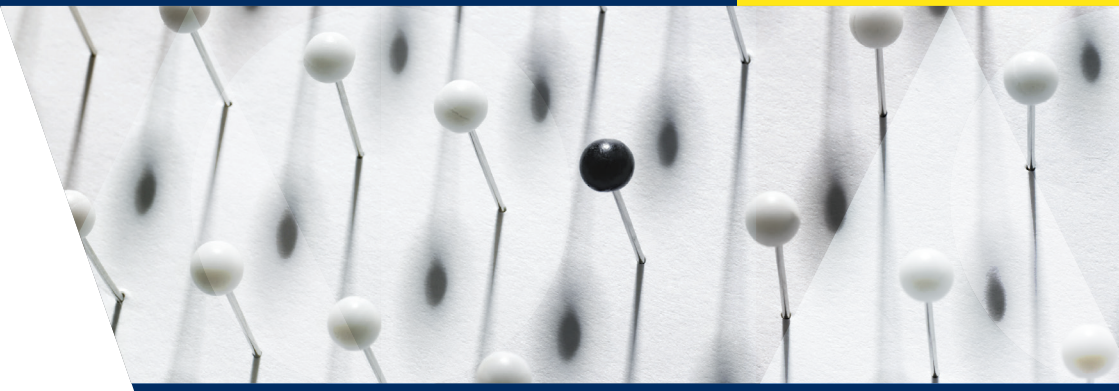
MANUEL



Manuel de droit européen en matière de protection des données

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Le manuscrit du présent manuel a été achevé en avril 2014.
Des versions actualisées seront publiées sur le site internet de la FRA à l'adresse fra.europa.eu, sur le site internet du Conseil de l'Europe à l'adresse coe.int/dataprotection ainsi que sur celui de la Cour européenne des droits de l'homme, rubrique « jurisprudence », à l'adresse echr.coe.int.

Europe Direct est un service destiné à vous aider à trouver des réponses aux questions que vous vous posez sur l'Union européenne.

Un numéro unique gratuit (*):

00 800 6 7 8 9 10 11

(*) Les informations sont fournies à titre gracieux et les appels sont généralement gratuits (sauf certains opérateurs, hôtels ou cabines téléphoniques).

Photo (couverture et intérieur): © iStockphoto

De nombreuses autres informations sur l'Union européenne sont disponibles sur l'internet via le serveur Europa (http://europa.eu).

Luxembourg: Office des publications de l'Union européenne, 2014

ISBN 978-92-871-9954-6 (CdE)
ISBN 978-92-9239-332-8 (FRA)
doi:10.2811/53800

Printed in Luxembourg

Imprimé sur papier recyclé sans chlore (PCF)

Le présent manuel a été rédigé en anglais. Le Conseil de l'Europe et la Cour européenne des droits de l'homme (la « CouEDH ») déclinent toute responsabilité quant à la qualité des traductions dans d'autres langues. Les opinions exprimées dans le présent manuel ne lient ni le Conseil de l'Europe ni la CouEDH. Le manuel fait référence à une série de commentaires et manuels. Le Conseil de l'Europe et la CouEDH déclinent toute responsabilité quant à leur contenu et leur inclusion dans la présente liste ne constitue pas une quelconque forme d'adhésion à ces publications. D'autres publications sont énumérées sur le site internet de la bibliothèque de la CouEDH à l'adresse: echr.coe.int.

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

Manuel de droit européen en matière de protection des données

Avant-propos

Le présent manuel de droit européen en matière de protection des données a été préparé conjointement par l'Agence des droits fondamentaux de l'Union européenne et le Conseil de l'Europe, en association avec le greffe de la Cour européenne des droits de l'homme. Il s'agit du troisième d'une série de manuels juridiques préparés conjointement par l'Agence des droits fondamentaux de l'Union européenne et le Conseil de l'Europe. Un premier manuel avait été publié en mars 2011 sur le droit européen en matière de non-discrimination et un deuxième en avril 2013 sur le droit européen en matière d'asile, de frontières et d'immigration.

Nous avons décidé de continuer notre coopération sur un sujet de grande actualité qui nous affecte tous au quotidien, celui de la protection des données à caractère personnel. L'Europe dispose de l'un des systèmes les plus protecteurs en la matière, basé sur la Convention 108 du Conseil de l'Europe, les instruments de l'Union européenne et la jurisprudence de la Cour européenne des droits de l'homme (CouEDH) et de la Cour de justice de l'Union européenne (CJUE).

L'objectif de ce manuel est de sensibiliser et d'améliorer les connaissances sur les règles en matière de protection des données dans les États membres de l'Union européenne et du Conseil de l'Europe en servant de principal document de référence vers lequel peuvent se tourner les lecteurs. Il est destiné aux praticiens du droit non spécialistes, aux juges, aux autorités nationales de protection des données et à toutes les autres personnes travaillant dans le secteur de la protection des données.

Avec l'entrée en vigueur du traité de Lisbonne en décembre 2009, la Charte des droits fondamentaux de l'Union européenne a acquis force juridique obligatoire et le droit à la protection des données à caractère personnel a été érigé au rang de droit fondamental autonome. Une meilleure compréhension de la Convention 108 du Conseil de l'Europe et des instruments de l'Union européenne, qui ont ouvert la voie à la protection des données en Europe, ainsi que de la jurisprudence de la CJUE et de la CouEDH est essentielle pour la protection de ce droit fondamental.

Nous remercions le Ludwig Boltzmann Institute of Human Rights pour sa contribution à la rédaction de ce manuel. Nos remerciements vont également au bureau du Contrôleur européen de la protection des données pour sa contribution pendant la phase de rédaction. Nous tenons enfin à remercier l'unité de protection des données de la Commission européenne pour son soutien dans la préparation du présent manuel.

Philippe Boillat

Directeur général de la Direction générale Droits de l'homme et État de droit du Conseil de l'Europe

Morten Kjaerum

Directeur de l'Agence des droits fondamentaux de l'Union européenne

Table des matières

Abréviations et acronymes

ACC	Autorité de contrôle commune
AELE	Association européenne de libre-échange
AEMF	Autorité européenne des marchés financiers
CCTV	Télévision en circuit fermé
CdE	Conseil de l'Europe
CE	Communauté européenne
CEDH	Convention européenne des droits de l'homme
CEPD	Contrôleur européen de la protection des données
Charte	Charte des droits fondamentaux de l'Union européenne
CJUE	Cour de justice de l'Union européenne (avant décembre 2009, Cour de justice des Communautés européennes, CJCE)
Convention 108	Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Conseil de l'Europe)
CouEDH	Cour européenne des droits de l'homme
CS-CIS	Système central d'information Schengen
DUDH	Déclaration universelle des droits de l'homme
EEE	Espace économique européen
ENISA	Agence européenne pour la sécurité des réseaux et de l'information
eTEN	Réseaux transeuropéens de télécommunications
eu-LISA	Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle
EuroPriSe	Label européen de protection de la vie privée
FRA	Agence des droits fondamentaux de l'Union européenne
GPS	Système de localisation GPS
GRC	Gestion de la relation client

MAE	Mandat d'arrêt européen
N-SIS	Système d'information Schengen national
OCDE	Organisation de coopération et de développement économiques
ONG	Organisation non gouvernementale
ONU	Organisation des Nations Unies
PIN	Numéro d'identification personnel
PNR	Dossier passager
REC	Règles d'entreprise contraignantes
SEPA	Espace unique de paiement en euros
SID	Système d'information douanier
SIS	Système d'information Schengen
STCE	Série des traités du Conseil de l'Europe
SWIFT	Société de télécommunications interbancaires mondiales
TFUE	Traité sur le fonctionnement de l'Union européenne
TUE	Traité sur l'Union européenne
UE	Union européenne
UNE	Unité nationale Europol
VIS	Système d'information sur les visas

Comment utiliser ce manuel ?

Le présent manuel offre une vue d'ensemble du droit applicable à la protection des données en relation avec l'Union européenne (UE) et le Conseil de l'Europe (CdE).

Le manuel a été conçu pour aider les praticiens du droit qui ne sont pas spécialisés dans le domaine de la protection des données ; il s'adresse aux avocats, aux juges et aux autres praticiens du droit, ainsi qu'à tous les collaborateurs d'autres organismes, y compris d'organisations non gouvernementales (ONG), qui peuvent être confrontés à des questions juridiques ayant trait à la protection des données.

Il s'agit d'un premier document de référence sur le droit de l'UE et la Convention européenne des droits de l'homme (CEDH) concernant la protection des données, qui explique comment ce domaine est réglementé dans le droit de l'UE et dans la CEDH, ainsi que dans la Convention du CdE pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (la « Convention 108 ») et d'autres actes du CdE. Chaque chapitre commence par un tableau récapitulant les dispositions légales applicables, y compris une importante sélection de la jurisprudence des deux systèmes juridiques européens distincts. Sont ensuite présentées les lois pertinentes de ces deux ordres européens applicables à chaque sujet, le but étant de permettre au lecteur de se rendre compte des points de convergence ou de divergence entre les deux systèmes.

Les tableaux au début de chaque chapitre énumèrent les sujets traités dans le chapitre en question et citent les dispositions légales applicables et autres sources pertinentes, telles que la jurisprudence. L'ordre des sujets peut être légèrement différent de la structure du texte dans le chapitre, si cela semble opportun pour la présentation concise du contenu du chapitre. Les tableaux couvrent à la fois le droit du CdE et de l'UE, ce qui devrait aider les utilisateurs à trouver les informations essentielles concernant leur situation, en particulier s'ils sont uniquement soumis au droit du CdE.

Les praticiens d'États non membres de l'UE, qui sont membres du CdE et parties à la CEDH et à la Convention 108 peuvent accéder aux informations pertinentes pour leur propre pays en consultant directement les sections consacrées au CdE. Les praticiens d'États membres de l'UE soumis aux deux ordres juridiques devront, en revanche, consulter les deux sections. Pour obtenir de plus amples informations sur un point particulier, les lecteurs pourront se reporter à la partie « Lectures complémentaires » du manuel où ils trouveront une liste de références à des sources plus spécialisées.

Le droit du CdE est présenté sous la forme de brèves références à des affaires de la Cour européenne des droits de l'homme (« CouEDH ») qui ont été sélectionnées parmi la multitude d'arrêts et de décisions de la CouEDH concernant les questions de protection des données.

Le droit de l'UE est constitué de mesures législatives et de dispositions pertinentes des traités et de la Charte des droits fondamentaux de l'Union européenne, telles qu'elles ont été interprétées par la Cour de justice de l'Union européenne [« CJUE », dénommée, avant 2009, Cour de justice des Communautés européennes (CJCE)].

La jurisprudence décrite ou citée dans ce manuel fournit des exemples tirés de l'important corpus de la jurisprudence de la CouEDH et de celle de la CJUE. Les lignes directrices présentées à la fin du manuel visent à aider le lecteur à rechercher la jurisprudence en ligne.

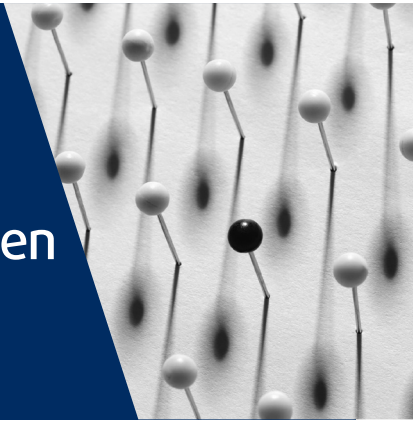
En outre, des exemples concrets et scénarios hypothétiques sont présentés dans des encadrés afin d'illustrer l'application pratique des règles européennes en matière de protection des données, en particulier quand il n'existe pas de jurisprudence spécifique de la CouEDH et de la CJUE.

Le manuel commence par une brève description du rôle des deux systèmes juridiques, tels qu'établis par le droit de la CouEDH et le droit de l'UE (Chapitre 1). Les Chapitres 2 à 8 couvrent les aspects suivants :

- terminologie de la protection des données ;
- principes clés du droit européen en matière de protection des données ;
- règles du droit européen en matière de protection des données ;
- droits des personnes concernées et leur application ;
- flux transfrontières de données ;
- protection des données dans le contexte de la police et de la justice pénale ;
- autres lois européennes spécifiques en matière de protection des données.

1

Contexte du droit européen en matière de protection des données



UE	Questions traitées	CdE
Le droit à la protection des données		
Directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (*directive relative à la protection des données*), JO 1995 L 281		CEDH, article 8 (droit au respect de la vie privée et familiale, du domicile et de la correspondance) Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108)
Mise en balance des droits		
CJUE, affaires jointes C-92/09 et C-93/09, *Volker und Markus Schecke GbR et Hartmut Eifert c. Land Hessen*, 2010	En général	
CJUE, C-73/07, *Tietosuojavaltuutettu c. Satakunnan Markkinapörssi Oy et Satamedia Oy*, 2008	Liberté d'expression	CouEDH, *Axel Springer AG c. Allemagne*, 2012 CouEDH, *Mosley c. Royaume-Uni*, 2011
	Liberté des arts et des sciences	CouEDH, *Vereinigung bildender Künstler c. Autriche*, 2007
CJUE, C-275/06, *Productores de Música de España (Promusicae) c. Telefónica de España SAU*, 2008	Protection de la propriété	
CJUE, C-28/08 P, *Commission européenne c. The Bavarian Lager Co. Ltd*, 2010	Accès aux documents	CouEDH, *Társaság a Szabadságjogokért c. Hongrie*, 2009

1.1. Le droit à la protection des données

Points clés

- Conformément à l'article 8 de la CEDH, le droit à la protection contre la collecte et l'utilisation de données à caractère personnel fait partie du droit au respect de la vie privée et familiale, du domicile et de la correspondance.
- La Convention 108 du CdE est le premier acte ayant force juridique obligatoire au niveau international explicitement consacré à la protection des données.
- Dans le droit de l'UE, la protection des données a été réglementée pour la première fois par la directive relative à la protection des données.
- Dans le droit de l'UE, la protection des données a été reconnue comme un droit fondamental.

Le droit à la protection de la sphère privée d'un individu contre toute intrusion de tiers, en particulier de l'État, a été énoncé pour la première fois dans un acte juridique international à l'article 12 de la Déclaration universelle des droits de l'homme (« DUDH ») de 1948 de l'Organisation des Nations Unies (« ONU ») sur le respect de la vie privée et familiale[1]. La DUDH a influencé l'élaboration d'autres actes sur les droits de l'homme en Europe.

1.1.1. La Convention européenne des droits de l'homme

Le Conseil de l'Europe a été créé après la Seconde Guerre mondiale pour réunir les États d'Europe dans le but de promouvoir l'État de droit, la démocratie, les droits de l'homme et le développement social. À cette fin, il a adopté la Convention européenne des droits de l'homme (CEDH) en 1950, qui est entrée en vigueur en 1953.

Les États parties ont l'obligation internationale de respecter la CEDH. Tous les États membres du CdE ont désormais transposé ou fait prendre effet à la CEDH dans leur droit national, de sorte qu'ils sont tenus d'agir conformément aux dispositions de la Convention.

1 Organisation des Nations Unies (ONU), Déclaration universelle des droits de l'homme (DUDH), 10 décembre 1948

La Cour européenne des droits de l'homme (CouEDH) a été créée à Strasbourg en 1959 pour garantir que les États contractants observent leurs obligations en vertu de la CEDH. La CouEDH veille au respect de leurs obligations en vertu de la Convention par les États en examinant les réclamations de particuliers, de groupes de particuliers, d'ONG ou de personnes morales invoquant des violations à la Convention. En 2013, le Conseil de l'Europe regroupait 47 États membres, dont 28 étaient aussi des États membres de l'UE. Un requérant devant la CouEDH ne doit pas forcément être un ressortissant de l'un des États membres. La CouEDH peut aussi examiner des affaires inter-États soumises par un ou plusieurs États membres du CdE contre un autre État membre.

Le droit à la protection des données à caractère personnel fait partie des droits protégés par l'article 8 de la CEDH, qui garantit le droit au respect de la vie privée et familiale, du domicile et de la correspondance, et énonce les conditions dans lesquelles des restrictions à ce droit sont admises[2].

Dans l'ensemble de sa jurisprudence, la CouEDH a examiné de nombreuses situations soulevant la question de la protection des données, notamment concernant l'interception de communications[3], diverses formes de surveillance[4], et la protection contre la conservation de données à caractère personnel par des autorités publiques[5]. Elle a précisé que l'article 8 de la CEDH impose non seulement aux États de s'abstenir de toutes actions susceptibles de violer ce droit de la Convention, mais les soumet également, dans certaines circonstances, à des obligations positives de garantir activement un respect effectif du droit au respect de la vie privée et familiale[6]. Nombre de ces affaires seront présentées en détail dans les chapitres correspondants.

2 CdE, Convention européenne des droits de l'homme, STCE n° 005, 1950.

3 Voir, par exemple, CouEDH, *Malone c. Royaume-Uni,* n° 8691/79, 2 août 1984 ; CouEDH, *Copland c. Royaume-Uni*, n° 62617/00, 3 avril 2007.

4 Voir, par exemple, CouEDH, *Klass et autres c. Allemagne*, n° 5029/71, 6 septembre 1978 ; CouEDH, *Uzun c. Allemagne*, n° 35623/05, 2 septembre 2010.

5 Voir, par exemple, CouEDH, *Leander c. Suède*, n° 9248/81, 11 juillet 1985 ; CouEDH, *S. et Marper c. Royaume-Uni*, n° 30562/04, 4 décembre 2008.

6 Voir, par exemple, CouEDH, *I. c. Finlande*, n° 20511/03, 17 juillet 2008 ; CouEDH, *K.U. c. Finlande*, n° 2872/02, 2 mars 2009.

1.1.2. Convention 108 du Conseil de l'Europe

L'émergence des technologies de l'information dans les années 1960 s'est accompagnée d'un besoin croissant de règles plus détaillées visant à protéger les individus, en protégeant leurs données (à caractère personnel). Dès le milieu des années 1970, le Comité des Ministres du Conseil de l'Europe a adopté plusieurs résolutions concernant la protection des données à caractère personnel, mentionnant l'article 8 de la CEDH[7]. En 1981, une Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108)[8] a été ouverte à la signature. La Convention 108 était, et reste aujourd'hui, le seul acte à force juridique obligatoire internationale dans le domaine de la protection des données.

La Convention 108 s'applique à tout traitement de données à caractère personnel dans les secteurs privé et public, tel que les traitements effectués par les autorités judiciaires ou celles chargées de l'application de la loi. Elle protège les individus contre les abus pouvant accompagner la collecte et le traitement de données à caractère personnel, tout en cherchant à réguler le flux transfrontières de données à caractère personnel. S'agissant de la collecte et du traitement de données à caractère personnel, les principes énoncés dans la Convention concernent, en particulier, une collecte licite et loyale et un traitement automatisé des données conservées à des fins légitimes définies, et non à des fins incompatibles avec ces dernières, ni conservées plus longtemps que nécessaire. Ils concernent également la qualité des données, en particulier le fait qu'elles doivent être adéquates, pertinentes, non excessives (proportionnalité) et exactes.

En plus de fournir des garanties concernant la collecte et le traitement de données à caractère personnel, la Convention 108 interdit, en l'absence de garanties juridiques convenables, le traitement de données « sensibles », telles que l'origine raciale, l'opinion politique, l'état de santé, les convictions religieuses, la vie sexuelle ou les condamnations pénales d'une personne.

7 CdE, Comité des Ministres (1973), résolution (73) 22 relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques dans le secteur privé, 26 septembre 1973 ; CdE, Comité des Ministres (1974), résolution (74) 29 relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques dans le secteur public, 20 septembre 1974.

8 CdE, Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, STCE n° 108, 1981.

La Convention consacre par ailleurs le droit de tout individu de savoir que des informations sont conservées à son sujet et, si nécessaire, de les faire rectifier. Les restrictions aux droits énoncées dans la Convention ne sont possibles que si des intérêts prépondérants, tels que la sécurité de l'Etat ou la sûreté publique, entrent en jeu.

Bien que la Convention prévoie une libre circulation des données à caractère personnel entre les États contractants, elle impose également certaines restrictions à cette circulation vers des États dont la réglementation ne prévoit pas une protection appropriée.

Afin de poursuivre le développement des principes généraux et des règles énoncés dans la Convention 108, plusieurs recommandations sans force obligatoire ont été adoptées par le Comité des Ministres du CdE (voir Chapitres 7 et 8).

Tous les États membres de l'UE ont ratifié la Convention 108. En 1999, la Convention 108 a été modifiée pour permettre à l'UE d'y adhérer[9]. En 2001, un protocole additionnel à la Convention 108 a été adopté. Il introduit des dispositions sur les flux transfrontières de données vers des pays n'étant pas parties à la Convention, appelés « pays tiers », et sur la création obligatoire d'autorités nationales de contrôle de la protection des données[10].

Perspective

Une consultation publique organisée en 2011 après une décision de moderniser la Convention 108 a permis de confirmer les deux principaux objectifs de cet exercice : renforcer la protection du droit au respect de la vie privée dans le domaine numérique et améliorer le mécanisme de suivi de la Convention.

