet de recherche doctorale sur les politiques publiques de protection des données personnelles au laboratoire COSTECH de l'Université de Technologie de Compiègne, dont il est une production annexe.

Plutôt que de présenter une liste d'arrêts suivis de commentaires, ce guide est structuré selon une liste de thèmes. Sous chaque thème, une analyse combinée de plusieurs arrêts dégage une synthèse d'arrêts de la Cour de justice de l'Union européenne et de la Cour européenne des droits de l'Homme permet de saisir rapidement les principaux éléments de précision apportée par la jurisprudence à chaque notion ou disposition analysée. Ceci explique que certains arrêts puissent être cités à plusieurs endroits du guide. Des liens infratextuels permettent d'assurer la cohérence de l'ensemble.

1 CJUE 24 novembre 2011 « ASNEF et FECEMD contre Administracion del Estado », Aff. C-468/10 et C-469/10
2 CJUE 8 avril 2014 « Commission contre Hongrie », Aff. C-288/12
3 CJUE 8 avril 2014 « Google contre Espagne », Aff. C-131/12

1. Champ d'application de la directive 95/46/CE

La directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données s'applique au territoire de l'Union européenne et de l'Espace économique européen.

Le champ d'application de la directive est précisé par les considérants 12 à 16, 18 à 21, 26, 27 et l'article 3, l'article 4 précisant les règles relatives au droit national applicable.

1.A. Absence de nécessité d'un élément transfrontalier et de lien avec la libre-circulation

Une des premières affaires dont la CJCE a eu à connaître, l'affaire « Österreichischer Rundfunk »[4], portait sur une plainte formulée par des employés de la société de radiodiffusion de droit public éponyme souhaitant s'opposer à la publication de données personnelles concernant leur rémunération en vertu de dispositions relatives au contrôle de certains organismes publics. Il s'agissait d'une affaire strictement nationale, n'impliquant pas le transfert de ces données vers un autre Etat membre que l'Autriche. Fallait-il alors appliquer au traitement, en plus du droit national autrichien, le droit communautaire et donc la directive 95/46/CE ?

Plusieurs intervenants auprès de la Cour avaient fait valoir que selon eux, la directive 95/46/CE ne s'appliquait pas au cas d'espèce, puisque, comme expliqué ci-dessus, le traitement de données personnelles en question n'entravait pas les libertés du marché intérieur, au nombre desquelles figure **la libre-circulation des travailleurs**[5]. D'autres intervenants, dont une compagnie aérienne[6] et la Commission ont souhaité démontrer, selon des arguments différents, qu'il y avait bien dans l'affaire un élément transfrontalier et que, dès lors, le traitement n'était pas étranger à la question de la libre-circulation des travailleurs dans l'espace communautaire.

La **CJCE a jugé cependant qu'il n'était de toutes façons pas nécessaire de démontrer un lien effectif entre la libre circulation et le traitement en cause pour que la directive 95/46/CE s'applique**. En effet, **tout traitement est susceptible de circuler** entre les Etats membres de l'Union[7]. De surcroît, l'obligation de démontrer systématiquement un tel lien effectif serait nuisible à la **sécurité juridique** ainsi qu'à **l'effet utile** de la directive[8]. Enfin, la Cour analyse de façon détaillée le texte de la directive et démontre que l'intention du législateur communautaire était bien que la directive s'applique nonobstant l'absence éventuelle de lien direct avec la libre-circulation[9].

Le principe décrit ci-dessus a été confirmé avec l'arrêt « Lindqvist » : « La Cour a déjà jugé à propos de la directive 95/46, fondée sur l'article 100 A du traité, que le recours à cette base

4 CJCE 20 mai 2003 « Österreichischer Rundfunk » Aff. C-465/00, C-138/01 et C-139/01
5 CJCE 20 mai 2003 « Österreichischer Rundfunk » Aff. C-465/00, C-138/01 et C-139/01, pt. 37
6 CJCE 20 mai 2003 « Österreichischer Rundfunk » Aff. C-465/00, C-138/01 et C-139/01, pt. 34 et pt. 38
7 CJCE 20 mai 2003 « Österreichischer Rundfunk » Aff. C-465/00, C-138/01 et C-139/01, pt. 40
8 CJCE 20 mai 2003 « Österreichischer Rundfunk » Aff. C-465/00, C-138/01 et C-139/01, pt. 42
9 CJCE 20 mai 2003 « Österreichischer Rundfunk » Aff. C-465/00, C-138/01 et C-139/01, pts. 43-46

juridique **ne présuppose pas l'existence d'un lien effectif avec la libre circulation** entre États membres dans chacune des situations visées par l'acte fondé sur une telle base »[10]

1.B. La relation entre l'art. 8 CEDH et la directive 95/46/CE

L'Union européenne n'est pas partie à la Convention européenne des droits de l'Homme. Cependant, dès son arrêt « Lindqvist » du 6 novembre 2003[11], la CJCE a cité l'article 8 de la CEDH protégeant le droit à la vie privée dans la liste des dispositions applicables. Elle a également, depuis un précédent arrêt, calqué son test de proportionnalité de l'ingérence à ce droit sur le modèle du test opéré par la CEDH[12] (voir la partie sur le test de proportionnalité).

Le droit à la protection des données à caractère personnel, et notamment le règlement 45/2001/CE établissant un Contrôleur européen de la protection des données, a, selon la CJUE, notamment pour base l'article 8 de la CEDH[13]. Mais ce n'est pas sa base légale exclusive. En effet, le règlement 45/2001/CE comme la directive 95/46/CE visent avant tout la mise en œuvre des droits garantis aux article 7 et 8 de la Charte des droits fondamentaux de l'Union européenne. Ceux-ci garantissent le respect, respectivement, du droit à la vie privée et du droit à la protection des données à caractère personnel.

Dans l'arrêt « Tele2 Sverige » du 21 décembre 2016, la CJUE a refusé d'expliciter la relation entre l'art. 8 CEDH et les articles 7 et 8 CJUE en rappelant que :

> « Si, comme le confirme l'article 6, paragraphe 3, TUE, les droits fondamentaux reconnus par la CEDH font partie du droit de l'Union en tant que principes généraux, ladite convention ne constitue pas, tant que l'Union n'y a pas adhéré, un instrument juridique formellement intégré à l'ordre juridique de l'Union »[14]

L'article 8 de la CEDH sert donc de source d'inspiration mais n'est donc **pas un instrument juridique formel** du droit de l'Union. La CJUE a cependant toujours veillé à la **compatibilité de sa jurisprudence** avec celle de la CEDH. Elle a même, parfois, **cité des décisions de la CEDH** dans ses considérants pour justifier ses positions, comme celle sur les données biométriques :

> « Les empreintes digitales relèvent de cette notion dès lors qu'elles contiennent objectivement des informations uniques sur des personnes physiques et permettent leur identification précise (voir en ce sens, notamment, Cour eur. D. H., arrêt S. et Marper c. Royaume-Uni du 4 décembre 2008, *Recueil des arrêts et décisions* 2008-V, p. 213 §68 et

10 CJCE 6 novembre 2003 « Lindqvist » Aff. C-101/01, pt. 40
11 CJCE 6 novembre 2003 « Lindqvist » Aff. C-101/01
12 CJCE 20 mai 2003 « Österreichischer Rundfunk » Aff. C-465/00, C-138/01 et C-139/01, pt. 71
13 CJUE 29 juin 2010 « Bavarian Lager » Aff. C-28/08/P pt. 61
14 CJUE 21 décembre 2016 « Tele2 Sverige » Aff. C-203/15 et C-698/15 pt. 127

84) »[15]

Pour la CEDH, les **directives communautaires** ne sont des instruments intégrés au droit national **que dans la mesure et dans la forme où ils sont transposés en droit interne**. A ce titre, il peut alors convenir d'en **vérifier la conformité** à la CEDH :

> « As regards Directive 95/46/EC, on which the applicant relies, the Court notes that for purposes of the Convention it binds domestic authorities only in the form in which it is transposed into national law »[16]

Quant à la relation entre les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne, protégeant respectivement le droit à la vie privée et le droit à la protection des données personnelles, celle-ci n'est pas claire non plus[17]. En général, la CJUE annonce que la Directive 95/46/CE sert à la mise en œuvre des deux articles avec des formules ne distinguant pas ce qui relève de l'un ou de l'autre. Néanmoins, il semblerait qu'il y ait un contrôle modulé en fonction de si l'affaire touche ou non à la vie privée et à l'intimité en plus de toucher à la protection des données personnelles. Ainsi d'une part, dans l'affaire ClientEarth[18], la CJUE a rappelé que des données pouvaient être personnelles et régies par la Directive 95/46/CE même lorsqu'elles ne relevaient pas de la vie privée[19] (voir la partie sur la définition de la notion de donnée à caractère personnel). Mais, d'autre part, elle accepte d'**atténuer son contrôle** lorsqu'il est question de **données personnelles qui ne relèvent pas de l'intimité**. Par exemple, dans une affaire où il était question de relevé d'empreintes digitales, elle a indiqué que :

> « […] il y a lieu de rappeler, d'une part, que le prélèvement ne consiste qu'à prendre l'empreinte de deux doigts. Ceux-ci sont d'ailleurs **normalement exposés à la vie des autres**, de sorte **qu'il ne s'agit pas d'une opération revêtant un caractère intime**. [...] »[20]

1.C. Directive 95/46/CE : une directive d'harmonisation complète

La CJCE a déclaré explicitement les dispositions suivantes de la directive 95/46/CE comme revêtues d'un effet direct car suffisamment claires, précises et inconditionnelles :

- Article 6 paragraphe 1 sous c)[21] ;

15 CJCE 17 octobre 2013 « Michael Schwarz c. Stadt Bochum » Aff. C-291/12, pt. 27
16 CEDH 14 février 2012 « Romet c. Pays-Bas » Req. 7094/06, pt. 39
17 Voir l'article : González Fuster G., 2014, « Fighting For Your Right to What Exactly? The Convoluted Case Law of the EU Court of Justice on Privacy and/or Personal Data Protection », Birkbeck Law Review, 2, 2, p. 263-278.
18 CJUE 16 juillet 2015 « ClientEarth contre EFSA » Aff. C-615/13P
19 CJUE 16 juillet 2015 « ClientEarth contre EFSA » Aff. C-615/13P, pt. 32
20 CJCE 17 octobre 2013 « Michael Schwarz c. Stadt Bochum » Aff. C-291/12, pt. 48
21 CJCE 20 mai 2003 « Österreichischer Rundfunk » Aff. C-465/00, C-138/01 et C-139/01, dispositif

- Article 7 sous c), sous e)[22] et sous f)[23].

Cette liste ne doit cependant pas être interprétée de façon limitative.

La CJCE a rappelé que la directive 95/46/CE est une **directive d'harmonisation complète**[24] [25]. Dès lors, un Etat membre ne peut prévoir de dispositions divergeant de cet état d'harmonisation que dans les domaines où la directive prévoit explicitement une telle marge de manœuvre.

Un Etat membre demeure toutefois loisible d'étendre le champ d'application de la directive, pour autant qu'aucune autre disposition du droit communautaire n'y fasse obstacle[26]. Il existe un exemple concret dans lequel la Cour a jugé qu'un Etat membre n'avait pas le droit de prévoir des dispositions plus strictes que la directive en raison du degré d'harmonisation complète de celle-ci : il s'agit de l'arrêt « ASNEF et FECEMD contre Espagne »[27]. Dans l'affaire au principal de cet arrêt, la législation espagnole prévoyait l'obligation pour les traitements fondés sur l'article 7 sous f) de la directive (notion d'intérêt légitime du responsable de traitement ; voir la partie sur la notion d'intérêt légitime du responsable de traitement) de ne porter que sur des données provenant de sources librement disponibles au public[28].

1.D. Notion de donnée à caractère personnel

L a **Convention européenne des droits de l'Homme** ne mentionne pas la notion de donnée personnelle. Seule est mentionnée, à l'article 8, la notion de vie privée, mais celle-ci n'était pas encore, à l'époque, une vie privée informationnelle. D'ailleurs, les jurisprudences nationales de l'époque de rédaction de cette convention n'était pas nécessairement favorable à la vie privée informationnelle[29]. Ceci n'a pas empêché, depuis, la **Cour européenne des droits de l'Homme** (CEDH), de développer une jurisprudence protectrice des données personnelles.

La CEDH a adopté une **définition large de la notion d'information relative à la vie privée d'un individu**. Dans « Amann c. Suisse », la CEDH a rappelé que la **vie professionnelle** d'une personne physique peut être dans certains cas protégée par les dispositions de **l'article 8 CEDH** sur le droit à la vie privée. Elle s'inspire d'ailleurs de la **convention 108 du Conseil de l'Europe** pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, rappelant qu'elle vise à protéger « **toute information concernant une personne physique identifiée ou identifiable** »[30].

22 CJCE 20 mai 2003 « Österreichischer Rundfunk » Aff. C-465/00, C-138/01 et C-139/01, dispositif
23 CJUE 24 novembre 2011 « ASNEF et FECEMD contre Administracion del Estado » Aff. C-468/10 et C-469/10, dispositif
24 CJUE 24 novembre 2011 « ASNEF et FECEMD contre Administracion del Estado » Aff. C-468/10 et C-469/10, pt. 29
25 CJUE 19 octobre 2016 « Breyer contre Allemagne » Aff. C-582/14, pt. 58
26 CJCE 6 novembre 2003 « Lindqvist » Aff. C-101/01, pt. 96 et pt. 99
27 CJUE 24 novembre 2011 « ASNEF et FECEMD contre Administracion del Estado » Aff. C-468/10 et C-469/10
28 CJUE 24 novembre 2011 « ASNEF et FECEMD contre Administracion del Estado » Aff. C-468/10 et C-469/10, dispositif
29 Voir par exemple : De Graaf, Frits. 1976. « The Protection of Privacy in Dutch Law », *Human Rights*, vol. 5, n°2, hiver, pp. 177-192
30 CEDH 16 février 2000, « Amann contre Suisse » Req. 27798/95, pt. 65

Cette notion d'« information concernant une personne physique identifiée ou identifiable » englobe les données de nature publique lorsqu'elles sont recueillies de façon systématique, et mémorisées dans des fichiers par les pouvoirs publics, et ce, dit la CEDH, d'autant plus lorsqu'il s'agit de données sur le passé lointain[31] d'une personne[32].

La **CJUE a retenu ce cadre jurisprudentiel de la CEDH comme source d'inspiration pour les précisions qu'elle apporte à la définition contenue dans la directive de la notion de donnée personnelle[33]**. Elle adopte une **interprétation large de la notion de donnée personnelle**. Ainsi : « la notion de «données à caractère personnel» employée à l'article 3, paragraphe 1, de la directive 95/46 englobe, conformément à la définition figurant à l'article 2, sous a), de celle-ci, «**toute information concernant une personne physique identifiée ou identifiable**». »[34]

Lorsque, dans une affaire, ClientEarth a cherché à argumenter que les noms d'experts ayant participé, dans le cadre d'une activité professionnelle rémunérée à la rédaction d'un rapport de l'Agence européenne de sécurité alimentaire (EFSA), n'étaient pas des données personnelles car elles ne relevaient pas de la vie privée, la CJUE a rappelé que **peu importe que la donnée contienne une information relevant de la vie privée des personnes ou non**, dès lors qu'une personne physique est directement ou indirectement identifiée ou identifiable dans une donnée, celle-ci est automatiquement qualifiée de donnée personnelle[35]. Par ailleurs, la notion de « **donnée relative à la vie privée** » contenue dans le règlement 1049/2001/CE relatif à l'accès du public aux documents des institutions de l'UE **ne doit pas être confondue avec la notion de « donnée à caractère personnel »** de la directive 95/46/CE sur la protection des données[36]. Elle le rappela deux ans plus tard dans l'arrêt « Peter Nowak contre DPC » en disant que la notion de donnée personnelle « n'est pas restreinte aux informations sensibles ou d'ordre privé, mais englobe potentiellement toute sorte d'informations, tant objectives que subjectives sous forme d'avis ou d'appréciations, à condition que celles-ci “concernent” la personne en cause »[37].

Un autre exemple bien concret de cette interprétation est qu'elle incluse par définition **les adresses IP**[38] [39], ou un **registre de temps de travail**[40], ou encore des **images de personnes enregistrées dans le cadre d'un dispositif de vidéosurveillance[41]**. Les **métadonnées de communication** sont aussi des données à caractère personnel, d'ailleurs particulièrement intrusives dans la vie privée d'un individu, selon la CJUE[42].

Les adresses IP ne permettent pourtant qu'une **identification indirecte de l'utilisateur**.

31 Préfiguration de la réflexion sur le droit à l'oubli ?
32 CEDH 4 mai 2000 « Rotaru contre Roumanie » Req. 28341/95
33 CJUE 9 novembre 2010 « Volker et Eifert contre Hesse » Aff. C-92/09 et C-93/09, pt. 52
34 CJCE 6 novembre 2003 « Lindqvist » Aff. C-101/01, pt. 24
35 CJUE 16 juillet 2015 « ClientEarth contre EFSA » Aff. C-615/13P, pts. 24, 29 et 30
36 CJUE 16 juillet 2015 « ClientEarth contre EFSA » Aff. C-615/13P, pt. 32
37 CJUE 20 décembre 2017 «Peter Nowak contre Data Protection Commissioner» Aff. C-434/16, pt. 34
38 Il semble que les adresses IP fixes soient dans tous les cas des données personnelles (CJUE, Scarlet c. SABAM, pt. 51). Cependant, dans des arrêts datant d'avant Scarlent c. SABAM, la CJUE n'avait donné la qualité de données personnelles qu'à la combinaison entre une adresse IP (en l'espèce dynamique) et un horaire de connexion (voir CJUE, LSG contre Tele2, pt. 39). L'évolution de la jurisprudence (depuis l'arrêt « Promusicae » de 2008 à l'arrêt « Scarlet contre SABAM » de 2011) va cependant assez nettement vers une affirmation selon laquelle une adresse IP constitue dans tous les cas une donnée personnelle.
39 CJUE 24 novembre 2011 « Scarlet contre SABAM » Aff. C-70/10, pt. 51
40 CJUE 30 mai 2013 « Worten contre ACT » Aff. C-342/12
41 CJUE 11 décembre 2013 « Frantisek Rynes » Aff. C-212/13, pt. 21
42 CJUE 21 décembre 2016 « Tele2 Sverige » Aff. C-203/15 et C-698/15, pts. 97-100

En consacrant le fait qu'il s'agit bien de données personnelles, la CJUE **consacre donc bel et bien le principe contenu dans la directive 95/46/CE selon lequel est donnée personnelle toute donnée *identifiant ou permettant d'identifier directement ou indirectement* une personne physique**.

Plus tard, la CJUE a confirmé cette approche en rappelant au commissaire irlandais à la protection des données (Data Protection Commissioner) que les copies d'examens sont bel et bien des données à caractère personnel. En effet, indépendamment de savoir si l'examinateur peut ou non identifier le candidat au moment de la correction de la notation[43], « **il n'est pas requis que toutes les informations permettant d'identifier la personne concernée se trouvent entre les mains d'une seule personne** »[44]. De plus, la question n'est pas de savoir si une personne ayant accès aux données peut les lier à un individu, mais si l'entité qui est responsable du traitement en est, dans son ensemble, capable[45].

La définition des données personnelles peut être élargie aux **données se rapportant à des personnes morales dont le nom social inclut le nom d'une personne physique[46]**, ce qui peut paraître un choix étonnant dans la mesure où **la règle générale veut que la directive ne s'applique pas aux données relatives à des personnes morales**.

Elle pourrait même – mais la formulation de la CJUE à ce sujet n'est pas claire – être élargie aux données calligraphiques, c'est-à-dire à tout document écrit à la main. En tout cas, le fait qu'un document contienne des **informations calligraphiques** contribue dans son raisonnement à en faire des données à caractère personnel, même s'il n'apparaît pas clairement – et nous pouvons nous risquer à parier que cela n'est pas le cas – si c'est un facteur suffisant[47].

L'extension de la définition de ce qu'est une donnée à caractère personnel au sens de la directive 95/46/CE a cependant connu une **limitation** : en effet, dans l'affaire « Breyer contre Allemagne », la CJUE a précisé que pour déterminer si une adresse IP dynamique était une donnée à caractère personnel, il fallait que le fournisseur du service en ligne traitant ce type de données dispose « des **moyens légaux** lui permettant de faire identifier la personne concernée grâce aux informations supplémentaires dont dispose le fournisseur d'accès à Internet »[48]. **Ceci limite la notion de donnée à caractère personnel**. Ainsi, en suivant le raisonnement de la Cour, **une donnée n'est personnelle plus qu'au regard des moyens dont dispose *légalement* le responsable de traitement pour identifier les personnes concernées**. Cela ne prend donc pas en compte le risque de fuites de données ou d'accès non-autorisé.

Dans l'arrêt « Y.S. contre minister voor immigratie »[49], la CJUE apporte **une seconde limite à la notion de donnée à caractère personnel** : une analyse juridique basée pour tout ou partie sur des données personnelles ne constitue pas en soi une donnée personnelle[50]. Mais si en soi une telle analyse ne constitue pas une donnée personnelle, cela n'exclut que, dans certains cas, elle en contienne. La qualification doit donc reposer sur une analyse au cas par cas cherchant à démontrer si la donnée permet l'identification directe ou indirecte d'une personne physique ou non. Ainsi, la CJUE a jugé en 2017 que les **annotations d'une copie d'examen** sont bien des

43 CJUE 20 décembre 2017 «Peter Nowak contre Data Protection Commissioner» Aff. C-434/16, pt. 30
44 CJUE 20 décembre 2017 «Peter Nowak contre Data Protection Commissioner» Aff. C-434/16, pt. 31
45 CJUE 20 décembre 2017 «Peter Nowak contre Data Protection Commissioner» Aff. C-434/16, pt. 31
46 CJUE 9 novembre 2011 « Volker et Eifert contre Hesse » Aff. C-92/09 et C-93/09, pts. 52-54
47 CJUE 20 décembre 2017 «Peter Nowak contre Data Protection Commissioner» Aff. C-434/16, pt. 37
48 CJUE 19 octobre 2016 « Breyer contre Allemagne » Aff. C-582/14
49 CJUE 17 juillet 2014 « Y.S. contre minister voor immigratie » Aff. C-141/12
50 CJUE 17 juillet 2014 « Y.S. contre minister voor immigratie » Aff. C-141/12, pt. 39

données à caractère personnel soumises au droit d'accès au titre du droit à la protection des données personnelles[51].

1.E. Catégories de traitements de données couvertes par la directive 95/46/CE

1.E.a. Données personnelles traitées à des fins « exlusivement personnelles ou domestiques »

Etant établi que la directive 95/46/CE s'applique sans qu'il soit nécessaire d'établir un lien direct avec la libre-circulation, une seconde étape dans l'élargissement jurisprudentiel du champ d'application de la directive a été atteinte avec l'arrêt « Lindqvist ». Dans cet arrêt, la CJCE a précisé que **la directive ne s'étend pas seulement aux traitements de données effectués à des fins économiques et commerciales**.

Dans l'affaire « Lindqvist », il a fallu examiner si le traitement de données visé, effectué dans le cadre d'une **activité associative, religieuse et sans but lucratif**, entrait ou non dans la catégorie « des traitements de données à caractère personnel «mis en œuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire» au sens de l'article 3, paragraphe 2, premier tiret, de la directive 95/46 »[52]. La Cour a **rejeté l'interprétation selon laquelle cette disposition limiterait le champ matériel d'application de la directive aux seuls traitements ayant une fin économique ou commerciale**. Les seules catégories de traitements qui ne sont pas couvertes par la directive sont celles qui correspondent aux activités prévues au titre V du Traité sur l'Union européenne (**politique étrangère et de sécurité commune**) et à la **coopération judiciaire et policière**[53], ou les traitements ayant pour objet **la sécurité publique, la défense, la sûreté de l'Etat et les activités relatives au droit pénal**[54] (ces traitements demeurent cependant soumis à la supervision de la CEDH, par exemple en matière de surveillance d'État (voir la partie sur la surveillance d'Etat) , et à la décision-cadre 2008/977/JAI). A ces exceptions s'ajoute celle prévue à l'article 3 paragraphe 2 deuxième tiret affirmant que **les traitements « effectué[s] par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques » ne sont pas soumis aux dispositions de la directive**.

1.E.b. L'application de la directive 95/46/CE aux établissements de droit public et ses limites

En raison de sa base juridique[55], la directive 95/46/CE vise principalement les acteurs économiques du marché intérieur. Mais les exceptions décrites ci-dessus à son champ

51 CJUE 20 décembre 2017 «Peter Nowak contre Data Protection Commissioner» Aff. C-434/16
52 CJCE 6 novembre 2003 « Lindqvist » Aff. C-101/01, pt. 39
53 Anciens titres V et VI TUE
54 CJCE 6 novembre 2003 « Lindqvist » Aff. C-101/01, pt. 43
55 La directive 95/46/CE est basée sur l'ex-art. 100 A TCE devenu l'article 114 paragraphe 1 TFUE

d'application ne couvrent pas pour autant l'intégralité des traitements de données personnelles dont le responsable de traitement est un Etat ou une autre personne morale de droit public national[56]. Ainsi, dans l'arrêt « Huber contre Allemagne »[57], la CJCE a rappelé que si les traitements ayant pour objet la **sécurité publique**, la **défense**, la **sûreté de l'Etat** et le **droit pénal** sont exclus du champ d'application de la directive, ceci n'est pas le cas pour les données collectées et traitées dans le cadre de la **règlementation sur le droit de séjour**[58]. Dans l'affaire Huber, le traitement avait plusieurs finalités : une de prévention et de répression des crimes, une finalité statistique, et une finalité qui concernait l'appui aux autorités gérant le droit de résidence des citoyens européens en Allemagne. Dès lors, la Cour n'a pas refusé d'évaluer la conformité de ces deux dernières finalités à la lumière du droit communautaire et notamment de la directive 95/46/CE et de l'ancien article 12 TCE (actuellement art. 18 TFUE), **interdisant les discriminations sur la base de la nationalité**.

Dans d'autres arrêts, comme « X. contre Bois-le-Duc »[59], où le traitement visé au principal était mis en œuvre par une collectivité locale, confirment que la **directive s'applique en principe aussi aux Etats et autres personnes de droit public**, sauf si le traitement est mis en œuvre pour une activité exclue explicitement du champ d'application de la directive. **Ce n'est donc pas la nature du responsable du traitement qui compte pour savoir si la directive s'applique ou non, mais la finalité du traitement**.

Dans l'affaire « Puškár contre Slovaquie »[60], portant sur une liste de personnes suspectées de jouer des fonctions de prête-noms par **l'administration fiscale** slovaque, le gouvernement espagnol avait soulevé une objection à la recevabilité de la requête[61] en prétendant qu'une telle liste aurait relevé de **l'article 3 de la directive 95/46/CE**, qui dispose que cette dernière ne s'applique pas aux traitements de données ayant pour objet la sécurité publique, la défense, la sûreté de l'Etat, « **y compris le bien-être économique de l'Etat** lorsque ces traitements sont liés à des questions de sûreté de l'Etat »[62] ou étant relatives aux domaines du droit pénal.

Après avoir précisé que les exceptions listées ci-dessus et prévues à **l'article 3 paragraphe 2 premier tiret de la directive 95/46/CE sont d'interprétation stricte**[63], elle relève que **l'article 13 paragraphe 1** de la même directive prévoit la possibilité d'adopter des mesures nationales restreignant certains des droits relatifs à la protection des données notamment pour **sauvegarder un intérêt économique ou financier important dans le domaine fiscal**[64]. Cela présuppose que **la directive s'applique bel et bien à ce type de finalités de traitement**.

Ainsi, les traitements de données à caractère personnel ayant pour objet des finalités dans le domaine fiscal sont soumis aux obligations de la directive 95/46/CE[65], **sauf** si un tel traitement a

56 En effet, les institutions de l'Union sont elles soumises au règlement 45/2001/CE
57 CJCE 16 décembre 2008 « Huber contre Allemagne » Aff. C-524/06
58 CJCE 16 décembre 2008 « Huber contre Allemagne » Aff. C-524/06, pt. 44 et pt. 45
59 CJUE 7 novembre 2013 « X. contre Bois-le-Duc » Aff. C-473/12
60 CJUE 27 septembre 2017 « Puškár contre Slovaquie » Aff. C-73/16
61 CJUE 27 septembre 2017 « Puškár contre Slovaquie » Aff. C-73/16, pt. 35
62 Art. 3 de la directive 95/46/CE
63 CJUE 27 septembre 2017 « Puškár contre Slovaquie » Aff. C-73/16, pt. 38
64 CJUE 27 septembre 2017 « Puškár contre Slovaquie » Aff. C-73/16, pt. 43
65 CJUE 27 septembre 2017 « Puškár contre Slovaquie » Aff. C-73/16, pt. 44

lieu dans le cadre d'une **enquête pénale**[66].

1.F. Sur la notion de traitement de données

1.F.a. Définition de la notion de traitement

L'arrêt « Google contre Espagne », connu principalement pour avoir consacré un droit au déréférencement des personnes concernées, a également permis d'apporter des précisions concernant la notion de responsable de traitement. En effet, cet arrêt définit les **moteurs de recherche**, qui ont une activité d'**indexation** des données (y compris personnelles) disponibles sur le **web**, comme des **responsables de traitement**. La CEDH avait déjà jugé que même disponibles de façon publique (par exemple en ligne), les données se rattachant à une personne physique sont par définition des données personnelles[67]. La CJUE se réfère quant à elle la **définition** de la notion de **traitement de données** contenue dans la directive pour rappeler l'évidence suivante : l'enregistrement ou encore la conservation de données personnelles constituent des traitements. Or, il n'était pas contesté dans le cas d'espèce que Google effectue de telles opérations dans l'exploitation de son moteur de recherche[68].

Dans l'arrêt « Rigas Satiksme » du 4 mai 2017, elle précise que **la communication de données** à caractère personnel constitue un traitement de données[69].

1.F.b. Traitement automatisé en tout ou partie

L'article 3-1 de la directive 95/46/CE dispose : « La présente directive s'applique au traitement de données à caractère personnel, **automatisé en tout ou en partie**, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier ». La question se pose dès lors de savoir qu'est-ce qui constitue ou non un traitement automatisé pour délimiter précisément le champ d'application matériel de la directive.

La CJCE a été amenée à se prononcer sur la question dans l'arrêt Lindqvist[70]. Dans la liste des questions préjudicielles sur lesquelles elle était en effet amenée à statuer dans le cadre de cette affaire, la toute première portait sur la question de savoir s'il suffisait qu'un traitement de données à caractère personnelle soit informatisé pour que le traitement soit qualifié d'automatique. Là-dessus, la Cour a répondu sans ambigüité que dès lors qu'Internet est utilisé pour faire apparaître ces données, il s'agit d'un traitement automatisé :

> « […] il convient de relever que faire apparaître des informations sur une page Internet implique, selon les procédures techniques et informatiques appliquées actuellement, de réaliser une opération de chargement de cette page sur un serveur ainsi que les opérations nécessaires pour rendre cette page accessible aux personnes qui se sont connectées à

66 CJUE 27 septembre 2017 « Puškár contre Slovaquie » Aff. C-73/16, pt. 40
67 CEDH 4 mai 2000 « Rotaru contre Roumanie » Req. 28341/95
68 CJUE 13 mai 2014 « Google contre Espagne » Aff. C-131/12, pt.
69 CJUE 4 mai 2017 « Rigas Satiksme », Aff. C-13/16, pt. 26
70 CJCE 6 novembre 2003 « Lindqvist » Aff. C-101/01

Internet. Ces opérations sont effectuées, au moins en partie, de manière automatisée »[71]

Mais elle ne dégage pas de critères généraux permettant de définir plus précisément la frontière entre un traitement automatisé en tout ou partie et un traitement non-automatisé, et il n'est donc pas, à ce stade, absolument possible de conclure au fait que le simple emploi d'un appareillage informatique suffise à faire qualifier un traitement d'automatisé en tout ou partie.

1.G. Sur les notions de responsable de traitement et de sous-traitant

1.G.a. Définitions

Dans l'affaire « Google contre Espagne », la CJUE a dit que, dès lors qu'il est établi qu'il procède à traitement de données dont il **détermine les finalités et les moyens**, Google est un responsable de traitement[72], dont, en l'espèce, l'objectif était de vendre sur le territoire espagnol des espaces publicitaires associés à des résultats de recherche.

Un tel traitement se fonde sur la base légale de l'article 7 sous f) de la directive 95/46/CE : **l'intérêt légitime du responsable de traitement**[73]. La CJUE consacre par là la définition contenue à l'article 2 sous d) de la directive ainsi que la substance de l'avis 01/2010 du Groupe de travail de l'Article 29 (G29) sur les notions de **responsable de traitement** et de **sous-traitant**, ce dernier exécutant (selon le G29) les opérations de traitement dans le cadre des instructions que le responsable de traitement lui transmet.

En tant que responsable de traitement, les moteurs de recherche doivent donc respecter les obligations qui découlent de la directive 95/46/CE.

Il peut exister des cas de **responsabilité conjointe** d'un traitement. Ainsi, un simple utilisateur de Facebook n'est pas co-responsable de traitement avec l'entreprise gérant ce réseau social[74]. En revanche, une personne morale créant une « page fan » sur Facebook est co-responsable de traitement avec Facebook de celle-ci, puisqu'elle contribue, par le paramétrage de la page et le fait que les données personnelles collectées par Facebook permettent de générer des statistiques qui lui sont utiles :

> « Ces traitements de données à caractère personnel visent notamment à permettre, d'une part, à Facebook, d'améliorer son système de publicité qu'il diffuse à travers son réseau et, d'autre part, à l'administrateur de la page fan d'obtenir des statistiques établies par Facebook à partir des visites de cette page [...] »[75]

> « Il ressort des indications soumises à la Cour que la création d'une page sur Facebook

71 CJCE 6 novembre 2003 « Lindqvist » Aff. C-101/01, pt. 26
72 CJUE 13 mai 2014 « Google contre Espagne » Aff. C-131/12, pt. 40
73 CJUE 13 mai 2014 « Google contre Espagne » Aff. C-131/12, pt. 73
74 CJUE 5 juin 2018 « Wirtschaftsakademie » Aff. C-210/16, pt. 35
75 CJUE 5 juin 2018 « Wirtschaftsakademie » Aff. C-210/16, pt. 34

> implique de la part de son administrateur une action de paramétrage, en fonction, notamment, de son audience cible ainsi que d'objectifs de gestion ou de promotion de ses activités, qui influe sur le traitement de données à caractère personnel aux fins de l'établissement de statistiques établies à partir des visites de la page fan. […] »[76]
>
> « En particulier, l'administrateur de la page fan peut demander à obtenir – et donc que soient traitées – des données démographiques concernant son audience [...] »[77]

Dès lors, « il y a lieu de considérer que l'administrateur d'une page hébergée sur Facebook […] **participe**, par son action de paramétrage […] **à la détermination des finalités et des moyens du traitement des données personnelles des visiteurs de sa page fan** »[78].

Qu'une personne soit ou non destinataire des données à caractère personnel, ou bien, comme pour le cas de l'administrateur d'une page fan sur Facebook, ne verra que des données statistiques agrégées et anonymes, ne veut pas forcément dire qu'il n'a pas été nécessaire de traiter des données à caractère personnel en amont, dans le cadre du service fourni à cette personne. Dès lors, « en tout état de cause, la directive 95/46 **n'exige pas, lorsqu'il y a une responsabilité conjointe de plusieurs opérateurs pour un même traitement, que chacun ait accès aux données à caractère personnel concernées** »[79]

Cependant, dans cette affaire, la CJUE a tenu à faire une distinction malgré tout entre les deux responsables du traitement : Facebook et l'administrateur de la page fan. C'est ainsi qu'émerge la notion de « **responsable du traitement à titre principal** » pour désigner Facebook[80], la CJUE précisant plus loin dans son arrêt que :

> « Il y a lieu de préciser […] que **l'existence d'une responsabilité conjointe ne se traduit pas nécessairement par une responsabilité équivalente des différents opérateurs concernés** par un traitement de données à caractère personnel. Au contraire, ces opérateurs peuvent être impliqués à différents stades de ce traitement et selon différents degrés, de telle sorte que **le niveau de responsabilité de chacun d'entre eux doit être évalué en tenant compte de toutes les circonstances pertinentes du cas d'espèce** »[81]

1.G.b. Le cas particulier de la sous-traitance de la facturation d'une prestation de services de télécommunications à une agence de recouvrement (impliquant tant les directives 95/46/CE que 2002/58/CE)

L'arrêt « Josef Probst contre Mr. Nexnet »[82] est à l'heure actuelle le seul arrêt de la CJUE concernant la question de la conformité des **organismes de recrouvement de créances** au droit de la protection des données. L'affaire au principal concernait la transmission par Verizon

76 CJUE 5 juin 2018 « Wirtschaftsakademie » Aff. C-210/16, pt. 36
77 CJUE 5 juin 2018 « Wirtschaftsakademie » Aff. C-210/16, pt. 37
78 CJUE 5 juin 2018 « Wirtschaftsakademie » Aff. C-210/16, pt. 39
79 CJUE 5 juin 2018 « Wirtschaftsakademie » Aff. C-210/16, pt. 38
80 CJUE 5 juin 2018 « Wirtschaftsakademie » Aff. C-210/16, pt. 30
81 CJUE 5 juin 2018 « Wirtschaftsakademie » Aff. C-210/16, pt. 43
82 CJUE 22 novembre 2012 « Josef Probst contre mr.nexnet » Aff. C-119/12

Deutschland GmbH (fournisseur d'accès à Internet - FAI), de données soumises aux règles de la **directive 2002/58/CE** (directive dite « ePrivacy » en anglais) à Mr. Nexnet, société concessionnaire de créances. Un requérant au principal, M. Probst, s'était opposé au règlement d'une facteur, considérant que le contrat liant Verizon et nexnet, incluant des dispositions sur le traitement de données personelles, est nul car entâché d'illégalité. La juridiction de renvoi avait demandé à la CJUE de déterminer si l'article 6 de la directive 2002/58/CE permettait à un FAI, qui fournit des services de télécommunications et y est donc soumis, de transmettre des **données relatives au trafic** à un cessionnaire de créances, et le cas échéant, sous quelles conditions[83]. Or, le paragraphe 5 de cet article 6 de la directive 2002/58/CE réglemente spécifiquement ce type de cas[84], ce qui fait que **le traitement et l'utilisation de données sur le trafic dans le cadre du recouvrement de créances obéit à un régime spécial dérogatoire à la directive 95/46/CE, issue de la directive 2002/58/CE.**

La CJUE a analysé le cas « Josef Probst contre Mr. Nexnet » sous l'angle de la **sous-traitance de données personnelles** (voir la partie sur la définition du responsable de traitement et du sous-traitant), mais n'a pas affirmé de principes généraux sur la collecte et le traitement de données par des agences de recouvrement, indépendamment du cas bien précis où une telle agence se voyait confier en qualité de sous-traitant des données personnelles qui sont des données de trafic soumises au régime de la directive 2002/58/CE dite « ePrivacy ». Dans ce cas particulier, elle a jugé que la sous-traitance de telles données était autorisée à l'article 6 paragaphe 5 de la directive 2002/58/CE dans le cadre de l'activité de facturation, ce qui inclut le recouvrement d'impayés. Les **deux conditions à respecter sont** :

1. L e **sous-traitant doit bel et bien agir sous l'autorité de la compagnie de télécommunications délivrant le service facturé** ;
2. Et : le sous-traitant **doit se limiter à traiter les données ainsi transmises par la compagnie de télécommunications, et aux seules fins de recouvrement prévues par le contrat**.

Enfin, ce contrat doit comporter les dispositions nécessaires de nature à garantir le **traitement licite** des données et d'assurer à tout moment le **respect de ces dispositions[85]**. Ce type d'exigences rappelle les exigences générales des contrats de sous-traitance du traitement de données personnelles (voir l'article 17 de la directive 95/46/CE).

83 CJUE 22 novembre 2012 « Josef Probst contre mr.nexnet » Aff. C-119/12, pt. 16

84 « Le traitement des données relatives au trafic effectué conformément aux dispositions des paragraphes 1, 2, 3 et 4 doit être restreint aux personnes agissant sous l'autorité des fournisseurs de réseaux publics de communications et de services de communications électroniques accessibles au public qui sont chargées *d'assurer la facturation ou la gestion du trafic*, de répondre aux demandes de la clientèle, de détecter les fraudes et de commercialiser les services de communications électroniques ou de fournir un service à valeur ajoutée; ce traitement doit se limiter à ce qui est nécessaire à de telles activités. »

85 CJUE 22 novembre 2012 « Josef Probst contre mr.nexnet » Aff. C-119/12, dispostif

1.H. Champ d'application territorial de la directive 95/46/CE et notion d'établissement au sens de cette directive

La CJUE a confirmé qu'il est **interdit de transférer des données personnelles vers des pays tiers qui ne garantissent pas un niveau de protection des données personnelles et de la vie privée équivalent au régime de protection garanti par le droit de l'Union** (voir l'arrêt « Digital Rights Ireland »[86]). Par ailleurs, tout transfert doit se faire dans des conditions permettant une **supervision** de la protection des données personnelles par une **autorité indépendante**, afin de satisfaire à l'article 8 de la Charte des droits fondamentaux de l'Union européenne. Suite à une plainte de Maximilien Schrems, un militant autrichien, contre l'autorité irlandaise de protection des données refusant de remettre en cause l'accord Safe Harbor, la Haute Cour irlandaise a posé une question préjudicielle à la CJUE pour savoir si l'entrée en vigueur de la Charte des droits fondamentaux de l'Union européenne, et notamment de son article 8, pouvait remettre en cause une décision d'équivalence de la Commission (en l'espèce l'accord Safe Harbor) s'il est démontré que l'Etat tiers visé par la décision d'équivalence enfreint les principes défendus par le droit de l'Union en matière de protection des données[87]. La CJUE a répondu par l'affirmative à la question et invalidé l'accord Safe Harbor[88] (voir la partie sur les transferts de données). Les autres outils juridiques permettant des transferts de données personnelles vers des pays tiers sont elles aussi potentiellement affectées[89].

Dans son arrêt « Google contre Espagne » de 2014[90], la CJUE a été amenée à trancher la question de savoir si la directive 95/46/CE s'appliquait ou non à des traitements de données mis en œuvre par Google Inc, entreprise dont le siège (l'établissement principal) est en Californie. Aux termes de cette directive, une APDP est compétente pour superviser un responsable de traitement dont **l'établissement principal** est situé dans un **pays tiers** si :

> «
> - Le traitement est effectué dans le cadre des activités d'un établissement du responsable de traitement sur le territoire de l'Etat membre […] [, ou]
> - le responsable du traitement n'est pas établi sur le territoire de l'État membre mais en un lieu où sa loi nationale s'applique en vertu du droit international public [, ou]
> - le responsable du traitement n'est pas établi sur le territoire de la Communauté et recourt, à des fins de traitement de données à caractère personnel, à des moyens, automatisés ou non, situés sur le territoire dudit État membre, sauf si ces moyens ne sont utilisés qu'à des fins de transit sur le territoire de la Communauté »[91]

Le considérant 19 de la directive 95/46/CE affirme que « **l'établissement** sur le territoire d'un État membre suppose **l'exercice effectif et réel d'une activité au moyen d'une installation stable**; que la forme juridique retenue pour un tel établissement, qu'il s'agisse d'une simple succursale ou d'une filiale ayant la personnalité juridique, n'est pas déterminante à cet égard ». Cette définition est utilisée par la CJUE pour confirmer que Google Espagne, filiale de Google Inc

86 CJUE 8 avril 2014 « Digital Rights Ireland » Aff. C-293/12 et C-594/12, pt. 68
87 High Court (Irlande) 18 juin 2014 « Maximilian Schrems contre Data Protection Commissioner » 2013 No. 765JR
88 CJUE 6 octobre 2015 « Schrems contre DPC Irlande » Aff. C-362/14
89 Voir la déclaration du Groupe de travail de l'Article 29 sur la décision de la CJUE du 6 octobre 2015 « Schrems contre DPC Irlande » (disponible en ligne)
90 CJUE 13 mai 2014 « Google contre Espagne » Aff. C-131/12
91 Article 4 paragraphe 1 de la directive 95/46/CE

dotée de la personnalité juridique, correspond aux critères permettant de la qualifier d'établissement sur le territoire d'un Etat membre[92]. Sachant que plus loin dans son arrêt, la CJUE conclut que l'**indexation** de données personnelles est un **traitement de données personnelles**, il est aussi demandé à la Cour de décider si le traitement à des fins d'indexation, réalisé par Google Inc, s'inscrit dans le cadre des activités de Google Espagne. Elle a examiné cette question sous l'angle de la théorie de l'effet utile selon laquelle la bonne interprétation est celle qui permet la réalisation effective des objectifs de la disposition étudiée[93] [94]. Il n'est alors pas nécessaire qu'un traitement soit réalisé par la filiale sise sur le territoire d'un Etat membre pour qu'il soit réalisé dans le cadre des activités de cette filiale[95]. Dans l'affaire au principal, Google Espagne utilisait le traitement de données de Google Inc. pour vendre des espaces publicitaires sur le territoire espagnol. Dès lors, la directive 95/46/CE s'appliquait au traitement de données réalisées par Google Inc dans le cadre de l'indexation des contenus web, y compris de façon extraterritoriale[96]. Ceci permet à l'APDP espagnole de superviser ces traitements.

Si dans l'arrêt Google de 2014[97], la CJUE a été amenée à se prononcer sur la question de l'établissement sur le territoire d'un Etat membre d'un responsable de traitement dont l'établissement principal est situé dans un Etat non membre, **l'arrêt Weltimmo du 1er octobre 2015[98] a lui permis de se prononcer sur un cas dans lequel le responsable de traitement disposait d'un établissement principal dans un pays membre** (ici la Slovaquie), **mais dirigeait ses services vers un autre Etat membre** (ici la Hongrie) au moyen d'un site web publiant des annonces immobilières. L'affaire au principal ayant abouti au renvoi préjudiciel sur lequel la CJUE s'est prononcée portait en substance sur la question de la compétence de l'autorité hongroise de protection des données à sanctionner cette société.

La Cour a tout d'abord rappelé, que selon les termes de l'arrêt « Google contre Espagne »[99], « **l'expression « dans le cadre des activités d'un établissement » ne saurait recevoir une interprétation restrictive** »[100]. En effet, une interprétation restrictive pourrait porter atteinte à l'objectif de la directive 95/46/CE d'assurer une protection « efficace et complète des libertés et des droits fondamentaux des personnes physiques, notamment du droit à la vie privée, à l'égard du traitement des données »[101]. Que ce soit pour analyser la présence sur le territoire de l'Union européenne d'un établissement d'un responsable de traitement principalement établi dans un Etat tiers, ou pour déterminer la présence d'un établissement du responsable de traitement dans un Etat membre autre que celui où il a son établissement principal, la CJUE reprend[102] la formule de l'arrêt « Google contre Espagne » , dans lequel, en se basant sur le considérant 19 de la directive 95/46/CE, elle avait affirmé que **l'établissement sur le territoire d'un Etat membre suppose l'exercice effectif et réel d'une activité au moyen d'une installation stable, la forme juridique de cet établissement n'ayant pas d'importance**[103]. Dès lors, il suffit pour dire qu'un responsable de traitement dispose d'un établissement au sens de la directive 95/46/CE, il suffit « d'évaluer tant le degré de stabilité de l'installation que la réalité de l'exercice des activités dans

92 CJUE 13 mai 2014 « Google contre Espagne » Aff. C-131/12, pt. 48 et pt. 49
93 Une telle approche est conforme au considérant 20 de la directive 95/46/CE : « l'établissement, dans un pays tiers, du responsable du traitement de données ne doit pas faire obstacle à la protection des personnes prévue par la présente directive […] »
94 CJUE 13 mai 2014 « Google contre Espagne » Aff. C-131/12, pt. 53
95 CJUE 13 mai 2014 « Google contre Espagne » Aff. C-131/12, pt. 52
96 CJUE 13 mai 2014 « Google contre Espagne » Aff. C-131/12, pt. 56
97 CJUE 13 mai 2014 « Google contre Espagne » Aff. C-131/12
98 CJUE 1er octobre 2015 « Weltimmo » Aff. C-230/14
99 CJUE 13 mai 2014 « Google contre Espagne » Aff. C-131/12, pt. 53
100 CJUE 1er octobre 2015 « Weltimmo » Aff. C-230/14, pt. 25
101 CJUE 1er octobre 2015 « Weltimmo » Aff. C-230/14, pt. 25
102 CJUE 1er octobre 2015 « Weltimmo » Aff. C-230/14, pt. 28
103 CJUE 13 mai 2014 « Google contre Espagne » Aff. C-131/12, pt. 48

cet autre Etat membre, en tenant compte de la nature spécifique des activités économiques et des prestations de services en question. Cela vaut tout particulièrement pour des entreprises qui s'emploient à offrir des services exclusivement sur Internet »[104]. Il n'y a donc pas de différence dans la définition d'établissement, au sens de la directive, que l'on analyse l'établissement secondaire d'un responsable de traitement dont l'établissement principal est dans un pays tiers ou dans un autre Etat membre de l'Union.

1.I. Détermination du droit national applicable

L'article 4 de la directive 95/46/CE porte sur la détermination du droit national applicable. La CJUE a été amenée à en préciser le contenu par la voie jurisprudentielle.

Selon le considérant 18 de la directive 95/46/CE, « il est opportun de soumettre les traitements de données effectués par toute personne opérant sous l'autorité du responsable du traitement établi dans un Etat membre à l'application de la législation de cet Etat ». Ainsi, en toute logique, l'article 4 paragraphe 1 sous a) dispose : « **si un même responsable du traitement est établi sur le territoire de plusieurs Etats membres, il doit prendre les mesures nécessaires pour assurer le respect, par chacun de ses établissements, des obligations prévuées par le droit national applicable** ».

Les conditions pratiques d'application de ces dispositions ont été précisées par la CJUE dans l'arrêt « Weltimmo » de 2015[105]. Pour qu'une législation nationale relative à la protection des données autre que celle de l'Etat membre dans lequel un responsable de traitement est immatriculé s'applique à ce dernier, il faut qu'il dispose d'un **établissement** dans ce second pays, c'est-à-dire, selon la directive 95/46/CE, qu'il « **exerce, au moyen d'une installation stable sur le territoire de cet Etat membre, une activité effective et réelle, même minime, dans le cadre de laquelle ce traitement est effectué** »[106]. Pour le déterminer, il faut notamment prendre en compte[107] :

- si l'activité du responsable de traitement est **dirigée en tout ou partie vers cet Etat membre** autre que celui où il est immatriculé ;
- si le responsable de traitement dispose ou non d'un **représentant dans l'Etat membre**.

La liste ci-dessus n'est pas limitative. Cependant, **la nationalité des personnes concernées par le traitement est un facteur dénué de toute pertinence** pour déterminer la législation applicable en matière de protection des données[108].

Cette jurisprudence a été confirmée en juillet 2016 dans l'arrêt « VKI contre Amazon UE »[109], dans lequel la CJUE évite de répondre à la question de la coordination entre la notion d'établissement contenue à l'article 4 paragraphe 1 sous a) de la directive 95/46/CE et les **règles de désignation du droit national applicable** en vertu des **règlements de Rome I**[110] **et de Rome**

104 CJUE 1er octobre 2015 « Weltimmo » Aff. C-230/14, pt. 29
105 CJUE 1er octobre 2015 « Weltimmo » Aff. C-230/14
106 CJUE 1er octobre 2015 « Weltimmo » Aff. C-230/14, pt. 41
107 CJUE 1er octobre 2015 « Weltimmo » Aff. C-230/14, pt. 41
108 CJUE 1er octobre 2015 « Weltimmo » Aff. C-230/14, pts. 40 et 41
109 CJUE 28 juillet 2016 « VKI contre Amazon UE » Aff. C-191/15, pts. 66 à 81
110 Règlement 593/2008/CE du Parlement européen et du Conseil du 17 juin 2008 sur la loi applicable aux obligations

II[111]. Alors que la juridiction de renvoi lui avait posé cette question, la CJUE n'y fait en effet que réitérer sa jurisprudence Weltimmo, et ne prend même pas la peine de rappeler à la juridiction de renvoi que l'article 23 du règlement de Rome I et l'article 27 du règlement de Rome II prévoient la possibilité que d'autres régimes de détermination du droit national applicable soient prévus dans d'autres textes communautaires, sauf en matière de contrats d'assurance, où il ne peut être dérogé à l'article 7 du règlement de Rome I dédié à ce sujet.

La question du lieu d'établissement du responsable de traitement est une question préalable à la détermination de la compétence d'une autorité nationale de protection des données (voir, à ce sujet, la partie sur les autorités de protection des données)[112].

Il est à noter que le mécanisme présenté ci-dessus sera profondément amendé par l'entrée en vigueur prévue en 2018 du nouveau règlement de protection des données, remplaçant la directive 95/46/CE.

contractuelles (Rome I)

111 Règlement 864/2007/CE du Parlement Européen et du Conseil du 11 juillet 2007 sur la loi applicable aux obligations non contractuelles (Rome II)

112 Voir notamment à ce sujet l'arrêt CJUE 5 juin 2018 « Wirtschaftsakademie » Aff. C-210/16

2. Principe de légalités : les bases légales des traitements

Pour être autorisé par la directive 95/46/CE, un traitement de données à caractère personnel doit obéir au principe de légalité. Ainsi, son article 7 interdit tout traitement entrant de son champ d'application (voir la partie sur le champ d'application de la directive 95/46/CE) sauf à ce que celui-ci soit légitimé par une des 6 bases légales proposées et listées limitativement :

> « a) la personne concernée a indubitablement donné son consentement
>
> ou
>
> b) il est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci
>
> ou
>
> c) il est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis
>
> ou
>
> d) il est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée
>
> ou
>
> e) il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées
>
> ou
>
> f) 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, qui appellent une protection au titre de l'article 1er paragraphe 1. »[113]

La CJUE a eu l'occasion de préciser certaines de ces bases légales.

2.A. Consentement

113 Art. 7 de la directive 95/46/CE

2.A.a. Consentement libre et éclairé

Pour être valide, le consentement donné en vertu de l'art. 7 sous a) de la Directive 95/46/CE doit être libre.

Dans sa décision « Schwarz contre Stadt Bochum » de 2013[114], la CJUE a ainsi jugé que le consentement ne pouvait être invoqué pour légitimer la collecte d'empreintes digitales, dès lors que la délivrance d'un passeport, document indispensable pour voyager hors de l'Union européenne, lui était subordonné[115].