La Convention 108 est ouverte à l'adhésion des États non-membres du CdE, y compris des pays non-européens. La capacité de la Convention à constituer une norme universelle et son ouverture pourraient servir de base à la promotion de la protection des données au niveau mondial.

9 CdE, amendements à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STCE n° 108) permettant aux Communautés européennes d'adhérer, adoptés par le Comité des Ministres, à Strasbourg, le 15 juin 1999 ; art. 23, para. 2, de la Convention 108 dans sa version amendée.

10 CdE, protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, concernant les autorités de contrôle et les flux transfrontières de données, STCE n° 181, 2001.

À ce jour, 45 des 46 États contractants à la Convention 108 sont des États membres du CdE. L'Uruguay, le premier pays non européen, a adhéré en août 2013. Le Maroc, qui a été invité à adhérer à la Convention 108 par le Comité des Ministres, formalise actuellement son adhésion.

1.1.3. Droit de l'Union européenne en matière de protection des données

Le droit de l'UE se compose des traités et du droit dérivé de l'UE. Les traités, à savoir, le traité sur l'Union européenne (TUE) et le traité sur le fonctionnement de l'Union européenne (TFUE), ont été adoptés par tous les États membres de l'UE ; ils forment ce que l'on désigne comme le « droit primaire de l'UE ». Les règlements, les directives et les décisions de l'UE sont adoptés par les institutions de l'UE auxquelles les traités ont conféré cette compétence ; ils constituent ce que l'on appelle le « droit dérivé de l'UE ».

Le principal acte juridique de l'UE en matière de protection des données est 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 (*directive relative à la protection des données*)[11]. Elle a été adoptée en 1995, date à laquelle plusieurs États membres avaient déjà adopté des lois nationales sur la protection des données. La libre circulation des marchandises, des capitaux, des services et des personnes au sein du marché intérieur imposait la libre circulation des données, impossible à concrétiser si les États membres ne pouvaient se fier à un niveau uniformément élevé de protection des données.

Dans la mesure où l'adoption de la directive relative à la protection des données répondait à une volonté d'harmonisation[12] du droit en matière de protection des données au niveau national, la directive offre un degré de précision comparable à celui des législations nationales en vigueur (à l'époque) en matière de protection des données. Pour la Cour de Justice de l'Union européenne (CJUE), « la directive 95/46 vise [...] à rendre équivalent dans tous les États membres le niveau de protection des droits et libertés des personnes à l'égard du traitement de données à caractère personnel. [...] [L]e rapprochement des législations nationales applicables en la matière ne doit pas conduire à affaiblir la protection qu'elles assurent, mais doit, au contraire,

11 Directive relative à la protection des données, JO 1995 L 281, p. 31.

12 Voir, par exemple, directive relative à la protection des données, considérants 1, 4, 7 et 8.

avoir pour objectif de garantir un niveau élevé de protection dans l'Union [...]. Ainsi, [...] l'harmonisation desdites législations nationales ne se limite pas à une harmonisation minimale, mais aboutit à une harmonisation qui est, en principe, complète. »[13] En conséquence, les États membres n'ont qu'une latitude limitée en ce qui concerne la mise en œuvre de la directive.

La directive relative à la protection des données a été conçue pour donner du poids aux principes du droit à la vie privée, déjà contenus dans la Convention 108, ainsi que pour les élargir. Le fait que les 15 États membres de l'UE en 1995 étaient également parties à la Convention 108 exclut l'adoption de règles contradictoires dans ces deux actes juridiques. La directive relative à la protection des données se fonde toutefois sur la possibilité prévue à l'article 11 de la Convention 108 d'étendre la protection. En particulier, l'introduction d'un contrôle indépendant comme outil d'amélioration de la conformité aux règles de protection des données s'est révélée une contribution importante au fonctionnement efficace du droit européen en matière de protection des données (Cette caractéristique a donc été reprise dans le droit du CdE, en 2001, par le protocole additionnel à la Convention 108).

L'application territoriale de la directive relative à la protection des données s'étend au-delà des 28 États membres de l'UE et inclut aussi les États non membres de l'UE qui font partie de l'Espace économique européen (EEE)[14] – à savoir l'Islande, le Liechtenstein et la Norvège.

La CJUE au Luxembourg est compétente pour déterminer si un État membre a honoré ses obligations en vertu de la directive relative à la protection des données et pour rendre des décisions préjudicielles concernant la validité et l'interprétation de la directive, afin de garantir son application effective et uniforme dans les États membres. Une exception importante à l'applicabilité de la directive relative à la protection des données est l'« exemption domestique », à savoir le traitement de données à caractère personnel par des particuliers à des fins simplement personnelles et domestiques[15]. Un tel traitement est généralement considéré comme faisant partie des libertés des particuliers.

13 CJEU, affaires jointes C-468/10 et C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) et Federación de Comercio Electrónico y Marketing Directo (FECEMD) c. Administración del Estado*, 24 novembre 2011, para. 28-29.

14 Accord sur l'espace économique européen, JO 1994 L 1, qui est entré en vigueur le 1er janvier 1994.

15 Directive relative à la protection des données, art. 3, para. 2, deuxième tiret.

Conformément au droit primaire de l'UE en vigueur à la date de l'adoption de la directive relative à la protection des données, le champ d'application matériel de la directive est limité aux affaires de marché intérieur. En outre, et c'est encore plus important, les questions de coopération avec la police et la justice pénale ne relèvent pas de son champ d'application. La protection des données dans ces affaires découle de différents actes juridiques, qui sont décrits en détail au Chapitre 7.

Dans la mesure où la directive relative à la protection des données pouvait uniquement concerner les États membres de l'UE, un autre acte juridique était nécessaire pour établir une protection des données à caractère personnel dans le cadre de leur traitement par des institutions et organes communautaires. Le règlement (CE) n° 45/2001 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données (*règlement relatif à la protection des données des institutions communautaires*) remplit cette fonction[16].

En outre, même dans des domaines couverts par la directive relative à la protection des données, des dispositions plus détaillées en la matière sont souvent nécessaires pour obtenir la clarté souhaitée dans la mise en balance d'autres intérêts légitimes. La directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (*directive vie privée et communications électroniques*)[17] et la directive 2006/24/CE sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communication, et modifiant la directive 2002/58/CE (*directive sur la conservation des données,* invalidée le 8 avril 2014)[18] en sont deux exemples. D'autres exemples seront abordés au Chapitre 8. De telles dispositions doivent être conformes à la directive relative à la protection des données.

16 Règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données, JO 2001 L 8.

17 Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), JO 2002 L 201.

18 Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE, (directive sur la conservation des données), JO 2006 L 105, invalidée le 8 avril 2014.

La Charte des droits fondamentaux de l'Union européenne

Les traités originaux des Communautés européennes ne contenaient pas de référence aux droits de l'homme ou à leur protection. À mesure que la Cour de justice des Communautés européennes (CJCE) de l'époque était saisie d'affaires invoquant des violations des droits de l'homme dans des domaines relevant de la compétence du droit de l'UE, celle-ci a développé une nouvelle approche. Pour offrir une protection aux individus, elle a intégré les droits fondamentaux dans les principes généraux du droit européen. Selon la CJUE, ces principes généraux reflètent le contenu de la protection des droits de l'homme prévue par les constitutions nationales et les traités sur les droits de l'homme, en particulier la CEDH. La CJUE a déclaré qu'elle garantirait la conformité du droit de l'UE à ces principes.

En reconnaissant que ses politiques pouvaient avoir un impact sur les droits de l'homme et dans le souci de veiller à ce que les citoyens se sentent « plus proches » de l'UE, la Charte des droits fondamentaux de l'Union européenne (la « Charte ») a été proclamée en 2000. Cette Charte intègre toute la gamme des droits civils, politiques, économiques et sociaux des citoyens européens, en synthétisant les traditions constitutionnelles et les obligations internationales communes aux États membres. Les droits décrits dans la Charte sont divisés en six parties : dignité, libertés, égalité, solidarité, droits des citoyens et justice.

Bien que ne constituant initialement qu'un document politique, la Charte a acquis force obligatoire[19] comme droit primaire de l'UE (voir article 6, paragraphe 1, du TUE) avec l'entrée en vigueur du traité de Lisbonne le 1er décembre 2009[20].

Le droit primaire de l'UE confère aussi à l'UE la compétence générale de légiférer sur les questions de protection des données (article 16 du TFUE).

La Charte garantit non seulement le droit au respect de la vie privée et familiale (article 7), mais établit également le droit à la protection des données (article 8), relevant explicitement le niveau de cette protection à celui d'un droit fondamental dans le droit de l'UE. Les institutions européennes ainsi que les États membres doivent respecter et garantir ce droit, qui s'applique aussi aux États membres dans la transposition du droit de l'Union (article 51 de la Charte). Formulé plusieurs années

19 UE (2012), Charte des droits fondamentaux de l'Union européenne, JO 2012 C 326.

20 Voir les versions consolidées des Communautés européennes (2012), Traité sur l'Union européenne, JO 2012 C 326 ; et des Communautés européennes (2012), TFUE, JO 2012 C 326.

après la directive relative à la protection des données, l'article 8 de la Charte doit être compris comme incarnant le droit préexistant de l'UE à la protection des données. Par conséquent, la Charte mentionne non seulement explicitement un droit à la protection des données à l'article 8, paragraphe 1, mais fait aussi référence aux principes clés de la protection des données à l'article 8, paragraphe 2. Enfin, l'article 8, paragraphe 3, de la Charte, garantit le contrôle de la mise en œuvre de ces principes par une autorité indépendante.

Perspective

En janvier 2012, la Commission européenne a proposé plusieurs réformes sur la protection des données, précisant que les règles actuelles en matière de protection des données devaient être modernisées compte tenu des évolutions technologiques rapides et de la mondialisation. Les réformes consistaient en une proposition de règlement général sur la protection des données[21], destiné à remplacer la directive relative à la protection des données, ainsi qu'une nouvelle directive relative à la protection des données[22] devant apporter une protection des données dans les domaines de la coopération policière et judiciaire en matière pénale. À la date de publication de ce manuel, les discussions sur les propositions de réformes étaient toujours en cours.

1.2. Mise en balance des droits

Point clé

- Le droit à la protection des données n'est pas un droit absolu ; il doit être mis en balance avec d'autres droits.

Le droit fondamental à la protection des données à caractère personnel prévu par l'article 8 de la Charte « n'apparaît toutefois pas comme une prérogative absolue,

21 Commission européenne (2012), *Proposition de règlement du Parlement européen et du Conseil 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 (règlement général sur la protection des données)*, COM(2012) 11 final, Bruxelles, 25 janvier 2012.

22 Commission européenne (2012), *Proposition de directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, ou d'exécution de sanctions pénales, et à la libre circulation de ces données (directive générale relative à la protection des donnée)*, COM(2012) 10 final, Bruxelles, 25 janvier 2012.

mais doit être pris en considération par rapport à sa fonction dans la société »[23]. L'article 52, paragraphe 1, de la Charte admet que des limitations peuvent être apportées à l'exercice de droits tels que ceux consacrés aux articles 7 et 8 de celle-ci, pour autant que ces limitations sont prévues par la loi, qu'elles respectent le contenu essentiel desdits droits et libertés et que, dans le respect du principe de proportionnalité, elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union européenne ou au besoin de protection des droits et libertés d'autrui[24].

Dans le système de la CEDH, la protection des données est garantie par l'article 8 (droit au respect de la vie privée et familiale) et, à l'instar du système de la Charte, ce droit doit être appliqué tout en respectant la portée d'autres droits concurrents. Conformément à l'article 8, paragraphe 2, de la CEDH, « il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire (...) à la protection des droits et libertés d'autrui ».

Par conséquent, la CouEDH et la CJUE n'ont eu de cesse de préciser qu'un exercice de mise en balance avec d'autres droits était nécessaire dans l'application et l'interprétation de l'article 8 de la CEDH et de l'article 8 de la Charte[25]. Plusieurs exemples importants illustreront la façon dont une telle mise en balance peut être atteinte.

1.2.1. Liberté d'expression

L'un des droits qu'il conviendra probablement de mettre en balance par rapport au droit à la protection des données est celui de à liberté d'expression.

La liberté d'expression est protégée par l'article 11 de la Charte (« Liberté d'expression et d'information »). Ce droit comprend « la liberté d'opinion et la liberté de

23 Voir, par exemple, CJUE, affaires jointes C-92/09 et C-93/09, *Volker und Markus Schecke GbR et Hartmut Eifert c. Land Hessen*, 9 novembre 2010, para 48.

24 *Ibid.*, para 50.

25 CouEDH, *Von Hannover c. Allemagne* (n° 2) [GC], n° 40660/08 et 60641/08, 7 février 2012 ; CJUE, affaires jointes C-468/10 et C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) et Federación de Comercio Electrónico y Marketing Directo (FECEMD) c. Administración del Estado*, 24 novembre 2011, para 48 ; CJUE, C-275/06, *Productores de Música de España (Promusicae) c. Telefónica de España SAU*, 29 janvier 2008, para 68. Voir également Conseil de l'Europe (2013), jurisprudence de la Cour européenne des droits de l'homme en matière de protection des données à caractère personnel, jurisprudence PD (2013), disponible à l'adresse : http://www.coe.int/t/dghl/standardsetting/dataprotection/Judgments/DP%202013%20Case%20Law_Eng_FINAL.pdf .

recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontières ». L'article 11 correspond à l'article 10 de la CEDH. Conformément à l'article 52, paragraphe 3, de la Charte, pour autant qu'elle contient des droits correspondant à des droits garantis par la CEDH, « leur sens et leur portée sont les mêmes que ceux que leur confère ladite convention ». Les limitations qui peuvent légalement être imposées au droit garanti par l'article 11 de la Charte ne peuvent donc pas aller au-delà de celles prévues à l'article 10, paragraphe 2, de la CEDH, c'est-à-dire qu'elles doivent être prévues par la loi et être nécessaires, dans une société démocratique, « à la protection [...] de la réputation ou des droits d'autrui ». Cette notion couvre le droit à la protection des données.

La relation entre la protection des données à caractère personnel et la liberté d'expression est régie par l'article 9 de la directive relative à la protection des données, intitulé « Traitements de données à caractère personnel et liberté d'expression »[26]. Selon cet article, « 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 ».

Exemple : dans l'affaire *Tietosuojavaltuutettu c. Satakunnan Markkinapörssi Oy and Satamedia Oy*[27], il était demandé à la CJUE d'interpréter l'article 9 de la directive relative à la protection des données, et de définir les rapports entre la protection des données et la liberté de la presse. La Cour devait examiner la diffusion par Markkinapörssi et Satamedia de données fiscales concernant plus d'un million deux cent mille personnes physiques, obtenues légalement auprès de l'administration fiscale finlandaise. En particulier, la Cour devait vérifier si le traitement de données à caractère personnel, fournies par l'administration fiscale, pour permettre à des utilisateurs de téléphones mobiles de recevoir des informations fiscales sur d'autres personnes physiques, devait être considéré comme une activité effectuée aux seules fins de journalisme. Après avoir conclu que les activités de Satakunnan constituaient un « traitement de données à caractère personnel » au sens de l'article 3, paragraphe 1, de la directive relative à la protection des données, la Cour s'est attachée à

26 Directive relative à la protection des données, art. 9.

27 CJUE, C-73/07, *Tietosuojavaltuutettu c. Satakunnan Markkinapörssi Oy and Satamedia Oy*, 16 décembre 2008, paras. 56, 61 et 62.

interpréter l'article 9 de la directive. La Cour a d'abord relevé l'importance du droit à la liberté d'expression dans toute société démocratique et a retenu que les notions y afférentes, dont celle du journalisme, devaient être interprétées de manière large. Elle a ensuite observé que, pour obtenir une pondération équilibrée entre les deux droits fondamentaux, les dérogations et limitations du droit à la protection des données devaient s'opérer dans les limites du strict nécessaire. Dans ces circonstances, la Cour a considéré que des activités telles que celles exercées par Markkinapörssi et Satamedia concernant des données provenant de documents considérés comme des documents publics en vertu de la législation nationale, pouvaient être qualifiées d'« activités de journalisme » si elles avaient pour finalité la divulgation au public d'informations, d'opinions ou d'idées, par quelque moyen de transmission que ce soit. La Cour a par ailleurs écarté la possibilité que ces activités soient réservées aux entreprises de médias et puissent être liées à un but lucratif. Toutefois, la CJUE a laissé à la juridiction nationale le soin d'apprécier si tel était le cas en l'espèce.

Concernant la pondération du droit à la protection des données avec le droit à la liberté d'expression, la CouEDH a rendu plusieurs arrêts qui font référence.

Exemple : dans l'affaire *Axel Springer AG c. Allemagne*[28], la CouEDH a retenu qu'une interdiction imposée par un tribunal au propriétaire d'un journal souhaitant publier un article sur l'arrestation et la condamnation d'un acteur connu était contraire à l'article 10 de la CEDH. La CouEDH a réaffirmé les critères qu'elle avait établis dans sa jurisprudence concernant la mise en balance du droit à la liberté d'expression et du droit au respect de la vie privée. Elle a posé les questions suivantes :

- premièrement, l'événement auquel l'article est consacré est-il d'intérêt général ? L'arrestation et la condamnation d'une personne est un fait judiciaire public ; le public a donc intérêt à en être informé ;

- deuxièmement, la personne concernée est-elle une personne publique ? La personne concernée était un acteur suffisamment connu pour être qualifié de personne publique ; et

28 CouEDH, *Axel Springer AG c. Allemagne* [GC], n° 39954/08, 7 février 2012, paras. 90 et 91.

- troisièmement, comment les informations ont-elles été obtenues et sont-elles fiables ? Les informations avaient été fournies par le parquet et l'exactitude des informations contenues dans les deux publications n'était pas contestée par les parties.

Par conséquent, la CouEDH a jugé que les restrictions à la publication imposées à la société n'étaient pas raisonnablement proportionnées au but légitime de la protection de la vie privée de l'acteur. La CouEDH a conclu à une violation de l'article 10 de la CEDH.

Exemple : dans l'affaire *Von Hannover c. Allemagne (n° 2)*[29], la CouEDH n'a pas constaté de violation du droit au respect de la vie privée au titre de l'article 8 de la CEDH lorsque la princesse Caroline de Monaco s'est vue refuser une injonction contre la publication d'une photographie la représentant avec son mari pendant des vacances au ski. La photographie était accompagnée d'un article faisant état, entre autres, de la dégradation de l'état de santé du prince Rainier. La CouEDH a conclu que les juridictions nationales avaient procédé à une mise en balance circonstanciée du droit des sociétés d'édition à la liberté d'expression avec le droit des requérants au respect de leur vie privée. La qualification donnée à la maladie du prince Rainier d'« événement de l'histoire contemporaine » par les juridictions nationales ne pouvait passer pour déraisonnable et la CouEDH a considéré que la photographie, considérée à la lumière des articles l'accompagnant, avait apporté, au moins dans une certaine mesure, une contribution à un débat d'intérêt général. La CouEDH a exclu la violation de l'article 8 de la CEDH.

Dans la jurisprudence de la CouEDH, l'un des critères fondamentaux concernant la mise en balance de ces droits est de savoir si l'expression en cause contribue à un débat d'intérêt général.

Exemple : dans l'affaire *Mosley c. Royaume-Uni*[30], un journal hebdomadaire national avait publié des photographies intimes du requérant. Celui-ci avait invoqué une violation de l'article 8 de la CEDH au motif qu'il n'avait pas été en mesure de demander une injonction avant la publication des photos en question, en raison de l'absence d'une obligation de notification préalable par le

29 CouEDH, *Von Hannover c. Allemagne (n° 2)* [GC], n° 40660/08 et 60641/08, 7 février 2012, paras. 118 et 124.

30 CouEDH, *Mosley c. Royaume-Uni*, n° 48009/08, 10 mai 2011, paras. 129 et 130.

journal de la publication de l'article susceptible de porter atteinte au droit au respect de la vie privée de l'intéressé. Bien que la divulgation de ce type d'information poursuive généralement un but de divertissement et non d'éducation, elle bénéficie incontestablement de la protection de l'article 10 de la CEDH, qui pourrait céder devant les exigences de l'article 8 de la CEDH lorsque l'information revêt un caractère privé et intime et que sa divulgation ne présente aucun intérêt public. Toutefois, il y avait lieu de procéder à un examen particulièrement minutieux des contraintes susceptibles de constituer une forme de censure avant la publication. Eu égard à l'effet dissuasif d'une éventuelle obligation de notification préalable, aux doutes quant à l'efficacité d'une telle obligation, et à la vaste marge d'appréciation laissée dans ce domaine, la CouEDH a conclu que l'article 8 n'exigeait pas une obligation légale de notification préalable. Par conséquent, la CouEDH a exclu la violation de l'article 8.