2.A.b. Cas particulier du croisement avec l'article 12 de la directive ePrivacy (2002/58/CE) et l'article 25 de la directive service universel (2002/22/CE)

Au sujet du consentement, la CJUE a été amenée à se prononcer dans une affaire concernant le consentement à figurer dans un annuaire téléphonique. La question impliquait le croisement avec **l'article 12 de la directive 2002/58/CE** (dite « ePrivacy » en anglais) concernant la protection de la vie privée sur les réseaux de télécommunication. Cet article impose le **recueil du consentement préalable de la personne concernée avant la publication de ses coordonnées dans un annuaire public d'annuaire**.

De plus, l'article 25 d'une autre directive, la **directive 2002/22/CE (dite « service universel) contraint les entreprises attribuant des numéros de téléphone** à des utilisateurs finaux **à divulguer aux entreprises dont l'activité consiste à fournir des services de renseignement téléphoniques accessibles au public d'annuaire**, lorsque ces dernières en font la demande, **les données pertinentes qu'elles détiennent au sujet de leurs abonnés**. Une loi nationale peut même étendre cette obligation au partage des données sur tout abonné – les leurs ou celle d'autres entreprises – dont elles auraient connaissance[116]. Mais **ce partage ne peut concerner que les personnes concernées ayant donné leur consentement préalable** (au sens de l'article 7 sous a) de la directive 95/46/CE) à ce qu'ils figurent dans un annuaire. Une fois ce **consentement libre et informé** recueilli, il n'est cependant plus nécessaire de redemander l'accord de la personne concernée pour faire figurer ses données dans un autre annuaire[117].

2.A.c. Le statut des fichiers « robots.txt »

La mise en œuvre ou non de normes techniques consensuelles, comme « robots.txt », permettant à l'administrateur d'un site web d'indiquer son opposition à l'indexation du contenu du site **n'est pas assimilable à un consentement de la personne concernée au sens de la**

114 CJCE 17 octobre 2013 « Michael Schwarz c. Stadt Bochum » Aff. C-291/12
115 CJCE 17 octobre 2013 « Michael Schwarz c. Stadt Bochum » Aff. C-291/12, pt. 32
116 CJUE 5 mai 2011 « Deutsche Telekom contre Allemagne » Aff. C-543/09, pts. 41, 42 et 47
117 CJUE 5 mai 2011 « Deutsche Telekom contre Allemagne » Aff. C-543/09, pts. 61-67

directive[118].

2.B. Les traitements de données nécessaires à l'exécution d'une mission de service public ou relevant de l'autorité publique (art. 7 sous e) de la directive 95/46/CE)

La CJUE a rappelé en 2013, dans son arrêt « Worten contre ACT »[119], que dans le cadre de l'exercice d'une mission de service public, **une autorité publique était en droit d'exiger l'accès à des données personnelles sans passer par le consentement de la personne concernée**. Un tel accès est **conditionné à ce que le traitement de ces données soit bel et bien nécessaire à l'accomplissement de l'obligation de service public en question**[120]. Ce principe rappelle celui déjà énoncé dans « Österreichischer Rundfunk » [121] selon lequel un tel accès demeure conditionné à l'exigence de proportionnalité : les données ne peuvent être collectées que pour des **finalités déterminées, explicites et légitimes** et doivent être **adéquates, pertinentes et non-excessives au regard des finalités poursuivies**[122].

2.C. Les traitements fondés sur l'intérêt légitime du responsable de traitement (art. 7 sous f) de la directive 95/46/CE)

L'arrêt « ASNEF et FECEMD contre Administracion del Estado » du 24 novembre 2011[123] porte sur la notion d'intérêt légitime du responsable de traitement et l'effet en droit interne de l'article 7 sous f) de la directive (voir la partie sur le champ d'application de la directive et ses effets en droit interne). **Les responsables de traitement se fondant sur l'article 7 sous f) ont le droit de collecter des données personnelles qui ne sont pas publiquement disponibles**[124]. Ils peuvent **notamment le faire pour garantir la sécurité de leurs systèmes d'information**[125].

Ce type de collecte constitue néanmoins **une atteinte plus grave à la vie privée** que si elle était issue de sources ouvertes[126], et cela doit demande à être pris en compte dans une démarche de pondération des intérêts, entre ceux du responsable du traitement et ceux de la

118 CJUE 13 mai 2014 « Google contre Espagne » Aff. C-131/12, pt. 39
119 CJUE 30 mai 2013 « Worten contre ACT » Aff. C-342/12
120 CJUE 30 mai 2013 « Worten contre ACT » Aff. C-342/12, pt. 35
121 CJCE 20 mai 2003 « Österreichischer Rundfunk » Aff. C-465/00, C-138/01 et C-139/01, pt. 66
122 CJCE 20 mai 2003 « Österreichischer Rundfunk » Aff. C-465/00, C-138/01 et C-139/01, pt. 66
123 CJUE 24 novembre 2011 « ASNEF et FECEMD contre Administracion del Estado » Aff. C-468/10 et C-469/10
124 CJUE 24 novembre 2011 « ASNEF et FECEMD contre Administracion del Estado » Aff. C-468/10 et C-469/10, pt. 39
125 CJUE 19 octobre 2016 « Breyer contre Allemagne » Aff. C-582/14, pts. 63 et 64
126 CJUE 24 novembre 2011 « ASNEF et FECEMD contre Administracion del Estado » Aff. C-468/10 et C-469/10, pt. 45

personne concernée[127].

Dans l'affaire au principal de l'arrêt « ASNEF et FECEMD contre Administracion del Estado »[128] , l'intérêt légitime servait de base légale par des entreprises de marketing électronique et par des entreprises financières, représentées par leurs organisations professionnelles respectives (ASNEF[129] et FECEMD[130]), ayant déposé un recours contre la législation espagnole de protection des données, laquelle était plus restrictive que la directive en matière d'intérêt légitime, et ce alors même que, comme l'a déclaré la CJUE, cet article est suffisamment clair et inconditionnel pour bénéficier d'un effet direct.

En combinaison avec l'article 14 sous a) de la directive 95/56/CE sur le **droit d'opposition** des personnes concernées, a permis à la CJUE de consacrer un droit au déréférencement sur les moteurs de recherche[131] (voir la partie sur le déréférencement). En effet, selon la CJUE, l'activité d'**indexation des pages web** des moteurs de recherche relève de l'**intérêt légitime** du responsable de traitement[132].

Si les arrêts « ASNEF et FECEMD contre Administracion del Estado »[133] et « Google contre Espagne »[134] portent sur l'article 7 sous f) de la Directive 95/46/CE, ils ne précisent pas **la méthodologie applicable à la pondération des intérêts prévue à cet article** entre ceux du responsable du traitement et ceux de la personne concernée. Cette lacune a été comblée par l'arrêt « Rigas satiksme » de la CJUE du 4 mai 2017[135].

La question posée à la CJUE, en l'espèce et dans cet arrêt, était de savoir si une compagnie de transport public dont un trolleybus avait été endommagé par un individu pouvait demander à l'autorité de police compétente qu'elle lui communique les coordonnées de cet individu sur la base de l'intérêt légitime du responsable de traitement. La Cour a répondu que cette communication n'était, selon la Directive 95/46/CE, ni obligatoire ni interdite[136] [137]. Pour cela, elle propose un raisonnement qui part de la formulation de l'article 7 sous f) de la Directive 95/46/CE :

> « f) [le traitement] 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** [...] »[138]

Ainsi, la méthode de pondération fondée sur cet article doit vérifier la présence de trois

127 Article 7 de la directive 95/46/CE : « Les États membres prévoient que le traitement de données à caractère personnel ne peut être effectué que si: […]f) 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*, qui appellent une protection au titre de l'article 1er paragraphe 1. »

128 CJUE 24 novembre 2011 « ASNEF et FECEMD contre Administracion del Estado » Aff. C-468/10 et C-469/10

129 Asociación Nacional de Establecimientos Financieros de Crédito

130 Federación de Comercio Electrónico y Marketing Directo

131 CJUE 13 mai 2014 « Google contre Espagne », Aff. C-131/12, pts. 75 à 77 et 82, 85, 86 et 88

132 CJUE 13 mai 2014 « Google contre Espagne », Aff. C-131/12

133 CJUE 24 novembre 2011 « ASNEF et FECEMD contre Administracion del Estado » Aff. C-468/10 et C-469/10

134 CJUE 13 mai 2014 « Google contre Espagne », Aff. C-131/12

135 CJUE 4 mai 2017 « Rigas Satiksme », Aff. C-13/16

136 CJUE 4 mai 2017 « Rigas Satiksme », Aff. C-13/16, dispositif

137 Notons au passage que cet arrêt permet de rappeler que la notion d'intérêt légitime (et cette base de légitimation d'un traitement de données personnelles) ne s'applique pas qu'aux responsables du traitement mais aussi aux tiers ayant un intérêt à ce que les données leur soient communiquées

138 Extrait de l'art. 7 de la Directive 95/46/CE

conditions cumulatives[139] :

1. L'existence effective et la **poursuite d'un intérêt légitime** par le responsable du traitement ou le ou les tiers à qui les données personnelles sont communiquées ;
2. L'existence d'une **nécessité réelle et stricte**[140] de procéder au traitement de données en question pour parvenir à cette finalité, sans qu'il soit possible de lui substituer une méthode moins intrusive en matière de collecte de données personnelles ;
3. La condition que **les droits des personnes concernées ne prévalent pas**.

La pondération de ce dernier critère dépend « des **circonstances concrètes du cas particulier** »[141]. Comme il a été déjà indiqué plus haut dans le présent chapitre de ce guide, le fait que les données utilisées ne soient pas publiquement disponibles[142] augmente la gravité de l'atteinte, de même que la circonstance que la personne concernée soit mineure au moment de la collecte des données (voir la partie sur les données relatives à des enfants)[143]. Cependant, en l'espèce, la CJUE a jugé que malgré la présence de ces deux circonstances, les droits de la personne concernée, en l'espèce, ne prévalaient pas sur ceux de la personne concernée.

Ainsi, comme l'avait noté l'avocat-général dans ses conclusions, qui a été suivi par la décision de la CJUE : l'exercice ou la défense d'un droit en justice est un intérêt légitime au sens de l'article 7 sous f) de la directive 95/46/CE. Cela est d'autant plus le cas que l'article 8 de la Directive 95/46/CE, sur les données sensibles, indique qu'il est autorisé de collecter des données sensibles lorsque cela est nécessaire à l'exercice ou à la défense d'un droit en justice, même si celles-ci n'ont pas été manifestement rendues publiques par la personne concernée[144].

Notons enfin que **la CEDH emploie** elle aussi **la notion d'intérêt légitime**, dans le cas spécifique des employeurs, pour que ceux-ci puissent mettre en œuvre une surveillance de leurs employés lorsque cela se justifie pour « assurer le bon fonctionnement de l'entreprise »[145]. Cet intérêt du responsable de traitement **doit être mis en balance avec celui des personnes concernées par la surveillance**[146], qui doivent bénéficier de certaines garanties que les Etats doivent garantir **même dans des rapports interindividuels**, au premier rang desquels le droit à disposer d'une **information préalable**[147] (la liste de ces garanties est synthétisée dans le chapitre sur le contrôle par la CEDH de la surveillance sur le lieu de travail).

139 CJUE 4 mai 2017 « Rigas Satiksme », Aff. C-13/16, pt. 28
140 CJUE 11 décembre 2014 « Frantisek Rynes », Aff. C-212/13, pt. 28
141 CJUE 4 mai 2017 « Rigas Satiksme », Aff. C-13/16, pt. 31
142 CJUE 24 novembre 2011 « ASNEF et FECEMD contre Administracion del Estado » Aff. C-468/10 et C-469/10, pt. 45
143 CJUE 4 mai 2017 « Rigas Satiksme », Aff. C-13/16, pt. 33
144 Conclusions de l'avocat-général Bobek présentées le 26 janvier 2017 dans l'affaire « Rigas Satiksme » C-13/16
145 CEDH 5 septembre 2017 « Barbulescu contre Roumanie » Req. 61496/08, pt. 127
146 CEDH 5 septembre 2017 « Barbulescu contre Roumanie » Req. 61496/08, pt. 132
147 CEDH 5 septembre 2017 « Barbulescu contre Roumanie » Req. 61496/08, pt. 133

3. Principe de loyauté et droits des personnes concernées

3.A. Test de proportionnalité, ingérence et notion de mise en balance des intérêts

La jurisprudence tant de la CEDH que de la CJUE font fréquemment référence à la notion de proportionnalité ou à celle de mise en balance (ou conciliation) des intérêts.

Du point de vue de la CEDH, le droit à la protection des données personnelles « joue un rôle fondamental pour l'exercice du **droit au respect de la vie privée et familiale consacré par l'article 8 de la [CEDH]**. La législation interne doit donc ménager des garanties appropriées pour empêcher toute utilisation de données à caractère personnel qui ne serait pas conforme aux garanties prévues dans cet article »[148]. Depuis l'entrée en vigueur du traité de Lisbonne en décembre 2009, la Convention européenne des droits de l'Homme a intégré le droit de l'Union, aux côtés de la Charte des droits fondamentaux de l'Union européenne. Cette dernière, qui lie les institutions de l'Union ainsi que les Etats membres dans l'exécution du droit de l'Union[149], comprend comme la CEDH une disposition relative à la protection de la vie privée en général[150] (à son article 7), mais aussi un article qui protège spécifiquement les données personnelles à son article 8[151].

Une ingérence au droit à la vie privée et à la protection des données personnelles peut être validée et acceptée par ces cours, mais à condition qu'elle parvienne à passer un test de proportionnalité dans lequel sont mis en balance ce droit d'une part, et l'intérêt général poursuivi par l'ingérence ainsi que les modalités de cette ingérence d'autre part.

L e **simple fait de mémoriser des données relatives à la vie privée d'un individu constitue une ingérence au sens de l'article 8 de la CEDH[152], sans qu'il soit besoin que celles-ci soient utilisées**[153]. L'**usurpation d'identité** par une personne physique constitue aussi une ingérence dans la vie privée d'une personne au sens de l'article 8 CEDH[154].

148 CEDH 4 décembre 2008 « S. et Marper contre Royaume-Uni » Req. 30562/04 et 30566/04, pt. 103

149 Les Etats membres ne sont cependant liés à la Charte que lorsqu'ils mettent en œuvre une disposition du droit de l'Union

150 Art. 7 de la Charte : « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications »

151 Art. 8 : « 1. Toute personne a droit à la protection des données à caractère personnel la concernant. 2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification. 3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante. »

152 CEDH 26 mars 1987 « Leander contre Suède » Req. 9248/81, pt. 48 ; et
CEDH 4 décembre 2008 « S. et Marper contre Royaume-Uni » Req. 30562/04 et 30566/04, pt. 67

153 CEDH 16 février 2000 « Amann contre Suisse » Req. 27798/95, pt. 69

154 CEDH 14 février 2012 « Romet contre Pays-Bas » Req. 7094/06, pt. 37

Du côté de la CEDH, le test de proportionnalité[155] consiste à vérifier que l'ingérence :

- soit **prévue par la loi**, laquelle doit être énoncée de façon claire, précise, et prévisible pour permettre à l'individu de régler sa conduite[156] [157];
- poursuive un **objectif légitime** ;
- soit « **nécessaire dans une société démocratique »** (notion qui correspond en fait à la notion de **proportionnalité**)

A noter que, pour être admissible, une requête portant sur la surveillance des télécommunications n'exige pas du requérant qu'il démontre qu'il soit effectivement mis sous écoute (voir la partie sur la surveillance d'État)[158].

Dans « Malone contre Royaume-Uni », la CEDH a jugé que l'ingérence, en l'occurrence l'**interception des communications** du requérant, n'était **pas prévue par la loi.** La raison invoquée est que **les dispositions auxquelles le gouvernement britannique se référait pour justifier sa pratique de surveillance étaient vagues et sujettes à des interprétations divergentes**[159]. Il est rare, cependant, qu'une ingérence échoue dès la première étape du test de proportionnalité dans des cas relatifs à la protection des données. Il est déjà plus courant que la CEDH déclare une disposition législative trop vague, bien qu'existante, pour permettre le respect du principe de proportionnalité : le test échoue donc pour des raisons similaires, mais à un stade ultérieur. Ce fut le cas par exemple dans l'arrêt « Funke contre France »[160]. Ce dernier marqua d'ailleurs l'affirmation du principe selon lequel la lutte contre l'évasion fiscale constitue (au même titre par exemple que la sécurité publique) un motif légitime invocable pour justifier une ingérence à l'article 8 de la CEDH.

La CEDH **examine au cas par cas** pour savoir si un Etat offre des « garanties adéquates et suffisantes contre les abus car un système de surveillance secrète destiné à protéger la sécurité nationale crée un risque de saper, voire de détruire, la démocratie au motif de la défendre »[161].

L'affaire « Leander contre Suède » concernait un ancien militant communiste et syndicaliste se plaignant de ne pas avoir été recruté par la marine militaire suite à une procédure de contrôle pour laquelle un fichier secret de police avait été mis à profit. La CEDH a alors estimé que cette interférence était prévue par la loi (étape 1), que son objectif, la **sécurité nationale**, était légitime (étape 2) et que la loi nationale garantissait l'équilibre entre droit à la vie privée et cet objectif légitime (étape 3), puisqu'elle offrait des voies de recours, notamment auprès d'un médiateur indépendant donc les avis sont généralement respectés et suivis[162].

Dans une autre affaire (« S. Marper contre Royaume-Uni »), par contre, la CEDH avait été

155 Voir, pour illustration du mécanisme complet de test de proportionnalité : CEDH 26 mars 1987 « Leander contre Suède » Req. 9248/81 CEDH 4 décembre 2008 « S. et Marper contre Royaume-Uni » Req. 30562/04 et 30566/04

156 CEDH 4 décembre 2008 « S. et Marper contre Royaume-Uni » Req. 30562/04 et 30566/04, pt. 95

157 « Il faut d'abord que la 'loi' soit suffisamment accessible: le citoyen doit pouvoir disposer de renseignements suffisants, dans les circonstances de la cause, sur les normes juridiques applicables à un cas donné. En second lieu, on ne peut considérer comme une 'loi' qu'une norme énoncée avec assez de précision pour permettre au citoyen de régler sa conduite; en s'entourant au besoin de conseils éclairés, il doit être à même de prévoir, à un degré raisonnable dans les circonstances de la cause, les conséquences de nature à dériver d'un acte déterminé » Extrait de l'arrêt CEDH « Sunday Times » du 26 avril 1979 (Req. 6538/74), cité au point 66 de l'arrêt CEDH « Malone contre Royaume-Uni » du 2 août 1984 (Req. 8691/79)

158 CEDH 4 décembre 2015 « Roman Zakharov contre Russie » Req. 47143/06, pt. 171

159 CEDH 2 août 1984 « Malone contre Royaume-Uni » Req. 8691/79, pt. 79

160 CEDH 25 février 1993 « Funke contre France » Req. 10828/84, pt. 57

161 CEDH 26 mars 1987 « Leander contre Suède » Req. 9248/81, pt. 60 ; et CEDH 6 septembre 1978 « Klass e.a. contre RFA » Req. 5026/71, pt. 49

162 CEDH 26 mars 1987 « Leander contre Suède » Req. 9248/81, pt. 81 et pt. 82

« frappée par le caractère général et indifférencié du pouvoir de **conservation** [des données biométriques prélevées sur des suspects, même une fois acquittés] en vigueur en Angleterre et au pays de Galles »[163]. De plus, dans cette affaire, le fait que la collecte portât sur des données de **personnes mineures** constituait une circonstance aggravante de l'ingérence constatée au droit à la vie privée. En l'espèce, les requérants se plaignaient de la conservation par les autorités britanniques de leurs **empreintes biométriques** (empreinte digitale et profil génétique), et ce malgré un classement sans suite un acquittement. Bien que l'ingérence fut prévue par la loi et justifiée par un motif d'intérêt général jugé légitime par la Cour, l'ingérence était de nature **disproportionnée** dans le cadre de ce qu'exige une société démocratique.

Dans une affaire où une **victime d'usurpation d'identité** suite au vol de son permis de conduire n'avait pas pu faire annuler ce titre par l'administration, ni faire annuler l'enregistrement par l'usurpateur de véhicules à son nom, alors que le vol avait été déclaré, la CEDH a jugé que l'**administration aurait pu facilement empêcher les conséquences de l'usurpation d'identité** et, ne l'ayant pas fait, **avait enfreint de façon disproportionnée le droit à la vie privée** de la victime[164].

La mise en balance entre **la liberté de la presse** et le **droit à la vie privée comprend une étape supplémentaire de raisonnement**. Dans « Axel Springer contre Allemagne »[165], CEDH précise les cas dans lesquels il est possible de limiter la liberté d'expression sur le fondement du droit à la vie privée garanti à l'article 8 CEDH. Le test de proportionnalité du droit à la vie privée avec ceuli de la liberté de l'expression doit prendre en compte :

- La contribution ou non à un **débat d'intérêt général** ;
- La **notoriété de la personne concernée** et **l'objet du reportage** ;
- Le **comportement antérieur** de la personne concernée ;
- Le **mode d'obtention des informations** ainsi que leur **véracité** ;
- Le **contenu**, la **forme** et les **conséquences** de la publication.

Dans « Ungváry et Irodalom Kft. contre Hongrie » [166] la CEDH a par exemple pris en compte la circonstance que l'auteur du reportage sur une personnalité publique était un historien reconnu pour juger le critère du mode d'obtention des informations et de leur véracité. Elle a considéré que la contribution à un **débat historique** était **d'intérêt général** (voir la partie sur les traitements de données à des fins statistiques, scientifiques et historiques).

Enfin, en 2016, **la CEDH a précisé deux éléments supplémentaires à prendre en compte dans le test de proportionnalité en matière de *surveillance d'État*** (voir la partie sur le contrôle de la surveillance d'État) : pour être considérée comme « nécessaire dans une société démocratique », une mesure de surveillance secrète autorisée par l'exécutif doit être **strictement nécessaire** soit à la **sauvegarde des institutions démocratiques**, soit à **l'obtention de renseignements dans une opération particulière**. Toute mesure de surveillance secrète ne répondant à l'un ou l'autre de ces critères est susceptible de constituer un abus de pouvoir de la part des autorités mettant en œuvre les technologies de surveillance[167]. De plus, la CEDH peut demander à ce que l'Etat signataire accusé de violation de l'article 8 CEDH **apporte la preuve de l'efficacité de son système de surveillance pour atteindre l'objectif** légitime poursuivi justifiant l'ingérence à la vie privée[168].

163 CEDH 4 décembre 2008 « S. et Marper contre Royaume-Uni » Req. 30562/04 et 30566/04m pt. 119
164 CEDH 14 février 2012 « Romet contre Pays-Bas » Req. 7094/06, pts. 42 et 43
165 CEDH 7 février 2012 « Axel Springer contre Allemagne » Req. 39954/08
166 CEDH 3 décembre 2013 « Ungváry et Irodalom Kft. contre Hongrie » Req. 64520/10
167 CEDH 12 janvier 2016 « Szabó and Vissy contre Hongrie » Aff. 37138/14, pt 73
168 CEDH 4 décembre 2015 « Roman Zakharov contre Russie » Aff. 47143/06, pt. 284

La CJCE, avant de devenir CJUE avec l'entrée en vigueur du traité de Lisbonne**, suivant un raisonnement calqué explicitement sur celui de la CEDH** pour son test de proportionnalité[169]. Ainsi, dans « Österreichischer Rundfunk »[170], elle a jugé que le **contrôle des finances publiques** et l'**intérêt de garantir une utilisation optimale des fonds publics** constituent bel et bien un **motif d'intérêt légitime** de nature à justifier une ingérence à la protection des données personnelles, qu'elle déclare à l'occasion être un **principe général du droit communautaire**[171].

Ce droit n'est cependant pas « une prérogative absolue, **mais doit être pris en considération par rapport à sa fonction dans la société** »[172]. Lorsqu'elles sont amenées à connaître de ce type d'affaires, les juridictions nationales doivent vérifier si la mesure destinée à assurer la poursuite de ces objectifs (en l'espèce : la divulgation des rémunérations de certains salariés soumis au contrôle de la Cour des comptes en Autriche) est **nécessaire et proportionnée** à l'objectif : « la Cour observe que c'est au Gouvernement d'illustrer à l'aide d'exemples appropriés l'effectivité concrète du système de contrôle ».[173]

Notons que selon la CJCE, dans un premier temps, « **la simple mémorisation** par l'employeur de données nominatives relatives aux rémunérations versées à son personnel **ne saurait, comme telle, constituer une ingérence dans la vie privée** »[174], même si cela peut porter atteinte aux règles de la directive 95/46/CE, **alors que selon la CEDH** :

> « Le simple fait de mémoriser des données relatives à la vie privée d'un individu constitue une ingérence au sens de l'article 8 »[175]

La CJUE opéra cependant un revirement en 2013 dans sa décision « Schwarz contre Sadt Bochum »[176] qui lui permit de rapprocher sa jurisprudence avec elle de la CEDH :

> « […] en principe, est susceptible de constituer une atteinte auxdits droits [à la vie privée et à la protection des données personnelles] tout traitement des données à caractère personnel par un tiers »[177]

L'affaire Volker contre Hesse[178] est une illustration d'ingérence disproportionnée dans la vie privée par rapport à l'objectif de contrôle des finances publiques. Il s'agissait en l'espèce de la publication, prévue par un règlement européen, des informations relatives aux bénéficiaires de fonds européens de la politique agricole commune. Cette publication était jugée trop large et portant sur des éléments trop substantiels de la rémunération des personnes concernées.

Le test de proportionnalité appliqué par CJUE a évolué sur la forme avec l'entrée en vigueur du traité de Lisbonne et donc de la Charte des droits fondamentaux de l'Union

169 CJCE 20 mai 2003 « Österreichischer Rundfunk » Aff. C-465/00, C-138/01 et C-139/01, pt. 71
170 CJCE 20 mai 2003 « Österreichischer Rundfunk » Aff. C-465/00, C-138/01 et C-139/01
171 CJCE 20 mai 2003 « Österreichischer Rundfunk » Aff. C-465/00, C-138/01 et C-139/01, pts. 68 et 84
172 CJUE 9 novembre 2010 « Volker et Eifert contre Hesse » Aff. C-92/09 et C-93/09, pt. 48
173 CJCE 20 mai 2005 « Österreichischer Rundfunk » Aff. C-465/00, C-138/01 et C-139/01, pt. 88
174 CJCE 20 mai 2005 « Österreichischer Rundfunk » Aff. C-465/00, C-138/01 et C-139/01, pt. 74
175 CEDH 4 décembre 2008 « S. et Marper contre Royaume-Uni » Req. 30562/04 et 30566/04, pt. 67
176 CJCE 17 octobre 2013 « Michael Schwarz c. Stadt Bochum » Aff. C-291/12
177 CJCE 17 octobre 2013 « Michael Schwarz c. Stadt Bochum » Aff. C-291/12, pt. 25
178 CJUE 9 novembre 2010 « Volker contre Hesse » Aff. C-92/09 et C-93/09

européenne, bien que **le nouveau test de proportionnalité, inspiré de l'article 52 paragraphe 1 de la Charte, colle à l'esprit du test de proportionnalité développé par la CEDH**.

Cet article[179] dessine un test de proportionnalité en quatre étapes[180] :

- La limitation du droit fondamental visé doit être **prévue par la loi** ;
- La limitation ne doit pas empêcher le **respect du contenu essentiel du droit fondamental** visé ;
- La limitation doit remplir un **but d'intérêt général** ;
- L a **proportionnalité** de la limitation du droit fondamental eu égard l'objectif visé, ce qui implique notamment que :
    - La limitation soit de nature à **atteindre l'objectif visé** ;
    - La limitation **ne dépasse pas les limites de ce qui est approprié et nécessaire** à la réalisation de l'objectif visé.

Le raisonnement ci-dessus a été illustré par l'arrêt « Digital Rights Ireland »[181] ayant abouti à l'**invalidation de la directive 2006/24/CE sur la conservation des données**. Voici le résumé du raisonnement de la Cour :

- La limitation du droit à la protection des données et à la vie privée, constituée par la conservation des méta-données de communication, est bel et bien prévue par la Loi : la directive attaquée elle-même ;
- Selon la CJUE, **le respect du contenu essentiel du droit fondamental visé** est garanti par la limitation de la conservation des données aux données de communication (méta-données) et ne concerne donc pas le contenu des communcations[182], d'une part, et que, d'autre part, la directive prévoit quelques mesures relatives à la protection des données [183] ;
- Cette limitation répond à plusieurs **objectifs d'intérêt général** comme la **lutte contre le terrorisme**, la **lutte contre la criminalité**, le **maintien de la sécurité publique** et le droit à celle-ci protégé à l'article 6 de la Charte européenne des droits fondamentaux, sans oublier la **poursuite et la détection d'infractions graves**[184] ;
- La directive 2006/24/CE comprend cependant des mesures disproportionnées eu égard aux objectifs poursuivis :

179 « Toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées 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 libertés d'autrui. »

180 CJUE 8 avril 2014 « Digital Rights Ireland » Aff. C-293/12 et C-594/12, pts. 38-46

181 CJUE 8 avril 2014 « Digital Rights Ireland » Aff. C-293/12 et C-594/12

182 CJUE 8 avril 2014 « Digital Rights Ireland » Aff. C-293/12 et C-594/12, pt. 39

183 CJUE 8 avril 2014 « Digital Rights Ireland » Aff. C-293/12 et C-594/12, pt. 40

184 CJUE 8 avril 2014 « Digital Rights Ireland » Aff. C-293/12 et C-594/12, pt. 41 et pt. 42

- Certes, elle est **apte à réaliser les objectifs poursuivis**[185] ;
- Mais **elle dépasse largement les limites de ce qui est *nécessaire et approprié* à la réalisation d' la finalité des limitations** au droit à la vie privée et à la protection des données[186]. Voici plusieurs éléments sur laquelle la CJUE s'est appuyée pour démontrer la disproportion des mesures prévues par la directive :
  - Elle vise la quasi-totalité de la population européenne[187]
  - Elle ne discrimine pas en fonction des différents objectifs[188]
  - Elle ne comprend pas d'exceptions relatives au secret professionnel[189]
  - Elle ne comprend pas de limitations des autorités nationales compétentes[190]
  - Elle ne limitait pas la finalité du traitement effectué par les données conservées par les autorités nationales compétentes et issues de la conservation des données tel qu'elle le prévoit[191]
  - Enfin, les délais de conservation sont déraisonnablement longs et ne sont pas modulés en fonction de l'objectif poursuivi[192].

3.B. La limite de la durée de conservation des données

Le raisonnement de la CEDH aboutit, comme d'ailleurs celui de la CJUE, à définir toute collecte de données à caractère personnel comme une ingérence dans la vie privée des personnes, qui doit être légitime (principe de licéité et de loyauté des traitements) et proportionnel à la finalité (légitime) recherchée. Cette proportionnalité entraîne :

- L'obligation de limiter la collecte des données collectées au strict nécessaire ;
- L'obligation de **ne pas conserver les données au-delà d'un délai nécessaire** à la réalisation de la finalité légitime du traitement (art. 6 paragraphe 1 sous e) de la directive 95/46/CE).

Ce délai doit être fixé si possible à l'avance, et son importance est rappelé par la

185 CJUE 8 avril 2014 « Digital Rights Ireland » Aff. C-293/12 et C-594/12, pt. 49
186 Le communiqué de presse de la CJUE offre un résumé exhaustif de la liste par ailleurs longue des griefs retenus à l'encontre de la directive 2006/24/CE : http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054fr.pdf
187 CJUE 8 avril 2014 « Digital Rights Ireland » Aff. C-293/12 et C-594/12, pt. 56
188 CJUE 8 avril 2014 « Digital Rights Ireland » Aff. C-293/12 et C-594/12, pt. 57
189 CJUE 8 avril 2014 « Digital Rights Ireland » Aff. C-293/12 et C-594/12, pt. 58
190 CJUE 8 avril 2014 « Digital Rights Ireland » Aff. C-293/12 et C-594/12, pt. 60
191 CJUE 8 avril 2014 « Digital Rights Ireland » Aff. C-293/12 et C-594/12, pt. 61
192 CJUE 8 avril 2014 « Digital Rights Ireland » Aff. C-293/12 et C-594/12, pt. 63

jurisprudence de la CJUE[193] [194]. **En cas de non-respect de cette obligation, la personne concernée dispose d'un droit d'opposition** en vertu de l'article 12 sous b) de la directive 95/46/CE[195].

La fixation de ce délai de conservation **dépend de la finalité du traitement**. Par exemple, dans le cas de copies d'examen, « leur conservation sous une forme permettant l'identification du candidat ne paraît, a priori, plus nécessaire une fois que la procédure d'examen est définitivement close et ne peut plus faire l'objet de recours »[196].

Mais dans certains cas, à l'inverse, **il peut être difficile de déterminer à l'avance une durée de conservation**.

Un cas de figure relevé par la CJCE dès 2009 dans l'arrêt « Rijkeboer » est le cas où des données personnelles ont été transmises à des tiers ; dans ce cas, **le responsable du traitement doit garder la trace des transmissions pour être capable d'en communiquer l'information aux personnes concernées**, sur leur demande, sauf dans des cas où un tel effort serait disproportionné (voir la partie sur l'information des personnes concernées).

Un autre cas de figure est celui où il est difficile de prévoir à l'avance quand la finalité du traitement s'éteint. Par exemple, la **directive 68/151/CEE**[197] prévoyait que les Etats membres tiennent des **registres du commerce ou des sociétés** contenant des informations sur certaines personnes ayant par exemple participé à l'administration ou à la liquidation des entreprises[198]. Ces informations sont nécessaires pour défendre les intérêts des associés et des tiers avec lesquels ces entreprises ont été en relation. Or, les obligations réciproques pouvant découler de ces relations ne s'éteignent pas forcément toujours avec la dissolution d'une société. Dès lors, la disponibilité de ces informations au public peut demeurer légitime même après une telle dissolution. Dans ces circonstances : « il paraît […] impossible d'identifier un délai unique, à compter de la dissolution d'une société, à l'expiration duquel l'inscription [de ces] données dans le registre et leur publicité ne serait plus nécessaire »[199].

Ainsi, **il n'est pas obligatoire de fixer une durée maximale de conservation des données lorsque cela n'est pas possible en raison de la nature de la finalité du traitement**. Mais même en l'absence d'un tel délai de conservation préalablement défini, les personnes concernées gardent, en vertu de l'article 12 sous b), un droit d'opposition lorsqu'elles estiment que la conservation de leurs données n'est plus utile à la finalité poursuivie. Dans ce cas, un examen au cas par cas est nécessaire pour évaluer cette demande.

193 CJUE 9 mars 2017 « Salvatore Manni » Aff. C-398/15, pts. 44 et 45
194 CJUE 8 avril 2014 « Digital Rights Ireland » Aff. C-293/12 et C-594/12, pt. 63
195 CJUE 9 mars 2017 « Salvatore Manni » Aff. C-398/15, pt. 45
196 CJUE 20 décembre 2017 «Peter Nowak contre Data Protection Commissioner» Aff. C-434/16, pt. 55
197 Première directive 68/151/CEE du Conseil, du 9 mars 1968, tendant à coordonner, pour les rendre équivalentes, les garanties qui sont exigées, dans les États membres, des sociétés au sens de l'article 58 deuxième alinéa du traité, pour protéger les intérêts tant des associés que des tiers
198 La liste intégrale de ces personnes est à l'article 2 de la directive 68/151/CEE
199 CJUE 9 mars 2017 « Salvatore Manni » Aff. C-398/15, pt. 55

3.C. L'information des personnes concernées (et la possibilité de la restreindre)

Lorsqu'un traitement de données est prévu par la loi, **l'existence (et la publication) de l'acte législatif permettent de remplir les obligations d'information**[200]. Mais il doit bel et bien s'agir d'un acte législatif publié[201], et le traitement effectué doit correspondre effectivement aux finalités prévues par celle-ci[202].

Par ailleurs, l'**article 13 de la directive 95/46/CE** permet aux Etats membres d'adopter des dispositions législatives « visant à **limiter la portée des obligations et des droits prévus à** […] **l'article 10, à l'article 11 paragraphe 1** […] » (il s'agit respectivement de l'article sur l'obligation d'information en cas d'informations collectées directement auprès de la personne concernée, et de l'obligation d'information lorsque les données n'ont pas été collectées directement auprès de la personne concernée). Aux termes de ce même article 13, une telle limitation de ces obligations doit viser à sauvegarder la sûreté de l'Etat, la défense, la sécurité publique, la prévention et la recherche et la poursuite d'infractions pénales ou de manquements à la déontologie de professions réglementées, ou bien encore poursuivre la sauvegarde d'intérêts économiques ou financiers importants de l'Etat concerné ou de l'UE, la protection de la personne concernée ou des droits et libertés d'autrui, ou encore permettre une mission de contrôle ou d'inspection ou de réglementation relevant de l'autorité publique. Et **ces limitations** à l'obligation d'information des personnes concernées, même poursuivant ces finalités, **ne peuvent être prévues que par la loi**[203].

En 2017, la CJUE a précisé la portée de cet article en ce qui concerne les traitements de données ayant pour finalité la **collecte de l'impôt et la lutte contre la fraude fiscale**[204]. Elle indique que **seule une autorité investie par la loi d'une telle mission** peut bénéficier des exemptions aux droits des personnes concernées permises par l'article 13 de la directive[205], et qu'une telle autorité doit **être en mesure de prouver la stricte nécessité** de recourir à ces exemptions[206].

Enfin, dans le cadre de la lutte contre la fraude fiscale, l'inscription sur une liste de données personnelles d'une personne **ne doit pas porter atteinte au principe de présomption d'innocence**. Dès lors, seule une personne envers laquelle il **existe des indices sérieux** et **suffisants** peut être inscrite **sans son consentement** sur une liste de **personnes suspectes** telle qu'une liste de gens soupçonnés d'être des prête-noms[207].

Peut se poser la question de la **conjonction entre les obligations relatives à la limitation du délai de conservation des données personnelles et celles relatives à l'information de la personne concernée**. Ainsi, dans « Rotterdam contre Rijkeboer »[208], la CJCE a affirmé que le : « [L]e droit au respect de la vie privée implique que la personne concernée puisse s'assurer que ses données à caractère personnel sont traitées de manière exacte et licite,

200 CJUE 1er octobre 2015 « Smaranda Bara e.a. » Aff. C-201/14, pts. 37 et 38
201 CJUE 1er octobre 2015 « Smaranda Bara e.a. » Aff. C-201/14, pt. 40
202 CJUE 1er octobre 2015 « Smaranda Bara e.a. » Aff. C-201/14, pts. 37 et 38
203 CJUE 1er octobre 2015 « Smaranda Bara e.a. » Aff. C-201/14 pts. 40 et 41
204 CJUE 27 septembre 2017 « Puškár contre Slovaquie » Aff. C-73/16
205 CJUE 27 septembre 2017 « Puškár contre Slovaquie » Aff. C-73/16, pts. 109 et 110
206 CJUE 27 septembre 2017 « Puškár contre Slovaquie » Aff. C-73/16, pts. 111-112
207 CJUE 27 septembre 2017 « Puškár contre Slovaquie » Aff. C-73/16, pt. 114
208 CJCE 7 mai 2009 « College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer » Aff. C-553/07

c'est-à-dire, en particulier, que les données de base la concernant sont exactes et qu'elles sont adressées à des destinataires autorisés. Ainsi qu'il est énoncé au quarante et unième considérant de la directive, afin de pouvoir effectuer les vérifications nécessaires, la personne concernée doit disposer d'un droit d'accès aux données la concernant qui font l'objet d'un traitement »[209]. En l'espèce, il s'agissait d'une affaire dans laquelle la commune de Rotterdam avait communiqué à des tiers des données personnelles concernant le requérant. Ces données, conservées un an par la commune, ont ensuite été supprimées, et lorsque, sur une période de deux ans précédant sa requête, le requérant demanda à savoir à qui les données ont été transmises, la commune ne fut plus en mesure de répondre.

Une telle obligation peut cependant constituer une charge disproportionnée aux termes de la directive, et il n'est donc pas toujours obligatoire de conserver les informations sur les destinataires pendant une durée identique à celle des données de base. Un examen au cas par cas est nécessaire.

Une autre affaire dans laquelle la CJUE a été amenée à se prononcer sur la limitation de l'obligation d'information préalable dans le cadre d'**enquêtes disciplinaires prévues par la loi menées par un détective privé** pour le compte d'un **organisme professionnel** : il s'agit de l'affaire « IPI contre Engelbert e.a. »[210]. La Cour a rappelé que : « conformément à une jurisprudence constante, la protection du droit fondamental à la vie privée exige que les dérogations à la protection des données à caractère personnel et les limitations de celles-ci doivent s'opérer dans les limites du strict nécessaire »[211].

3.D. Droit d'opposition

Les personnes concernées disposent d'un **droit d'opposition** au traitement de leurs données. En vertu de l'article 14, premier alinéa sous a) de la directive 95/46/CE, ce droit d'opposition s'applique notamment aux traitements de données qui se basent sur l'exercice d'une mission de service public (art. 7 sous e) de la directive) ou sur l'intérêt légitime du responsable du traitement (art. 7 sous f) de la directive)[212].

C e **droit d'opposition n'est cependant pas absolu** : il faut « tenir compte de manière plus spécifique de toutes les circonstances entourant la situation de la personne concernée »[213].

Un autre cas de figure relevant de l'article 12 sous b) de la directive 95/46/CE est lorsque la personne concernée **souhaite s'opposer** à **la poursuite du traitement** de ses données personnelles **passé le délai de conservation** utile à la réalisation des finalités légitimes de ce traitement[214].

209 CJCE 7 mai 2009 « College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer » Aff. C-553/07, pt. 49
210 CJUE 7 novembre 2013 « IPI contre Engelbert e.a. » Aff. C-473/12
211 CJUE 7 novembre 2013 « IPI contre Engelbert e.a. » Aff. C-473/12, pt. 39
212 CJUE 9 mars 2017 « Salvatore Manni » Aff. C-398/15, pt. 47
213 CJUE 9 mars 2017 « Salvatore Manni » Aff. C-398/15, pt. 47
214 CJUE 9 mars 2017 « Salvatore Manni » Aff. C-398/15, pt. 46 et
CJUE 13 mai 2014 « Google contre Espagne » Aff. C-131/12, pt. 70

3.E. Droit d'accès et de rectification des personnes concernées

Le droit d'accès des personnes concernées est un des éléments essentiels garantissant l'effectivité d'un droit à la protection des données personnelles. Il permet de notamment aux personnes concernées de **vérifier l'exactitude des données** les concernant[215], et de vérifier le respect des délais de conservation[216]. Sans droit d'accès, il n'est en effet pas possible de prendre connaissance de l'existence de données erronées sur soi et donc de demander dans un second temps leur **rectification**.

L'**article 12 de la directive 95/46/CE** oblige donc logiquement les responsables de traitement à garantir un **droit d'accès** aux personnes concernées « s**ans contrainte, à des intervalles raisonnables et sans délais ou frais excessifs** ». La CJUE en a précisé la portée dans « X. contre Bois-le-Duc »[217] en 2013. En effet, il posait des questions d'interpétation en fonction des langues officielles dans lesquelles la directive a été traduite. Il n'était pas clair si l'adjectif « excessif » se rapportait uniquement aux délais ou également aux frais. S'il se rapportait aux frais, alors de tels frais eurent été autorisés dans certaines limites. Dans le cas inverse, tout frais eut été contraire à la directive. La Cour a tranché en faveur d'une interprétation selon laquelle **il est possible de fracturer des frais pour l'accès des personnes concernées à leurs données personnelles, sous réserve que le montant ne dépasse les stricts coûts de communication**, n'entrave pas l'exercice des droits garantis par la directive, la Charte des droits fondamentaux et la Convention européenne des droits de l'Homme.

Le droit d'accès **n'oblige pas** le responsable de traitement à fournir une **copie conforme du document ou fichier ou tout autre support des données personnelles**. Les Etats membres détiennent en effet une marge de manœuvre prévue par la directive 95/46/CE pour déterminer le format de la communication. Dès lors que ce format est un **format intelligible permettant effectivement à la personne concernée de prendre connaissance des données, d'en vérifier l'exactitude et la conformité du traitement à la loi**, celui-ci est conforme à la directive[218].

Le droit **ne couvre** cependant **que l'accès aux données personnelles de la personne concernée**. Ceci signifie d'une part qu'il ne s'étend bien entendu pas aux données personnelles de tiers, mais également que le droit d'accès ne couvre pas les analyses juridiques de ces données, sauf si ces analyses contiennent elles mêmes des données personnelles sur la personne concernée[219]. A partir du moment où une information ou un document détenu par une administration publique ne correspond pas à la définition de ce qu'est une donnée personnelle (voir la partie sur la définition de la notion de donnée personnelle), le régime juridique applicable est celui de l'**accès aux documents administrations et aux informations d'intérêt public**.

Par contre, **une règle de droit spécifique**, si elle ne s'inscrit pas dans le cadre des

215 CJUE 20 décembre 2017 «Peter Nowak contre Data Protection Commissioner» Aff. C-434/16, pts. 51-54
216 CJUE 20 décembre 2017 «Peter Nowak contre Data Protection Commissioner» Aff. C-434/16, pt. 57
217 CJUE 12 décembre 2013 « X. contre Bois-le-Duc » Aff. C-486/12
218 CJUE 17 juillet 2014 « Y.S. contre minister voor Immigratie » Aff. C-141/12, pt. 57
219 CJUE 17 juillet 2014 « Y.S. contre minister voor Immigratie » Aff. C-141/12, pt. 45

exceptions visées à l'article 13 de la directive 95/46/CE ou ne se situe pas hors du champ d'application du droit de l'Union, **ne peut venir restreindre le droit d'accès** des personnes concernées dès lors que l'on est en présence de données à caractère personnel. Ainsi, « il y a lieu de considérer que le fait de donner au candidat [à un examen] un droit d'accès à ses réponses et [aux] annotations [sur sa copie d'examen] […] sert l'objectif […] 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** »[220].

Enfin, la CJUE a indiqué qu'il est possible de restreindre le droit à la rectification des données personnelles, même dans des cas où il n'est pas possible de restreindre le droit d'accès. Ainsi, il n'est pas possible pour un candidat malheureux à un examen de rectifier après coup les réponses qu'il avait données à l'examen[221], car « il résulte de l'article 6, paragraphe 1, sous d), de la directive 95/46 que **le caractère exact et complet de données à caractère personnel doit être apprécié au regard de la finalité pour laquelle ces données ont été collectées** »[222].

Si la CJUE a logiquement été amenée à se prononcer sur les dispositions de la directive 95/46/CE concernant le droit d'accès, la CEDH a elle aussi développé une jurisprudence indirecte sur le sujet du droit d'accès. Si elle n'interprète pas cette directive – laquelle ne fait pas partie de ses normes de référence – et que la notion de droit d'accès n'existe pas en tant que telle dans le cadre de la CEDH, la jurisprudence de la CEDH fournit un cadre d'interprétation auquel la directive est elle-même soumise.

Dans « Gaskin contre Royaume-Uni »[223], la CEDH conclut à la **violation de l'article 8 CEDH pour non-communcation de données personnelles le concernant au requérant**. S'il est permis à un Etat de refuser une telle communication, la CEDH affirme que cela n'est nécessaire dans une société démocratique que si **la décision finale de refus de communication est prise par une autorité indépendante**. Dans « Segerstedt-Wiberg e.a. contre Suède »[224], la CEDH conclut aussi à la violation de l'article 8 CEDH, mais non en raison du refus de communiquer des données personnelles à la personne concernée, puisque celles-ci avaient été collectées dans le cadre de la **lutte contre le terrorisme**. Par contre, dans « Turek contre Slovaquie »[225], elle a condamné le fait que le requérant n'ait pas pu avoir aux données personnelles sur la base desquelles il s'était vu refuser un certificat de sécurité, et accusé d'avoir collaboré avec les services secrets tchécoslovaques à l'époque de la dictature communiste[226] (voir la partie sur les procédures d'habilitation défense).

3.F. Droit au déréférencement (droit à l'oubli ?)

220 CJUE 20 décembre 2017 «Peter Nowak contre Data Protection Commissioner» Aff. C-434/16, pt. 56
221 CJUE 20 décembre 2017 «Peter Nowak contre Data Protection Commissioner» Aff. C-434/16, pt. 52
222 CJUE 20 décembre 2017 «Peter Nowak contre Data Protection Commissioner» Aff. C-434/16, pt. 53
223 CEDH 7 juillet 1989 « Gaskin contre Royaume-Uni » Req. 10454/83
224 CEDH 6 juin 2006 « Segerstedt-Wiberg e.a. contre Suède » Req. 62332/00
225 CEDH 14 février 2006 « Turek contre Slovaquie » Req. 57986/00
226 CEDH 14 février 2006 « Turek contre Slovaquie » Req. 57986/00

3.F.a. Présentation du droit au déréférencement

L'arrêt « Google contre Espagne »[227] de 2014 de la CJUE a consacré un droit au déréférencement, auquel il est souvent fait référence comme un « droit à l'oubli ». La notion de droit à l'oubli renvoyant plutôt dans la littérature à un effacement complet de ses traces numériques, il nous a semblé préférable pour parler d'un simple déréférencement d'une donnée accessible depuis un moteur de recherche de parler de droit au déréférencement, par souci de rigueur.

Conformément au **principe de légalité**, tout traitement de données doit reposer sur un des **fondements énumérés à l'article 7 de la directive 95/46/CE**. L'article 12 de cette même directive permet aux personnes concernées de demander la **rectification**, l'**effacement** ou le **verrouillage** de leurs données personnelles inexactes ou collectées de façon non-conforme à la loi. L'article 14 sous a) permet à la personne concernée de **s'opposer au traitement** « pour des raisons prépondérantes et légitimes tenant à sa situation particulière », au moins pour les traitements fondés sur l'exercice d'une **mission de service public (art. 7 sous e))** ou la réalisation de l'**intérêt légitime du responsable de traitement (art. 7 sous f))**.

Selon la CJUE, la lecture combinée de ces dispositions appliquée aux moteurs de recherche, dont l'indexation des contenus contenant des données personnelles se fonde sur l'article 7 sous f) de la directive 95/46/CE sur l'intérêt légitime (voir la partie sur l'intérêt légitime des responsables de traitement) offre à la personne concernée, sous réserve qu'un intérêt prépondérant du public n'en exige pas autrement en raison du rôle public joué par celle-ci, de demander à ce que ses données personnelles ne soient plus affichées dans la liste des résultats d'un moteur de recherche[228]. Ceci est possible même si le contenu d'origine a été mis en ligne de façon parfaitement légale, et y compris si ce contenu d'origine demeure en ligne sur le site d'origine après déréférencement par le moteur de recherche[229].

3.F.b. Les limites du droit au déréférencement

En même temps qu'elle y consacre le principe, la CJUE, dans son arrêt « Google contre Espagne »[230], apporte une **limitation au droit au déréférencement** : « 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 […] accès à l'information en question** »[231], alors la demande de déréférencement peut être rejetée. L'arrêt précise cependant mal les conouts de la limitation, ce qui explique la publication par le Groupe de travail de l'Article 29 d'un avis sur le sujet[232].

227 CJUE 13 mai 2014 « Google contre Espagne » Aff. C-131/12

228 CJUE 13 mai 2014 « Google contre Espagne » Aff. C-131/12

229 En l'espèce, le site d'origine était celui d'un organe de presse, dont les traitements de données disposent d'un statut particulier (voir la partie sur les traitements à seules fins de journalisme). Par ailleurs, l'arrêt Google sur le droit à l'oubli ne concerne pour le moment que les traitements de données fondés sur l'article 7 sous f) de la directive 95/46/CE, c'est-à-dire sur la disposition relative à l'intérêt légitime du responsable de traitement.

230 CJUE 13 mai 2014 « Google contre Espagne » Aff. C-131/12

231 CJUE 13 mai 2014 « Google contre Espagne » Aff. C-131/12, pt. 99

232 Document WP 225, disponible en-ligne (en anglais uniquement) : http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf

3.G. Droit à la suppression de données personnelles collectées dans le cadre d'une procédure pénale

La CEDH a été amenée dans « S. et Marper contre Royaume-Uni » à se prononcer sur la question de la **suppression des données** et les **limitations à apporter à la durée de conservation**. En l'espèce, la CEDH a été amenée à connaître d'une affaire dans laquelle les requérants avaient demandé la suppression de leurs **données biométriques** des fichiers de police suite, pour l'un, à son **acquittement**, et pour l'autre, **au classement sans suite de la poursuite** dont il faisait l'objet. Si l'objectif de **prévention des infractions pénales** est bel et bien un objectif légitime pouvant légitimer une ingérence dans le droit à la vie privée garantir par l'article 8 CEDH, une telle atteinte doit être proportionnée (voir la partie sur le test de proportionnalité effectué par la CEDH). Or, la CEDH a relevé qu'à la date du litige, la législation en vigueur en Angleterre et au Pays de Galle **ne limitait pas la durée de conservation des données**[233]. De surcroît, elle a jugé « particulièrement préoccupant » le fait que les données de **personnes non-condamnées** bénéficiant du principe de **présomption d'innocence** soient traitées de la même façon quant à leurs données personnelles que les personnes condamnées[234]. Dès lors, l'ingérence dans la vie privée des requérants a été juége comme étant disproportionnée et contraire à la CEDH. Ceci consacre un droit à l'effacement des données biométriques collectées dans le cadre d'une enquête pénale sur des personnes qui ne font pas, à l'issue du processus, l'objet d'une condamnation. Certaines exceptions à ce principe sont ouvertes par la CEDH dans son arrêt dans des cas d'enquêtes sur des crimes graves, mais se réserve dans ce cas la possibilité d'étudier au cas par cas la proportionnalité de la mesure de conservation des données personnelles des personnes non-condamnées.

3.H. Recevabilité de données à caractère personnel dans le cadre d'une procédure judiciaire

En vertu de l'article 3 de la directive 95/46/CE, celle-ci ne s'applique pas aux données personnelles collectées et traitées dans le cadre d'une finalité relevant du domaine pénal. La CJUE n'a donc pas été amenée à se prononcer sur la recevabilité de données à caractère personnel, notamment obtenues sans le consentement de la personne concernée, dans le cadre d'une procédure pénale.