Exemple : dans l'affaire *Biriuk c. Lituanie*[31], la requérante réclamait des dommages-intérêts à un quotidien qui avait publié un article déclarant qu'elle était séropositive. L'information aurait été confirmée par le personnel soignant de l'hôpital local. La CouEDH n'a pas jugé que l'article en question contribuait à un débat d'intérêt général et a rappelé que la protection des données à caractère personnel, à plus forte raison de données médicales, est une composante essentielle du droit de toute personne au respect de sa vie privée et familiale, tel que garanti par l'article 8 de la CEDH. La CouEDH a attaché une importance particulière au fait que, selon l'article du journal, le personnel médical de l'hôpital aurait fourni des informations sur l'infection de la requérante par le virus du VIH, en violation évidente de son obligation au secret médical. Par conséquent, l'État a échoué à garantir le droit de la requérante au respect de sa vie privée. La CouEDH a conclu à une violation de l'article 8.

1.2.2. Accès aux documents

La liberté d'information conformément à l'article 11 de la Charte et à l'article 10 de la CEDH protège non seulement le droit de communiquer mais aussi celui de recevoir des informations. L'importance de la transparence gouvernementale pour le fonctionnement d'une société démocratique se fait de plus en plus ressentir. Au cours des deux dernières décennies, le droit d'accès aux documents détenus par des autorités publiques a donc été reconnu comme un droit important de tout citoyen

31 CouEDH, *Biriuk c. Lituanie*, n° 23373/03, 25 novembre 2008.

européen, ainsi que de toute personne physique ou morale ayant son domicile ou son siège social dans un État membre.

Dans le droit du CdE, on peut renvoyer aux principes consacrés dans la recommandation sur l'accès aux documents officiels, dont les auteurs de la Convention sur l'accès aux documents officiels (*Convention 205*)[32] se sont inspirés.

Dans le droit européen, le droit d'accès aux documents est garanti par le règlement 1049/2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission (*règlement relatif à l'accès aux documents*)[33]. L'article 42 de la Charte et l'article 15, paragraphe 3, du TFUE ont étendu ce droit d'accès aux « documents des institutions, organes et organismes de l'Union, quelle que soit leur forme ». Conformément à l'article 52, paragraphe 2, de la Charte, le droit d'accès aux documents s'exerce également dans les conditions et limites définies à l'article 15, paragraphe 3, du TFUE. Ce droit peut s'opposer au droit à la protection des données si l'accès aux documents peut avoir pour conséquence de révéler les données à caractère personnel de tiers. Des demandes d'accès à des documents ou informations détenus par des autorités publiques peuvent donc nécessiter une mise en balance avec le droit à la protection des données des personnes dont les données figurent dans les documents demandés.

Exemple : dans l'affaire *Commission c. Bavarian Lager*[34], la CJUE a défini l'étendue de la protection des données à caractère personnel dans le contexte de l'accès aux documents des institutions communautaires, ainsi que les relations entre les règlements 1049/2001 (*règlement relatif à l'accès aux documents*) et 45/2001 (*règlement relatif à la protection des données*). La société Bavarian Lager, créée en 1992, importait de la bière allemande en bouteille au Royaume-Uni, principalement pour des pubs et des bars. Elle avait toutefois rencontré des difficultés car la législation britannique favorisait de fait les producteurs nationaux. En réponse à la plainte de Bavarian Lager, la Commission européenne a décidé d'engager une procédure contre le Royaume-Uni pour manquement à ses obligations, ce qui a abouti à la modification des dispositions contestées et à leur alignement sur le droit communautaire. Bavarian Lager a ensuite demandé

32 Conseil de l'Europe, Comité des Ministres (2002), Recommandation Rec (2002) 2 aux États membres sur l'accès aux documents publics, 21 février 2002 ; Conseil de l'Europe, Convention sur l'accès aux documents officiels, STCE n° 205, 18 juin 2009. La Convention n'est pas encore entrée en vigueur.

33 Règlement (CE) n °1049/2001 du Parlement européen et du Conseil du 30 mai 2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission, JO 2001 L 145.

34 CJUE, C-28/08 P, *Commission européenne c. The Bavarian Lager Co. Ltd.*, 29 juin 2010, paras. 60, 63, 76, 78 et 79.

à la Commission, entre autres documents, une copie du procès-verbal d'une réunion à laquelle avaient participé des représentants de la Commission, des autorités britanniques et de la Confédération des Brasseurs du Marché Commun (CBMC). La Commission a accepté de communiquer certains documents relatifs à la réunion mais a occulté cinq noms dans le procès-verbal, deux personnes s'étant expressément opposées à la divulgation de leur identité et la Commission n'ayant pu contacter les trois autres. Par décision du 18 mars 2004, la Commission a rejeté un nouveau recours de Bavarian Lager visant à obtenir le procès-verbal complet de la réunion, citant notamment la protection de la vie privée de ces personnes, telle que garantie par le règlement relatif à la protection des données. Insatisfaite de cette position, Bavarian Lager a formé un recours devant le tribunal de première instance, qui avait annulé la décision de la Commission par une décision du 8 novembre 2007 (affaire T-194/04, *Bavarian Lager c. Commission*), considérant en particulier que la simple inscription des noms des personnes en question sur la liste des participants à une réunion pour le compte de l'institution qu'elles représentaient ne constituait pas une atteinte à la vie privée et n'exposait pas la vie privée de ces personnes à un quelconque danger.

Sur pourvoi de la Commission, la CJUE a annulé la décision du tribunal de première instance. La CJUE a retenu que le règlement relatif à l'accès aux documents établit « un régime spécifique et renforcé de protection d'une personne dont les données à caractère personnel pourraient, le cas échéant, être communiquées au public ». Selon la CJUE, lorsqu'une demande fondée sur le règlement relatif à l'accès aux documents vise à obtenir l'accès à des documents comprenant des données à caractère personnel, les dispositions dudit règlement deviennent intégralement applicables. La CJUE a ensuite conclu que c'était à bon droit que la Commission avait rejeté la demande d'accès au procès-verbal complet de la réunion d'octobre 1996. En l'absence du consentement des cinq participants à cette réunion, la Commission avait dûment respecté son obligation d'ouverture en communiquant une version du document en question occultant leurs noms.

De plus, selon la CJUE, « Bavarian Lager n'ayant fourni aucune justification expresse et légitime ni aucun argument convaincant pour démontrer la nécessité du transfert de ces données personnelles, la Commission n'avait pas pu mettre en balance les différents intérêts des parties en cause. Elle ne pouvait non plus vérifier que ce transfert ne pourrait pas porter atteinte aux intérêts

légitimes des personnes concernées », ainsi que le prescrit le règlement relatif à la protection des données.

Selon cet arrêt, une ingérence dans le droit à la protection des données à l'égard de l'accès à des documents requiert un motif spécifique et justifié. Le droit d'accès à des documents ne peut automatiquement écarter le droit à la protection des données[35].

Un aspect particulier d'une demande d'accès a été traité dans l'arrêt suivant de la CouEDH.

Exemple : dans l'affaire *Társaság a Szabadságjogokért c. Hongrie*[36], la requérante, une ONG ayant pour objectif la défense des droits de l'homme, demandait à la Cour constitutionnelle l'accès à des informations sur une affaire pendante. Sans consulter le parlementaire lui ayant soumis l'affaire, la Cour constitutionnelle a refusé l'accès au motif que des griefs dont elle était saisie ne pouvaient être communiqués à des tiers sans l'autorisation du plaignant. Les juridictions nationales ont confirmé ce refus au motif que la protection de telles données à caractère personnel ne pouvait s'effacer devant d'autres intérêts juridiques tels que l'accessibilité à des informations publiques. La requérante a agi comme « organisme de surveillance pour la société », ses activités visant à garantir une protection similaire à celle accordée à la presse. S'agissant de la liberté de la presse, la CouEDH a constamment retenu que le public a le droit d'obtenir des informations d'intérêt général. Les renseignements demandés par la requérante étaient « prêts et disponibles » et ne nécessitaient aucune collecte de données. Dans de telles circonstances, l'État avait l'obligation de ne pas entraver la circulation des informations demandées. En résumé, la CouEDH a considéré que les obstacles conçus pour empêcher l'accès à des informations d'intérêt général étaient de nature à dissuader les personnes travaillant dans le secteur des médias et d'autres secteurs connexes d'exercer leur rôle essentiel de « organisme de surveillance pour la société ». La CouEDH a conclu à une violation de l'article 10.

35 Voir, toutefois, le détail des délibérations dans Contrôleur européen de la protection des données (CEPD) (2011), *Accès du public aux documents contenant des données à caractère personnel après l'arrêt rendu dans l'affaire* Bavarian Lager, Bruxelles, 24 mars 2011, disponibles à l'adresse : www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_FR.pdf.

36 CouEDH, *Társaság a Szabadságjogokért c. Hongrie*, n° 37374/05, 14 avril 2009 ; voir paras. 27, 36, 37 et 38.

Dans le droit de l'UE, l'importance de la transparence est fermement établie. Le principe de la transparence est consacré aux articles 1 et 10 du TUE et à l'article 15, paragraphe 1, du TFUE[37]. Aux termes du considérant 2 du règlement (CE) n° 1049/2001, la transparence permet d'assurer une meilleure participation des citoyens au processus décisionnel, ainsi que de garantir une plus grande légitimité, efficacité et responsabilité de l'administration à l'égard des citoyens dans un système démocratique[38].

Suivant ce raisonnement, le règlement (CE) n° 1290/2005 du Conseil relatif au financement de la politique agricole commune et le règlement (CE) n° 259/2008 de la Commission portant modalités de son application requièrent la publication d'informations sur les bénéficiaires de certains fonds européens dans le secteur agricole et des montants perçus par chaque bénéficiaire[39]. La publication doit contribuer au contrôle public de l'utilisation appropriée de fonds publics par l'administration. La proportionnalité de cette publication a été contestée par plusieurs bénéficiaires.

Exemple : dans les affaires jointes *Volker und Markus Schecke et Hartmut Eifert c. Land Hessen*[40], la CJUE devait se prononcer sur la proportionnalité de la publication, requise par la législation européenne, du nom des bénéficiaires d'aides agricoles européennes, et des montants qu'ils avaient reçus.

La Cour, relevant que le droit à la protection des données n'est pas une prérogative absolue, a soutenu que la publication sur un site internet des données nominatives relatives aux bénéficiaires de deux fonds agricoles européens et aux montants précis perçus par ceux-ci constitue une ingérence dans leur vie privée en général, et dans la protection de leurs données à caractère personnel, en particulier.

La Cour a considéré qu'une telle atteinte aux articles 7 et 8 de la Charte était prévue par la loi et répondait à un objectif d'intérêt général reconnu par l'UE, à

37 UE (2012), versions consolidées du TUE et du TFUE, JO 2012 C 326.

38 CJUE, C-41/00 P, *Interporc Im- und Export GmbH c. Commission des Communautés européennes*, 6 mars 2003, para. 39 ; et CJUE, C-28/08 P, *Commission européenne c. The Bavarian Lager Co. Ltd.*, 29 juin 2010, para. 54.

39 Règlement (CE) n° 1290/2005 du Conseil du 21 juin 2005 relatif au financement de la politique agricole commune, JO 2005 L 209 ; et règlement (CE) n° 259/2008 de la Commission du 18 mars 2008 portant modalités d'application du règlement (CE) n° 1290/2005 du Conseil en ce qui concerne la publication des informations relatives aux bénéficiaires de fonds en provenance du Fonds européen agricole de garantie (FEAGA) et du Fonds européen agricole pour le développement rural (Feader), JO 2008 L 76.

40 CJUE, affaires jointes C-92/09 et C-93/09, *Volker und Markus Schecke GbR et Hartmut Eifert c. Land Hessen*, 9 novembre 2010, paras. 47 à 52, 58, 66 et 67, 75, 86 et 92.

savoir accroître la transparence de l'utilisation des fonds communautaires. Toutefois, la CJUE a considéré que la publication des noms des personnes physiques bénéficiaires des aides agricoles européennes relevant de ces deux fonds, et du montant exact reçu, constituait une mesure disproportionnée et n'était pas justifiée au regard de l'article 52, paragraphe 1, de la Charte. La Cour a donc jugé partiellement nulle la législation européenne sur la publication d'informations relatives aux bénéficiaires de fonds agricoles européens.

1.2.3. Liberté des arts et des sciences

Un autre droit qui doit être mis en balance avec le droit au respect de la vie privée et à la protection des données est la liberté des arts et des sciences, explicitement protégée par l'article 13 de la Charte. Ce droit découle principalement du droit à la liberté de pensée et d'expression et il s'exerce au regard de l'article 1 de la Charte (dignité humaine). La CouEDH considère que la liberté des arts est protégée par l'article 10 de la CEDH[41]. Le droit garanti par l'article 13 de la Charte peut aussi faire l'objet de restrictions autorisées par l'article 10 de la CEDH[42].

Exemple : dans l'affaire *Vereinigung bildender Künstler c. Autriche*[43], les juridictions autrichiennes ont interdit à l'association requérante de continuer à exposer un tableau contenant des photos des visages de diverses personnalités publiques dans des positions à connotation sexuelle. Un parlementaire autrichien, dont la photo avait été utilisée dans le tableau, avait engagé des poursuites contre l'association requérante, demandant l'interdiction d'exposer le tableau. La juridiction nationale a fait droit à sa demande et a délivré une injonction. La CouEDH a rappelé que l'article 10 de la CEDH s'applique à la communication d'idées heurtant, choquant ou inquiétant l'État ou une fraction quelconque de la population. Ceux qui créent, interprètent, diffusent ou exposent une œuvre d'art contribuent à l'échange d'idées et d'opinions, et l'État a l'obligation de ne pas empiéter indûment sur leur liberté d'expression. Dans la mesure où le tableau était un collage et utilisait uniquement des photos de visages de personnes, leur corps étant peint de manière irréaliste et exagérée, ce qui n'avait manifestement pas pour but de refléter, ni même de suggérer, une réalité ; la CouEDH a également précisé que l'on pouvait « difficilement considérer que le

41 CouEDH, *Müller et autres c. Suisse*, n° 10737/84, 24 mai 1988.

42 Explications relatives à la Charte des droits fondamentaux, JO 2007 C 303.

43 CouEDH, *Vereinigung bildender Künstler c. Autriche*, n° 68345/01, 25 janvier 2007 ; voir notamment paras. 26 et 34.

tableau décrit des détails de la vie privée [de la personne dépeinte] ; [mais] plutôt qu'il se rapporte à la situation de celui-ci : un homme politique », et que « en cette qualité, [la personne dépeinte] doit faire preuve d'une plus grande tolérance à l'égard de la critique ». Pondérant les différents intérêts en jeu, la CouEDH a retenu que l'interdiction illimitée de toute nouvelle exposition du tableau était disproportionnée. La CouEDH a conclu à une violation de l'article 10 de la CEDH.

S'agissant des sciences, le droit européen en matière de protection des données connaît la valeur particulière des sciences pour la société. Par conséquent, les restrictions générales à l'usage de données à caractère personnel sont moindres. La directive relative à la protection des données et la Convention 108 permettent toutes deux la conservation de données pour des recherches scientifiques lorsqu'elles ne sont plus nécessaires dans le but initial de leur collecte. En outre, l'utilisation ultérieure de données à caractère personnel pour des recherches scientifiques n'est pas considérée comme une finalité incompatible. Il appartient au législateur national de développer des dispositions plus détaillées, y compris les garanties nécessaires, pour concilier les intérêts de la recherche scientifique et le droit à la protection des données (voir également Sections 3.3.3 et 8.4).

1.2.4. Protection de la propriété

Le droit à la protection de la propriété est consacré à l'article 1 du premier protocole à la CEDH et à l'article 17, paragraphe 1, de la Charte. Un aspect important du droit à la propriété est la protection de la propriété intellectuelle, explicitement mentionnée à l'article 17, paragraphe 2, de la Charte. Il existe plusieurs directives dans l'ordre juridique européen, qui visent à protéger efficacement la propriété intellectuelle, en particulier le droit d'auteur. La propriété intellectuelle couvre non seulement la propriété littéraire et artistique, mais également les droits de brevets, marques et associés.

Ainsi qu'il ressort clairement de la jurisprudence de la CJUE, la protection du droit fondamental à la propriété doit être mise en balance avec la protection d'autres droits fondamentaux, en particulier avec le droit à la protection des données[44]. Dans certaines affaires, des organismes de protection du droit d'auteur ont réclamé des fournisseurs d'accès à Internet qu'ils divulguent l'identité d'utilisateurs de plateformes de partage de fichiers en ligne. De telles plateformes permettent à des internautes

44 CouEDH, *Ashby Donald et autres c. France*, n° 36769/08, 10 janvier 2013.

de télécharger gratuitement des titres musicaux, alors même que ces titres sont protégés par le droit d'auteur.

Exemple : l'affaire *Promusicae c. Telefónica de España*[45] concernait le refus d'un fournisseur d'accès internet espagnol, Telefónica, de communiquer à Promusicae, une organisation à but non lucratif de producteurs et éditeurs d'enregistrements musicaux et audiovisuels, les données à caractère personnel concernant certaines personnes auxquelles il avait fourni des services d'accès à Internet. Promusicae avait demandé la communication des informations afin de pouvoir engager des poursuites au civil contre ces personnes qui, selon elle, utilisaient un programme d'échange de fichiers donnant accès à des phonogrammes dont les droits d'exploitation étaient détenus par des membres de Promusicae.

La juridiction espagnole a renvoyé l'affaire devant la CJUE, demandant si de telles données à caractère personnel devaient être communiquées, en vertu du droit communautaire, dans le contexte de procédures civiles destinées à assurer la protection effective du droit d'auteur. Elle a fait référence aux directives 2000/31, 2001/29 et 2004/48, également lues à la lumière des articles 17 et 47 de la Charte. La Cour a conclu que ces trois directives, ainsi que la directive vie privée et communications électroniques (directive 2002/58), n'empêchaient pas des États membres de prévoir, en vue d'assurer la protection effective du droit d'auteur, l'obligation de communiquer des données à caractère personnel dans le cadre d'une procédure civile.

La CJUE a souligné que l'affaire soulevait donc la question de la conciliation nécessaire des exigences liées à la protection de différents droits fondamentaux, à savoir, d'une part, le droit au respect de la vie privée et, d'autre part, les droits à la protection de la propriété et à un recours effectif.

La Cour a conclu qu'il incombait aux « États membres, lors de la transposition des directives susmentionnées, de veiller à se fonder sur une interprétation de ces dernières qui permette d'assurer un juste équilibre entre les différents droits fondamentaux protégés par l'ordre juridique communautaire. Ensuite, lors de la mise en œuvre des mesures de transposition de ces directives, il incombe aux autorités et aux juridictions des États membres, non seulement d'interpréter leur droit national d'une manière conforme auxdites directives, mais également

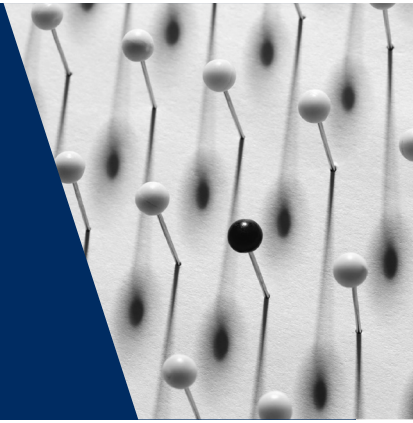
45 CJUE, C-275/06, *Productores de Música de España (Promusicae) c. Telefónica de España SAU*, 29 janvier 2008, paras. 54 et 60.

de veiller à ne pas se fonder sur une interprétation de celles-ci qui entrerait en conflit avec lesdits droits fondamentaux ou avec les autres principes généraux du droit communautaire, tels que le principe de proportionnalité »[46].

46 *Ibid.*, paras. 65 et 68 ; voir également CJUE, C-360/10, *SABAM c. Netlog N.V.*, 16 février 2012.