Elle a cependant été amenée à se prononcer, dans l'arrêt « Puškár contre Slovaquie » du 27 septembre 2017[235], sur la recevabilité d'une liste de données à caractère personnel obtenue à l'insu du responsable du traitement dans le cadre d'un **recours juridictionnel portant sur une violation alléguée des droits garantis par la directive 95/46/CE** et les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne. Un tel recours non seulement rendu possible par l'article 22 de cette directive, mais également par l'article **47 de la Charte des droits fondamentaux**.

233 CEDH 4 décembre 2008 « S. et Marper contre Royaume-Uni » Req. 30562/04 et 30566/04, pt. 113
234 CEDH 4 décembre 2008 « S. et Marper contre Royaume-Uni » Req. 30562/04 et 30566/04, pt. 122
235 CJUE 27 septembre 2017 « Puškár contre Slovaquie » Aff. C-73/16

Selon la CJUE, l'article 47 de la Charte des droits fondamentaux ne permet de refuser qu'une liste de données personnelles soit admise comme moyen de preuve dans un tel procès que si une loi nationale limite de façon justifiée au regard de l'article 13 les droits d'information et d'accès énoncés aux articles 10 à 12 de la directive 95/46/CE les droits des personnes concernées en rapport avec ces données[236].

236 CJUE 27 septembre 2017 « Puškár contre Slovaquie » Aff. C-73/16, pts. 97-98

4. Surveillance d'État (dont la question des fichiers de police)

4.A. Cadre général

Un premier élément de cadre général à avoir en tête est que pour la CEDH effectue un contrôle de l'ensemble des activités de surveillance d'État sur la base de l'**article 8 de la CEDH protégeant le droit à la vie privée**. Ce contrôle s'étend aux traitements de données à des fins de sécurité et de police, contrairement au contrôle de la CJUE, qui sauf cas limites exceptionnels[237], ne peut avoir à connaître que des affaires relevant du domaine de compétence communautaire de l'Union.

Comme pour toute affaire impliquant une limitation d'un droit garanti par la Convention européenne des droits de l'Homme, une limitation du droit à la vie privée doit être **prévue par la loi** (voir la partie sur le test de proportionnalité). Ainsi, dans « Malone contre Royaume-Uni », une décision de 1984, la CEDH a rappelé que la **surveillance de la correspondance** et les **écoutes téléphoniques** doivent être prévues par la loi, ce qui, en l'espèce, n'était pas le cas en raison de dispositions parcellaires et peu claires[238]. Plus tard, en 2010, dans « Kennedy contre Royaume-Uni »[239], la CEDH a cependant validé le régime britannique d'interception des télécommunications.

La question de l'intérêt à agir est une question qui a amené des divergences de jurisprudence. En effet, comme rappelé au point 164 de l'arrêt « Roman Zakharov contre Russie »[240] : « selon la jurisprudence constante de la Cour, la **Convention ne reconnaît pas l'actio popularis** et la Cour n'a pas normalement pour tâche d'examiner dans l'abstrait la législation et la pratique pertinentes, mais de rechercher si la manière dont elles ont été appliquées au requérant ou l'ont touché a donné lieu à une violation de la Convention ». Les mesures de surveillance secrète constituent l'exception à cette règle, puisque la Cour reconnaît depuis l'arrêt « Klass et autres »[241] que : « un **individu pouvait, sous certaines conditions, se prétendre victime d'une violation entraînée par la simple existence de mesures secrètes ou d'une législation permettant de telles mesures, sans avoir besoin d'avancer qu'on les lui avait**

237 En effet, dans l'arrêt « Digital Rights Europe » du 8 avril 2014, la CJUE a été amenée à analyser la compatibilité des programmes de surveillance de la National Security Agency des Etats-Unis au regard du droit européen à la protection des données. L'absence de garantie pour les citoyens européens des garanties minimales de protection de leur vie privée face aux programmes de surveillance de masse de la NSA ayant pour conséquence l'absence d'équivalence dans la protection des données entre les Etats-Unis et l'Union européenne, la CJUE a alors annulé la décision « Safe Harbor » permettant sous certaine condition le transfert de données personnelles depuis l'UE vers les Etats-Unis. De ce fait, matériellement, la CJUE ne s'est prononcée que sur une décision de l'Union relevant des compétences communautaires de celle-ci, mais a tout de même été amenée à énoncer un certain nombre de principes encadrant la surveillance d'État sur la base de la Charte des droits fondamentaux de l'Union européenne et de la Convention européenne des droits de l'Homme.

238 CEDH 2 août 1984 « Malone contre Royaume-Uni » Req. 8691/79, pt. 79

239 CEDH 18 mai 2010 « Kennedy contre Royaume-Uni » Req. 26839/05

240 CEDH 4 décembre 2015 « Roman Zakharov contre Russie » Aff. 47143/06, pt. 164

241 CEDH 6 septembre 1978 « Klass e. a. contre RFA » Aff. 5026/71

réellement appliquées »[242]. La reconnaissance de cet intérêt à agir était cependant assorti de certaines conditions[243]. De plus, cet arrêt permit pour la première fois à la Cour d'affirmer qu'en matière de surveillance secrète, **la charge de la preuve reposait sur l'Etat dont la mesure était attaquée**. Par la suite, il y eut deux conceptions de la qualité de victime dans des affaires de surveillance secrète qui se sont développées en parallèle et de façon contradictoire[244] : dans certaines affaires, la CEDH a considéré qu'il ne fallait pas interpréter « Klass e.a. contre RFA » de façon extensive et ouvrir une possibilité de recours à toute personne souhaitant introduire un recours général contre une législation instaurant une surveillance généralisée des télécommunications[245]. Dans « Kenney contre Royaume-Uni »[246] de 2010, la CEDH a confirmé qu'en matière de surveillance secrète, il fallait déroger à l'approche générale déniant aux particuliers le droit de se plaindre *in abstracto* d'une législation. En effet, elle estima qu'il fallait éviter que « le caractère secret de pareilles mesures ne conduisît [...] à ce qu'elles fussent en pratique inattaquables et qu'elles échappassent au contrôle des autorités judiciaires nationales et de la Cour »[247]. Dans ce contexte, la CEDH a dans cet arrêt énoncé qu'elle prendrait en compte la **possibilité en droit interne ouverte aux individus pour se plaindre d'une ingérence du seul fait de l'existence d'une législation autorisant des mesures de surveillance secrète** et le **risque que des mesures de surveillance secrète fussent appliquées au requérant**. En cas **d'absence de possibilité de contester en droit interne l'application de mesures de surveillance, les soupçons d'un usage abusif des pouvoirs de surveillance secrète étaient accrus et qu'en pareil cas, un contrôle accru de la part de la CEDH était justifié**[248].

La relative disparité des approches adoptées par la Cour depuis l'arrêt « Klass e.a. contre RFA » l'a amenée à préciser et unifier son approche dans l'arrêt « Roman Zakharov contre Russie » de 2015[249], qu'elle cite désormais dans ses arrêts en lieu et place de l'arrêt « Klass e.a. contre RFA »[250]. Elle y annonce adopter désormais l'approche issue de l'arrêt « Kennedy contre Royaume-Uni »[251]. Selon cette approche : un requérant peut se prétendre victime d'une violation entraînée par la seule existence de mesures de surveillance secrète **à condition que la législation attaquée puisse toucher le requérant**[252]. Par ailleurs, **la Cour tiendra compte de la disponibilité de recours internes et ajuste le niveau de son contrôle à l'effectivité de celui-ci**[253]. Cette possibilité d'un recours interne est notamment importante pour garantir un contrôle du pouvoir discrétionnaire dont dispose l'exécutif en matière de surveillance d'État, et qui lui est d'ailleurs reconnu comme « nécessaire dans une société démocratique » par la CEDH.

La CEDH admet un **certain degré de pouvoir discrétionnaire** à l'exécutif pour décider des individus à mettre sur écoute, mais ce pouvoir discrétionnaire doit être **strictement encadré**[254], notamment en ce qui concerne les **finalités du traitement** et les **personnes pouvant**

242 CEDH 4 décembre 2015 « Roman Zakharov contre Russie » Aff. 47143/06, pt. 165
243 Voir : CEDH 6 septembre 1978 « Klass e. a. contre RFA » Aff. 5026/71, pts. 34 à 38 (la jurisprudence Klass et autres ayant été amendées par la décision Roman Zakharov contre Russie, l'étude de ces conditions n'a cependant plus qu'un intérêt d'ordre historique)
244 CEDH 4 décembre 2015 « Roman Zakharov contre Russie » Aff. 47143/06, pt. 166
245 CEDH 4 décembre 2015 « Roman Zakharov contre Russie » Aff. 47143/06, pts. 167 et 168
246 CEDH 18 mai 2010 « Kennedy contre Royaume-Uni » Aff. 26839/05
247 CEDH 18 mai 2010 « Kennedy contre Royaume-Uni » Aff. 26839/05, pt. 124 et CEDH 4 décembre 2015 « Roman Zakharov contre Russie » Aff. 47143/06, pt. 169
248 CEDH 18 mai 2010 « Kennedy contre Royaume-Uni » Aff. 26839/05, pt. 124
249 CEDH 4 décembre 2015 « Roman Zakharov contre Russie » Aff. 47143/06, pt. 170
250 CEDH 31 mars 2016 « Šantare et Labaņikovs contre Lettonie » Aff. 34148/07, pt. 53
251 CEDH 18 mai 2010 « Kennedy contre Royaume-Uni » Aff. 26839/05
252 Ce qui n'est pas difficile à démontrer en cas de législation instaurant des mesures de surveillance généralisées, comme le faisait par exemple la directive 2006/24/CE
253 CEDH 4 décembre 2015 « Roman Zakharov contre Russie » Aff. 47143/06, pt. 171
254 CEDH 12 janvier 2016 « Szabó and Vissy contre Hongrie » Aff. 37138/14, pt. 65 et CEDH 4 décembre 2015

être soumises à surveillance. Moyennant les garanties suffisantes, la CEDH admet la possibilité de mises sur écoute téléphonique sans l'autorisation d'un juge[255]. Les demandes administratives de mise sur écoute **doivent être motivées** et **fondées sur des éléments factuels** permettant d'apprécier la légitimité de la demande[256].

L'obligation d'autorisation par un membre de l'exécutif autre que le ministre de l'Intérieur (en l'espèce le ministre de la Justice) des demandes de mise sur écoute, formulées par les services de renseignement ou de police compétents, ne remplit pas le **critère d'indépendance indispensable pour garantir la stricte nécessité** d'une telle mesure[257], surtout en l'absence de toute possibilité de recours judiciaire. Dans l'arrêt « Szabó and Vissy contre Hongrie », la CEDH a rappelé ce qu'elle avait déjà affirmé dans « Dumitru Popescu » : lorsque l'autorisation de procéder à des écoutes n'est pas octroyée par une autorité indépendante de l'exécutif, ces mesures doivent pouvoir être contestées devant un **juge ou une autre forme d'autorité indépendante**[258]. Si de telles garanties ne sont pas apportées, cela constitue une **violation de l'article 3 CEDH**. Mais de de bons mécanismes de contrôle *ex post* peuvent aussi, selon la CEH, justifier d'un allègement des procédures *ex ante*[259].

Quant aux **objectifs justifiant une mesure de surveillance d'État**, l'arrêt « Klass e.a. contre RFA »[260] est le premier d'une longue série portant sur le sujet. En l'espèce, les requérants dénonçaient une loi adoptée en RFA restreignant le secret de la correspondance et permettant à l'Etat de procéder à une **surveillance de la correspondance** sans avoir à en informer la personne concernée, ni permettre de recours effectif. La CEDH y a pour la première affirmé le principe selon lequel : **« caractéristique de l'États policier, le pouvoir de surveiller en secret les citoyens n'est tolérable d'après la Convention que dans la mesure strictement nécessaire à la sauvegarde des institutions démocratiques »**[261]. **La lutte contre le terrorisme est donc un objectif légitime** pouvant justifier, moyennant un examen de proportionnalité (voir la partie la notion d'ingérence et le test de proportionnalité), l'ingérence au droit à la vie privée garanti par l'art. 8 CEDH. A noter que l**a CEDH a précisé** à l'occasion de l'arrêt « Szabó and Vissy contre Hongrie » **deux éléments supplémentaires à prendre en compte dans le test de proportionnalité en matière de *surveillance d'État*** : pour être considérée comme « nécessaire dans une société démocratique », une mesure de surveillance secrète autorisée par l'exécutif doit être strictement nécessaire soit à la sauvegarde des institutions démocratiques, soit à l'obtention de renseignements dans une opération particulière. Toute mesure de surveillance secrète ne répondant à l'un ou l'autre de ces critères est susceptible de constituer un abus de pouvoir de la part des autorités mettant en œuvre les technologies de surveillance[262].

L'arrêt « Klass e.a. contre RFA » affirme pour la première fois que l'objectif de lutter contre

« Roman Zakharov contre Russie » Aff. 47143/06, pt. 247

255 CEDH 6 septembre 1978 « Klass e. a. contre RFA » Aff. 5026/71, pt. 51, cité par : CEDH 12 janvier 2016 « Szabó and Vissy contre Hongrie » Aff. 37138/14, pt. 77

256 CEDH 12 janvier 2016 « Szabó and Vissy contre Hongrie » Aff. 37138/14, pt. 71

257 CEDH 12 janvier 2016 « Szabó and Vissy contre Hongrie » Aff. 37138/14, pt. 75

258 CEDH 26 avril 2007 « Dumitru Popescu contre Roumanie » Aff. 49234/99, pts. 70-73

259 CEDH 18 mai 2010 « Kennedy contre Royaume-Uni » Aff. 26839/05, pt. 167, cité par : CEDH 12 janvier 2016 « Szabó and Vissy contre Hongrie » Aff. 37138/14, pt. 77

260 CEDH 6 septembre 1978 « Klass e.a. contre RFA » Req. 5026/71

261 CEDH 6 septembre 1978 « Klass e.a. contre RFA » Req. 5026/71, pt. 42

262 CEDH 12 janvier 2016 « Szabó and Vissy contre Hongrie » Aff. 37138/14, pt 73

des « **actes terroristes** » constitue une justification légitime de l'ingérence à l'article 8 de la CEDH. Dans «Szabó and Vissy contre Hongrie », la CEDH a rappelé que cet objectif **n'est pas trop vague** pour remplir le critère selon lequel toute ingérence doit être **prévue par la Loi**[263]. Ainsi « la Cour juge inhérente au système de la Convention une certaine forme de **conciliation entre les impératifs de la défense de la société démocratique et ceux de la sauvegarde des droits individuels** »[264]. Cependant, « la Cour souligne néanmoins que les États contractants ne disposent pas pour autant d'une latitude illimitée pour assujettir à des mesures de surveillance secrète les personnes soumises à leur juridiction. Consciente du danger, inhérent à pareille loi, de saper, voire de détruire, la démocratie au motif de la défendre, elle affirme qu'ils ne sauraient prendre, au nom de la lutte contre l'espionnage et le terrorisme, n'importe quelle mesure jugée par eux appropriée. »[265] En l'espèce, dans l'affaire « Klass e.a. contre RFA », elle a conclu à la conformité des mesures attaquées à la CEDH, car elles disposaient de garanties assorties suffisantes, notamment une **limitation de la conservation des données**[266] **dans le temps**, **des conditions procédurales strictes**[267] et un système de **supervision parlementaire** où l'opposition était représentée[268].

Dans son arrêt « S. et Marper contre Royaume-Uni », la CEDH avait déjà été amenée à affirmer le principe selon lequel : « il est essentiel de **fixer des règles claires et détaillées** régissant […] l'utilisation, l'accès des tiers [aux données personnelles traitées par les services de police] »[269]. Ainsi, la question de l'accès participe aux mécanismes de supervision devant limiter les abus.

La collecte de données, y compris dans le cadre d'enquêtes pénales, **doit respecter le principe de limitation des finalités** : seules les données personnelles nécessaires à l'objet de l'enquête doivent être collectées et conservées[270]. Ce principe implique aussi que la surveillance ne soit pas une surveillance de masse. Les mises sur écoute doivent correspondre bel et bien aux nécessités d'une enquête et doivent être ciblées[271].

Certaines catégories de données personnelles doivent, selon la CEDH, bénéficier d'une protection accrue. Outre les données de santé[272], sont des données particulièrement sensibles la **correspondance entre un avocat et son client**. En effet ces échanges sont non seulement couverts par l'article 8 de la CEDH, mais constituent également une mesure préparatoire à l'exercice du **droit à un procès équitable** protégé à l'**article 6 CEDH**[273].

Enfin, la CEDH énonce un autre principe relative à la surveillance d'État qui est qu'il

263 CEDH 12 janvier 2016 « Szabó and Vissy contre Hongrie » Aff. 37138/14, pt. 64
264 CEDH 6 septembre 1978 « Klass e.a. contre RFA » Req. 5026/71, pt. 59
265 CEDH 6 septembre 1978 « Klass e.a. contre RFA » Req. 5026/71, pt. 49
266 La limitation de la durée de conservation des données est un critère souvent rappelé par la CEDH. Dans un arrêt de 2011, la CEDH a ainsi reproché à la Roumanie le fait que des données collectées en 1990, ayant perdu toute pertinence, aient continué à produire des effets plus de 15 ans plus.
Voir : CEDH 24 mai 2011 « Association '21 décembre 1989' contre Roumanie » Req. 33810/07 et 18817/08
267 CEDH 6 septembre 1978 « Klass e.a. contre RFA » Req. 5026/71, pt. 52
268 CEDH 6 septembre 1978 « Klass e.a. contre RFA » Req. 5026/71, pt. 53
269 CEDH 4 décembre 2008 « S. et Marper contre Royaume-Uni » Req. 30562/04 et 30566/04, pt. 99
270 CEDH 3 juillet 2012 « Robathin contre Autriche » Req. 30457/06, pt. 52
271 CEDH 12 janvier 2016 « Szabó et Vissy contre Hongrie » Req. 37138/14 et CEDH 4 décembre 2015 « Zakharov contre Russie » Req. 47143/06
272 CEDH 27 août 1997 « M. S. contre Suède » Req. 20837/92
273 CEDH 20 juin 1988 « Schönenberger et Durmaz contre Suisse » Req. 11368/85, pt. 29

convient toujours de **vérifier, avant la mise en œuvre d'une mesure de surveillance, si une mesure moins invasive de la vie privée de la personne concernée permettrait d'atteindre la finalité poursuivie**. **Si tel est le cas, la solution alternative moins intrusive devra *toujours* être préférée**[274].

4.B. La surveillance d'État dans la jurisprudence de la CJUE

Traditionnellement, la CJUE n'a eu que de façon incidente l'occasion de se prononcer sur la surveillance d'État. En effet, les traitements effectués à des fins de police échappent à la directive 95/46/CE et ne sont couverts que dans certains cas par la décision-cadre 2008/977/JAI.

Mais la frontière entre surveillance la surveillance d'État et les traitements soumis à la directive 95/46/CE est parfois ténue, comme en témoigne la participation d'entreprises à des programmes de surveillance mis en œuvre par des agences de renseignement ; le programme PRISM développé entre la NSA et les GAFA en est la parfaite illustration. Un tel entremêlement des deux types de traitement amène nécessairement la CJUE à se prononcer de façon incidente sur la question de la surveillance d'État.

Elle a ainsi rappelé en 2015 que l'**article 13 de la directive 95/46/CE permet d'échapper à certaines des exigences de loyauté des traitements** notamment pour des **raisons liées à la sûreté de l'Etat, à la défense, ou la sécurité publique**[275]. Cependant, l'emploi de cette dérogation doit être **prévue par la loi** et ne saurait être fondée uniquement sur une convention non-publiée passée entre deux établissements publics[276].

De façon plus emblématique, la CJUE s'est prononcée sur la surveillance d'État dans l'arrêt « **Schrems contre DPC Irlande** »[277] (voir la partie sur les transferts de données) et « **Digital Rights Ireland** »[278].

Enfin, l'arrêt « Digital Rights Ireland » portait la question de la validité de la directive 2006/54/CE imposant une conservation des données de télécommunication pendant une durée déterminée. **La CJUE a donc joué un rôle important dans la fixation d'un cadre restreignant les politiques de conservation des données de communication**.

Dans cet arrêt la CJUE a rappelé qu'il arrive que, dans l'exercice de leurs fonctions, les autorités publiques aient besoin d'accéder à des données personnelles collectées et traitées pour une finalité initiale différente de la leur. Ceci est autorisé, mais la CJUE rappelle que cet accès ne

274 CEDH 2 septembre 2010 « Uzun contre Allemagne » Req. 35623/05, pt. 78
275 CJUE 1er octobre 2015 « Smaranda Bara e.a. » Aff. C-201/14, pt. 9
276 CJUE 1er octobre 2015 « Smaranda Bara e.a. » Aff. C-201/14, pts. 40 et 41
277 CJUE 6 octobre 2015 « Schrems contre DPC Irlande » Aff. C-362/14
278 CJUE 8 avril 2015 « Digital Rights Europe » Aff. C-293/12 et C-594/12

saurait être **universel, indiscriminé et inconditionnel**[279]. La **directive 2006/24/CE** a été invalidée notamment en raison de l'absence de **critères objectifs** permettant de délimiter l'accès des **autorités compétentes** aux **méta-données** (données de communication, sans le contenu des communications) dont elle imposait la conservation aux opérateurs de services de télécommunication. Or, de tels critères auraient dû être définis afin de garantir qu'un tel accès ne soit possible **qu'en lien avec l'objectif légitimement poursuivi de lutte contre les infractions graves et la criminalité**[280]. Ainsi, la CJUE rappelle, tout comme la CEDH, que **la surveillance d'État doit elle aussi obéir au principe de limitation des finalités**.

Plusieurs Etats membres ont considéré que l'invalidation de la directive 2006/54/CE n'avait pas d'incidence sur la validité de leur législation nationale de conservation des données. La CJUE a **rappelé à l'ordre** ces Etats dans un arrêt du 21 décembre 2016[281], où elle était amenée à juger de la validité d'une loi britannique et d'une loi suédoise comportant des dispositions similaires à la directive 2006/54/CE au regard de la directive de protection de la vie privée dans les communications électroniques (**2002/58/CE**) et des **articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne**.

Elle rappelle que la directive 2002/58/CE est une loi spéciale qui entre dans le cadre général de la directive 95/46/CE de protection des données qu'elle précise et complète. Elle vise également à garantir le plein respect des articles 7 (vie privée) et 8 (protection des données) de la Charte des droits fondamentaux de l'Union européenne[282], la protection des données concourant notamment à la protection de la vie privée[283]. Elle s'applique aux réseaux et services de télécommunications, comme les fournisseurs d'accès à Internet et les opérateurs téléphoniques, et impose des règles de confidentialité concernant les données relatives au trafic[284] et les données de localisation[285]. L'**article 15 paragraphe 1** de la directive 2002/58/CE introduit une disposition permettant aux Etats membres d'adopter des mesures limitant cette garantie de confidentialité en vue de garantir la **sécurité nationale**, la **défense** et la **sécurité publique**. Dès lors, les mesures nationales imposant la conservation de ces données sont une application de l'article 15 paragraphe 1 de la directive 2002/58/CE, et appliquent le droit de l'Union. De ce fait, elles sont soumises au respect de la Charte des droits fondamentaux de l'Union européenne, et notamment ses articles 7 et 8[286].

Dans le dispositif de son arrêt, et après avoir repris le même raisonnement que celui appliqué dans « Digital Rights Ireland »[287], la CJUE donne quelques **critères** permettant

279 CJUE 8 avril 2014 « Digital Rights Ireland » Aff. C-293/12 et C-594/12, pts. 54 à 60
280 CJUE 8 avril 2014 « Digital Rights Ireland » Aff. C-293/12 et C-594/12, pt. 60
281 CJUE 21 décembre 2016 « Tele2 Sverige » Aff. C-203/15 et C-698/15
282 CJUE 21 décembre 2016 « Tele2 Sverige » Aff. C-203/15 et C-698/15, pt. 82
283 CJUE 9 mars 2017 « Salvatore Manni » Aff. C-398/15, p. 39
284 « Toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation » (art. 2 directive 2002/58/CE)
285 « Toutes les données traitées dans un réseau de communications électroniques ou par un service de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public » (art. 2 directive 2002/58/CE)
286 CJUE 21 décembre 2016 « Tele2 Sverige » Aff. C-203/15 et C-698/15, pts. 73-78
287 CJUE 8 avril 2015 « Digital Rights Europe » Aff. C-293/12 et C-594/12

d'apprécier la conformité d'une mesure nationale de conservation des données de communication et de localisation traitées par les fournisseurs de services de télécommunications électroniques avec le droit de l'Union :

- La mesure ne doit pas imposer une **conservation « généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés »**[288] ;
- L'accès des autorités aux données conservées doit être **limité** « aux **seules fins de lutte contre la criminalité** » et soumis « à un **contrôle préalable par une juridiction** ou une **autorité administrative indépendante** »[289] ;
- Les données doivent être **conservées sur le territoire de l'Union européenne**.

Un des griefs contre la directive était l'**absence de dispositions visant à garantir la sécurité des données**[290]. Les autorités publiques, y compris dans le cadre de traitements qui tombent en dehors du domaine communautaire auquel s'applique la directive 95/46/CE, doivent, lorsqu'ils accèdent à des données qui elles tombent dans le champ d'application de cette directive, en assurer la sécurité. (voir la partie sur le principe de sécurité).

Dans « Schrems contre DPC Irlande »[291], la CJUE a affirmé qu'une des raisons pour lesquelles les Etats-Unis n'assuraient pas un niveau jugé adéquat de protection aux données personnelles transférées depuis l'Union européenne dans le cadre de l'accord Safe Harbor était **l'absence de recours juridictionnel** pour les citoyens européens face aux programmes de surveillance des agences de renseignement américaines, dont le caractère massif et indiscriminé a été révélé par Edward Snowden[292]. Pour la CJUE comme la CEDH, **l'existence d'un recours effectif** auprès d'une juridiction ou d'une autorité indépendante capable de superviser la surveillance secrète des télécommunications est donc un élément essentiel pour prévenir les abus d'une telle mesure.

4.C. Surveillance par géolocalisation

Dans « Uzun contre Allemagne »[293], la CEDH s'est prononcée sur la question de la **surveillance par GPS du véhicule sans le consentement de la personne concernée**, dans le cadre d'une procédure d'enquête pénale. Une telle surveillance constitue une ingérence à l'article 8 CEDH, mais **cette surveillance est jugée moins grave qu'une surveillance de la surveillance**[294]. Malgré cela, la Cour rappelle que les actions de surveillance (y compris par

288 CJUE 21 décembre 2016 « Tele2 Sverige » Aff. C-203/15 et C-698/15, dispositif
289 CJUE 21 décembre 2016 « Tele2 Sverige » Aff. C-203/15 et C-698/15, dispositif
290 CJUE 8 avril 2014 « Digital Rights Ireland » Aff. C-293/12 et C-594/12
291 CJUE 6 octobre 2015 « Schrems contre DPC » Aff. C-362/14
292 CJUE 6 octobre 2015 « Schrems contre DPC » Aff. C-362/14, pt. 89
293 CEDH 2 septembre 2010 « Uzun contre Allemagne » Req. 35623/05
294 CEDH 2 septembre 2010 « Uzun contre Allemagne » Req. 35623/05, pt. 66

géolocalisation) doivent être **limitées dans le temps**, ce qui implique une **limitée de la durée de conservation des données** tout autant qu'une **limitation de la durée de l'action de surveillance**.