2

Terminologie de la protection des données



UE	Questions traitées	CdE
Données à caractère personnel		
Directive relative à la protection des données, article 2, point a) CJUE, affaires jointes C-92/09 et C93/09, *Volker und Markus Schecke GbR et Hartmut Eifert c. Land Hessen*, 9 novembre 2010 CJUE, C-275/06, *Productores de Música de España (Promusicae) c. Telefónica de España SAU*, 29 janvier 2008	**Définition juridique**	Convention 108, article 2, point a) CouEDH, *Bernh Larsen Holding AS et autres c. Norvège*, n° 24117/08, 14 mars 2013
Directive relative à la protection des données, article 8, paragraphe 1 CJUE, C-101/01, *Bodil Lindqvist*, 6 novembre 2003	**Catégories particulières de données à caractère personnel (données sensibles)**	Convention 108, article 6
Directive relative à la protection des données, article 6, paragraphe 1, point e)	**Données anonymisées et pseudonymisées**	Convention 108, article 5, point e) Convention 108, rapport explicatif, article 42
Traitement de données		
Directive relative à la protection des données, article 2, point b) CJUE, C-101/01, *Bodil Lindqvist*, 6 novembre 2003	**Définitions**	Convention 108, article 2, point c)

Utilisateurs de données		
Directive relative à la protection des données, article 2, point b)	**Responsable du traitement**	Convention 108, article 2, point d) Recommandation profilage, article 1, point g)*
Directive relative à la protection des données, article 2, point e) CJUE, C-101/01, *Bodil Lindqvist*, 6 novembre 2003	**Sous-traitant**	Recommandation profilage, article 1, point h)
Directive relative à la protection des données, article 2, point g)	**Destinataire**	Convention 108, protocole additionnel, article 2, paragraphe 1
Directive relative à la protection des données, article 2, point f)	**Tiers**	
Consentement		
Directive relative à la protection des données, article 2, point h) CJUE, C-543/09, *Deutsche Telekom AG c. Bundesrepublik Deutschland*, 5 mai 2011	**Définition et exigences applicables à un consentement valable**	Recommandation relative à la protection des données médicales, article 6, et diverses recommandations ultérieures

Note : * *Conseil de l'Europe, Comité des Ministres (2010), Recommandation Rec (2010) 13 sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage (recommandation profilage), 23 novembre 2010.*

2.1. Données à caractère personnel

Points clés

- Les données sont des données à caractère personnel dès lors qu'elles portent sur une personne identifiée ou identifiable, la personne concernée.
- Une personne est identifiable si des informations complémentaires peuvent être obtenues sans effort déraisonné, permettant l'identification de la personne concernée.
- L'authentification s'entend du fait de démontrer qu'une certaine personne possède une certaine identité et/ou est autorisée à exercer certaines activités.
- Il existe des catégories particulières de données, appelées « données sensibles », énumérées dans la Convention 108 et dans la directive relative à la protection des données, qui requièrent une protection accrue et, par conséquent, sont soumises à un régime juridique spécial.

- Les données sont anonymisées si elles ne contiennent plus d'identifiants; elles sont pseudonymisées si les identifiants sont cryptés.
- Contrairement aux données anonymisées, les données pseudonymisées sont des données à caractère personnel.

2.1.1. Principaux aspects de la notion de données à caractère personnel

Dans le droit de l'UE tout comme dans le **droit du CdE**, les « données à caractère personnel » sont définies comme des informations concernant une personne physique identifiée ou identifiable[47], c'est-à-dire des informations sur une personne dont l'identité est manifestement claire ou peut au moins être établie par l'obtention d'informations complémentaires.

Si des données sur une telle personne font l'objet d'un traitement, cette personne est appelée la « personne concernée ».

Une personne

Le droit à la protection des données découle du droit au respect de la vie privée. Le concept de vie privée est lié aux êtres humains. Les personnes physiques sont donc les principales bénéficiaires de la protection des données. En outre, selon l'avis du groupe de travail Article 29, seule une *personne vivante* est protégée par le droit européen en matière de protection des données[48].

La jurisprudence de la CouEDH concernant l'article 8 de la CEDH montre qu'il peut être difficile de séparer totalement les affaires de vie privée et de vie professionnelle[49].

Exemple : dans l'affaire *Amann c. Suisse*[50], les autorités avaient intercepté un appel téléphonique professionnel au requérant. Sur la base de cet appel, les autorités avaient enquêté sur le requérant et rédigé une fiche à son sujet pour

47 Directive relative à la protection des données, art. 2, point a) ; Convention 108, art. 2, point a).

48 Groupe de travail Article 29 (2007), Avis 4/2007 sur le concept de données à caractère personnel, WP 136, 20 juin 2007, p. 22.

49 Voir, par exemple, CouEDH, *Rotaru c. Roumanie [GC]*, n° 28341/95, 4 mai 2000, para. 43 ; CouEDH, *Niemitz c. Allemagne*, n° 13710/88, 16 décembre 1992, para. 29.

50 CouEDH, *Amann c. Suisse* [GC], n° 27798/95, 16 février 2000, para. 65.

le fichier national destiné à assurer la protection de l'État. Bien que l'interception concernait un appel téléphonique professionnel, la CouEDH a considéré que la sauvegarde des données relatives à cet appel touchait à la vie privée du requérant. Elle a souligné que le terme « vie privée » ne devait pas être interprété de façon restrictive, en particulier dans la mesure où le respect de la vie privée englobe le droit pour l'individu de nouer et de développer des relations avec ses semblables. De surcroît, aucune raison de principe ne permettait d'exclure les activités professionnelles ou commerciales de la notion de « vie privée ». Cette interprétation large correspondait à celle qui était formulée dans la Convention 108. La CouEDH a également retenu que l'ingérence, dans le cas du requérant, n'était pas prévue par la loi puisque la législation nationale ne contenait pas de dispositions claires et détaillées sur la collecte, l'enregistrement et la conservation de tels renseignements. Elle a donc conclu à une violation de l'article 8 de la CEDH.

Par ailleurs, si des questions liées à la vie professionnelle peuvent aussi faire l'objet d'une protection des données, il semble contestable que seules les personnes physiques bénéficient d'une telle protection. Les droits conférés par la CEDH sont garantis non seulement aux personnes physiques, mais aussi à tout un chacun.

Il existe une jurisprudence de la CouEDH statuant sur des recours de personnes morales invoquant une violation de leur droit à la protection contre l'utilisation de leurs données en vertu de l'article 8 de la CEDH. La CouEDH a, cependant, examiné l'affaire sous l'angle du droit au respect du domicile et de la correspondance, et non du droit à la vie privée :

Exemple : l'affaire *Bernh Larsen Holding AS et autres c. Norvège*[51] portait sur une plainte déposée par trois sociétés norvégiennes concernant une décision de l'administration fiscale leur ordonnant de remettre aux contrôleurs fiscaux une copie de toutes les données figurant sur un serveur informatique utilisé conjointement par les trois sociétés.

La CouEDH a considéré qu'une telle obligation imposée aux sociétés requérantes constituait une ingérence dans leurs droits au respect du « domicile » et de la « correspondance » au sens de l'article 8 de la CEDH. Mais la CouEDH a aussi considéré que l'administration fiscale disposait de garanties adéquates

51 CouEDH, *Bernh Larsen Holding AS et autres c. Norvège*, n° 24117/08, 14 mars 2013. Voir aussi, toutefois, CouEDH, *Liberty et autres c. Royaume-Uni*, n° 58243/00, 1er octobre 2008.

et suffisantes contre les abus : les sociétés requérantes avaient été informées longtemps à l'avance ; étaient présentes et en mesure de faire des observations pendant les interventions sur site ; et les documents devaient être détruits à l'issue de l'examen fiscal. Dans de telles circonstances, un juste équilibre avait été trouvé entre le droit des sociétés requérantes au respect du « domicile » et de la « correspondance » et leur intérêt à protéger la vie privée des personnes travaillant pour elles, d'une part, et l'intérêt public de garantir une inspection efficace à des fins d'évaluation fiscale, d'autre part. La CouEDH a donc exclu la violation de l'article 8.

Selon la Convention 108, la protection des données concerne principalement la protection des personnes physiques ; toutefois, les parties contractantes peuvent étendre la protection des données aux personnes morales, telles que les sociétés commerciales et les associations, dans leur droit national. De manière générale, le **droit européen en matière de protection des données** ne couvre pas la protection des personnes morales au regard du traitement des données les concernant. Les législateurs nationaux sont libres de réglementer sur ce sujet[52].

Exemple : dans l'affaire *Volker and Markus Schecke et Hartmut Eifert c. Land Hessen*[53], la CJUE, faisant référence à la publication de données à caractère personnel relatives à des bénéficiaires d'aides agricoles, a retenu que « les personnes morales ne peuvent se prévaloir de la protection des articles 7 et 8 de la Charte à l'égard d'une telle identification que dans la mesure où le nom légal de la personne morale identifie une ou plusieurs personnes physiques. [L]e respect du droit à la vie privée à l'égard du traitement des données à caractère personnel, reconnu par les articles 7 et 8 de la Charte, se rapporte à toute information concernant une personne physique identifiée ou identifiable (...) »[54].

Caractère identifiable d'une personne

Dans le droit de l'UE et dans le **droit du CdE**, une information contient des données sur une personne si :

- une personne est identifiée dans cette information ; ou

52 Directive relative à la protection des données, considérant 24.

53 CJUE, affaires jointes C-92/09 et C-93/09, *Volker und Markus Schecke GbR et Hartmut Eifert c. Land Hessen*, 9 novembre 2010, para. 53.

54 *Ibid.*, para. 52.

- si une personne, bien que non identifiée, est décrite dans cette information d'une manière permettant de découvrir qui est la personne concernée en menant d'autres recherches.

Les deux types d'informations sont protégés de la même manière par le droit européen en matière de protection des données. La CouEDH a régulièrement déclaré que la notion de « données à caractère personnel » au sens de la CEDH était la même que dans la Convention 108, en particulier concernant l'exigence selon laquelle elles doivent concerner des personnes identifiées ou identifiables[55].

Les définitions juridiques des données à caractère personnel ne donnent pas plus de précisions quant à savoir quand une personne est considérée comme identifiée[56]. De toute évidence, l'identification requiert des éléments qui décrivent une personne de telle façon qu'elle peut être distinguée de toutes les autres personnes et reconnue comme un individu. Le nom d'une personne est un exemple majeur de tels éléments descriptifs. Dans certains cas exceptionnels, d'autres identifiants peuvent avoir un effet similaire à un nom. Par exemple, il peut être suffisant, pour les personnes publiques, de faire référence à la fonction de la personne, comme « président de la Commission européenne ».

Exemple : dans l'affaire *Promusicae*[57], la CJUE a indiqué : « il n'est par ailleurs pas contesté que la communication, sollicitée par Promusicae, des noms et des adresses de certains utilisateurs [d'une certaine plate-forme de partage de fichiers en ligne] implique la mise à disposition de données à caractère personnel, c'est-à-dire d'informations sur des personnes physiques identifiées ou identifiables, conformément à la définition figurant à l'article 2, point a), de la directive 95/46 [...]. Cette communication d'informations qui, selon Promusicae, sont stockées par Telefónica – ce que cette dernière ne conteste pas –, constitue un traitement de données à caractère personnel, au sens de l'article 2, premier alinéa, de la directive 2002/58, lu conjointement avec l'article 2, sous b), de la directive 95/46 ».

55 Voir CouEDH, *Amann c. Suisse* [GC], n° 27798/95, 16 février 2000, para. 65 et autres.

56 Voir également CouEDH, *Odièvre c. France* [GC], n° 42326/98, 13 février 2003 ; et CouEDH, *Godelli c. Italie*, n° 33783/09, 25 septembre 2012.

57 CJUE, C-275/06, *Productores de Música de España (Promusicae) c. Telefónica de España SAU*, 29 janvier 2008, para. 45.

Dans la mesure où de nombreux noms ne sont pas uniques, établir l'identité d'une personne peut nécessiter d'autres identifiants pour éviter toute confusion avec une autre. La date et le lieu de naissance sont souvent utilisés. En outre, des numéros personnalisés ont été introduits dans certains pays pour mieux distinguer les citoyens. À l'ère du numérique, les données biométriques, telles que les empreintes digitales, photos numériques ou aspects rétiniens, prennent de plus en plus d'importance dans l'identification des personnes.

Mais pour l'applicabilité du droit européen en matière de protection des données, une identification de qualité de la personne concernée n'est cependant pas nécessaire ; il suffit que celle-ci soit identifiable. Une personne est considérée comme identifiable si des renseignements contiennent des éléments d'identification qui peuvent permettre de l'identifier, directement ou indirectement[58]. Conformément au considérant 26 de la directive relative à la protection des données, la référence consiste à savoir s'il est probable que des moyens raisonnables d'identification seront disponibles et gérés par les utilisateurs prévisibles des informations, ce qui inclut également les tiers destinataires (voir Section 2.3.2).

Exemple : une autorité locale décide de collecter des données sur les voitures roulant à grande vitesse dans les rues de la ville. Elle photographie les voitures, enregistrant automatiquement le lieu et l'endroit, afin de transmettre les données à l'autorité compétente pour que celle-ci puisse verbaliser les personnes ne respectant pas les limitations de vitesse. Une personne concernée porte plainte, affirmant que la législation relative à la protection des données ne contenait aucune base juridique autorisant l'autorité locale à collecter ces données. L'autorité locale soutient qu'elle ne collecte pas de données à caractère personnel. Les plaques d'immatriculation, selon elle, sont des données relatives à des personnes anonymes. L'autorité locale n'a pas légalement le pouvoir d'accéder au registre général des véhicules pour découvrir l'identité du propriétaire ou du conducteur du véhicule.

Ce raisonnement n'est pas conforme au considérant 26 de la directive relative à la protection des données. Dans la mesure où la finalité de la collecte des données est manifestement d'identifier et de verbaliser les contrevenants, il est prévisible qu'il y aura tentative d'identification. Bien que les autorités locales ne disposent pas de moyens d'identification, elles transmettront les données

58 Directive relative à la protection des données, art. 2, point a).

à l'autorité compétente, la police qui, elle, en a les moyens. Le considérant 26 inclut d'ailleurs explicitement un scénario dans lequel il est prévisible que d'autres destinataires des données, différents de l'utilisateur immédiat des données, puissent tenter d'identifier la personne. À la lumière du considérant 26, l'action de l'autorité locale correspond à une collecte de données relatives à des personnes identifiables et, par conséquent, requiert une base légale dans le droit en matière de protection des données.

Dans le droit du CdE, le caractère identifiable est compris de la même façon. L'article 1, paragraphe 2, de la recommandation sur les données de paiement[59], par exemple, indique qu'une personne physique n'est pas considérée comme « identifiable » si cette identification nécessite des délais, des coûts et des activités déraisonnables.

Authentification

L'authentification est la procédure par laquelle une personne peut prouver qu'elle possède une certaine identité et/ou est autorisée à faire certaines choses, comme pénétrer dans une zone de sécurité ou retirer de l'argent d'un compte bancaire. L'authentification peut être obtenue par la comparaison de données biométriques (une photo ou les empreintes digitales d' un passeport) avec les données de la personne qui se présente à un contrôle d'immigration, par exemple ; en demandant des informations que seule la personne possédant une certaine identité ou autorisation devrait connaître, telles qu'un numéro d'identification personnel (PIN) ou un mot de passe ; ou en demandant la présentation d'un certain objet qui devrait exclusivement se trouver en la possession de la personne ayant une certaine identité ou autorisation, comme une carte magnétique spéciale ou la clé d'un coffre en banque. Outre les mots de passe ou cartes magnétiques, parfois associés à des codes PIN, les signatures électroniques sont un outil particulièrement utile pour identifier ou authentifier une personne dans des communications électroniques.

Nature des données

Tout type d'informations peut constituer des données à caractère personnel dès lors qu'elles concernent une personne.

59 CdE, Comité des Ministres (1990), Recommandation Rec (90) 19 sur la protection des données à caractère personnel utilisées à des fins de paiement et autres opérations connexes, 13 septembre 1990.

Exemple : l'évaluation par un supérieur hiérarchique du travail d'un salarié, enregistrée dans le dossier personnel du salarié, est une donnée à caractère personnel relative au salarié, quand bien même il est possible qu'elle ne reflète que tout ou partie de l'opinion personnelle du supérieur, par exemple : « le salarié n'est pas dévoué à son travail » et non des faits comme : « le salarié a été absent de son travail pendant cinq semaines au cours des six derniers mois ».

Les données à caractère personnel couvrent les informations relatives à la vie privée d'une personne, ainsi que les renseignements sur sa vie professionnelle ou publique.

Dans l'affaire *Amann*[60], la CouEDH avait interprété le terme « données à caractère personnel » comme n'étant pas limité aux affaires de la sphère privée d'un individu (voir Section 2.1.1). Cette signification du terme « données à caractère personnel » est aussi valable pour la directive relative à la protection des données :

Exemple : dans l'affaire *Volker und Markus Schecke et Hartmut Eifert c. Land Hessen*[61], la CJUE a indiqué : « demeure sans incidence le fait que les données publiées ont trait à des activités professionnelles [...]. La Cour européenne des droits de l'homme a jugé, à cet égard, concernant l'interprétation de l'article 8 de la CEDH, que les termes "vie privée" ne devaient pas être interprétés de façon restrictive et qu'aucune raison de principe ne permet d'exclure les activités professionnelles [...] de la notion de vie "privée" ».

Des données portent également sur des personnes si le contenu des informations révèle indirectement des informations sur une personne. Dans certains cas, lorsqu'il existe un lien étroit entre un objet ou un événement (par ex. téléphone potable, voiture, accident), d'une part, et une personne (par ex. son propriétaire, utilisateur, victime), d'autre part, des informations relatives à un objet ou un événement doivent aussi être considérées comme des données à caractère personnel.

Exemple : dans l'affaire *Uzun c. Allemagne*[62], le requérant et un autre homme avaient été placés sous surveillance grâce à un système de localisation GPS installé dans le véhicule du deuxième homme en raison de leur implication sup-

60 Voir CouEDH, *Amann c. Suisse*, n° 27798/95, 16 février 2000, para. 65.

61 CJUE, affaires jointes C-92/09 et C-93/09, *Volker und Markus Schecke GbR et Hartmut Eifert c. Land Hessen*, 9 novembre 2010, para. 59

62 CouEDH, *Uzun c. Allemagne*, n° 35623/05, 2 septembre 2010.

posée dans des attaques à la bombe. Dans cette affaire, la CouEDH a retenu que l'observation du requérant par GPS constituait une ingérence dans sa vie privée, telle que protégée par l'article 8 de la CEDH. Toutefois, la surveillance GPS était prévue par la loi, ainsi que proportionnée au but légitime d'enquête sur plusieurs chefs de tentative de meurtre et, par conséquent, elle était nécessaire dans une société démocratique. La CouEDH a exclu la violation de l'article 8 de la CEDH.

Forme de présentation des données

La forme sous laquelle les données à caractère personnel sont sauvegardées ou utilisées n'est pas pertinente pour l'applicabilité du droit en matière de protection des données. Des communications écrites ou orales peuvent contenir des données à caractère personnel ainsi que des images[63], y compris des séquences[64] ou des sons de télévision en circuit fermé (CCTV)[65]. Les informations enregistrées électroniquement, ainsi que les informations imprimées, peuvent être des données à caractère personnel ; des échantillons de cellules de tissu humain peuvent aussi être des données à caractère personnel, puisqu'ils enregistrent l'ADN d'une personne.

2.1.2. Catégories particulières de données à caractère personnel

Dans le droit de l'UE comme dans le **droit du CdE**, il existe des catégories particulières de données qui, par leur nature, peuvent faire courir un risque aux personnes concernées quand elles font l'objet d'un traitement et requièrent donc une protection accrue. Le traitement de ces catégories particulières de données (appelées « données sensibles ») ne doit donc être autorisé qu'avec des garanties spécifiques.

Sur la définition des données sensibles, la Convention 108 (article 6) et la directive relative à la protection des données (article 8) citent toutes deux les catégories suivantes :

63 CouEDH, *Von Hannover c. Allemagne*, n° 59320/00, 24 juin 2004 ; CouEDH, *Sciacca c. Italie*, n° 50774/99, 11 janvier 2005.

64 CouEDH, *Peck c. Royaume-Uni*, n° 44647/98, 28 janvier 2003 ; CouEDH, *Köpke c. Allemagne*, n° 420/07, 5 octobre 2010.

65 Directive relative à la protection des données, considérants 16 et 17 ; CouEDH, *P.G. et J.H. c. Royaume-Uni*, n° 44787/98, 25 décembre 2001, paras. 59 et 60 ; CouEDH, *Wisse c. France*, n° 71611/01, 20 décembre 2005.

- données à caractère personnel révélant l'origine raciale ou ethnique ;
- données à caractère personnel révélant les opinions politiques, convictions religieuses ou autres convictions ; et
- données à caractère personnel relatives à la santé ou à la vie sexuelle.

Exemple : dans l'affaire *Bodil Lindqvist*[66], la CJUE a précisé que « l'indication du fait qu'une personne s'est blessée au pied et est en congé de maladie partiel constitue une donnée à caractère personnel relative à la santé, au sens de l'article 8, paragraphe 1, de la directive 95/46 ».

La directive relative à la protection des données cite en plus l'« appartenance syndicale » comme donnée sensible, cette information pouvant être un indicateur fort d'une conviction politique ou d'une affiliation.

La Convention 108 considère également comme sensibles les données à caractère personnel concernant des condamnations pénales.

L'article 8, paragraphe 7, de la directive relative à la protection des données impose aux États membres de l'UE de déterminer « les conditions dans lesquelles un numéro national d'identification ou tout autre identifiant de portée générale peut faire l'objet d'un traitement ».

2.1.3. Données anonymisées et pseudonymisées

Selon le principe de la conservation des données pendant une durée limitée, inscrit dans la directive relative à la protection des données comme dans la Convention 108 (et évoqué plus en détail au Chapitre 3), les données doivent être conservées « sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement »[67]. Par conséquent, il pourrait être nécessaire d'anonymiser des données si un responsable du traitement souhaite les conserver alors qu'elles ne sont plus d'actualité et qu'elles ne servent plus leur finalité initiale.

66 CJUE, C-101/01, *Bodil Lindqvist*, 6 novembre 2003, para. 51.

67 Directive relative à la protection des données, art. 6, para. 1, point e) ; et Convention 108, art. 5, point e).

Données anonymisées

Des données sont anonymisées si tous les éléments identifiants ont été supprimés d'un ensemble de données à caractère personnel. Les informations ne doivent plus contenir aucun élément qui soit susceptible, au moyen d'un effort raisonnable, de servir à réidentifier la ou les personnes concernées[68]. Lorsque des données ont été correctement anonymisées, elles ne sont plus des données à caractère personnel.

Si des données à caractère personnel ne servent plus leur finalité initiale, mais sont conservées sous une forme personnalisée à des fins historiques, statistiques ou scientifiques, la directive relative à la protection des données et la Convention 108 autorisent une telle conservation à condition qu'il existe des garanties appropriées contre les abus[69].

Données pseudonymisées

Les informations personnelles contiennent des identifiants, tels que le nom, la date de naissance, le sexe ou l'adresse. Lorsque des informations personnelles sont pseudonymisées, les identifiants sont remplacés par un pseudonyme. La pseudonymisation est notamment obtenue par cryptage des identifiants figurant dans les données à caractère personnel.

Les données pseudonymisées ne sont pas expressément mentionnées dans les définitions légales de la Convention 108 ou de la directive relative à la protection des données. Toutefois, le rapport explicatif sur la Convention 108 précise, en son article 42, que « [l]'exigence [...] concernant la durée limitée de la conservation des données sous leur forme nominative ne signifie pas qu'elles doivent être, après quelque temps, définitivement dissociées du nom de la personne à laquelle elles se réfèrent, mais seulement qu'il ne doit pas être possible de relier facilement les données et les identifiants ». Cet effet peut être obtenu par la pseudonymisation des données. Pour quiconque ne possède pas la clé de décryptage, les données pseudonymisées peuvent être difficilement identifiables. Le lien avec l'identité demeure sous la forme du pseudonyme associé à la clé de décryptage. Pour toute personne habilitée à utiliser la clé de décryptage, une nouvelle identification est possible aisément. Il convient de veiller particulièrement à éviter toute utilisation de clés de cryptage par des personnes non autorisées.

68 *Ibid.*, considérant 26.

69 *Ibid.*, art. 6, para. 1, point e) ; et Convention 108, art. 5, point e).

Dans la mesure où la pseudonymisation des données est l'un des moyens les plus importants pour obtenir une protection des données à grande échelle, la logique et l'effet d'une telle action doivent être expliqués plus en détail quand il n'est pas possible d'éviter totalement l'utilisation de données à caractère personnel.

Exemple : la phrase « Charles Spencer, né le 3 avril 1967, est le père d'une famille de quatre enfants, deux garçons et deux filles » peut par exemple être pseudonymisée comme suit :

« C.S. 1967 est le père d'une famille de quatre enfants, deux garçons et deux filles » ; ou

« 324 est le père d'une famille de quatre enfants, deux garçons et deux filles » ; ou

« YESz320l est le père d'une famille de quatre enfants, deux garçons et deux filles ».

Les utilisateurs accédant à ces données pseudonymisées ne pourront généralement pas identifier « Charles Spencer, né le 3 avril 1967 » à partir de « 324 » ou « YESz320l ». Les données pseudonymisées sont donc probablement mieux protégées contre les abus.

Mais le premier exemple est le moins sûr. Si la phrase « C.S. 1967 est le père d'une famille de quatre enfants, deux garçons et deux filles » est utilisée dans le petit village où vit Charles Spencer, M. Spencer pourra facilement être reconnu. La méthode de pseudonymisation affecte l'efficacité de la protection des données.

Des données à caractère personnel contenant des identifiants cryptés sont utilisées dans de nombreux contextes comme moyen de préserver la confidentialité de l'identité de certaines personnes. Cela est particulièrement utile quand des responsables du traitement de données doivent s'assurer qu'ils s'intéressent aux mêmes personnes concernées, mais n'ont pas besoin, ou ne devraient pas avoir besoin, de connaître les véritables identités des personnes concernées. C'est le cas, par exemple, quand un chercheur étudie l'évolution d'une maladie chez des patients dont l'identité est connue du seul hôpital où ils sont traités et auprès duquel le chercheur obtient les historiques pseudonymisés. La pseudonymisation est donc un lien fort dans l'arsenal des technologies renforçant la protection de la vie privée. Elle peut représenter un élément important dans la mise en œuvre de

la vie privée dès la conception (« *privacy by design* »), ce qui requiert que la protection des données soit intégrée au maillage de systèmes avancés de protection des données.

2.2. Traitement de données

Points clés

- Le terme « traitement » fait principalement référence au traitement automatisé.
- Dans le droit de l'UE, le « traitement » fait également référence au traitement manuel dans des systèmes d'archivage structurés.
- Dans le droit du CdE, le sens du mot « traitement » peut être élargi par la législation nationale pour inclure le traitement manuel.

La protection des données en vertu de la Convention 108 et de la directive relative à la protection des données est principalement axée sur le traitement automatisé de données.

Dans le **droit du CdE**, la définition du traitement automatisé reconnaît cependant que certaines étapes de l'utilisation manuelle de données à caractère personnel peuvent s'avérer nécessaires entre des opérations automatisées. De même, dans le **droit de l'UE**, le traitement automatisé de données est défini comme des « opérations effectuées sur des données à caractère personnel en totalité ou en partie à l'aide de procédés automatisés »[70].

Exemple : dans l'affaire *Bodil Lindqvist*[71], la CJUE a retenu ce qui suit :

« L'opération consistant à faire référence, sur une page internet, à diverses personnes et à les identifier soit par leur nom, soit par d'autres moyens, par exemple leur numéro de téléphone ou des informations relatives à leurs conditions de travail et à leurs passe-temps, constitue un "traitement de données à caractère personnel, automatisé en tout ou en partie", au sens de l'article 3, paragraphe 1, de la directive 95/46. »

70 Convention 108, art. 2, point c) ; et directive relative à la protection des données, art. 2, point b), et art. 3, para. 1.

71 CJUE, C-101/01, *Bodil Lindqvist*, 6 novembre 2003, para. 27.

Le traitement manuel de données requiert également une protection.

La protection des données, dans le **droit de l'UE,** n'est nullement limitée au traitement automatisé de données. Par conséquent, dans le droit de l'UE, la protection des données s'applique au traitement de données à caractère personnel dans un système manuel d'archivage, c'est-à-dire un dossier papier structuré de manière spécifique[72]. La raison de cette extension de la protection des données est que :

- les dossiers papier peuvent être structurés d'une façon rendant l'obtention d'informations facile et simple ; et

- la sauvegarde de données à caractère personnel dans des dossiers papier structurés facilite le contournement des restrictions énoncées par la législation pour le traitement automatisé de données[73].

Dans le droit du CdE, la Convention 108 réglemente principalement le traitement de données dans des fichiers automatisés de données[74]. Mais elle prévoit aussi la possibilité d'étendre la protection au traitement manuel dans la législation nationale. De nombreuses parties à la Convention 108 ont fait usage de cette possibilité et formulé des déclarations à cette fin au Secrétaire général du CdE[75]. L'extension de la protection des données en vertu d'une telle déclaration doit concerner tous les traitements manuels de données et ne peut se limiter au traitement dans des systèmes manuels d'archivage[76].

S'agissant de la nature des opérations de traitement en question, le concept de traitement est étendu, **tant dans le droit de l'UE que dans le droit du CdE** : « "traitement de données à caractère personnel" (...) désigne toute opération (...) telle que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction »[77] appliquée à des données à caractère personnel. Le terme « traitement » comprend également les actions dans

72 Directive relative à la protection des données, art. 3, para. 1.

73 *Ibid.*, considérant 27.

74 Convention 108, art. 2, point b).

75 Voir les déclarations faites au titre de la Convention 108, art. 3, para. 2, point c).

76 Voir les termes de la Convention 108, art. 3, para. 2.

77 Directive relative à la protection des données, art. 2, point b). De même, voir Convention 108, art. 2, point c).

le cadre desquelles les données ne relèvent plus des obligations d'un responsable du traitement et sont transférées aux obligations d'un autre responsable du traitement.

Exemple : des employeurs collectent et traitent des données relatives à leurs salariés, y compris des informations concernant leurs salaires. Le fondement juridique qui rend cette opération légitime est le contrat de travail.

Les employeurs doivent transmettre les données salariales de leur personnel à l'administration fiscale. Ce transfert de données sera aussi considéré comme un « traitement » au sens de la Convention 108 et de la directive. Le fondement juridique de cette communication n'est toutefois pas le contrat de travail. Il doit exister un autre fondement juridique aux traitements entraînant le transfert de données salariales de l'employeur à l'administration fiscale. Cette base légale est généralement contenue dans les dispositions de la législation fiscale nationale. En l'absence de telles dispositions, le transfert de données constitue un traitement illicite.

2.3. Les utilisateurs de données à caractère personnel

Points clés

- Quiconque décide de traiter les données à caractère personnel de tierces personnes est un « responsable du traitement » au sens du droit en matière de protection des données ; si plusieurs personnes prennent cette décision collectivement, elles peuvent être des « responsables conjoints du traitement ».
- Un « sous-traitant » est une entité légalement distincte qui traite des données à caractère personnel pour le compte d'un responsable du traitement.
- Un sous-traitant devient un responsable du traitement s'il utilise des données à ses propres fins, sans suivre les instructions d'un responsable du traitement.
- Toute personne qui reçoit des données de la part d'un responsable du traitement est un « destinataire ».
- Un « tiers » est une personne physique ou morale qui n'agit pas sur les instructions du responsable du traitement (et qui n'est pas la personne concernée).
- Un « tiers destinataire » est une personne ou entité qui est légalement distincte du responsable du traitement, mais qui reçoit des données à caractère personnel de la part de ce dernier.

2.3.1. Responsables du traitement et sous-traitants

La conséquence la plus importante de la fonction de responsable du traitement ou de sous-traitant est l'obligation légale de respecter les obligations respectives prévues par le droit en matière de protection des données. Seules les personnes qui peuvent être tenues responsables en vertu du droit applicable peuvent donc exercer cette fonction. Dans le secteur privé, il s'agit habituellement d'une personne physique ou morale ; dans le secteur public, d'une autorité. D'autres entités, telles que des organes ou institutions sans personnalité juridique, ne peuvent être responsables du traitement ou agir en tant que sous-traitants que si des dispositions légales particulières le permettent.

Exemple : si le service marketing de la société Sunshine envisage de traiter des données pour une étude de marché, c'est la société Sunshine, et non le service marketing, qui sera le responsable de ce traitement. Le service marketing ne peut pas être le responsable du traitement parce qu'il n'a pas de personnalité juridique distincte.

Dans des groupes de sociétés, la société-mère et chaque société affiliée, dans la mesure où il s'agit de personnes morales distinctes, constituent des responsables du traitement et des sous-traitants distincts. Du fait de ce statut juridiquement distinct, le transfert de données entre les membres d'un groupe de sociétés requiert une base légale particulière. Il n'existe aucun privilège permettant l'échange de données à caractère personnel en tant que tel entre les entités légales distinctes au sein du groupe.

Le rôle de particuliers doit être mentionné dans ce contexte. **Dans le droit de l'UE**, les particuliers qui traitent des données relatives à des tiers dans le cadre d'une activité purement personnelle ou domestique ne relèvent pas des règles de la directive relative à la protection des données ; ils ne sont pas considérés comme des responsables du traitement[78].

Toutefois, la jurisprudence a retenu que le droit en matière de protection des données doit néanmoins s'appliquer lorsqu'une personne privée publie des données sur des tiers dans le cadre de l'utilisation d'Internet.

78 Directive relative à la protection des données, considérant 12 et art. 3, para. 2, dernier tiret.

Exemple : dans l'affaire *Bodil Lindqvist*[79], la CJUE a retenu que :

« L'opération consistant à faire référence, sur une page internet, à diverses personnes et à les identifier soit par leur nom, soit par d'autres moyens (...) constitue un "traitement de données à caractère personnel, automatisé en tout ou en partie", au sens de l'article 3, paragraphe 1, de la directive 95/46[80] ».

Un tel traitement de données ne relève pas d'activités purement personnelles ou domestiques, qui échappent au champ d'application de la directive relative à la protection des données, dans la mesure où cette exception « doit (...) être interprétée comme visant uniquement les activités qui s'insèrent dans le cadre de la vie privée ou familiale des particuliers, ce qui n'est manifestement pas le cas du traitement de données à caractère personnel consistant dans leur publication sur Internet de sorte que ces données sont rendues accessibles à un nombre indéfini de personnes[81] ».

Responsable du traitement

Dans le droit de l'UE, un responsable du traitement est défini comme une personne qui « seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel[82] ». La décision d'un responsable du traitement explique pourquoi et comment des données doivent être traitées. **Dans le droit du CdE**, la définition du responsable du traitement (appelé « maître du fichier ») mentionne, en outre, que celui-ci décide des catégories de données à caractère personnel qui doivent être enregistrées[83].

Dans sa définition du responsable du traitement, la Convention 108 fait référence à un autre aspect de la responsabilité qu'il convient de relever. Cette définition pose la question de la personne légalement autorisée à traiter certaines données à une certaine fin. Toutefois, en cas de traitements prétendument illicites, lorsqu'il faut identifier le responsable du traitement, c'est la personne ou l'entité, telle qu'une entreprise ou une autorité, qui a décidé que les données devaient être traitées,

79 CJUE, C-101/01, *Bodil Lindqvist*, 6 novembre 2003.

80 *Ibid.*, para. 27.

81 *Ibid.*, para. 47.

82 Directive relative à la protection des données, art. 2, point d).

83 Convention 108, art. 2, point d).

peu importe qu'elle soit légalement habilitée à le faire ou non[84], qui est considérée comme le responsable du traitement. Une demande de suppression doit donc toujours être adressée au responsable « de fait » du traitement.

Responsabilité conjointe

La définition du « responsable du traitement » dans la directive relative à la protection des données dispose qu'il peut également y avoir plusieurs entités légalement distinctes qui agissent ensemble ou conjointement avec des tiers comme responsables du traitement. Cela signifie qu'elles décident ensemble de traiter des données à des fins communes[85]. Toutefois, cela n'est légalement possible que dans les cas où une base légale spéciale prévoit le traitement des données de façon conjointe à des fins communes.

Exemple : une base de données tenue conjointement par plusieurs établissements de crédit au sujet de leurs clients défaillants est un exemple courant de responsabilité conjointe. Lorsqu'une personne sollicite une ligne de crédit auprès d'une banque qui est l'un des responsables conjoints du traitement, les banques consultent la base de données pour les aider à prendre des décisions avisées sur la solvabilité du demandeur.

La réglementation ne précise pas explicitement si la responsabilité conjointe requiert que la finalité commune soit la même pour chaque responsable du traitement ou s'il suffit que leurs finalités coïncident en partie. Toutefois, il n'existe encore aucune jurisprudence au niveau européen et les conséquences en matière de responsabilité ne sont pas claires. Le groupe de travail Article 29 plaide en faveur d'une interprétation plus large de la notion de responsabilité conjointe afin de créer une certaine flexibilité permettant de faire face à la complexité croissante de la réalité actuelle du traitement de données[86]. Une affaire impliquant la Société de télécommunications interbancaires mondiales (SWIFT) illustre la position du groupe de travail.

Exemple : dans l'affaire « SWIFT », des établissements bancaires européens avaient employé SWIFT, initialement comme sous-traitant, pour procéder à

84 Voir également groupe de travail Article 29 (2010), *Avis* 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », WP 169, Bruxelles, 16 février 2010, p. 15.

85 Directive relative à la protection des données, art. 2, point d).

86 Groupe de travail Article 29 (2010), *Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant »*, WP 169, Bruxelles, 16 février 2010, p. 19.

des transferts de données dans le cadre de transactions bancaires. SWIFT avait divulgué ces données, conservées dans un centre informatique aux États-Unis, au département du Trésor des États-Unis, sans en avoir reçu l'instruction explicite des établissements bancaires européens qui l'employaient. Examinant la légalité de cette situation, le groupe de travail Article 29 était parvenu à la conclusion que les établissements bancaires européens employant SWIFT, ainsi que la société SWIFT elle-même, devaient être considérés comme des responsables conjoints du traitement, et devaient à ce titre répondre auprès des clients européens de la divulgation de leurs données aux autorités américaines[87]. Lors de la décision de divulguer les données, SWIFT avait assumé (illégalement) le rôle de responsable du traitement ; les établissements bancaires n'avaient manifestement pas honoré leur obligation de superviser leur sous-traitant et, par conséquent, ne pouvaient être totalement exonérés de leur responsabilité. Cette situation emporte responsabilité conjointe.

Sous-traitant

Un sous-traitant est défini **dans le droit de l'UE** comme une personne qui traite des données à caractère personnel pour le compte du responsable du traitement[88]. Les activités confiées à un sous-traitant peuvent être limitées à une tâche ou un contexte très spécifique ou peuvent être très générales et complètes.

Dans le droit du CdE, la notion de sous-traitant a la même signification que dans le droit de l'UE.

Les sous-traitants, en plus de traiter des données pour des tiers, seront aussi des responsables du traitement de plein droit à l'égard du traitement qu'ils réalisent à leurs propres fins, par exemple la gestion de leurs propres salariés, ventes et comptabilité.

Exemples : la société Everready est spécialisée dans le traitement de données pour la gestion de données de ressources humaines d'autres sociétés. À ce titre, Everready est un sous-traitant.

87 Groupe de travail Article 29 (2006), *Avis 10/2006 sur le traitement des données à caractère personnel par la Société de télécommunications interbancaires mondiales (SWIFT),* WP 128, Bruxelles, 22 novembre 2006.

88 Directive relative à la protection des données, art. 2, point e).

Quand Everready traite les données de ses propres salariés, elle est le responsable du traitement de ces données aux fins de remplir ses obligations d'employeur.

Relation entre responsable du traitement et sous-traitant

Comme nous l'avons vu, le responsable du traitement est défini comme celui qui détermine la finalité et les moyens du traitement.

Exemple : le directeur de la société Sunshine décide que la société Moonlight, spécialisée dans l'analyse de marché, doit réaliser une analyse de marché des données clients de Sunshine. Par conséquent, même si la détermination des moyens du traitement est déléguée à Moonlight, la société Sunshine reste le responsable du traitement et Moonlight n'est qu'un sous-traitant puisque, aux termes du contrat, Moonlight ne peut utiliser les données clients de Sunshine qu'aux fins déterminées par Sunshine.

Si le pouvoir de déterminer les moyens du traitement est délégué à un sous-traitant, le responsable du traitement doit néanmoins être en mesure d'influer sur les décisions du sous-traitant concernant les moyens du traitement. La responsabilité générale reste celle du responsable du traitement, qui doit superviser les sous-traitants afin de s'assurer que leurs décisions sont conformes au droit en matière de protection des données. Un contrat interdisant au responsable du traitement d'influer sur les décisions du sous-traitant serait donc probablement interprété comme entraînant une responsabilité conjointe, les deux parties partageant les obligations légales d'un responsable du traitement.

En outre, si un sous-traitant ne respectait pas les limites de l'utilisation des données imposées par le responsable du traitement, le sous-traitant deviendrait un responsable du traitement, au moins dans la mesure du non-respect des instructions du responsable du traitement. Cela ferait probablement du sous-traitant un responsable du traitement agissant illégalement. À son tour, le responsable initial du traitement serait tenu d'expliquer comment le sous-traitant a pu ne pas honorer son mandat. En effet, le groupe de travail Article 29 tend à présumer une responsabilité conjointe dans de telles situations, puisque c'est la solution qui assure la meilleure protection

des intérêts des personnes concernées[89]. Une conséquence importante du contrôle commun devrait être la responsabilité conjointe et solidaire pour tous les dommages, ce qui offrirait aux personnes concernées un plus large éventail de voies de recours.

Des problèmes peuvent également survenir quant à la répartition des obligations lorsqu'un responsable du traitement est une petite entreprise et le sous-traitant une grande entreprise ayant le pouvoir de dicter les conditions de ses services. Dans de telles circonstances, le groupe de travail Article 29 maintient toutefois que la norme de responsabilité ne devrait pas être abaissée au motif du déséquilibre économique, et que la compréhension de la notion de responsable du traitement devrait être maintenue[90].

Dans un souci de clarté et de transparence, les détails des rapports entre un responsable du traitement et un sous-traitant devraient être consignés dans un contrat écrit[91]. L'absence de contrat est une infraction à l'obligation du responsable du traitement de fournir une documentation écrite sur les obligations mutuelles, et pourrait donner lieu à des sanctions[92].

Certains sous-traitants pourraient vouloir déléguer certaines tâches à d'autres sous-traitants. La loi le permet et cette délégation dépendra, en détail, des clauses contractuelles convenues entre le responsable du traitement et le sous-traitant, y compris de la question de savoir si l'autorisation du responsable du traitement est nécessaire dans chaque cas, ou si une simple information suffit.