4.D. Question de l'accès aux données personnelles par les autorités publiques autre que des autorités de police, et de sa communication

La CJUE a, dans l'arrêt « Smaranda Bara », imposé que l'accès aux données personnelles par des autorités publiques soit **prévue par la loi**, et non par exemple par une convention non-publiée passée entre deux établissements publics[295].

Selon l'**article 7 sous e) de la directive 95/46/CE**, une autorité publique y compris autre qu'une autorité de police (par exemple une inspection du travail) peut exiger l'accès immédiat à des données personnelles lorsque cela est pertinent dans le cadre de ses missions et moyennant certaines garanties. Ainsi, dans « Worten contre ACT »[296], la CJUE a affirmé qu'une inspection du travail pouvait exiger l'accès à des données sur les horaires travaillés par des salariés au sein de l'entreprise indépendamment de la finalité initiale du traitement. L'**article 13 de la directive 95/46/CE** permet aussi dans certains cas de **déroger à l'obligation d'information des personnes concernées**, mais cela n'est possible que si cela est **prévu par la loi** (voir la partie sur la surveillance d'État selon la jurisprudence de la CJUE) et que cela répond à **un des objectifs énumérés cet article** de la directive. En l'occurrence, la sauvegarde d'intérêts économiques, financiers, budgétaires ou monétaires de l'Etat membre ou de l'UE fait partie des objectifs listés[297].

Pour une personne privée physique ou morale, l'accès à des données personnelles détenues par des autorités de police sur le fondement repose sur **l'article 7 sous f)** de la directive 95/46/CE (voir la partie sur les traitements fondés sur l'intérêt légitime des personnes concernées), comme l'a rappelé la CJUE dans son arrêt « Rigas Satiksme »[298]. La question de savoir si une telle transmission était compatible avec le principe de limitation des finalités du traitement des données en cause dans l'affaire n'a pas été soulevée.

La CEDH s'est prononcée dans une affaire sur l'**accès d'un organisme de sécurité sociale au dossier médical d'une patiente**[299]. La communication de telles données à un

295 CJUE 1er octobre 2015 « Smaranda Bara e.a. » Aff. C-201/14, pts. 40 et 41
296 CJUE 30 mai 2013 « Worten contre ACT » Aff. C-342/12
297 CJUE 1er octobre 2015 « Smaranda Bara e.a. » Aff. C-201/14
298 CJUE 4 mai 2017 « Rigas Satiksme », Aff. C-13/16
299 CEDH 27 août 1997 « M. S. contre Suède » Req. 20837/92

organisme de sécurité sociale, lorsqu'elles sont nécessaires afin de vérifier le respecte des critères d'attribution de fonds publics répond à l'objectif de **sauvegarde du bien-être économique du pays**, ce que la CEDH accepte comme constituant une finalité légitime[300]. La requérante ne contestait pas cela, mais considérait qu'il n'était pas nécessaire, pour instruire sa demande d'indemnisation au titre de l'invalidité professionnelle et de déterminer les causes de ladite invalidité, d'inclure des informations relatives à son avortement. La CEDH a donc rappelé que les **données personnelles médicales** sont des données particulièrement **sensibles** (voir la partie sur les données de santé) et que le **secret médical** est nécessaire pour « préserver [la] confiance dans le corps médical »[301]. Ceci étant dit, en l'espèce, la demande de la caisse de sécurité sociale avait bien été cironscrite à une période donnée et notamment à des éléments relatifs à une blessure au dos, laquelle avait été la cause de l'avortement de la requérante. Dès lors, celle-ci n'est selon la Cour pas parvenue à démontrer que les données de santé transmises à l'organisme de sécurité sociale étaient sans pertinence avec la finalité poursuivie. L'ingérence, en l'espèce, fut donc considérée comme non-disproportionnée et donc autorisée[302].

4.E. La question des procédures d'habilitation au secret de la défense

Certains emplois en rapport avec la **sûreté de l'Etat** et la **défense nationale** peuvent voir leur accès restreint aux personnes disposant d'une autorisation délivrée suite à une **enquête personnelle** sur le candidat à l'emploi. Si en raison de son objet, un tel traitement de données personnelles tombe hors du champ d'application de la directive 95/46/CE, ils demeurent soumis aux règles de la Convention européenne des droits de l'Homme et donc à la jurisprudence de la CEDH.

Celle-ci s'est prononcée en effet à plusieurs reprises sur des affaires relatives à des procédures d'habilitation défense. Par exemple, dans « Leander contre Suède »[303], elle avait jugée **l'objectif légitime** sous réserve de l'existence de garanties intégrées au processus d'enquête. Elle se réserve par ailleurs le droit d'évaluer au cas par cas si une telle ingérence passe ou non le test de proportionnalité (voir la partie sur le test de proportionnalité).

Si dans l'affaire ci-dessus, la CEDH a considéré en l'ingérence en cause en l'espèce comme justifiée et proportionnée, dans « Turek contre Slovaquie »[304], elle a constaté une violation de l'article 8 CEDH. En effet, si une enquête préalable à l'obtention d'un certificat de sécurité, prévue par la loi, pour garantir la sûreté de l'Etat, est un **but légitime**, en l'espèce, le requérant n'avait pas eu accès aux documents sur la base desquels il avait, suite à l'enquête aboutissant à

300 CEDH 27 août 1997 « M. S. contre Suède » Req. 20837/92, pt. 38
301 CEDH 27 août 1997 « M. S. contre Suède » Req. 20837/92, pt. 41
302 CEDH 27 août 1997 « M. S. contre Suède » Req. 20837/92, pts. 41-44
303 CEDH 26 mars 1987 « Leander contre Suède » Req. 9248/81
304 CEDH 14 février 2006 « Turek contre Slovaquie » Req. 57986/00

un refus de délivrance du certificat, été accusé d'avoir collaboré avec le service de sécurité de la dictature communiste. Il n'a eu accès ni à ces éléments, ni aux documents qui réglementaient à l'époque la collaboration avec ces services de sécurité. Le refus de lui accorder un droit d'accès, en l'espèce, l'empêchait de contrôler la régularité du refus de son habilitation.

5. Surveillance sur le lieu de travail

5.A. Principes généraux

La CEDH s'est prononcée[305] une fois sur une affaire de **surveillance sur le lieu de travail**. En l'espèce, la requérante travaillait pour le compte d'un opérateur public (une école) et avait vu ses communications professionnelles (par téléphone et courriel) mises sous surveillance. A l'occasion de cette affaire, la CEDH a rappelé que toute ingérence dans la vie privée des individus devait être prévue par la Loi[306]. Ceci implique la communication aux employés d'un opérateur public des **conditions de leur surveillance sur le lieu de travail**, lesquelles doivent être conformes à Loi. Or, en l'espèce, la requérante n'avait pas été prévenue de **règles pré-établies** concernant l'utilisation des outils de communication mis à sa disposition à titre professionnel. Dès lors, elle pouvait à juste titre considérer comme privées et confidentielles les communications effectuées avec ces outils[307]. Ainsi, la CEDH a énoncé le principe selon lequel **en l'absence de règles claires et pré-établies prévoyant une surveillance des communications professionnelles des employés, la mise en place d'une telle mesure par un employeur constitue une ingérence dans la vie privée** du salarié[308].

En 2016, dans le premier arrêt « Barbulescu contre Roumanie »[309], qui a fait en 2017 l'objet d'un jugement en Grande Chambre suite à un renvoi[310], la CEDH, qui fait référence à des avis du **Groupe de travail de l'Article 29** comme élément d'interprétation de la directive 95/46/CE, laquelle fait partie droit applicable analysé[311]. L'affaire portait sur la surveillance par une entreprise privée, alors que dans « Copland contre Royaume-Uni »[312], arrêt analysé plus haut, elle portait sur la surveillance d'une employée par un employeur public. Dans cette hypothèse, quel est le rôle de la CEDH ?

La Cour rappelle dans son premier arrêt de 2016 que **les Etats ont l'obligation positive de protéger la vie privée des individus** y compris dans les relations entre personnes privées, les Etats signataires gardant une **marge d'appréciation**[313]. Dès lors, dans un tel contexte, **il ne revient à la Cour que de vérifier si l'Etat membre a respecté ses obligations positives au regard de l'article 8 CEDH**[314]. Elle entame son examen en relevant que le requérant avait pu présenter ses observations un tribunal[315]. Elle relève également que le requérant avait dit à son employeur qu'il n'utilisait un compte de messagerie électronique qu'il avait créé, et qui avait fait l'objet d'une surveillance par l'employeur, qu'à des fins professionnelles. Dès lors, selon le tribunal

305 CEDH 3 avril 2007 « Copland contre Royaume-Uni » Req. 62617/00
306 CEDH 3 avril 2007 « Copland contre Royaume-Uni » Req. 62617/00, pt. 42
307 CEDH 3 avril 2007 « Copland contre Royaume-Uni » Req. 62617/00, pt. 42
308 CEDH 3 avril 2007 « Copland contre Royaume-Uni » Req. 62617/00, pts. 45-49
309 CEDH 12 janvier 2016 « Barbulescu contre Roumanie » Req. 61496/08
310 CEDH 5 septembre 2017 « Barbulescu contre Roumanie » Req. 61496/08
311 CEDH 12 janvier 2016 « Barbulescu contre Roumanie » Req. 61496/08, pt. 19
312 CEDH 3 avril 2007 « Copland contre Royaume-Uni » Req. 62617/00
313 CEDH 12 janvier 2016 « Barbulescu contre Roumanie » Req. 61496/08, pt. 52
314 CEDH 12 janvier 2016 « Barbulescu contre Roumanie » Req. 61496/08, pt. 54
315 CEDH 12 janvier 2016 « Barbulescu contre Roumanie » Req. 61496/08, pt. 56

roumain ayant jugé l'affaire au principal, l'employeur pouvait dans le cadre de ses pouvoirs disciplinaires y accéder de bonne foi, puisqu'il pensait qu'il s'agissait d'une adresse purement professionnelle. Dès lors, la **CEDH avait conclu à la non-violation de l'article 8 CEDH** dans cette affaire, **sans vérifier l'existence de règles claires et pré-établies par l'employeur au sujet de la surveillance des communications des employés**. Or, ceci semble être contradictoire avec les principes dégagés dans « Copland contre Royaume-Uni » selon lequel la surveillance d'un employé ne peut se faire que selon des règles préétablies.

La question se posait alors à l'époque de savoir s'il s'agissait d'un revirement de jurisprudence, ou si le contrôle de la CEDH variait en fonction de la publique ou privée de l'employeur. Par ailleurs, si dans cet arrêt la CEDH affirmait que les Etats signataires devant cependant faire respecter l'équilibre entre les différents équilibres en jeu[316], elle ne précise cependant pas les obligations minimales à faire respecter par les Etats signataires en matière de protection de la vie privée entre personnes privées[317].

La décision de la Grande Chambre[318], devant laquelle M. Barbulescu s'est pourvu, vient corriger un certain nombre d'erreurs commises lors du premier jugement, et conclure à la **violation de l'article 8 de la CEDH** par la Roumanie.

Tout d'abord, la CEDH note dans ce deuxième arrêt que comme « la mesure prise par l'employeur [ayant surveillé puis licencié le requérant] a été validé par les juridictions nationales »[319], il y avait lieu « d'analyser le grief sous l'angle des **obligations positives de l'Etat** »[320] car « la responsabilité de ces autorités serait engagée si les faits litigieux résultaient d'un droit consacré par l'article 8 de la Convention »[321]. Et comme l'article 8 de la CEDH s'applique y compris à des communications émanant de locaux professionnels[322], surtout dès lors que l'individu pouvait « **raisonnablement s'attendre à ce que sa vie privée soit protégée** et respectée »[323] (mais sans que ce critère d'attente raisonnable ne soit pour autant décisif[324]), le litige relève bien de l'article 8 CEDH.

Le raisonnement de la CEDH a alors consisté en l'examen du fait de savoir si le requérant, qui avait fait l'objet d'une surveillance puis d'un licenciement, avait bénéficié réellement d'une information préalable à la mise en œuvre de cette surveillance. En particulier, la CEDH note que « **l'avertissement de l'employeur doit être donné avant que celui-ci ne commence son activité de surveillance, *a fortiori* lorsque la surveillance implique également l'accès au contenu des communications des employés** »[325]. De plus, **si un employeur peut bénéficier d'un motif d'intérêt légitime pour surveiller les communications de ses salariés**[326], la surveillance mise en œuvre ne doit **pas être disproportionnée**.

Or, la CEDH a relevé que ni les juges nationaux, ni elle-même en première instance, n'avait recherché si l'intérêt poursuivi par l'employeur (voir la partie sur la notion d'intérêt légitime) justifiait une surveillance aussi stricte qu'en l'espèce du requérant, et qu'il n'avait pas non été procédé au test consistant à voir s'il **n'existait pas de solution moins intrusive** que l'enregistrement en continu du contenu des communications électroniques du requérant, à son insu[327].

Dans un tel contexte, elle conclue qu'« il apparaît que les juridictions nationales ont manqué, d'une part, à vérifier, en particulier, si le requérant avait été préalablement averti par son

316 CEDH 12 janvier 2016 « Barbulescu contre Roumanie » Req. 61496/08, pt. 52
317 CEDH 12 janvier 2016 « Barbulescu contre Roumanie » Req. 61496/08, pt. 52
318 CEDH 5 septembre 2017 « Barbulescu contre Roumanie » Req. 61496/08
319 CEDH 5 septembre 2017 « Barbulescu contre Roumanie » Req. 61496/08, pt. 110
320 CEDH 5 septembre 2017 « Barbulescu contre Roumanie » Req. 61496/08, pt. 111
321 CEDH 5 septembre 2017 « Barbulescu contre Roumanie » Req. 61496/08, pt. 110
322 CEDH 5 septembre 2017 « Barbulescu contre Roumanie » Req. 61496/08, pt. 72
323 CEDH 5 septembre 2017 « Barbulescu contre Roumanie » Req. 61496/08, pt. 73
324 CEDH 5 septembre 2017 « Barbulescu contre Roumanie » Req. 61496/08, pt. 73
325 CEDH 5 septembre 2017 « Barbulescu contre Roumanie » Req. 61496/08, pt. 133
326 CEDH 5 septembre 2017 « Barbulescu contre Roumanie » Req. 61496/08, pt. 127
327 CEDH 5 septembre 2017 « Barbulescu contre Roumanie » Req. 61496/08, pt. 138

employeur de la possibilité que ses communications […] soient surveillées et, d'autre part, à tenir compte du fait qu'il n'avait été informé ni de la nature ni de l'étendue de la surveillance dont il avait fait l'objet, ainsi que du degré d'intrusion dans sa vie privée et sa correspondance. De surcroît, elles ont failli à déterminer, premièrement, quelles raisons concrètes avaient justifié la mise en place des mesures de surveillance, deuxièmement, si l'employeur aurait pu faire usage de mesures moins intrusives pour la vie privée […] et, troisièmement, si l'accès au contenu des communications avait été possible à son insu »[328].

Compte tenu de ses éléments, la CEDH conclue à une violation d'article 8 CEDH car « nonobstant la marge d'appréciation de l'Etat défendeur, la Cour estime que les autorités internes n'ont pas protégé de manière adéquate le droit du requérant au respect de la vie privée »[329]. **Ce même arrêt est alors l'occasion pour la CEDH de préciser les limites de la marge d'appréciation des Etats dans la protection qu'ils doivent accorder à la vie privée des individus dans les rapports interindividuels** tels que les relations d'un individu avec un employeur privé.

Elle indique tout d'abord que, de façon générale, « les juridictions internes doivent s'assurer que la mise en place par un employeur de mesures de surveillance […] s'accompagne de garanties adéquates et suffisantes contre les abus »[330], et indique que, pour procéder à cette évaluation, six facteurs doivent être pris en compte[331] :

1. L'employé a-t-il été **informé** de façon suffisamment claire de la possibilité qu'une surveillance soit mise en œuvre à son encontre ?
2. Quelle a été **l'étendue** de la surveillance mise en œuvre ? Cette étendue doit tendre à la minimisation tant sur le plan qualitatif (la surveillance porte-t-elle sur les seuls flux ou y compris sur le contenu?) que quantitatif (par exemples, y a-t-il eu des limitations dans le temps ou dans l'espace).
3. L'employeur peut-il faire état de **motifs légitimes** (voir la partie sur l'intérêt légitime du responsable de traitement) justifiant la mesure de surveillance ?
4. Aurait-il été possible de **mettre en place un système moins intrusif atteignant les mêmes finalités légitimes** ?
5. Quelles ont été **les conséquences** de la surveillance pour l'employé, et ces conséquences sont-elles compatibles avec la finalité légitime de la mesure de surveillance ?
6. L'employé surveillé a-t-il bénéficié de **garanties adéquates**, permettant notamment **d'empêcher que l'employeur accède au contenu des communications sans son information préalable** ?

5.B. Activités de détective privé dans le cadre d'une enquête disciplinaire

Selon la CJUE,une **organisation professionnelle** représentant une **profession réglementée** peut demander à une agence de **détectives privés**, dans le cadre de soupçons de

328 CEDH 5 septembre 2017 « Barbulescu contre Roumanie » Req. 61496/08, pt. 140
329 CEDH 5 septembre 2017 « Barbulescu contre Roumanie » Req. 61496/08, pt. 141
330 CEDH 5 septembre 2017 « Barbulescu contre Roumanie » Req. 61496/08, pt. 120
331 CEDH 5 septembre 2017 « Barbulescu contre Roumanie » Req. 61496/08, pt. 121

violation des règles de la profession, de mener une enquête disciplinaire[332]. Dans ce cas, l'**obligation d'information des personnes concernées** peut sauter si la finalité du traitement entre dans les cas énumérés à l'**article 13 de la directive 95/46/CE**.

332 CJUE 7 novembre 2013 « IPI contre Engelbert e.a. » Aff. C-473/12

6. Protection des données personnelles dans le cadre de la liberté de l'information et de l'Open Data

En dehors de la directive PSI[333] qui harmonise la licence de réutilisation des données issues du secteur public, et du règlement régissant l'accès aux documents administratifs détenus par le Parlement européen, le Conseil et la Commission[334], pour l'instant, le droit relatif au libre-accès aux informations et documents d'intérêt public n'est pas harmonisé au niveau européen.

Ces dispositions relatives aux différentes politiques d'**open data** entrent cependant régulièrement en conflit avec le droit à la protection des données, qui est lui bel et bien harmonisé par la directive 95/46/CE. Ceci explique que, de façon incidente, la CJUE ait eu à se prononcer sur ce type d'affaires, en plus des affaires portant sur la communicabilité de données détenues par les institutions de l'Union elles-mêmes.

Sur ces derniers cas, la CJUE a rappelé que **règlement 45/2001** s'applique à toutes les données personnelles, y compris celles contenues dans des documents administratifs auxquels le public demande l'accès[335]. En dehors des cas où la personne concernée y consent, les institutions de l'Union ne peuvent communiquer les données personnelles contenues dans un document administratif que si, le demandeur en ayant démontré la nécessité, l'institution concernée par la demande a proécdé à un raisonomment de mise en balance de l'intérêt de la personne concernée avec celle du public et du requérant[336].

Le raisonnement à suivre pour effectuer cette balance des intérêts a été précisé en 2016 dans l'arrêt « ClientEarth contre EFSA » du 16 juillet 2015[337].

Pour la CJUE, une demande de communication d'un document administratif d'une institution de l'Union, fondée sur les dispositions du règlement **1049/2001/CE**, est un **transfert de donnée à caractère personnel à un tiers au sens de l'article 8 du règlement 45/2001/CE**[338]. Dès lors, même si une information contenue dans le document demandé ne relève pas de la vie privée[339], il convient qu'il ne s'agit pas d'une donnée à caractère personnel (voir la partie sur la définition de la notion de donnée à caractère personnel) avant de procéder à la communication.

S'il s'agit bel et bien d'une donnée à caractère personnel au sens de l'article 2 sous a) du règlement 45/2001/CE, alors il faut appliquer ces dispositions de l'article 8 de ce règlement relatives au transfert à un tiers de données personnelles détenues par une institution de l'Union[340].

Cet article impose **deux conditions cumulatives** permettant au transfert d'avoir lieu :

333 Directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 sur la réutilisation des informations du secteur public, révisée par la directive 2013/37/UE du Parlement européen et du Conseil du 26 juin 2013 modifiant la directive 2003/98/CE

334 Règlement 1049/2001/CE du Parlement européen et du Conseil du 30 mai 2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission

335 CJUE 29 juin 2010 « Commission contre Bavarian Lager » Aff. C-28/08, pt. 63

336 CJUE 29 juin 2010 « Commission contre Bavarian Lager » Aff. C-28/08, pt. 77

337 CJUE 16 juillet 2015 « ClientEarth contre EFSA » Aff. C-615/13P

338 CJUE 16 juillet 2015 « ClientEarth contre EFSA » Aff. C-615/13P, pts. 45 et 46

339 CJUE 16 juillet 2015 « ClientEarth contre EFSA » Aff. C-615/13P, pt. 32

340 CJUE 16 juillet 2015 « ClientEarth contre EFSA » Aff. C-615/13P, pt. 45

1. **Le requérant** doit **démontrer la nécessité que lui soit communiquée la donnée** à caractère personnel qu'il demande[341] ;
2. **L'institution** à laquelle est transmise la demande de communication doit **évaluer s'il existe une « raison de penser que le transfert en cause pourrait porter atteinte aux intérêts légitimes de la personne concernée »** pouvant s'opposer à la demande[342].

Dans l'affaire d'espèce, dans laquelle l'Agence européenne de sécurité des aliments (EFSA) refusait de communiquer à des ONG (ClientEarth et PAN Europe) le nom des experts ayant rendu un avis sur les effets sanitaires de pesticides, la CJUE a rappelé que « la transparence du processus suivi par une autorité publique pour l'adoption d'un acte […] contribue […] à conférer à cette autorité une plus grande légitimité aux yeux des destinataires de cet acte et à augmenter la confiance de ceux-ci à l'égard de ladite autorité »[343]. Or, « pour permettre de vérifier l'impartialité de chacun de ces experts dans l'accomplissement de sa mission scientifique au service de l'EFSA »[344], la communication des noms des auteurs du rapport dont est demandée la communication est nécessaire.

Cependant, la Cour ne procède pas à la vérification de l'intérêt des personnes concernées (en l'espèce : les experts ayant rédigé les rapports) car si cet argument a bien été soulevé par l'EFSA pour refuser la communication du nom des experts ayant rédigé les rapports demandés par les requérants, cette allégation « relevait d'une considération générale non autrement étayée par un quelconque élément propre à l'espèce »[345]. Il en résulte qu'**une institution de l'Union, pour refuser la communication d'une donnée personnelle** contenue dans un document administratif dont la communication est demandée **au motif qu'elle lèserait les droits et intérêts de la personne concernée** par cette donnée personnelle, **doit être en mesure d'indiquer précisément les droits et intérêts ainsi lésés**, sans quoi il n'est pas possible de les mettre en balance avec ceux du requérant.

Le règlement 1049/2001/CE relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission ne s'applique cependant pas aux Etats membres.

L'arrêt « Österreichischer Rundfunk »[346] concernait ces derniers. Il permit à la CJCE de consacrer le principe selon lequel **le droit à l'accès aux informations d'intérêt public peut justifier une limitation du droit à la protection des données** tel que régi par la directive 95/46/CE. L'affaire au principal portait sur l'accès par la Cour des comptes à des données sur la rémunération de certains salariés d'un organisme soumis à son contrôle et la divulgation de ces données. Dans « Volker contre Hesse »[347], la CJUE a jugé dispropotionnée une ingérence se fondant sur l'objectif de contrôle des finances publiques. Dans cette affaire, il s'agissait de la publication, prévue par un règlement européen, d'informations relatives aux bénéficiaires de fonds européens de la politique agricole commune, dont la CJUE a jugé qu'elles contenaient des éléments trop substantiels de la rémunération des personnes concernées. La CJUE effectue donc un raisonnement au cas par cas.

341 CJUE 16 juillet 2015 « ClientEarth contre EFSA » Aff. C-615/13P, pt. 47
342 CJUE 16 juillet 2015 « ClientEarth contre EFSA » Aff. C-615/13P, pt. 47
343 CJUE 16 juillet 2015 « ClientEarth contre EFSA » Aff. C-615/13P, pt. 56
344 CJUE 16 juillet 2015 « ClientEarth contre EFSA » Aff. C-615/13P, pt. 58
345 CJUE 16 juillet 2015 « ClientEarth contre EFSA » Aff. C-615/13P, pt. 69
346 CJCE 20 mai 2005 « Österreichischer Rundfunk » Aff. C-465/00, C-138/01 et C-139/01
347 CJUE 9 novembre 2010 « Volker contre Hesse » Aff. C-92/09 et C-93/09

La question de l'**anonymisation des décisions de justice** a été abordée par la CEDH en 1997[348]. L'affaire portait sur l'accès à des **données médicales** par les autorités dans le cadre d'une procédure pénale ou judiciaire, mais comportait aussi, de façon incidente, des éléments sur l'anonymisation des décisions de justice. Un arrêt d'une cour d'appel finlandaise transmis à la presse contenait en effet des informations sur l'état de santé de l'un des requérants[349], et la CEDH a jugé qu'une telle ingérence dans le droit du requérant à la vie privée, garanti par l'article 8 CEDH, ne connaissait en l'espèce et après analyse aucune justification d'intérêt général[350].

348 CEDH 25 février 1997 « Z. contre Finlande » Req. 22009/93
349 CEDH 25 février 1997 « Z. contre Finlande » Req. 22009/93, pt. 113
350 CEDH 25 février 1997 « Z. contre Finlande » Req. 22009/93, pt. 113

7. Le principe de sécurisation des données

Le **principe de sécurité** est énoncé à l'article 17 paragraphe 1 de la directive 95/46/CE :

« Les États membres prévoient que le responsable du traitement doit mettre en oeuvre les **mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel** contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite.

Ces mesures doivent assurer, **compte tenu de l'état de l'art et des coûts liés à leur mise en oeuvre**, un **niveau de sécurité approprié** au regard des risques présentés par le traitement et de la nature des données à protéger. »

Cet article est mentionné pour la première par la CJUE, mais de façon accessoire, en 2009, dans l'arrêt « Rotterdam contre Rijkeboer »[351]. La sécurité des données personnelles est par contre un élément important dans l'arrêt « Worten contre ACT »[352]. L'ACT, un organisme portugais d'inspection du travail, s'était vu refuser par une entreprise l'accès à son registre des horaires travaillés par ses employés en invoquant l'obligation de sécurisation de l'accès aux données personnelles, qui doivent être protégées contre des accès illégitimes. Cependant la CJUE a rappelé que l'accès à ces données par une autorité publique, sur le fondement de l'**article 7 sous e) de la directive** (voir la partie sur la notion d'intérêt légitime du responsable du traitement) (voir la partie sur l'accès par des autorités publiques autre que des autorités de police aux données personnelles), ne saurait être assimilé à un accès illégitime prohibé à l'article 17 paragraphe 1[353]. Un tel accès doit bien sûr obéir au **principe de proportionnalité** (voir la partie sur le test de proportionnalité) et **répondre aux exigences de sécurisation des données** au sujet desquelles **les Etats membres sont dans l'obligation d'adopter des dispositions**[354].