Dans le droit du CdE, l'interprétation des notions de responsable du traitement et de sous-traitant, comme expliqué ci-dessus, est pleinement applicable, ainsi qu'il ressort des recommandations qui ont été élaborées conformément à la Convention 108[93].

89 Groupe de travail Article 29 (2010), *Avis 1/2010 sur les notions de « responsable du traitement » et de « soustraitant »*, WP 169, Bruxelles, 16 février 2010, p. 25 ; et groupe de travail Article 29 (2006), Avis 10/2006 sur le traitement des données à caractère personnel par la Société de télécommunications interbancaires mondiales (SWIFT), WP 128, Bruxelles, 22 novembre 2006.

90 Groupe de travail Article 29 (2010), *Avis* 1/2010 sur les notions de « responsable du traitement » et de « soustraitant », WP 169, Bruxelles, 16 février 2010, p. 26.

91 Directive relative à la protection des données, art. 17, paras. 3 et 4.

92 Groupe de travail Article 29 (2010), *Avis 1/2010 sur les notions de « responsable du traitement » et de « soustraitant »*, WP 169, Bruxelles, 16 février 2010, p. 27.

93 Voir, par exemple, recommandation profilage, art. 1.

2.3.2. Destinataires et tiers

La différence entre ces deux catégories de personnes ou entités, qui ont été introduites par la directive relative à la protection des données, se situe principalement dans leurs rapports avec le responsable du traitement et, par conséquent, dans leur autorisation d'accès aux données à caractère personnel détenues par le responsable du traitement.

Un « tiers » est une personne légalement distincte du responsable du traitement. Divulguer des données à un tiers nécessitera donc toujours une base légale spécifique. Conformément à l'article 2, point f), de la directive relative à la protection des données, un tiers est « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme distinct de la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont habilitées à traiter les données ». Cela signifie que les personnes qui travaillent pour une organisation qui est légalement différente du responsable du traitement (même si elle appartient au même groupe ou à la même société holding) seront (ou appartiendront à) des « tiers ». En revanche, les succursales d'une banque qui traitent les comptes de ses clients sous l'autorité directe de leur siège ne seraient pas des « tiers »[94].

Le terme de « destinataire » est plus large que celui de « tiers ». Selon l'article 2, point g), de la directive relative à la protection des données, un destinataire désigne « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données, qu'il s'agisse ou non d'un tiers ». Ce destinataire peut ne pas relever du responsable du traitement ou du sous-traitant, auquel cas il s'agit d'un tiers, ou relever du responsable du traitement ou du sous-traitant, comme un salarié ou un autre service de la même entreprise ou autorité.

La distinction entre les destinataires et les tiers n'est importante qu'en raison des conditions de la communication légale de données. Les salariés d'un responsable du traitement ou d'un sous-traitant peuvent, sans autre exigence légale, être des destinataires de données à caractère personnel s'ils participent aux traitements du responsable ou du sous-traitant. En revanche, un tiers, dans la mesure où il est légalement distinct du responsable du traitement ou du sous-traitant, n'est pas autorisé à utiliser des données à caractère personnel traitées par le responsable du traitement, sauf sur la base de motifs juridiques spécifiques dans un cas particulier. Les

94 Groupe de travail Article 29 (2010), Avis *1/2010 sur les notions de « responsable du traitement » et de « soustraitant »*, WP 169, Bruxelles, 16 février 2010, p. 31.

« destinataires tiers » de données auront donc toujours besoin d'une base légale pour recevoir légalement des données à caractère personnel.

Exemple : un salarié du sous-traitant, qui utilise des données à caractère personnel dans la limite des missions qui lui ont été confiées par l'employeur, est un destinataire de données, mais pas un tiers, puisqu'il utilise les données au nom et selon les instructions du sous-traitant.

Toutefois, si le même salarié décide d'utiliser les données auxquelles il peut accéder en qualité de salarié du sous-traitant à ses propres fins et de les vendre à une autre société, le salarié agit comme un tiers. Il ne suit plus les instructions du sous-traitant (l'employeur). En tant que tiers, le salarié aurait besoin d'une base légale pour acquérir et vendre les données. Dans cet exemple, le salarié ne dispose certainement pas de base légale, de sorte que ces actes sont illégaux.

2.4. Consentement

Points clés

- Le consentement comme base légale du traitement de données à caractère personnel doit être libre, informé et spécifique.
- Le consentement doit avoir été donné de manière non équivoque. Le consentement peut avoir été donné de façon explicite ou implicite, en agissant d'une façon ne laissant aucun doute sur le fait que la personne concernée accepte le traitement des données.
- Le traitement de données sensibles sur la base d'un consentement requiert un consentement explicite.
- Le consentement peut être retiré à tout moment.

Consentement signifie « toute manifestation de volonté, libre, spécifique et informée de la personne concernée[95] ». Dans de nombreux cas, il constitue la base légale d'un traitement légitime de données (voir Section 4.1).

95 Directive relative à la protection des données, art. 2, point h).

2.4.1. Les éléments d'un consentement valable

Le **droit de l'UE** définit trois éléments de la validité du consentement, l'objectif étant de garantir que les personnes concernées souhaitent véritablement accepter l'utilisation de leurs données :

- la personne concernée ne doit pas avoir fait l'objet de pressions quand elle a donné son consentement ;
- la personne concernée doit avoir été dûment informée de l'objet et des conséquences du consentement ; et
- la portée du consentement doit être raisonnable et concrète.

Le consentement n'est valable au sens du droit en matière de protection des données que si ces exigences sont satisfaites.

La Convention 108 ne contient pas de définition du consentement ; celle-ci est laissée à l'appréciation du législateur national. Toutefois, **dans le droit du CdE**, les éléments de validité du consentement correspondent à ceux exposés ci-dessus, ainsi qu'il ressort des recommandations qui ont été élaborées conformément à la Convention 108[96]. Les exigences du consentement sont les mêmes que pour une déclaration d'intention valable en droit civil européen.

Les exigences complémentaires du droit civil afférentes à un consentement valable, telles que la capacité juridique, s'appliquent naturellement aussi dans le contexte de la protection des données, puisqu'il s'agit d'exigences juridiques préalables essentielles. Le consentement nul de personnes dépourvues de capacité juridique entraîne l'absence de base légale pour le traitement de données concernant ces personnes.

Le consentement peut être donné de façon explicite[97] ou non explicite. Le consentement explicite ne laisse aucun doute sur les intentions de la personne concernée et peut être donné par oral ou par écrit ; le consentement non explicite est déduit des circonstances. Chaque consentement doit être donné de façon non-équivoque[98]. Cela signifie qu'il ne doit pas exister de doute raisonnable quant au fait que

96 Voir, par exemple, Convention 108, recommandation sur les données statistiques, para. 6.

97 Directive relative à la protection des données, art. 8, para. 2.

98 *Ibid.*, art. 7, point a), et art. 26, para. 1.

la personne concernée souhaite communiquer son accord pour permettre le traitement de ses données. Un consentement déduit d'une simple inaction ne saurait constituer un consentement non équivoque, par exemple. Lorsque les données à traiter sont sensibles, un consentement explicite est obligatoire et il doit être non équivoque.

Consentement libre

L'existence d'un consentement libre n'est valable que « si la personne concernée est véritablement en mesure d'exercer un choix et s'il n'y a pas de risque de tromperie, d'intimidation, de coercition ou de conséquences négatives importantes si elle ne donne pas son consentement[99] ».

Exemple : dans de nombreux aéroports, les passagers doivent passer dans des scanners corporels pour entrer dans la zone d'embarquement[100]. Dans la mesure où des données concernant les passagers sont traitées pendant la détection, le traitement doit être conforme à l'un des motifs juridiques prévus à l'article 7 de la directive relative à la protection des données (voir Section 4.1.1). Le passage dans un scanner corporel est parfois présenté aux passagers comme une option, impliquant que leur consentement pourrait justifier le traitement. Les passagers pourraient toutefois craindre que leur refus de passer par le scanner corporel fasse naître une suspicion ou génère d'autres contrôles, tels que des fouilles corporelles. De nombreux passagers acceptent de passer au scanner corporel parce que cela leur permet d'éviter d'éventuels problèmes ou retards. Il y a lieu de présumer qu'un tel consentement n'est pas suffisamment libre.

Par conséquent, seul un acte du législateur, sur la base de l'article 7, point e), de la directive relative à la protection des données, peut fournir une base juridique solide entraînant pour les passagers l'obligation de coopérer en raison d'un intérêt public prépondérant. Une telle législation pourrait néanmoins donner le choix entre le scanner et une palpation de sécurité, mais uniquement dans le cadre de mesures complémentaires de contrôle aux frontières, nécessaires dans

99 Voir également groupe de travail Article 29 (2011), Avis 15/2011 sur la notion de « consentement », WP 187, Bruxelles, 13 juillet 2011, p. 12.

100 Cet exemple est extrait d'*ibid.*, p. 15.

des circonstances particulières. C'est ce qu'a retenu la Commission européenne dans deux règlements couvrant les scanners de sécurité en 2011[101].

La liberté du consentement pourrait également être remise en question dans des situations de subordination lorsqu'il existe un déséquilibre économique, ou autre, significatif entre le responsable du traitement qui obtient le consentement et la personne concernée qui le donne[102].

Exemple : une grande société envisage de créer un annuaire contenant le nom de tous les salariés, leurs fonctions dans la société et leur adresse professionnelle, dans le seul but d'améliorer les communications internes de la société. Le responsable du personnel propose d'ajouter une photo de chaque salarié, par exemple pour faciliter la reconnaissance de collègues lors de réunions. Les représentants des salariés exigent que la photo ne soit ajoutée qu'avec le consentement individuel de chaque salarié.

Dans une telle situation, le consentement d'un salarié devrait être reconnu comme base légale du traitement des photos dans l'annuaire, puisqu'il est clair que la publication d'une photo dans l'annuaire n'a pas de conséquences négatives en soi et, de plus, il est probable que le salarié ne devra pas faire face à de quelconques conséquences négatives de la part de l'employeur s'il refuse que sa photo soit publiée dans l'annuaire.

Cela ne signifie toutefois pas qu'un consentement ne puisse jamais être valable dans des situations dans lesquelles son refus aurait des conséquences négatives. Si, par exemple, le fait de refuser une carte de fidélité dans un supermarché a uniquement pour conséquence la non-réception de réductions de prix sur certains produits, le consentement reste une base légale valable pour le traitement de données

101 Règlement (UE) n° 1141/2011 de la Commission du 10 novembre 2011 modifiant le règlement (CE) n° 272/2009 complétant les normes de base communes en matière de sûreté de l'aviation civile en ce qui concerne l'utilisation de scanners de sûreté dans les aéroports de l'Union européenne, JO 2011 L 293, et règlement d'exécution (UE) n° 1147/2011 de la Commission du 11 novembre 2011 modifiant le règlement (UE) n° 185/2010 fixant des mesures détaillées pour la mise en œuvre des normes de base communes dans le domaine de la sûreté de l'aviation civile en ce qui concerne l'utilisation de scanners de sûreté dans les aéroports de l'Union européenne, JO 2011 L 294.

102 Voir également groupe de travail Article 29 (2001), *Avis 8/2001 sur le traitement des données à caractère personnel dans le contexte professionnel*, WP 48, Bruxelles, 13 septembre 2001 ; et groupe de travail Article 29 (2005), *Document de travail relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995*, WP 114, Bruxelles, 25 novembre 2005.

à caractère personnel des clients qui ont accepté une telle carte. Il n'y a pas de situation de subordination entre la société et le client et les conséquences d'un refus de consentement ne sont pas suffisamment sérieuses pour empêcher le libre choix de la personne concernée.

En revanche, dès lors que des produits ou services suffisamment importants peuvent être obtenus uniquement et exclusivement si certaines données à caractère personnel sont divulguées à des tiers, le consentement de la personne concernée à la communication de ses données ne peut généralement pas être considéré comme une décision libre et, par conséquent, n'est pas valable au sens du droit en matière de protection des données.

Exemple : un accord donné par des passagers à une compagnie aérienne l'autorisant à transférer des dossiers passagers (PNR), c'est-à-dire les données relatives à leur identité, leurs habitudes alimentaires ou leurs problèmes de santé, aux services de l'immigration d'un pays étranger, ne peut être considéré comme un consentement valable en vertu du droit en matière de protection des données car les passagers en déplacement n'ont pas d'autre choix s'ils souhaitent se rendre dans le pays en question. Pour que de telles données soient transférées de manière licite, une base légale autre que le consentement est requise : très probablement une législation spéciale.

Consentement informé

La personne concernée doit disposer d'informations suffisantes avant de prendre sa décision. La question de savoir si les informations données sont suffisantes peut uniquement être appréciée au cas par cas. De façon générale, le consentement informé comprendra une description précise et facilement compréhensible de l'affaire nécessitant un consentement, ainsi qu'une explication des conséquences d'un consentement ou d'une absence de consentement. La langue utilisée devrait être adaptée aux destinataires prévisibles des informations.

En outre, les informations doivent être facilement accessibles par la personne concernée. L'accessibilité et la visibilité des informations sont des éléments importants. Dans un environnement en ligne, des avis d'information stratifiés peuvent être une bonne solution puisque, en plus d'une version concise des informations, une version plus extensive peut aussi être consultée par la personne concernée.

Consentement spécifique

Pour être valable, le consentement doit aussi être spécifique. Cela va de pair avec la qualité des informations données sur l'objet du consentement. Dans ce contexte, les attentes raisonnables d'une personne concernée lambda seront pertinentes. Il convient de redemander le consentement de la personne concernée si des opérations de traitement doivent être ajoutées ou modifiées d'une façon qui ne pouvait être raisonnablement prévue lorsque le consentement initial a été donné.

Exemple : dans l'affaire *Deutsche Telekom AG*[103], la CJUE a statué sur la question de savoir si un fournisseur de services de télécommunications chargé de transférer des données à caractère personnel concernant des abonnés en vertu de l'article 12 de la *directive vie privée et communications électroniques*[104], devait obtenir un nouveau consentement des personnes concernées, dans la mesure où les destinataires n'étaient pas nommément connus lorsque le consentement avait été délivré.

La CJUE a retenu que, conformément à cet article, un nouveau consentement avant la transmission des données n'était pas nécessaire car les personnes concernées, aux termes dudit article, avaient uniquement la possibilité d'accepter la finalité du traitement, à savoir la publication de leurs données, et ne pouvaient pas choisir entre différents annuaires dans lesquels ces données pourraient être publiées.

La CJUE a souligné [qu']« il ressort d'une interprétation contextuelle et systématique de l'article 12 de la directive vie privée et communications électroniques, que le consentement au titre du deuxième paragraphe de cet article porte sur la finalité de la publication des données à caractère personnel dans un annuaire public et non sur l'identité d'un fournisseur d'annuaire en particulier[105] ». En outre, « c'est la publication même des données à caractère personnel dans un annuaire ayant une finalité particulière qui peut s'avérer préjudiciable pour un abonné »[106] et non la personne qui est l'auteur de cette publication.

103 CJUE, C-543/09, *Deutsche Telekom AG c. Bundesrepublik Deutschland*, 5 mai 2011 ; voir en particulier paras. 53 et 54.

104 Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, JO 2002 L 201 (*directive vie privée et communications électroniques*).

105 CJUE, C-543/09, *Deutsche Telekom AG c. Bundesrepublik Deutschland*, 5 mai 2011 ; voir en particulier para. 61.

106 *Ibid.*, voir en particulier para. 62.

2.4.2. Droit de retirer le consentement à tout moment

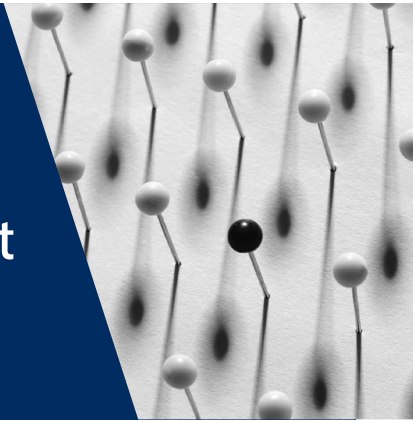
La directive relative à la protection des données ne mentionne pas de droit général de retirer le consentement à tout moment. L'existence d'un tel droit est toutefois largement présumée et la personne concernée doit pouvoir l'exercer à son entière discrétion. Il ne devrait pas être nécessaire de justifier le retrait et celui-ci ne devrait pas entraîner de conséquences négatives supérieures aux avantages pouvant découler de l'utilisation préalablement autorisée des données.

Exemple : un client accepte de recevoir des courriers promotionnels à une adresse qu'il communique à un responsable du traitement de données. Si le client retire son consentement, le responsable du traitement doit immédiatement cesser l'envoi des courriers promotionnels. Aucune conséquence punitive, telle que des frais, ne devrait être imposée.

Si le client bénéficiait d'une réduction de 5 % sur le coût d'une chambre d'hôtel en contrepartie de l'autorisation de l'utilisation de ses données pour des courriers promotionnels, le retrait du consentement ne devrait pas entraîner l'obligation ultérieure de rembourser ces réductions.

3

Les principes clés du droit européen en matière de protection des données



UE	Questions traitées	CdE
Directive relative à la protection des données, article 6, paragraphe 1, points a) et b). CJUE, C-524/06, *Huber c. Allemagne*, 16 décembre 2008 CJUE, affaires jointes C-92/09 et C-93/09, *Volker und Markus Schecke GbR et Hartmut Eifert c. Land Hessen*, 9 novembre 2010	**Le principe du traitement licite**	Convention 108, article 5, points a) et b) CouEDH, *Rotaru c. Roumanie* [GC], n° 28341/95, 4 avril 2000 CouEDH, *TaylorSabori c. Royaume-Uni*, n° 47114/99, 22 octobre 2002 CouEDH, *Peck c. Royaume-Uni*, n° 44647/98, 28 janvier 2003 CouEDH, *Khelili c. Suisse*, n° 16188/07, 18 octobre 2011 CouEDH, *Leander c. Suède*, n° 9248/81, 11 juillet 1985
Directive relative à la protection des données, article 6, paragraphe 1, point b)	**Le principe de la spécification et de la limitation des finalités**	Convention 108, article 5, point b)
	Les principes de la qualité des données	
Directive relative à la protection des données, article 6, paragraphe 1, point c)	**Pertinence des données**	Convention 108, article 5, point c)
Directive relative à la protection des données, article 6, paragraphe 1, point d)	**Exactitude des données**	Convention 108, article 5, point d)

Directive relative à la protection des données, article 6, paragraphe 1, point e)	**Conservation des données pendant une durée limitée**	Convention 108, article 5, point e)
Directive relative à la protection des données, article 6, paragraphe 1, point e)	**Exception à des fins de statistiques ou de recherches scientifiques**	Convention 108, article 9, paragraphe 3
Directive relative à la protection des données, article 6, paragraphe 1, point a)	**Le principe de loyauté de traitement**	Convention 108, article 5, point a) CouEDH, *Haralambie c. Roumanie*, n° 21737/03, 27 octobre 2009 CouEDH, *K.H. et autres c. Slovaquie*, n° 32881/04, 6 novembre 2009
Directive relative à la protection des données, article 6, paragraphe 2	**Le principe de la responsabilité**	

Les principes énoncés à l'article 5 de la Convention 108 représentent l'essence du droit européen en matière de protection des données. Ils figurent également à l'article 6 de la directive relative à la protection des données, comme point de départ de dispositions plus détaillées dans les articles suivants de la directive. L'ensemble de la législation ultérieure relative à la protection des données, que ce soit au niveau du CdE ou de l'UE, doit respecter ces principes, qui doivent être gardés à l'esprit dans l'interprétation de la législation. Toute exception ou toute restriction afférente à ces principes clés doit être prévue au niveau national[107] ; elle doit être prévue par la loi, poursuivre un objectif légitime et être nécessaire dans une société démocratique. Les trois conditions doivent être satisfaites cumulativement.

107 Convention 108, art. 9, para. 2 ; directive relative à la protection des données, art. 13, para. 2.

3.1. Le principe de licéité du traitement

Points clés

- Pour comprendre le principe de licéité du traitement, il faut se référer aux conditions des limites légales du droit à la protection des données à la lumière de l'article 52, paragraphe 1, de la Charte et aux exigences d'une ingérence justifiée telles que visées à l'article 8, paragraphe 2, de la CEDH.
- Selon ces dispositions, le traitement de données à caractère personnel n'est licite que s'il :
  - est conforme à la législation ;
  - poursuit une finalité légitime ; et
  - est nécessaire dans une société démocratique pour atteindre le but légitime.

Dans le droit de l'UE et du CdE en matière de protection des données, le principe de licéité du traitement est le premier principe cité ; il est exprimé en termes quasiment identiques à l'article 5 de la Convention 108 et à l'article 6 de la directive relative à la protection des données.

Aucun de ces articles ne contient de définition d'un « traitement licite ». Pour comprendre ce terme juridique, il est nécessaire de se référer à l'ingérence justifiée, telle que prévue par la CEDH et telle qu'elle a été interprétée par la CouEDH, ainsi qu'aux conditions des limites licites énoncées à l'article 52 de la Charte.