Le fait de **devoir garantir la sécurité d'un système d'information**, et son bon fonctionnement, au-delà même de la simple garantie de l'intégrité et de la sécurité des données personnelles traitées par un tel système d'information, **peut fonder l'utilisation de la notion d'intérêt légitime pour fonder un tel traitement de données** (voir la partie sur l'intérêt légitime). En effet, bien que dans l'arrêt « Breyer contre Allemagne »[355], la CJUE se soit bornée à affirmer que l'article 7 sous f) de la directive 95/46/CE, sur l'intérêt légitime, pouvait justifier la collecte de données personnelles (dont les adresses IP font généralement partie) en vue de garantir le maintien du fonctionnement d'un service de média en ligne, il n'est pas difficile d'en déduire que le fait d'utiliser un certain nombre de données personnelles à des fins techniques, sans le consentement des personnes concernées, pour garantir la sécurité d'autres données personnelles, pourra être admis au titre de l'intérêt légitime du responsable de traitement.

351 CJUE 7 mai 2009 « Rotterdam contre Rijkeboer » Aff. C-533/07, pt. 17 et pt. 62
352 CJUE 30 mai 2013 « Worten contre ACT » Aff. C-342/12
353 CJUE 30 mai 2013 « Worten contre ACT » Aff. C-342/12, pt. 34
354 CJUE 30 mai 2013 « Worten contre ACT » Aff. C-342/12, pt. 24
355 CJUE 19 octobre 2016 « Breyet contre Allemagne » Aff. C-582/14

Enfin, dans l'arrêt « Digital Rights Ireland » invalidant la directive 2006/24/CE sur la conservation des données, un des griefs retenus par la CJUE contre celle-ci était l'absence de dispositions visant à garantir la sécurité des données. Elle y affirme que ce principe, contenu à l'article 17 paragraphe 1 de la directive 95/46/CE, est un **élément essentiel** du droit à la protection des données, et ne saurait notamment être mis en balance avec des intérêts de nature strictement économiques :

> « L'article 7 de la directive 2006/24, lu en combinaison avec les articles 4, paragraphe 1, de la directive 2002/58 et 17, paragraphe 1, second alinéa, de la directive 95/46, ne garantit pas que soit appliqué par lesdits fournisseurs un niveau particulièrement élevé de protection et de sécurité par des mesures techniques et organisationnelles, mais autorise notamment ces fournisseurs à tenir compte de considérations économiques lors de la détermination du niveau de sécurité qu'ils appliquent, en ce qui concerne les coûts de mise en œuvre des mesures de sécurité. En particulier, la directive 2006/24 ne garantit pas la destruction irrémédiable des données au terme de la durée de conservation de celles-ci. »[356]

356 CJUE 8 avril 2014 « Digital Rights Ireland » Aff. C-293/12 et C-594/12

8. Transfert de données personnelles vers des pays tiers

La jurisprudence de la CJUE a permis de clarifier quelques **éléments de définition** relatifs à la notion de **transfert de données personnelles vers un pays tiers**. Notons que la notion de transfert de données dont il sera question dans le présent chapitre porte sur celle définie **au chapitre IV de la directive 95/46/CE (transfert vers un pays tiers)** et **non** la notion de **transfert à des destinataires autres que les institutions et organes communautaires** de l'**article 8 du règlement 45/2001/CE**.

Ainsi, la **mise en ligne d'un contenu contenant des données personnelles sur un site web**, même si un site web est en principe accessible partout dans le monde, **n'est pas assimilé à un transfert de données vers un pays tiers** par la Cour de Luxembourg depuis son arrêt « Lindqvist » de 2003[357]. En effet il n'y a pas de mise en relation directe entre l'émetteur et le destinataire de la donnée[358], et il n'a pas semblé à la Cour qu'il ait été dans l'intention du législateur européen d'inclure dans la notion une simple mise en ligne de contenu sur le Web[359].

Par ailleurs, la CJUE a précisé par ailleurs en 2015 que « **l'opération consistant à faire transférer des données** à caractère personnel depuis un Etat membre **vers un pays tiers constitue**, en tant que tel, **un traitement de données** à caractère personnel au sens de l'article 2, sous b), de la directive 95/46 […] **effectué sur le territoire d'un Etat membre**»[360].

Dans l'affaire « Schrems contre DPC »[361], la CJUE a conclu à l'invalidité de l'accord **Safe Harbor** concernant le transfert de données vers les Etats-Unis. Par cet accord, lequel correspond à la décision 2000/520 de la Commission européenne, cette dernière affirme que les responsables de traitement s'étant auto-certifiés dans le cadre de ce programme garantissaient un niveau de protection adéquat aux termes de l'article 25 de la directive 95/46/CE. La Cour relève à cette occasion que la Commission avait constaté dans plusieurs de ses communications que les Etats-Unis ne respectaient pas les termes de l'accord. Or, la Cour souligne que l'article 25, paragraphe 4, oblige celle-ci à agir pour empêcher les transferts de données personnelles vers un pays, dès lors qu'elle constate que celui-ci n'accorde pas un niveau de protection adéquat aux données personnelles.

Tant qu'une décision de la Commission fondée sur l'article 25 paragraphe 6 est en vigueur, elle s'impose aux Etats membres, donc également aux autorités nationales de protection des données. Cependant, il est nécessaire qu'une telle autorité de contrôle puisse tout de même mener une enquête en cas de doute sur la mise en œuvre effective de cette décision, ou sur le

357 CJCE 6 novembre 2003 « Lindqvist » Aff. C-101/01

358 « 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 de son fournisseur de services d'hébergement qui est établi 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. » CJCE 6 novembre 2003 « Lindqvist » Aff. C-101/01, pt. 71

359 CJCE 6 novembre 2003 « Lindqvist » Aff. C-101/01, pt. 68

360 CJUE 6 octobre 2015 « Schrems contre DPC » Aff. C-362/14, pt. 45

361 CJUE 6 octobre 2015 « Schrems contre DPC » Aff. C-362/14

niveau réel de protection des données dans le pays tiers visé. Et cette autorité doit disposer des moyens de recours suffisants si elle constate un manquement[362]. Il incombe au législateur national de prévoir ces voies de recours auprès des juridictions nationales, qui peuvent ensuite saisir la CJUE par voie de recours préjudiciel[363].

A l'occasion de cet arrêt, la CJUE a continué son travail de définition des notions liées à celle de transfert vers un pays tiers, et a apporté des précisions à la notion du « niveau de protection adéquat » que les pays tiers doivent assurer pour pouvoir bénéficier d'une décision de la Commission européenne y autorisant les transferts.

Cette notion d'**exigence de « niveau de protection adéquat »** n'est en effet pas définie de façon claire par la directive 95/46/CE. Elle **n'implique pas un niveau de protection identique[364]**, mais « **substantiellement équivalent** »[365]. Et c'est bien **l'ordre juridique du pays tiers** qui est concerné par cette évaluation, tant dans les textes que dans la pratique[366]. Ceci ne veut pas pour autant que le recours à un système d'auto-certification tel que prévu par la décision Safe Harbor est exclu, mais un tel mécanisme ne peut être conforme à la directive 95/46/CE sans qu'il soit assorti de mécanismes efficaces de contrôle[367].

Parmi les exigences pour que la Commission puisse déclarer l'adéquation d'un régime étranger de protection des données, **le critère de la protection juridique** est souligné par la Cour dans l'arrêt de 2015 invalidant la décision Safe Harbor, étant donné que les citoyens européens ne disposaient d'une capacité de recours effective contre les écoutes aux Etats-Unis[368].

362 CJUE 6 octobre 2015 « Schrems contre DPC » Aff. C-362/14, pt. 57
363 CJUE 6 octobre 2015 « Schrems contre DPC » Aff. C-362/14, pt. 65
364 CJUE 6 octobre 2015 « Schrems contre DPC » Aff. C-362/14, pt. 73
365 CJUE 6 octobre 2015 « Schrems contre DPC » Aff. C-362/14, pt. 73
366 CJUE 6 octobre 2015 « Schrems contre DPC » Aff. C-362/14, pt. 74
367 CJUE 6 octobre 2015 « Schrems contre DPC » Aff. C-362/14, pt. 81
368 CJUE 6 octobre 2015 « Schrems contre DPC » Aff. C-362/14, pt. 89

9. Les autorités de protection des données personnelles (APDP) prévues à l'article 28 de la directive 95/46/CE

Les autorités de protection des données personnelles (APDP) sont une **garantie essentiel** du droit à la protection des données à caractère personnel. Elles sont d'ailleurs mentionnées à l'article 8 alinéa 3[369] de la Charte des droits fondamentaux de l'Union européenne. Ceci a été à de nombreuses reprises rappelé par la CJUE[370]. La CEDH les considère aussi comme étant essentielles : dans un arrêt de 1989[371], déjà, elle affirmait l'importance de l'existence d'une autorité indépendante capable de garantir l'équilibre entre les droits de la personne concernée avec les autres intérêts pouvant être en jeu[372].

9.A. L'indépendance des autorités de protection des données

Trois arrêts en manquement de la CJUE en rapport avec la directive 95/46/CE (contre **l'Allemagne[373]**, **l'Autriche[374]** et la **Hongrie[375]**) concernent la **protection de l'indépendance des APDP** et l'interprétation des mots « **en toute indépendance** » employés à l'**article 28 de la directive 95/46/CE** pour désigner la modalité d'existence et d'exercice de leurs missions de ces autorités.

Les **APDP doivent être indépendantes**. Cette indépendance doit être garantie d'une telle façon qu'il ne puisse y avoir **aucun doute** sur celle-ci. **Le moindre soupçon de partialité**[376] **d'une APDP entraîne la violation des termes « en toute indépendance »** de l'article 28 de la directive 95/46/CE. Dès lors : « le seul risque que les autorités de tutelle puissent exercer une influence politique sur les décisions des autorités de contrôle suffit pour entraver l'exercice indépendant des missions de celles-ci »[377].

Cette indépendance vaut vis-à-vis des responsables de traitement, bien entendu, mais également vis-à-vis de **toute pression extérieure**, dont celle de l'Etat :

369 « Le respect [des règles de protection des données] est soumis au contrôle d'une autorité indépendante »
370 Voir, entre autres :
CJUE 9 mars 2010 « Commission contre Allemagne » Aff. C-518/07, pt. 23
CJUE 16 octobre 2012 « Commission contre Autriche » Aff. C-614/10, pt. 36
CJUE 8 avril 2014 « Digital Rights Ireland » Aff. C-293/12 et C-594/12, pt. 68
371 CEDH 7 juillet 1989 « Gaskin contre Royaume-Uni » Req. 10454/83
372 CEDH 7 juillet 1989 « Gaskin contre Royaume-Uni » Req. 10454/83, pt. 49
373 CJUE 9 mars 2010 « Commission contre Allemagne » Aff. C-518/07
374 CJUE 16 octobre 2012 « Commission contre Autriche » Aff. C-614/10
375 CJUE 8 avril 2014 « Commission contre Hongrie » Aff. C-288/12
376 CJUE 16 octobre 2012 « Commission contre Autriche » Aff. C-614/10, pt. 61
377 CJUE 9 mars 2010 « Commission contre Allemagne » Aff. C-518/07, pt. 36

> « […] Lors de l'exercice de leurs missions, les autorités de contrôle doivent agir de manière objective et impartiale. À cet effet, elles doivent être à l'abri de toute influence extérieure, y compris celle, directe ou indirecte, de l'État ou des Länder, et pas seulement de l'influence des organismes contrôlés. »[378]

Cette indépendance doit également être garantie **vis-à-vis de la Commission européenne**. En effet, dans la décision de 2015 invalidant la décision Safe Harbor, un des griefs retenus par la Cour était que cette décision privait les APDP de tout moyen permettant de contrôler la légalité des traitements effectués dans le cadre d'un transfert de données vers un pays tiers bénéficiant d'une décision d'adéquation de la Commission fondée sur l'article 25 de la directive 95/46/CE[379].

Conformément au principe de démocratie, la CJUE admet malgré tout l'existence d'un **contrôle parlementaire**, cette supervision pouvant se traduire par exemple par l'obligation annuelle de rendre des comptes dans un rapport[380].

La CJUE analyse **au cas-par-cas** l'indépendance des APDP. Elle prend appui pour cela notamment sur les modalités de garantie de l'indépendance du Contrôleur européen des données personnelles prévu par le règlement 45/2001/CE[381]. Il n'existe pas de liste établie de mécanismes d'indépendance obligatoirement présents. Ainsi, en soi, le fait que l'ancienne Commission autrichienne de protection des données (Datenschutzkomision – DSK, devenue depuis Autorité de protection des données : Datenschutzbehörde, DSB) ne dispose pas de sa propre ligne budgétaire n'a pas été jugé en soi contraire à la directive 95/46/CE, mais cet élément a joué dans l'analyse ayant conduit la CJUE a déclaré que cette APDP n'exerçait pas ses missions en toute indépendance[382].

Si comme indiqué dans le paragraphe ci-dessus, il n'existe pas de liste *a minima* dressée par la CJUE de garanties de la protection des APDP qui doivent obligatoirement être présentes, les trois arrêts de la Cour en la matière peuvent donner quelques lignes directrices. Ainsi, en Allemagne, les APDP des Länder en charge des responsables de traitement privés, étaient soumises **à la tutelle du gouvernement des Länder**, chose contraire au principe d'indépendance des APDP selon la CJCE. Une telle indépendance suppose aussi l'**interdiction du recours à des instructions**, et d'un **lien de service** entre un membre administrateur d'une APDP et l'exécutif (en l'espèce : la chancellerie fédérale autrichienne)[383]. Le fait que le service administratif mettant en œuvre les décisions de l'organe collégial prenant les décisions de l'APDP soit intégré à l'organigramme d'un ministère, ou encore le fait qu'un membre du gouvernement dispose d'un droit

378 CJUE 9 mars 2010 « Commission contre Allemagne » Aff. C-518/07, pt. 25
379 CJUE 6 octobre 2015 « Schrems contre DPC » Aff. C-362/14, pt. 102
380 CJUE 9 mars 2010 « Commission contre Allemagne » Aff. C-518/07, pt. 44
381 CJUE 9 mars 2010 « Commission contre Allemagne » Aff. C-518/07, pt. 28
382 CJUE 16 octobre 2012 « Commission contre Autriche » Aff. C-614/10, pt. 58
383 CJUE 16 octobre 2012 « Commission contre Autriche » Aff. C-614/10, pt. 66

inconditionnel à l'information sur tous les aspects de la gestion d'une APDP, sont aussi contraires au principe d'indépendance de celle-ci[384].

En outre, il est **interdit de mettre fin avant son terme au mandat de l'autorité de protection des données** sans suivre pour cela une procédure prévue par la loi. Même la circonstance, comme ce fut le cas en Hongrie, d'une réforme même constitutionnelle, ne peut justifier une telle interruption. Selon la Cour, « 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 alors 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 »**[385].

Enfin, **les autorités de contrôle étaient, jusqu'à l'entrée en vigueur du mécanisme de l'autorité cheffe-de-file du RGPD, également indépendantes les unes des autres** :

> « Ainsi que le prévoit l'article 28, paragraphe 1, second alinéa, de la [Directive 95/46/CE], les autorités de contrôle […] exercent en toute indépendance les missions dont elles sont investies. »[386]
>
> « […] cette même directive ne prévoit aucun critère de priorité régissant l'intervention des autorités de contrôle les unes par rapport aux autres ni ne prescrit l'obligation pour une autorité de contrôle d'un Etat membre de se conformer à la position exprimée, le cas échéant, par l'autorité de contrôle d'un autre Etat membre »[387]

9.C. Autres éléments de jurisprudence sur les autorités de protection des données

Si jusqu'en 2015, la CJCE puis la CJUE n'avait été amenée à se prononcer que sur l'indépendance des autorités de protection des données. A partir de cette année-là, des précisions ont été données sur la **délimitation de leur compétence territoriale** (voir la partie sur le droit applicable), sur les **compétences des autorités de supervision** prévues à l'article 28 de la directive 95/46/CE, ainsi que sur des **éléments de procédure**.

En 2015, la CJUE a précisé les **compétences que les APDP doivent avoir dans le cadre de la supervision des transferts de données personnelles vers des pays tiers** bénéficiant d'une décision de conformité de la Commission en vertu de l'article 25 paragraphe 6 de la directive 95/46/CE.

384 CJUE 16 octobre 2012 « Commission contre Autriche » Aff. C-614/10, pt. 66
385 CJUE 8 avril 2014 « Commission contre Hongrie » Aff. C-288/12, pt. 54
386 CJUE 5 juin 2018 « Wirtschaftsakademie » Aff. C-210/16, pt. 68
387 CJUE 5 juin 2018 « Wirtschaftsakademie » Aff. C-210/16, pt. 69

9.C.1. Faut-il avoir saisi l'autorité de protection des données pour pouvoir saisir un juge ?

En 2017, elle a également précisé qu'un Etat membre **ne pouvait subordonner l'introduction** par une personne concernée **d'un recours juridictionnel**, en vertu de l'**article 47 de la Charte des droits fondamentaux** et de l'**article 22 de la directive 95/46/CE**[388], pour violation de son droit à la protection des données, à l'**épuisement des voies de recours administratif** notamment auprès d'une autorité de protection des données **qu'à certaines conditions**. Une telle condition vient en effet limiter le droit à un recours juridictionnel effectif. Elle ne peut donc être justifiée « que si elle est **prévue par la loi**, si elle respecte le **contenu essentiel dudit droit** et si, dans le respect du **principe de proportionnalité**, elle est **nécessaire et répond effectivement à des objectifs d'intérêt général** reconnus par l'Union **ou au besoin de protection des droits et des libertés d'autrui** »[389]

L'amélioration de l'efficacité de la procédure judiciaire est à cet égard un objectif légitime pouvant venir limiter les droits évoqués ci-dessus[390]. Pour passer le test de proportionnalité, la subordination du recours judiciaire en matière de violation de la protection des données à un recours administratif doit remplir les **trois conditions** suivantes[391] :

1. Le fait de devoir au préalable épuiser les voies de recours administratifs ne doit pas entraîner de retard substantiel pour l'introduction d'un recours juridictionnel ;
2. L'introduction d'un recours administratif doit entraîner la suspension du délai de prescription des droits concernés par le recours de la personne concernée ;
3. Cette exigence procédurale ne doit pas aboutir à des frais excessifs pour le requérant.

Une telle décision permet de renforcer le rôle joué par les autorités de protection des données en permettant aux Etats membres de leur garantir une sorte de « priorité » pour connaître des affaires en rapport avec la protection des données.

9.C.2. Dans le cadre de la directive 95/46/CE, quelle est l'autorité compétente ?

388 Cet article dispose : « Sans préjudice du recours administratif qui peut être organisé, notamment devant l'autorité de contrôle visée à l'article 28, antérieurement à la saisine de l'autorité judiciaire, les Etats membres prévoient que toute personne dispose d'un recours juridictionnel en cas de violation des droits qui lui sont garantis par les dispositions nationales applicables au traitement en question »

389 CJUE 27 septembre 2017 « Puškár contre Slovaquie » Aff. C-73/16, pt. 62

390 CJUE 27 septembre 2017 « Puškár contre Slovaquie » Aff. C-73/16, pts. 66-68

391 CJUE 27 septembre 2017 « Puškár contre Slovaquie » Aff. C-73/16, pt. 76

Cette question est presque un point de nostalgie. Alors que le RGPD venait d'entrer en vigueur quelques semaines auparavant, la CJUE a répondu à une question sur l'interprétation des articles 4 et 28 de la Directive 95/46/CE, respectivement sur le droit national applicable et sur les compétences des autorités nationales de supervision de la protection des données à caractère personnel. La question était de savoir :

> « Lorsqu'une entreprise établie en dehors de l'Union dispose de plusieurs établissements dans différents Etats membres, l'autorité de contrôle d'un Etat membre est[-elle] habilitée à exercer les pouvoirs que lui confère l'article 28, paragraphe 3, de cette directive, à l'égard d'un établissement situé sur le territoire de cet Etat membre, alors même que, en vertu de la répartition des missions au sein d'un 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 Etat 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, à un établissement situé dans un autre Etat membre […] ? »[392]

Cette question n'est plus tout à fait d'actualité depuis l'entrée en vigueur du RGPD, sauf peut-être en ce qui concerne les mesures correspondant aux marges de manœuvre nationales laissées dans le RGPD.

Pour rappel, sous le régime de la directive 95/46, afin qu'une législation nationale relative à la protection des données autre que celle de l'Etat membre dans lequel un responsable de traitement est immatriculé s'applique à ce dernier, il fallait qu'il dispose d'un **établissement** dans ce second pays, c'est-à-dire, selon la directive 95/46/CE, qu'il « **exerce, au moyen d'une installation stable sur le territoire de cet Etat membre, une activité effective et réelle, même minime, dans le cadre de laquelle ce traitement est effectué** »[393] (voir la partie sur la détermination du droit national applicable).

Ceci entraînait, sous cette même directive, la compétence de l'autorité de protection des données compétente sur ce territoire, puisque « **lorsque le droit national de l'Etat membre dont relève l'autorité de contrôle est applicable** […], **cette autorité de contrôle peut exercer l'ensemble des pouvoirs** qui lui sont conférés par ce droit à l'égard de cet établissement, et ce indépendamment du point de savoir si le responsable du traitement dispose d'établissements également dans d'autres Etats membres »[394].

La notion d'établissement contenue à l'article 4 de la directive 95/46/CE lue combinaison avec le considérant 19 est une notion autonome, la Cour a confirmé dans sa décision « Wirtschaftsakademie » de juin 2018[395] la jurisprudence « Weltimmo » de 2015[396] en rappelant que :

392 CJUE 5 juin 2018 « Wirtschaftsakademie » Aff. C-210/16, pt. 45
393 CJUE 1er octobre 2015 « Weltimmo » Aff. C-230/14, pt. 41
394 CJUE 5 juin 2018 « Wirtschaftsakademie » Aff. C-210/16, pt. 52
395 CJUE 5 juin 2018 « Wirtschaftsakademie » Aff. C-210/16
396 CJUE 1er octobre 2015 « Weltimmo » Aff. C-230/14

> « L'établissement sur le territoire d'un Etat membre suppose l'exercice effectif et réel d'une activité au moyen d'une installation stable et […] **la forme juridique retenue pour un tel établissement**, qu'il s'agisse d'une simple succursale ou d'une filiale ayant la personnalité juridique, **n'est pas déterminante** »[397]

Par ailleurs, et l'arrêt « Google contre Espagne »[398] rappelait déjà qu'**une autorité de contrôle était compétente pour superviser les activités de traitement de données personnelles d'un établissement dont le siège est dans un pays hors-UE si** :

- « Le traitement est effectué **dans le cadre des activités** d'un établissement du responsable de traitement sur le territoire de l'Etat membre […] [, ou]
- le responsable du traitement n'est pas établi sur le territoire de l'État membre mais en un lieu où sa loi nationale s'applique en vertu du droit international public [, ou]
- le responsable du traitement n'est pas établi sur le territoire de la Communauté et recourt, à des fins de traitement de données à caractère personnel, à des moyens, sauf si ces moyens ne sont utilisés qu'à des fins de transit sur le territoire de la Communauté »[399]

La CJUE rappelle cela dans son arrêt « Wirtschaftsakademie »[400]. Or, Facebook Germany, dont il était question en l'espèce, fournissait des services de vente d'espace publicitaire indissociables des traitements de données à caractère personnel de son réseau social[401] (voir, *mutantis mutandis*, l'affaire « Google contre Espagne »[402]). Les traitements de données effectués par Facebook Inc et Facebook Ireland entrent donc « dans le cadre des activités » de Facebook Germany, qui dépend en l'espèce de l'autorité de contrôle compétent en vertu du droit allemand[403] (voir la partie sur la notion d'établissement en vertu de la directive 95/46/CE).

En outre, « […] la circonstance […] selon laquelle **les stratégies décisionnelles quant à la collecte et au traitement de données relatives à des personnes résidant sur le territoire de l'Union** sont prises par une société mère établie dans un payes tiers, telle que, en l'occurence, Facebook Inc., **n'est pas de nature à remettre en cause la compétence de l'autorité de contrôle relevant du droit d'un Etat membre** à l'égard d'un établissement, situé sur le territoire de ce même Etat, du responsable du traitement desdites données »[404].

Et enfin, les termes « **en toute indépendance** » qui décrit les autorités de protection des données à l'article 28 de la directive 95/46/CE sont à interpréter en ce sens qu'elles ont été, jusqu'à l'entrée

397 CJUE 5 juin 2018 « Wirtschaftsakademie » Aff. C-210/16, pt. 54
398 CJUE 13 mai 2014 « Google contre Espagne » Aff. C-131/12, pt. 52
399 Article 4 paragraphe 1 de la directive 95/46/CE
400 CJUE 5 juin 2018 « Wirtschaftsakademie » Aff. C-210/16, pt. 57
401 CJUE 5 juin 2018 « Wirtschaftsakademie » Aff. C-210/16, pt. 60
402 CJUE 13 mai 2014 « Google contre Espagne » Aff. C-131/12, pt. 52
403 CJUE 5 juin 2018 « Wirtschaftsakademie » Aff. C-210/16, pt. 61
404 CJUE 5 juin 2018 « Wirtschaftsakademie » Aff. C-210/16, pt. 63

en vigueur du RGPD et de son mécanisme de cohérence, indépendantes y compris **les unes des autres**. Elles peuvent « apprécier, de manière autonome par rapport aux évaluations effectuées par [une autre autorité de contrôle], la légalité du traitement de données en cause »[405] (voir la partie sur l'indépendance des autorités de supervision).

405 CJUE 5 juin 2018 « Wirtschaftsakademie » Aff. C-210/16, pt. 73

10. Lutte contre le téléchargement illégal

La protection des données personnelles dans le cadre de la lutte contre le téléchargement illégal a été l'objet d'une assez importante jurisprudence de la part la CJUE, nécessitant la lecture croisée de plusieurs directives :

- La directive 95/46/CE sur la protection des données à caractère personnel ;
- La directive 2000/31/CE sur le commerce électronique ;
- La directive 2001/29/CE sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information ;
- La directive 2002/58/CE, dite « e-Privacy » ;
- La directive 2004/46/CE relative au respect des droits de la propriété intellectuelle ;
- La directive 2006/24/CE sur la conservation des données est également citée dans certains arrêts, mais elle est désormais invalidée par l'arrêt « Digital Rights Ireland »[406].

Dans le cadre de la lutte contre le téléchargement illégal, certains Etats membres ont adopté des mesures prévoyant la **transmission à des personnes privées tierces des données personnelles relatives au trafic**. Cette transmission a pour objectif que ces personnes tierces puissent engager des **procédures civiles contre les atteintes au droit d'auteur**. De telles dispositions sont autorisées par le droit de l'Union. Les fournisseurs d'accès sont des **intermédiaires** au sens de l'art. 8, paragraphe 3 de la **directive 2001/29/CE**[407]. Ils permettent en effet techniquement le partage illégal d'œuvres protégées par le droit d'auteur (via FTP ou des réseaux de pair-à-pair). Les droits sur ces œuvres sous souvent gérés voire détenus par des sociétés de droits d'auteur, qui sont les personnes tierces auxquelles les données de communication sont communiquées pour lutter contre le téléchargement illégal.