3.1.1. Les exigences d'une ingérence justifiée en vertu de la CEDH

Le traitement de données à caractère personnel peut constituer une ingérence dans le droit au respect de la vie privée de la personne concernée. Le droit au respect de la vie privée n'est toutefois pas une prérogative absolue, mais doit être mis en balance et concilié avec d'autres intérêts légitimes, que ce soit ceux d'autres personnes (intérêts privés) ou de la société dans son ensemble (intérêts publics).

Les conditions qui justifient l'ingérence de l'État sont les suivantes :

Ingérence prévue par la loi

Selon la jurisprudence de la CouEDH, l'ingérence est prévue par la loi si elle repose sur un article du droit national qui présente certaines caractéristiques. La loi doit être « accessible aux personnes concernées et prévisible quant à ses répercussions »[108]. Une règle est prévisible « si elle est formulée avec une précision suffisante pour permettre à toute personne – bénéficiant éventuellement d'une assistance appropriée – d'adapter son comportement »[109]. « Le degré de précision requis de la "loi" à cet égard dépendra du sujet en question. »[110]

Exemple : dans l'affaire *Rotaru c. Roumanie*[111], la CouEDH a conclu à une violation de l'article 8 de la CEDH au motif que le droit roumain permettait la collecte, l'enregistrement et l'archivage, dans des dossiers secrets, d'informations affectant la sécurité nationale, sans poser les limites de l'exercice de ces pouvoirs, laissées à la discrétion des autorités. Par exemple, le droit national ne définissait pas le type d'informations qui pouvaient être traitées, les catégories de personnes à l'égard desquelles des mesures de surveillance pouvaient être prises, les circonstances dans lesquelles de telles mesures pouvaient être prises ou la procédure à suivre. En raison de ces irrégularités, la CouEDH a conclu que le droit national n'était pas conforme à l'exigence de prévisibilité visée à l'article 8 de la CEDH et que cet article avait été violé.

Exemple : dans l'affaire *Taylor-Sabori c. Royaume-Uni*[112], le requérant avait fait l'objet d'une surveillance policière. Utilisant un « clone » du téléavertisseur du requérant, la police avait pu intercepter des messages qui lui étaient adressés. Le requérant avait ensuite été arrêté et inculpé pour conspiration en vue

108 CouEDH, *Amann c. Suisse* [GC], n° 27798/95, 16 février 2000, para. 50 ; voir également CouEDH, *Kopp c. Suisse*, n° 23224/94, 25 mars 1998, para. 55 et CouEDH, *Iordachi et autres c. Moldavie*, n° 25198/02, 10 février 2009, para. 50.

109 CouEDH, *Amann c. Suisse* [GC], n° 27798/95, 16 février 2000, para. 56 ; voir également CouEDH, *Malone c. Royaume-Uni*, n° 8691/79, 26 avril 1985, para. 66 ; CouEDH, *Silver et autres c. Royaume-Uni*, n° 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 mars 1983, para. 88.

110 CouEDH, *The Sunday Times c. Royaume-Uni*, n° 6538/74, 26 avril 1979, para. 49 ; voir également CouEHD, *Silver et autres c. Royaume-Uni*, n° 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 mars 1983, para. 88.

111 CouEDH, *Rotaru c. Roumanie [GC]*, n° 28341/95, 4 avril 2000, para. 57 ; voir également CouEDH, *Association pour l'intégration européenne et les droits de l'homme et Ekimdzhiev c. Bulgarie*, n° 62540/00, 28 juin 2007 ; CouEDH, *Shimovolos c. Russie*, n° 30194/09, 21 juin 2011 ; et CouEDH, *Vetter c. France*, n° 59842/00, 31 mai 2005.

112 CouEDH, *Taylor-Sabori c. Royaume-Uni*, n° 47114/99, 22 octobre 2002.

de la vente d'une substance réglementée. Une partie des éléments à charge du ministère public était des notes manuscrites récentes sur les messages du téléavertisseur qui avaient été transcrites par la police. Toutefois, au moment du procès du requérant, le droit britannique n'était pas doté de dispositions régissant l'interception de communications transmises par un système de télécommunications privé. L'ingérence dans ses droits n'était donc pas « prévue par la loi ». La CouEDH a conclu à une violation de l'article 8 de la CEDH.

Poursuite d'un but légitime

Le but légitime peut être celui des intérêts publics précités ou celui des droits et libertés d'autrui.

Exemple : dans l'affaire *Peck c. Royaume-Uni*[113], le requérant a tenté de se suicider dans la rue en se taillant les poignets, sans savoir qu'une caméra de surveillance avait filmé toute la scène. Après avoir été sauvé par la police, qui regardait les caméras de surveillance, la police a diffusé la séquence dans les médias, qui l'ont publiée sans masquer le visage du requérant. La CouEDH a constaté l'absence de motifs pertinents ou suffisants pour justifier la divulgation directe de la séquence par les autorités au public sans obtenir préalablement le consentement du requérant ou sans masquer son identité. La CouEDH a conclu à une violation de l'article 8 de la CEDH.

Ingérence nécessaire dans une société démocratique

La CouEDH a précisé que « la notion de nécessité implique une ingérence fondée sur un besoin social impérieux et notamment proportionnée au but légitime recherché[114] ».

Exemple : dans l'affaire *Khelili c. Suisse*[115], la police a découvert lors d'un contrôle que la requérante transportait des cartes de visite indiquant : « Femme belle et charmante, la trentaine, cherche à rencontrer un homme pour boire un verre ou sortir de temps en temps. Tél. : [...] ». Selon la requérante, suite à cette découverte, les policiers l'ont enregistrée dans leurs dossiers comme prostituée,

113 CouEDH, *Peck c. Royaume-Uni*, n° 44647/98, 28 janvier 2003, en particulier para. 85.

114 CouEDH, *Leander c. Suède*, n° 9248/81, 11 juillet 1985, para. 58.

115 CouEDH, *Khelili c. Suisse*, n° 16188/07, 18 octobre 2011.

une profession qu'elle a toujours niée. La requérante a demandé que le terme « prostituée » soit supprimé des dossiers informatiques de la police. La CouEDH a reconnu que la conservation des données à caractère personnel de certains individus, au motif que l'individu pourrait commettre une autre infraction, peut en principe être proportionnée dans certaines circonstances. Toutefois, dans le cas de la requérante, l'allégation de prostitution illégale semblait trop vague et générale, n'était étayée par aucun élément concret, celle-ci n'ayant jamais été condamnée pour prostitution illicite, et ne pouvait donc pas être considérée comme fondée sur un « besoin social impérieux » au sens de l'article 8 de la CEDH. Considérant qu'il appartenait aux autorités de démontrer l'exactitude des données enregistrées sur la requérante, et compte tenu de la gravité de l'ingérence dans les droits de la requérante, la CouEDH a conclu que la conservation du terme « prostituée » dans les dossiers de la police pendant des années n'était pas nécessaire dans une société démocratique. La CouEDH a conclu à une violation de l'article 8 de la CEDH.

Exemple : dans l'affaire *Leander c. Suède*[116], la CouEDH a retenu que l'observation secrète de personnes postulant à un emploi à des fonctions importantes pour la sécurité nationale n'est pas, en soi, contraire à l'exigence de démocratie. Les garanties spéciales prévues par la législation nationale dans le but de protéger les intérêts de la personne concernée (par exemple : contrôles exercés par le parlement et le ministre de la Justice) ont amené la CouEDH à conclure que le système suédois de contrôle du personnel est conforme à l'exigence de l'article 8, paragraphe 2, de la CEDH. Eu égard à la grande marge d'appréciation dont il disposait, l'État défendeur était habilité à considérer que, dans le cas du requérant, les intérêts de la sécurité nationale prévalaient sur les intérêts individuels. La CouEDH a exclu la violation de l'article 8 de la CEDH.

3.1.2. Les conditions des limitations licites en vertu de la Charte de l'UE

La structure et le libellé de la Charte sont différents de ceux de la CEDH. La Charte ne parle pas d'ingérences dans des droits garantis, mais contient un article consacré aux limitations relatives à l'exercice des droits et libertés reconnus par la Charte.

Selon l'article 52, paragraphe 1, toute limitation à l'exercice des droits et libertés reconnus par la Charte et, par conséquent, à l'exercice du droit à la protection des

116 CouEDH, *Leander c. Suède*, n° 9248/81, 11 juillet 1985, paras. 59 et 67.

données à caractère personnel, tel que le traitement de données à caractère personnel, n'est recevable que si :

- elle est prévue par la loi ;
- elle respecte le contenu essentiel du droit à la protection des données ;
- elle est nécessaire, sous réserve du principe de proportionnalité ; et
- elle répond effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui.

> Exemples : dans l'affaire *Volker und Markus Schecke*[117], la CJUE a conclu que le Conseil et la Commission, en imposant la publication de données à caractère personnel relatives aux bénéficiaires d'une aide (provenant d'un fonds agricole), sans opérer de distinction selon des critères pertinents, tels que les périodes pendant lesquelles ils ont perçu de telles aides, la fréquence ou encore le type et l'importance de celles-ci, excédaient les limites qu'impose le respect du principe de proportionnalité.
>
> Par conséquent, la CJUE a jugé nécessaire d'annuler certaines dispositions du règlement (CE) n° 1290/2005 du Conseil, et d'annuler le règlement n° 259/2008[118].

Malgré des libellés différents, les conditions du traitement licite énoncées à l'article 52, paragraphe 1, de la Charte rappellent celles de l'article 8, paragraphe 2, de la CEDH. En effet, les conditions énumérées à l'article 52, paragraphe 1, de la Charte doivent être comprises comme conformes à celles visées à l'article 8, paragraphe 2, de la CEDH, puisque l'article 52, paragraphe 3, de la Charte dispose, en sa première phrase, que « dans la mesure où la présente Charte contient des droits correspondant à des droits garantis par la Convention européenne de sauvegarde des droits

117 CJUE, affaires jointes C-92/09 et C-93/09, *Volker und Markus Schecke GbR et Hartmut Eifert c. Land Hessen*, 9 novembre 2010, paras. 86 et 89.

118 Règlement (CE) n° 1290/2005 du Conseil du 21 juin 2005 relatif au financement de la politique agricole commune, JO 2005 L 209 ; règlement (CE) n° 259/2008 de la Commission du 18 mars 2008 portant modalités d'application du règlement (CE) n° 1290/2005 du Conseil en ce qui concerne la publication des informations relatives aux bénéficiaires de fonds en provenance du Fonds européen agricole de garantie (FEAGA) et du Fonds européen agricole pour le développement rural (Feader), JO 2008 L 76.

de l'homme et des libertés fondamentales, leur sens et leur portée sont les mêmes que ceux que leur confère ladite convention ».

Toutefois, la dernière phrase de l'article 52, paragraphe 3, précise que « cette disposition ne fait pas obstacle à ce que le droit de l'Union accorde une protection plus étendue ». Dans le contexte de la comparaison de l'article 8, paragraphe 2, de la CEDH, et de la première phrase de l'article 52, paragraphe 3, de la Charte, cela peut uniquement signifier que les conditions d'ingérences justifiées selon l'article 8, paragraphe 2, de la CEDH sont les exigences minimales applicables à des limitations licites du droit à la protection des données selon la Charte. Par conséquent, le traitement licite de données à caractère personnel requiert au minimum, dans le droit de l'Union, que les conditions de l'article 8, paragraphe 2, de la CEDH soient satisfaites ; le droit de l'UE pourrait toutefois imposer d'autres exigences pour certains cas particuliers.

La correspondance du principe du traitement licite dans le droit de l'UE avec les dispositions pertinentes de la CEDH est également corroborée par l'article 6, paragraphe 3, du TUE, qui dispose que « les droits fondamentaux, tels qu'ils sont garantis par la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales (...) font partie du droit de l'Union en tant que principes généraux ».

3.2. Le principe de la spécification et de la limitation des finalités

Points clés

- La finalité du traitement des données doit être définie de manière claire et accessible avant le début du traitement.
- Dans le droit de l'UE, la finalité du traitement doit être définie de façon explicite ; dans le droit du CdE, cette question est laissée à l'appréciation du législateur national.
- Un traitement à des fins indéterminées n'est pas conforme au droit en matière de protection des données.
- Une utilisation ultérieure à d'autres fins requiert une nouvelle base légale si la nouvelle finalité du traitement est incompatible avec la finalité initiale.
- Le transfert de données à des tiers constitue une nouvelle finalité nécessitant une nouvelle base légale.

En substance, le principe de la spécification et de la limitation des finalités signifie que la légitimé du traitement de données à caractère personnel dépend de la finalité du traitement[119]. Le responsable du traitement doit avoir précisé et indiqué la finalité de manière évidente avant le début du traitement[120]. **Dans le droit de l'UE**, cela doit être fait par déclaration, en d'autres termes, par notification, à l'autorité de contrôle compétente ou, au minimum, par documentation interne soumise par le responsable du traitement pour inspection par les autorités de traitement et accessible à la personne concernée.

Le traitement de données à caractère personnel pour des finalités non définies et/ou illimitées est illicite.

Toute nouvelle finalité du traitement de données doit reposer sur sa propre base légale particulière et ne peut se fonder sur le fait que les données ont été acquises ou traitées initialement pour une autre finalité légitime. À son tour, le traitement légitime est limité à sa finalité initialement précisée et toute nouvelle finalité de traitement requiert une nouvelle base légale distincte. La communication de données à des tiers devra être envisagée avec prudence car la divulgation constituera généralement une nouvelle finalité et, par conséquent, nécessitera une nouvelle base légale, distincte de celle de la collecte des données.

> Exemple : une compagnie aérienne collecte des données auprès de ses passagers pour effectuer des réservations afin d'organiser le vol correctement. La compagnie aérienne aura besoin de données sur : les numéros de sièges des passagers ; les éventuels handicaps physiques, notamment les besoins liés à des fauteuils roulants ; et les exigences alimentaires particulières, telles qu'une nourriture casher ou halal. S'il est demandé à des compagnies aériennes de transférer ces données, contenues dans le PNR, aux services de l'immigration de l'aéroport d'arrivée, ces données sont alors utilisées à des fins de contrôle de l'immigration, différentes de la finalité initiale de collecte des données. Le transfert de ces données à un service de l'immigration nécessitera donc une nouvelle base légale distincte.

Dans l'examen de l'étendue et des limites d'une finalité particulière, la Convention 108 et la directive relative à la protection des données s'en remettent au

119 Convention 108, art. 5, point b) ; directive relative à la protection des données, art. 6, para. 1, point b).

120 Voir également groupe de travail Article 29 (2013), Avis 03/2013 sur la limitation des finalités, WP 203, Bruxelles, 2 avril 2013.

concept de la compatibilité : l'utilisation de données à des fins compatibles est permise sur le fondement de la base légale initiale. Cependant, la signification des fins « compatibles » n'est pas définie et doit faire l'objet d'une interprétation au cas par cas.

Exemple : la vente des données clients de la société Sunshine, acquises dans le cadre de la gestion de la relation client (GRC), à une société de marketing direct, Moonlight, qui souhaite utiliser ces données pour contribuer aux campagnes marketing d'autres entreprises constitue une nouvelle finalité, incompatible avec la GRC, finalité initiale de la société Sunshine pour la collecte des données clients. La vente des données à Moonlight requiert donc sa propre base légale.

Par opposition, l'utilisation par la société Sunshine de données GRC à ses propres fins marketing, c'est-à-dire pour l'envoi de messages marketing à ses propres clients pour ses propres produits, est généralement acceptée comme une finalité compatible.

La directive relative à la protection des données dispose expressément qu'un « traitement ultérieur à des fins historiques, statistiques ou scientifiques n'est pas réputé incompatible pour autant que les États membres prévoient des garanties appropriées[121] ».

Exemples : la société Sunshine a collecté et conservé des données GRC concernant ses clients. Une utilisation ultérieure de ces données par la société Sunshine dans le but de réaliser une analyse statistique du comportement d'achat de ses clients est permise car les statistiques constituent une finalité compatible. Aucune base légale nouvelle, telle que le consentement des personnes concernées, n'est nécessaire.

Si ces mêmes données devaient être transmises à un tiers, comme la société Starlight, à des fins statistiques exclusives, la transmission serait permise sans nouvelle base légale, mais uniquement à condition qu'il existe des garanties appropriées, telles que le masquage de l'identité des personnes concernées, les identités n'étant généralement pas nécessaires à des fins statistiques.

121 La loi autrichienne relative à la protection des données (*Datenschutzgesetz*) constitue un exemple de telles dispositions nationales, Fed. Law Gazette I n° 165/1999, para. 46, disponible en anglais à l'adresse : www.dsk.gv.at/DocView.axd?CobId=41936.

3.3. Principes de la qualité des données

Points clés

- Les principes de la qualité des données doivent être mis en œuvre par le responsable du traitement dans toutes les opérations de traitement.
- Le principe de la conservation des données pendant une durée limitée impose de supprimer les données dès qu'elles ne sont plus nécessaires aux finalités pour lesquelles elles ont été collectées.
- Les exceptions au principe de la conservation pendant une durée limitée doivent être définies par la législation et requièrent des garanties spéciales pour la protection des personnes concernées.

3.3.1. Le principe de la pertinence des données

Seules les données « adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement » peuvent faire l'objet d'un traitement[122]. Les catégories de données choisies pour le traitement doivent être nécessaires pour atteindre l'objectif général déclaré du traitement et un responsable du traitement devrait limiter strictement la collecte de données aux informations directement pertinentes pour la finalité spécifique poursuivie par le traitement.

Dans la société contemporaine, le principe de la pertinence des données a une autre dimension : grâce à l'utilisation de technologies spéciales renforçant la protection de la vie privée, il est parfois possible d'éviter d'utiliser des données à caractère personnel ou d'utiliser plutôt des données pseudonymisées, ce qui constitue une solution favorable au respect de la vie privée. Ceci est particulièrement approprié dans le cadre de systèmes de traitement plus étendus.

Exemple : un conseil municipal propose aux utilisateurs réguliers du système de transport public de la ville une carte magnétique à un certain prix. Le nom de l'utilisateur est inscrit sur la carte et enregistré sous forme électronique dans la puce. Chaque fois qu'un bus ou un tram est utilisé, la carte magnétique doit être validée sur les appareils installés dans ces moyens de transport. Les données

122 Convention 108, art. 5, point c) ; et directive relative à la protection des données, art. 6, para. 1, point c).

lues par l'appareil font l'objet d'une vérification électronique dans la base de données contenant les noms des personnes ayant acheté la carte de voyage.

Ce système n'est pas totalement conforme au principe de la pertinence : vérifier si une personne est autorisée à utiliser des infrastructures de transport pourrait se faire sans comparer les données à caractère personnel de la puce de la carte avec la base de données. Il suffirait, par exemple, de disposer d'une image électronique spéciale, comme un code barre, sur la puce de la carte qui confirmerait la validité de la carte quand celle-ci est passée devant un lecteur. Un tel système n'enregistrerait pas l'identité des personnes qui utilisent les transports et l'heure à laquelle elles se déplacent. Aucune donnée à caractère personnel ne serait collectée, ce qui est la solution idéale au sens du principe de la pertinence, puisque ce principe entraîne l'obligation de minimiser la collecte de données.

3.3.2. Le principe de l'exactitude des données

Un responsable du traitement qui détient des informations à caractère personnel ne peut utiliser ces informations sans prendre de mesures pour s'assurer, avec une certitude raisonnable, que les données sont exactes et à jour.

L'obligation de garantir l'exactitude des données doit être vue dans le contexte de la finalité du traitement des données.

Exemple : une société de vente de mobilier a collecté des données sur l'identité et l'adresse d'un client pour pouvoir lui adresser la facture. Six mois plus tard, la même société veut débuter une campagne marketing et souhaite contacter d'anciens clients. Pour les joindre, la société souhaite accéder au registre national des résidents, qui contient probablement des adresses actualisées puisque les résidents sont tenus d'informer le registre de leur adresse actuelle. L'accès aux données de ce registre est limité aux personnes et entités qui peuvent fournir une justification.

Dans cette situation, la société ne peut pas utiliser l'argument de l'actualisation et de la mise à jour des données pour justifier son habilitation à collecter les nouvelles adresses de tous ses anciens clients à partir du registre des résidents. Les données avaient été collectées dans le cadre de la facturation ; à cette fin, c'est l'adresse à la date de la vente qui est pertinente. Il n'existe pas de base légale pour la collecte de nouvelles adresses, puisque le marketing ne constitue

pas un intérêt supérieur au droit à la protection des données et, par conséquent, ne peut justifier l'accès aux données du registre.

Il est donc possible, dans certains cas, que l'actualisation de données enregistrées soit interdite par la loi, parce que la finalité de la conservation des données est principalement de documenter des événements.

Exemple : un protocole d'opération médicale ne doit pas être modifié, en d'autres termes « mis à jour », même si des conclusions mentionnées dans le protocole s'avèrent ensuite inexactes. Dans de telles circonstances, il est uniquement possible d'apporter des ajouts aux remarques dans le protocole, à condition qu'ils soient clairement présentés comme des contributions intervenues à une date ultérieure.