Un argument soulevé lors d'affaires de ce type par la défense est que la **directive 2006/24/CE** ne prévoyait pas la conservation de méta-données de communication à des fins d'utilisation dans des procédures civiles. Mais outre le fait que cette directive est de toutes façons invalidée et est donc réputée n'avoir jamais existé[408], la CJUE a affirmé qu'elle ne s'appliquait pas à ce type de cas[409].

Si la directive sur la conservation des données 2006/24/CE désormais invalidée ne s'appliquait pas à ce type d'affaires, la directive « ePrivacy » 2002/58/CE, quant à elle, s'applique, et laisse la possibilité aux Etats membres la possibilité de prévoir la transmission par les fournisseurs de services de télécommunication électronique des données relatives au trafic à des personnes privées tierces dans le cadre de procédures civiles[410]. Mais une telle communication doit bel et bien être **prévue par la loi**. Par exemple, dans l'affaire « Promusicae »[411], la loi espagnole ne prévoyait la communication de données liées à une adresse IP que dans le cadre de procédures pénales. Dès lors, le fournisseur d'accès concerné par l'affaire au principal avait raison, selon la CJCE, de ne pas communiquer à une personne tierce (ici : Promusicae) les

406 CJUE 8 avril 2014 « Digital Rights Ireland » Aff. C-293/12 et C-594/12
407 CJCE 19 février 2009 « LSG contre Tele2 » Aff. C-557/07
408 CJUE 8 avril 2014 « Digital Rights Ireland » Aff. C-293/12 et C-594/12
409 CJUE 19 avril 2012 « Bonnier e.a. contre Perfect Communication Sweden » Aff. C-461/10
410 CJCE 29 janvier 2008 « Promusicae » Aff. C-275/06
411 CJCE 29 janvier 2008 « Promusicae » Aff. C-275/06

données de communication dans le cadre d'une procédure civile[412]. Mais il eut suffi que la loi espagnole prévoit la transmission dans le cadre de procédures civiles et là, le fournisseur d'accès n'aurait pu s'opposer à la requête de la société de droits d'auteurs.

Le droit de l'Union est donc permissif en matière de communication aux ayants-droits d'informations de trafic (et notamment des **adresses IP**) détectées dans le cadre d'une infraction au droit de la propriété intellectuelle et des droits voisins. Après tout, le **droit à la protection de la propriété intellectuelle** est protégé par la Charte des droits fondamentaux de l'Union européenne. Mais la CJUE rappelle néanmoins un certain nombre de limites à la surveillance des internautes. Le droit à la protection des données n'est ni absolu ni intangible et doit être mis en balance avec d'autres droits, dont le droit à la protection des données, et la liberté d'entreprise des fournisseurs de services de télécommunication électronique[413]. Cet arrêt porte sur la conciliation entre l'intérêt de la personne concernée à la protection de ses données, et l'intérêt des ayants droits.

Dans un autre arrêt, la CJUE s'est prononcée sur la conciliation entre l'intérêt des fournisseurs d'accès qui bénéficient du droit à la liberté d'entreprendre, et les ayants-droits, qui bénéficient du droit à la propriété privée. Il s'agit de l'arrêt « Scarlet contre SABAM »[414]. La SABAM, une société belge de gestion représentant auteurs, compositions et éditeurs d'œuvres musicales, a demandé au tribunal de première instance de Bruxelles d'enjoindre au fournisseur d'accès à Internet Scarlet de mettre en place à ses frais des mécanismes techniques visant à rendre impossible ou à réprimer le téléchargement illégal. Appelée à par la juridiction d'appel à se prononcer sur une question préjudicielle à ce sujet, la CJUE a indiqué qu'obliger les intermédiaires au sens de la directive 2001/29/CE à mettre en place, à titre préventif, à l'égard de toute sa clientèle et à ses seuls frais, sans limitation dans le temps, un **système de filtrage des communications électroniques**, le tout afin de lutter contre le téléchargement illégal, était disproportionné car ne prenant pas suffisamment en compte les autres droits fondamentaux en jeu, dont le droit à la vie privée et à la liberté d'expression. C'est également un système contraire à l'article 15 paragraphe 1 de la directive 2000/31/CE sur le commerce électronique[415], laquelle précise que :« Les États membres ne doivent pas imposer aux prestataires, pour la fourniture [de leurs] services […], une obligation générale de surveiller les informations qu'ils transmettent ou stockent, ou une obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites ».

412 CJCE 29 janvier 2008 « Promusicae » Aff. C-275/06
413 Voir l'arrêt : CJCE 29 janvier 2008 « Promusicae » Aff. C-275/06
414 CJUE 24 novembre 2011 « Scarlet contre SABAM » Aff. C-70/10
415 CJUE 24 novembre 2011 « Scarlet contre SABAM » Aff. C-70/10, pt. 40

11. Les régimes particuliers

11.A. Détectives privés

La CJUE a eu à se prononcer une fois sur l'activité de détectives privés. Ces derniers peuvent-ils se prévaloir de l'article 13, paragraphe 1 sous d) de la directive 95/46/CE qui prévoit la possibilité d'adopter un régime particulier pour les données traitées pour **« la prévention, la recherche, la détection et la poursuite d'infractions pénales ou de manquements à la déontologie dans le cas des professions réglementées »** ? L'article 13 permet dans ces cas au responsable de traitement de ne pas avoir à informer les personnes concernées de l'existence du traitement. Or, notamment dans des cas relatifs à un manquement à la déontologie dans le cas de professions réglementées, il est possible de déléguer tout ou partie de l'enquête à des détectives professionnels. C'est ce qu'avait fait Institut professionnel des agents immobiliers (IPI), créé par un arrêté royal de 1995 en Belgique, chargé de veiller aux conditions d'accès à la fonction d'agent immobilier et à son bon exercice. L'IPI avait saisi le tribunal de commerce de Charleroi pour y dénoncer des actes contraires à la réglementation professionnelle. Les preuves apportées ayant été collectées par des détectives privés, sans en avoir informé les personnes concernées, la question de la recevabilité de ces preuves s'est posée, jusqu'à ce que la CJUE réponde à la question préjudicielle posée au cours de la procédure qu'une agence de détectives pouvait, dans un tel contexte, se prévaloir des possibilités offertes à l'article 13 de la directive 95/46/CE. **Les règles sur l'application du régime dérogatoire prévu à l'article 13 de la directive 95/46/CE doit cependant être précisée en droit national**[416].

11.B. Journalisme

Le journalisme est un des vecteurs principaux de la libre expression des citoyens, et la liberté de la presse est une liberté fondamentale protégée tant par la Charte des droits fondamentaux de l'Union européenne que la Convention européenne des droits de l'Homme. Ainsi, lorsqu'elle doit concilier la protection des données et de la vie privée avec la liberté de la presse, la CEDH ajoute une étape à son raisonnement classique de balance des intérêts (voir la partie sur la conciliation des intérêts).

La directive 95/46/CE prévoit à son article 9 que :« Les États membres prévoient, pour les traitements de données à caractère personnel effectués **aux seules fins de journalisme ou d'expression artistique ou littéraire**, des exemptions et dérogations au présent chapitre, au chapitre IV et au chapitre VI dans la seule mesure où elles s'avèrent nécessaires pour concilier le droit à la vie privée avec les règles régissant la liberté d'expression ». La CJCE en a donné une **définition large**. Ainsi, sont des traitements de données aux seules fins de journalisme ceux qui « ont pour seule finalité la divulgation au public, sous quelque moyen de transmission que ce soit, d'informations, d'opinions ou d'idées »[417], **peu importe la nature du responsable de traitement**,

416 CJUE 7 novembre 2013 « IPI contre Engelbert e.a. » Aff. C-473/12

417 CJCE 16 décembre 2008 « Tietosuojavaltuutettu contre Satakunnan Markkinapörssi Oy et Satamedia Oy » Aff. C-73/07, pt. 2

dont il n'est nullement pas qu'il soit un organe de presse ou un journaliste.

Enfin, dans « Google contre Espagne »[418], la CJUE a indiqué que si, **de façon générale, les sites web peuvent bénéficier de l'exception prévue à l'article 9** de la directive 95/46/CE concernant les **traitements aux seules fins de journalisme**, **les moteurs de recherche eux en sont par principe exclus**[419]. La CJUE a ainsi confirmé une décision de l'APDP espagnole (Agencia Espaňola de Protección de Datos) qui enjoignait à Google de retirer de son index une référence à un article de presse contenant des données personnelles, sans pour autant demander au site d'origine de le retirer. En effet, des deux responsables de traitement – le moteur de recherche et l'organe de presse – seul le second traitait les données en question à des seules fins de journalisme.

11.C. Données de santé

Les données de santé sont des données sensibles. L'article 8 de la directive 95/46/CE, qui porte sur les « catégories particulières de données », énonce à son premier alinéa l'interdiction, par principe général, du traitement des données « 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 ». Le second paragraphe permet de déroger à cette règle générale pour un certain nombre de motifs, dont le consentement de la personne concernée au traitement des données (art. 8 paragraphe 2 sous a) ou la préservation de la vie et de la santé de la personne concernée « ou d'une autre personne dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement » (art. 8 paragraphe 2 sous c)).

La CJCE a adopté une **définition large** de la notion de **donnée de santé**. Ainsi :

> « **il convient de donner à l'expression «données relatives à la santé» employée à son article 8, paragraphe 1, une interprétation large de sorte qu'elle comprenne des informations concernant tous les aspects, tant physiques que psychiques, de la santé d'une personne** »[420].

L'information sur une personne s'étant blessée au pied et partie à cause de cela en congé maladie a ainsi été qualifiée dans l'arrêt « Lindqvist » de donnée de santé[421].

Quant à la CEDH, elle a affirmé que la confidentialité des données de santé répond en réalité à **deux objectifs d'intérêt général** : la protection de la vie privée des patients, mais aussi

418 CJUE 13 mai 2014 « Google contre Espagne » Aff. C-131/12
419 CJUE 13 mai 2014 « Google contre Espagne » Aff. C-131/12, pt. 85
420 CJCE 6 novembre 2003 « Lindqvist » Aff. C-101/01, pt. 51
421 CJCE 6 novembre 2003 « Lindqvist » Aff. C-101/01, pt. 51

la préservation de «leur confiance dans le corps médical et les services de santé en général »[422]. Ceci justifie que « la législation interne [doive] ménager des garanties appropriées pour empêcher toute communication ou divulgation de données à caractère personnel relatives à la santé qui ne serait pas conforme aux garanties prévues à l'article 8 de la Convention »[423].

Par ailleurs, elle a rappelé qu'il est possible de communiquer des données de santé du dossier médical d'un patient à un **organisme de sécurité sociale**[424], et que ceci participe à l'**objectif légitime** de **sauvegarde du bien-être économique du pays**[425] (voir plus de détails sur cette affaire, l'affaire « M. S. contre Suède », dans la partie sur la question de l'accès aux données personnelles par les autorités publiques autre que des autorités de police).

11.D. Fins statistiques, historiques ou scientifiques

La recherche scientifique répond à un intérêt général. Or, de nombreuses études ont démontré la tension qui existe entre l'utilité d'une donnée et son anonymisation. Selon Paul Ohm, chercheur américain ayant travaillé sur ce sujet, une donnée est soit utile dans la recherche, soit anonyme[426]. De plus, dans le domaine du Big Data, les données sont souvent collectées avant qu'une finalité leur soit trouvée. Ceci fait des données de recherche une problématique particulière méritant une réflexion particulière.

Les traitements de données à des fins statistiques et de recherche scientifique peuvent, conformément à l'article 6 paragraphe 1 de la directive 95/46/CE, bénéficier d'une exemption à certaines obligations, concernant la limitation du délai de conservation des données et le principe de limitation des finalités. Les Etats membres précisent les modalités de ce régime dérogatoire dans leur droit interne.

L'arrêt « Huber contre Allemagne »[427] de la CJCE porte principalement sur des questions relatives à la libre-circulation des citoyens européens, mais de façon incidente, il a permis de préciser que le **régime prévu à l'article 6 paragraphe 1 de la directive 95/46/CE s'applique en fonction non de la nature du responsable de traitement mais de la finalité du traitement**.

422

423 CEDH 27 août 1997 « M. S. contre Suède » Req. 20837/92, pt. 41

424 CEDH 27 août 1997 « M. S. contre Suède » Req. 20837/92

425 CEDH 27 août 1997 « M. S. contre Suède » Req. 20837/92, pt. 38

426 OHM, Paul. “Broken Promises of Privacy: Responding to the Surprising Failure of Anonimity” pp. 1701-1777 in 57 *UCLA Law Review*, 2010

427 CJCE 16 décembre 2008 « Huber contre Allemagne » Aff. C-524/06

La CEDH ne s'est pas prononcée, bien entendu, sur l'article 6 paragraphe 1 de la directive 95/46/CE, mais elle a aussi jugé des cas impliquant des traitements de données à des fins de recherche scientifique.

La CEDH, dans « Ungváry et Irodalom Kft. contre Hongrie »[428] porte sur la conciliation des intérêts entre la liberté d'expression et le droit à la vie privée. Elle s'est prononcée sur la confirmation par la Cour suprême hongroise de la condamnation d'un historien et de l'organe de presse ayant publié son article faisant été de liens passés entre un juge de la Cour constitutionnelle et l'ancien parti unique de la dictature communiste. La Cour a fait à cette occasion, comme à chaque fois, un raisonnement de conciliation des intérêts, **en prenant en compte de façon déterminante la participation à un débat historique**. Ainsi, de même que pour les traitements à des fins de journalisme, lorsqu'ils participent à un débat public d'intérêt général, les traitements et publications de données personnelles sont un argument retenu par la Cour pour justifier une limitation au droit à la vie privée (voir la partie sur la balance des intérêts).

11.E. Le cas où la personne concernée est mineure

En France, la Loi pour une République numérique[429] a introduit par son article 56 des dispositions particulières en matière de recherche médicale lorsque les personnes concernées participant sont mineures à l'article 58 de la loi Informatique et Libertés[430]. Elle a également inséré une procédure particulière en matière de droit à l'oubli à l'article 40, alinéa II de la loi Informatique et Libertés[431] lorsque la demande porte sur des données collectées lorsque la personne concernée était mineure.

L'article 6 sous f) du Règlement général de protection des données[432] prévoit d'ailleurs que l'intérêt des personnes concernées, pour déterminer s'il est possible de recourir au fondement de **l'intérêt légitime** (voir la partie sur l'intérêt légitime des personnes concernées), est renforcé vis-à-vis des intérêts légitimes du responsable du traitement si la personne concernée est mineure au moment de la collecte de ses données :

> « f) le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, **notamment lorsque la personne concernée est un enfant**. »[433]

428 CEDH 3 décembre 2013 « Ungváry et Irodalom Kft. contre Hongrie » Req. 64520/10
429 Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, JORF n°0235 du 8 octobre 2016
430 Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée
431 *Idem*
432 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)
433 Article 6 du Règlement général de protection des données (Règlement 2016/679/UE)

Toujours dans le Règlement général de protection des données[434], il existe un article 8 qui détermine les conditions applicables au **recueil du consentement d'un enfant** pour le traitement de ses données à caractère personnel.

Le Règlement général de protection des données n'entrera en vigueur qu'en 2018. Cependant, la CJUE a déjà anticipé cette entrée en vigueur en rappelant dans son arrêt du 4 mai 2017 « Rigas satiksme » que :

> « […] **il convient de relever que l'âge de la personne concernée peut constituer l'un des éléments dont il convient de tenir compte** dans le cadre de [la] pondération [à effectuer entre l'intérêt de la personne concernée et l'intérêt légitime du responsable du traitement lorsque celui-ci souhaite s'en prévaloir pour fonder son traitement] »[435]

11.F. Données biométriques

La CEDH a rappelé en 2008 que **les données biométriques sont des données à caractère personnel**[436]. La CJUE l'a rejoint sur ce sujet, en citant sa décision, dans une décision de 2013[437] (voir la partie sur les relations entre la CJUE et la CEDH) :

> « Les empreintes digitales relèvent de [la notion de donnée à caractère personnel] dès lors qu'elles contiennent objectivement des informations uniques sur des personnes physiques et permettent leur identification précise »[438]

Lorsque l'Etat impose un traitement de données biométriques, il doit faire en sorte, selon la jurisprudence de la CEDH, que cela soit proportionné et donc « nécessaire dans une société démocratique (voir la partie sur la balance des intérêts). Cependant, lorsque cela est prévu par la loi, il est possible d'imposer une telle collecte pour des **buts légitimes**, par exemple pour « prévenir la falsification des passeports »[439], « empêcher leur utilisation frauduleuse »[440], ou encore « empêcher […] l'entrée illégale de personnes sur le territoire de l'Union »[441].

434 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)
435 CJUE 4 mai 2017 « Rigas Satiksme », Aff. C-13/16
436 CEDH 4 décembre 2008 « S. et Marper contre Royaume-Uni » Req. 30562/04 et 30566/04, pts. 68 et 84
437 CJCE 17 octobre 2013 « Michael Schwarz c. Stadt Bochum » Aff. C-291/12, pt. 27
438 CJCE 17 octobre 2013 « Michael Schwarz c. Stadt Bochum » Aff. C-291/12, pt. 27
439 CJCE 17 octobre 2013 « Michael Schwarz c. Stadt Bochum » Aff. C-291/12, pt. 36
440 CJCE 17 octobre 2013 « Michael Schwarz c. Stadt Bochum » Aff. C-291/12, pt. 36
441 CJCE 17 octobre 2013 « Michael Schwarz c. Stadt Bochum » Aff. C-291/12, pt. 37

La CJUE admet « que la conservation des empreintes digitales sur un support de stockage hautement sécurisé […] implique une sophistication technique, de sorte que cette conservation est susceptible de réduire le risque de falsification des passeports et de faciliter la tâche des autorités chargées d'examiner aux frontières l'authenticité de ceux-ci »[442]. En outre, elle admet que la biométrie n'est pas infaillible[443]. Mais comme elle est plus fiable que d'autres méthodes, elle est **apte à poursuivre le but légitime** pour lequel elle est mise en œuvre[444].

Si la CJUE peut donc accepter que soit imposée la collecte de données biométriques pour certains buts légitimes, dont ceux cités un peu plus haut, cela ne l'empêche pas de poser des limites.

En effet, elle pose la question des **conséquences**, surtout en cas d'erreur. Peuvent-elles entraîner un préjudice ? Elle souligne l'importance du fait que, dans le règlement attaqué par le requérant, « le défaut de concordance des empreintes digitales du détenteur du passeport avec les données intégrées dans ce document ne signifie pas […] que la personne concernée se voit automatiquement refuser l'entrée sur le territoire de l'Union. Un **tel défaut de concordance aura pour seule conséquence d'attirer l'attention des autorités compétentes sur la personne concernée** et d'entraîner, à l'égard de celle-ci, un examen approfondi destiné à établir son identité d'une manière définitive »[445].

Enfin, la loi prévoyant d'imposer la collecte de d'empreintes biométriques, même pour un objectif légitime, ne peut être proportionnée à cet objectif que si elle respecte le **principe de limitation des finalités** et ne peut être détournée à autre chose[446].

442 CJCE 17 octobre 2013 « Michael Schwarz c. Stadt Bochum » Aff. C-291/12, pt. 41
443 CJCE 17 octobre 2013 « Michael Schwarz c. Stadt Bochum » Aff. C-291/12, pts. 42 et 43
444 CJCE 17 octobre 2013 « Michael Schwarz c. Stadt Bochum » Aff. C-291/12, pt. 43
445 CJCE 17 octobre 2013 « Michael Schwarz c. Stadt Bochum » Aff. C-291/12, pt. 44
446 CJCE 17 octobre 2013 « Michael Schwarz c. Stadt Bochum » Aff. C-291/12, pts. 55 et 60 à 62

ANNEXE : Liste des arrêts étudiés

Juridiction	Date	Affaire	N° ECLI	Affaire (nom court)
CEDH	06/09/1978	5026/71	-	Klass e.a. contre RFA
CEDH	02/08/1984	8691/79	-	Malone contre Royaume-Uni
CEDH	26/03/1987	9248/81	-	Leander contre Suède
CEDH	20/06/1988	11368/85	-	Schönenberger contre Suisse
CEDH	07/07/1989	10454/83	-	Gaskin contre Royaume-Uni
CEDH	25/02/1993	10828/84	-	Funke contre France
CEDH	25/02/1997	22009/93	-	Z. contre Finlande
CEDH	27/08/1997	20837/92	-	M. S. contre Suède
CEDH	16/02/2000	27798/95	-	Amann contre Suisse
CEDH	04/05/2000	28341/95	-	Rotaru contre Roumanie
CJUE/CJCE	20/05/2003	C-465/00 , C-138/01 et C-139/01	ECLI:EU:C:2003:294	Österreichischer Rundfunk
CJUE/CJCE	06/11/2003	C-101/01	ECLI:EU:C:2003:596	Lindqvist
CEDH	14/02/2006	57986/00	-	Turek contre Slovaquie
CEDH	06/06/2006	62332/00	-	Segerstedt-Wiberg e.a. contre Suède
CEDH	03/04/2007	62617/00	-	Copland contre Royaume-Uni
CJUE/CJCE	29/01/2008	C-275/06	ECLI:EU:C:2008:54	Promusicae
CEDH	04/12/2008	30562/04 et 30566/04	-	S. et Marper contre Royaume-Uni
CJUE/CJCE	16/12/2008	C-73/07	ECLI:EU:C:2008:727	Tietosuojavaltuutettu contre Satakunnan Markkinapörssi Oy et Satamedia Oy
CJUE/CJCE	16/12/2008	C-524/06	ECLI:EU:C:2008:724	Huber contre Allemagne
CJUE/CJCE	19/02/2009	C-557/07	ECLI:EU:C:2009:107	LSG contre Tele2
CJUE/CJCE	07/05/2009	C-533/07	ECLI:EU:C:2009:257	Rotterdam contre Rijkeboer
CJUE/CJCE	09/03/2010	C-518/07	ECLI:EU:C:2010:125	Commission contre Allemagne
CEDH	18/05/2010	26839/05	-	Kennedy contre Royaume-Uni
CJUE/CJCE	29/06/2010	C-28/08	ECLI:EU:C:2010:378	Commission européenne contre Bavarian Lager
CEDH	02/09/2010	35623/05	-	Uzun contre Allemagne
CJUE/CJCE	09/11/2010	C-92/09 et C-93/09	ECLI:EU:C:2010:662	Volker et Eifert contre Hesse
CJUE/CJCE	05/05/2011	C-543/09	ECLI:EU:C:2011:279	Deutsche Telekom contre Allemagne
CEDH	24/05/2011	33810/07 et 18817/08	-	Association 21 décembre 1989 e.a. contre Roumanie
CJUE/CJCE	24/11/2011	C-468/10 et C-469/10	ECLI:EU:C:2011:777	ASNEF et FECEMD contre Administracion del Estado
CJUE/CJCE	24/11/2011	C-70/10	ECLI:EU:C:2011:771	Scarlet contre SABAM
CEDH	07/02/2012	39954/08	-	Axel Springer contre Allemagne
CEDH	14/02/2012	7094/06	-	Romet contre Pays-Bas

CJUE/CJCE	19/04/2012	C-461/10	ECLI:EU:C:2012:219	Bonnier e.a. contre Perfect Communication Sweden
CEDH	03/07/2012	30457/06	-	Robathin contre Autriche
CJUE/CJCE	16/10/2012	C-614/10	ECLI:EU:C:2012:631	Commission contre Autriche
CJUE/CJCE	22/11/2012	C-119/12	ECLI:EU:C:2012:748	Josef Probst contre mr.nexnet
CJUE/CJCE	30/05/2013	C-342/12	ECLI:EU:C:2013:355	Worten contre ACT
CJUE/CJCE	17/10/2013	C-291/12	ECLI:EU:C:2013:670	Michael Schwarz contre Stadt Bochum
CJUE/CJCE	07/11/2013	C-473/12	ECLI:EU:C:2013:715	IPI contre Engelbert et autres
CEDH	03/12/2013	64520/10	-	Ungváry et Irodalom Kft. contre Hongrie
CJUE/CJCE	12/12/2013	C-486/12	ECLI:EU:C:2013:836	X contre Bois-le-Duc
CJUE/CJCE	08/04/2014	C-288/12	ECLI:EU:C:2014:237	Commission contre Hongrie
CJUE/CJCE	08/04/2014	C-293/12 et C-594/12	ECLI:EU:C:2014:238	Digital Rights Ireland
CJUE/CJCE	13/05/2014	C-131/12	ECLI:EU:C:2014:317	Google contre Espagne
CJUE/CJCE	17/07/2014	C-141/12	ECLI:EU:C:2014:2081	Y.S. contre minister voor immigratie
CJUE/CJCE	2014.12.11	C-212/13	ECLI:EU:C:2014:2428	František Ryneš contre Úřad pro ochranu osobních údajů
CJUE/CJCE	2015.07.16	C-615/13P	ECLI:EU:C:2015:489	ClientEarth et Pesticide Action Network Europe (PAN Europe) contre Autorité européenne de sécurité des aliments (EFSA) et Commission européenne
CJUE/CJCE	01/10/2015	C-230/14	ECLI:EU:C:2015:639	Weltimmo
CJUE/CJCE	01/10/2015	C-201/14	ECLI:EU:C:2015:638	Bara e. a.
CJUE/CJCE	2015/10/06	C-362/14	ECLI:EU:C:2015:650	Schrems contre DPC Irlande
CEDH	2015/12/04	47143/06	-	Zakharov contre Russie
CEDH	2016/01/12	37138/14	-	Szabó et Vissy contre Hongrie
CEDH	2016/01/12	61496/08	-	Barbulescu contre Roumanie
CEDH	2016/03/31	34148/07	-	Šantare et Labaņikovs contre Lettonie
CJUE/CJCE	2016/07/28	C-191/15	ECLI:EU:C:2016:612	Verein für Konsumenteninformation contre Amazon EU Sàrl (VKI contre Amazon UE)
CJUE/CJCE	2016/10/19	C-582/14	ECLI:EU:C:2016:779	Patrick Breyer contre République fédérale d'Allemagne
CJUE/CJCE	2016/12/21	C-203/15 et C-698/15	ECLI:EU:C:2016:970	Tele2 Sverige AB contre Post- och telestyrelsen et Secretary of State for the Home Department contre Tom Watson, Peter Brice et Geoffrey Lewis
CJUE/CJCE	2017/03/09	C-398/15	ECLI:EU:C:2017:197	Camera di Commercio contre Salvatore Manni
CJUE/CJCE	2017/05/04	C-13/16	ECLI:EU:C:2017:336	Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde contre

				Rīgas pašvaldības SIA « Rīgas satiksme »
CEDH	2017/09/05	61496/08	-	Barbulescu contre Roumanie
CJUE	2017/09/27	C-73/16	ECLI:EU:C:2017:725	Peter Puškár contre Finančné riaditeľstvo Slovenskej republiky et Kriminálny úrad finančnej správy
CJUE	2017/12/20	C-434/16	ECLI:EU:C:2017:994	Peter Nowak contre Data Protection Commissioner
CJUE	2017/06/05	C-210/16	ECLI:EU:C:2018:388	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein contre Wirtschaftsakademie Schleswig-Holstein GmbH

ANNEXE : Liste des abréviations

APDP	Autorité de Protection des Données Personnelles
CEDH	Cour européenne des droits de l'Homme
CJCE	Cour de Justice des Communautés Européennes (devenue CJUE)
CJUE	Cour de Justice de l'Union Européenne