Ceci étant, il existe des situations dans lesquelles un contrôle régulier de l'exactitude des données, y compris leur mise à jour, est une nécessité absolue en raison du dommage potentiel qui pourrait être causé à la personne concernée si les données restaient inexactes.

Exemple : si une personne veut conclure un contrat avec un établissement bancaire, la banque vérifie généralement la solvabilité du client potentiel. Pour ce faire, il existe des bases de données spéciales qui contiennent des données sur les antécédents de crédit de particuliers. Si une telle base de données fournit sur une personne des données incorrectes ou qui ne sont plus d'actualité, cette personne peut rencontrer des problèmes graves. Les responsables de telles bases de données doivent donc faire des efforts particuliers pour respecter le principe de l'exactitude.

En outre, les données qui ne portent pas sur des faits, mais sur des suspicions, telles que des enquêtes pénales, peuvent être collectées et conservées tant que le responsable du traitement dispose d'une base légale pour collecter ce type d'information et tant qu'il a une justification suffisante pour former une telle suspicion.

3.3.3. Le principe de la conservation des données pendant une durée limitée

L'article 6, paragraphe 1, point e), de la directive relative à la protection des données, et de façon similaire, l'article 5, point e), de la Convention 108, imposent aux États membres de garantir que des données à caractère personnel soient « conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement ». Les données doivent donc être supprimées lorsque ces finalités ont été satisfaites.

Dans l'affaire *S. et Marper*, la CouEDH avait conclu que les principes essentiels des instruments pertinents du Conseil de l'Europe, ainsi que ceux du droit et de la pratique en vigueur dans les autres États contractants, nécessitaient que la conservation des données soit proportionnée au but pour lequel elles avaient été recueillies et limitée dans le temps, en particulier dans le secteur de la police[123].

La limitation dans le temps de la conservation de données à caractère personnel ne s'applique toutefois qu'aux données conservées sous une forme permettant l'identification des personnes concernées. La conservation licite de données qui ne sont plus nécessaires pourrait donc être obtenue par l'anonymisation des données ou la pseudonymisation.

La conservation de données aux fins d'une future utilisation scientifique, historique ou statistique est explicitement exemptée du principe de la conservation pendant une durée limitée prévu par la directive relative à la protection des données[124]. Le maintien de la conservation et de l'utilisation de données à caractère personnel doit cependant s'accompagner de garanties spéciales en vertu du droit national.

123 CouEDH, *S. et Marper c. Royaume-Uni*, n° 30562/04 et 30566/04, 4 décembre 2008 ; voir également, par exemple, CouEDH, *M.M. c. Royaume-Uni*, n° 24029/07, 13 novembre 2012.

124 Directive relative à la protection des données, art. 6, para. 1, point e).

3.4. Le principe de loyauté du traitement

Points clés

- Le traitement loyal signifie la transparence du traitement, en particulier vis-à-vis des personnes concernées.
- Les responsables du traitement doivent informer les personnes concernées avant le traitement de leurs données, au moins sur la finalité du traitement et l'identité et l'adresse du responsable du traitement.
- Sauf si la législation l'autorise, il ne doit pas y avoir de traitement secret ou caché de données à caractère personnel.
- Les personnes concernées ont le droit d'accéder à leurs données quel que soit l'endroit où elles sont traitées.

Le principe du traitement loyal régit principalement les rapports entre le responsable du traitement et la personne concernée.

3.4.1. Transparence

Ce principe impose au responsable du traitement de tenir les personnes concernées informées sur la façon dont leurs données sont utilisées.

Exemple : dans l'affaire *Haralambie c. Roumanie*[125], le requérant demandait l'accès au dossier que l'organisation du service secret avait constitué à son sujet, mais sa demande n'avait été satisfaite que cinq ans plus tard. La CouEDH a rappelé que les personnes faisant l'objet de fichiers personnels détenus par les pouvoirs publics ont un intérêt primordial à pouvoir y accéder et que les autorités se doivent de leur offrir une procédure effective d'accès à ces informations. La CouEDH a considéré que ni la quantité de fichiers transférés ni la défaillance du système d'archivage ne justifiaient un retard de cinq ans pour accéder à la demande du requérant visant à consulter son dossier. Les autorités n'ont pas offert au requérant une procédure effective et accessible lui permettant d'accéder à son fichier personnel dans un délai raisonnable. La CouEDH a donc conclu à une violation de l'article 8 de la CEDH.

125 CouEDH, *Haralambie c. Roumanie*, n° 21737/03, 27 octobre 2009.

Les traitements doivent être expliqués aux personnes concernées d'une façon aisément accessible garantissant qu'elles comprennent ce qu'il va advenir de leurs données. Une personne concernée a également le droit, si elle en fait la demande auprès du responsable du traitement, de savoir si ses données font l'objet d'un traitement et, le cas échéant, de quel type de traitement il s'agit.

3.4.2. Établir la confiance

Les responsables du traitement doivent documenter de façon légale et transparente, à l'attention des personnes concernées et du grand public, le fait qu'ils vont traiter des données. Aucun traitement ne doit être réalisé en secret et ne devrait avoir des effets négatifs imprévisibles. Les responsables du traitement devraient s'assurer que les consommateurs, clients ou citoyens soient informés de l'utilisation de leurs données. En outre, dans la mesure du possible, les responsables du traitement doivent agir de façon à se conformer rapidement aux souhaits des personnes concernées, en particulier quand leur consentement constitue la base légale du traitement des données.

Exemple : dans l'affaire *K.H. et autres c. Slovaquie*[126], les requérantes étaient huit femmes d'origine ethnique rom, qui avaient été suivies dans deux hôpitaux de l'est de la Slovaquie pendant leur grossesse et leur accouchement. Par la suite, aucune d'elle n'avait plus jamais pu concevoir d'autre enfant, en dépit de tentatives répétées. Les juridictions nationales avaient ordonné aux hôpitaux de permettre aux requérantes et à leurs représentants de consulter leur dossier médical et d'en recopier des extraits à la main, mais avaient refusé leur demande de photocopier des documents, dans le but annoncé d'empêcher des abus. Les obligations positives des États en vertu de l'article 8 de la CEDH incluent nécessairement une obligation de fournir des copies de leur dossier aux personnes concernées. Il appartenait à l'État de fixer les modalités de copie des dossiers personnels ou, si nécessaire, d'exposer les motifs d'un refus. Dans le cas des requérantes, les juridictions nationales ont justifié l'interdiction de photocopier les dossiers médicaux principalement par la nécessité de protéger les informations pertinentes contre tout abus. La CouEDH n'a cependant pas compris comment les requérantes, qui n'avaient jamais eu accès à l'intégralité de leur dossier médical, auraient pu faire une utilisation abusive des informations les concernant. En outre, le risque d'un tel abus aurait pu être évité d'une autre façon qu'en interdisant la copie des dossiers aux requérantes, par exemple en

126 CouEDH, *K.H. et autres c. Slovaquie*, n° 32881/04, 6 novembre 2009.

limitant le nombre de personnes autorisées à accéder aux dossiers. L'État n'a pas démontré l'existence de raisons de principe suffisantes pour refuser aux requérantes l'accès effectif aux informations relatives à leur santé. La CouEDH a donc conclu à une violation de l'article 8.

S'agissant de services internet, les caractéristiques des systèmes de traitement de données doivent permettre aux personnes concernées de véritablement comprendre ce qu'il va advenir de leurs données.

Un traitement loyal signifie aussi que les responsables du traitement sont prêts à aller au-delà des obligations légales minimales de service envers la personne concernée, si les intérêts légitimes de celle-ci le requièrent.

3.5. Le principe de la responsabilité

Points clés

- La responsabilité requiert la mise en œuvre active de mesures par les responsables du traitement pour promouvoir et garantir la protection des données dans le cadre de leurs activités de traitement.
- Les responsables du traitement répondent de la conformité de leurs traitements avec le droit en matière de protection des données.
- Les responsables du traitement doivent être en mesure de démontrer à tout moment aux personnes concernées, au grand public et aux autorités de contrôle la conformité avec les dispositions relatives à la protection des données.

L'Organisation de coopération et de développement économiques (OCDE) a adopté des lignes directrices sur la vie privée en 2013 qui soulignent le fait que les responsables du traitement jouent un rôle important dans le fonctionnement pratique de la protection des données. Les lignes directrices ont développé un principe de responsabilité disposant qu'« un maître de fichier devrait être responsable du respect des mesures donnant effet aux principes énoncés ci-dessus »[127].

Tandis que la Convention 108 ne fait aucune référence à la responsabilité des responsables du traitement, laissant essentiellement cette question à l'appréciation du

127 OCDE (2013), *Lignes directrices sur la protection de la vie privée et les flux transfrontières de données de caractère personnel*, art. 14.

législateur national, l'article 6, paragraphe 2, de la directive relative à la protection des données, dispose que le responsable du traitement doit veiller aux principes relatifs à la qualité des données visés au paragraphe 1.

Exemple : l'amendement de 2009[128] à la directive 2002/58/CE vie privée et communications électroniques est un exemple législatif soulignant le principe de la responsabilité. Selon l'article 4 de sa version modifiée, la directive impose une obligation de mise en œuvre d'une politique de sécurité, notamment pour assurer « la mise en œuvre d'une politique de sécurité relative au traitement des données à caractère personnel ». En ce qui concerne les dispositions de cette directive relatives à la sécurité, le législateur a jugé nécessaire d'introduire une exigence explicite de mise en œuvre d'une politique de sécurité.

Selon l'avis du groupe de travail Article 29[129], l'aspect fondamental de la responsabilité est l'obligation du responsable du traitement de :

- mettre en place des mesures qui, dans des circonstances normales, garantissent que les règles de la protection des données sont respectées dans le contexte de traitements ; et

- disposer de documents démontrant aux personnes concernées et aux autorités de traitement quelles mesures ont été prises pour obtenir le respect des règles relatives à la protection des données.

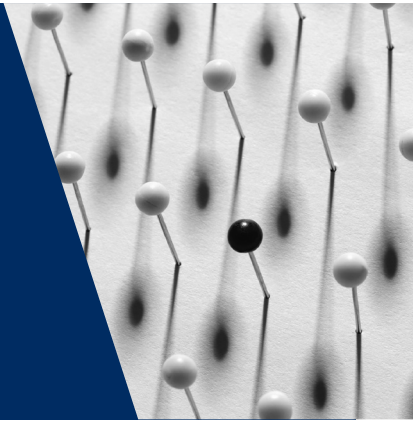
Le principe de la responsabilité requiert donc des responsables du traitement qu'ils démontrent activement une conformité, et pas uniquement qu'ils attendent que les personnes concernées ou les autorités de contrôle signalent des irrégularités.

128 Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) n° 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs, JO 2009 L 337, p. 11.

129 Groupe de travail Article 29 (2011), *Avis 3/2010 sur le principe de la responsabilité*, WP 173, Bruxelles, 13 juillet 2010.

4

Les règles du droit européen en matière de protection des données



UE	Questions traitées	CdE
Règles relatives au traitement licite de données non sensibles		
Directive relative à la protection des données, article 7, point a)	Consentement	Recommandation profilage, articles 3.4, point b), et 3.6
Directive relative à la protection des données, article 7, point b)	Relations (pré) contractuelles	Recommandation profilage, article 3.4, point b)
Directive relative à la protection des données, article 7, point c)	Obligations légales du responsable du traitement	Recommandation profilage, article 3.4, point a)
Directive relative à la protection des données, article 7, point d)	Intérêt vital de la personne concernée	Recommandation profilage, article 3.4, point b)
Directive relative à la protection des données, article 7, point e), et article 8, paragraphe 4 CJUE, affaire C-524/06, *Huber c. Bundesrepublik Deutschland*, 16 décembre 2008	Intérêt public et exercice de l'autorité publique	Recommandation profilage, article 3.4, point b)
Directive relative à la protection des données, article 7, point f) et article 8, paragraphes 2 et 3 CJUE, affaires jointes C-468/10 et C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) et Federación de Comercio Electrónico y Marketing Directo (FECEMD) c. Administración del Estado*, 24 novembre 2011	Intérêts légitimes de tiers	Recommandation profilage, article 3.4, point b)

Règles relatives au traitement licite de données sensibles		
Directive relative à la protection des données, article 8, paragraphe 1	**Interdiction générale de traitement**	Convention 108, article 6
Directive relative à la protection des données, article 8, paragraphes 2, 3 et 4	**Exceptions à l'interdiction générale**	Convention 108, article 6
Directive relative à la protection des données, article 8, paragraphe 5	**Traitement de données relatives à des condamnations (pénales)**	Convention 108, article 6
Directive relative à la protection des données, article 8, paragraphe 7	**Numéros d'identification du traitement**	
Règles relatives à la sécurité du traitement		
Directive relative à la protection des données, article 17	**Obligation de veiller à la sécurité du traitement**	Convention 108, article 7
		CouEDH, *I. c. Finlande*, n° 20511/03, 17 juillet 2008
Directive vie privée et communications électroniques, article 4, paragraphe 2	**Notifications de violations de données**	
Directive relative à la protection des données, article 16	**Obligation de confidentialité**	
Règles relatives à la transparence du traitement		
	Transparence en général	Convention 108, article 8, point a)
Directive relative à la protection des données, articles 10 et 11	**Information**	Convention 108, article 8, point a)
Directive relative à la protection des données, articles 10 et 11	**Exceptions à l'obligation d'informer**	Convention 108, article 9
Directive relative à la protection des données, articles 18 et 19	**Notification**	Recommandation profilage, article 9.2, point a)
Règles relatives à la promotion de la conformité		
Directive relative à la protection des données, article 20	**Contrôle préalable**	
Directive relative à la protection des données, article 18, paragraphe 2	**Délégués à la protection des données à caractère personnel**	Recommandation profilage, article 8.3
Directive relative à la protection des données, article 27	**Codes de conduite**	

Les principes sont nécessairement d'ordre général. Leur application à des situations concrètes laisse une certaine marge d'interprétation et un certain choix de moyens. Dans le **droit du CdE**, la clarification de cette marge d'interprétation est laissée au législateur national des parties à la Convention 108. La situation est différente dans le **droit de l'UE** : pour l'établissement d'une protection des données au sein du marché intérieur, il a été jugé nécessaire de disposer de règles plus détaillées au niveau communautaire afin d'harmoniser le niveau de protection des données des législations nationales des États membres. La directive relative à la protection des données établit, conformément aux principes énoncés en son article 6, une série de règles détaillées qui doivent être transposées fidèlement dans le droit national. Les observations ci-après concernant les règles détaillées en matière de protection des données au niveau européen traitent donc principalement du droit de l'UE.

4.1. Règles relatives à la licéité du traitement

Points clés

- Des données à caractère personnel peuvent faire l'objet d'un traitement licite si :
  - le traitement repose sur le consentement de la personne concernée ;
  - l'intérêt vital de la personne concernée impose le traitement de ses données ; ou
  - des intérêts légitimes de tiers sont la raison du traitement, mais uniquement pour autant qu'ils ne s'effacent pas devant des intérêts à la protection des droits fondamentaux des personnes concernées.
- Le traitement licite de données à caractère personnel sensibles est soumis à un régime spécial plus strict.

La directive relative à la protection des données contient deux ensembles de règles pour le traitement licite de données : un pour les données non sensibles (article 7) et un pour les données sensibles (article 8).

4.1.1. Traitement licite de données non sensibles

Le chapitre II de la directive 95/46, intitulé « Conditions générales de licéité des traitements de données à caractère personnel », dispose que, sous réserve des dérogations admises au titre de son article 13, tout traitement de données à caractère personnel doit être conforme, premièrement, aux principes relatifs à la qualité des

données énoncés à l'article 6 de la directive relative à la protection des données, et deuxièmement, à l'un des principes relatifs à la légitimation des traitements de données, énumérés à l'article 7[130]. Ce dernier article explique les cas dans lesquels le traitement de données à caractère personnel non sensibles est légitime.

Consentement

Dans le droit du CdE, le consentement n'est pas mentionné à l'article 8 de la CEDH ou dans la Convention 108. Il est toutefois mentionné dans la jurisprudence de la CEDH et dans plusieurs recommandations du CdE. **Dans le droit de l'UE**, le consentement comme base de traitement légitime de données est fermement établi à l'article 7, point a), de la directive relative à la protection des données, et il est explicitement mentionné à l'article 8 de la Charte.

Relations contractuelles

Une autre base du traitement légitime de données à caractère personnel dans le **droit de l'UE**, énuméré à l'article 7, point b), de la directive relative à la protection des données, est que le traitement soit « nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ». Cette clause couvre également les relations pré-contractuelles. Par exemple : une partie souhaite conclure un contrat, mais ne l'a pas encore fait, peut-être en raison de certaines vérifications qui restent à effectuer. Si une partie doit traiter des données à cette fin, un tel traitement est légitime dans la mesure où il est nécessaire « à l'exécution de mesures précontractuelles prises à la demande de celle-ci ».

S'agissant du droit du CdE, « la protection des droits et des libertés d'autrui » est mentionnée à l'article 8, paragraphe 2, de la CEDH comme motif d'ingérence légitime dans le droit à la protection des données.

Obligations légales du responsable du traitement

Le droit de l'UE mentionne ensuite explicitement un autre critère de légitimation du traitement des données, à savoir s'« il est nécessaire au respect d'une obligation

130 CJUE, affaires jointes C-465/00, C-138/01 et C-139/01, *Rechnungshof c. Österreichischer Rundfunk et autres et Neukomm and Lauermann c. Österreichischer Rundfunk*, 20 mai 2003, para. 65 ; CJUE, C-524/06, *Huber c. Bundesrepublik Deutschland*, 16 décembre 2008, para. 48 ; CJUE, affaires jointes C-468/10 et C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) c. Administración del Estado*, 24 novembre 2011, para. 26.

légale à laquelle le responsable du traitement est soumis » (article 7, point c), de la directive relative à la protection des données). Cet article fait référence aux responsables du traitement qui agissent dans le secteur privé ; les obligations légales de responsables du traitement dans le secteur public relèvent de l'article 7, point e), de la directive. Il existe de nombreux cas dans lesquels des responsables du traitement du secteur privé sont tenus par la loi de traiter des données de tiers ; par exemple, les médecins et les hôpitaux ont l'obligation légale d'enregistrer des données sur le traitement de patients pendant plusieurs années, les employeurs doivent traiter des données sur leurs salariés pour des raisons liées à la sécurité sociale et à la fiscalité et les entreprises doivent traiter des données sur leurs clients à des fins de fiscalité.

Dans le contexte du transfert obligatoire des données sur les passagers par des compagnies aériennes aux services étrangers de contrôle de l'immigration, la question s'est posée de savoir si des obligations légales découlant d'une législation *étrangère* peuvent constituer une base légitime au traitement de données en vertu du droit de l'UE (cette question est abordée plus en détail dans la Section 6.2).

Les obligations légales du responsable du traitement servent également de base au traitement légitime de données **dans le droit du CdE**. Ainsi qu'exposé précédemment, les obligations légales d'un responsable du traitement du secteur privé ne sont qu'un cas particulier d'intérêts légitimes de tiers, comme mentionné à l'article 8, paragraphe 2, de la CEDH. L'exemple ci-dessus est donc aussi pertinent pour le droit du CdE.

Intérêt vital de la personne concernée

Dans le droit de l'UE, l'article 7, point d), de la **directive relative à la protection des données,** dispose que le traitement de données à caractère personnel est licite s'il « est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée ». Un tel intérêt, étroitement lié à la survie de la personne concernée, pourrait être la base de l'utilisation légitime de données relatives à la santé ou de données concernant des personnes disparues, par exemple.

Dans le droit du CdE, l'intérêt vital de la personne concernée n'est pas mentionné à l'article 8 de la CEDH comme motif d'ingérence légitime dans le droit à la protection des données. Dans certaines recommandations du CdE complétant la Convention 108 dans des domaines particuliers, l'intérêt vital de la personne concernée est toutefois explicitement mentionné comme base du traitement légitime de

données[131]. De toute évidence, l'intérêt vital de la personne concernée est considéré comme implicite dans l'ensemble des motifs justifiant le traitement de données : la protection des droits fondamentaux ne devrait jamais mettre en danger l'intérêt vital de la personne qui est protégée.

Intérêt public et exercice de l'autorité publique

Compte tenu des nombreuses possibilités d'organisation des affaires publiques, l'article 7, point e), de la **directive relative à la protection des données,** dispose que le traitement de données à caractère personnel peut être légalement effectué s'« 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[132] ».

Exemple : dans l'affaire *Huber c. Bundesrepublik Deutschland*[133], M. Huber, un ressortissant autrichien domicilié en Allemagne, a demandé à l'Office fédéral de la migration et des étrangers de supprimer les données le concernant dans le registre central des étrangers (l'« AZR »). Ce registre, qui contient des données à caractère personnel concernant des ressortissants européens non allemands vivant en Allemagne depuis plus de trois mois, est utilisé à des fins statistiques et par les autorités répressives et judiciaires dans le cadre d'activités d'enquête et de poursuites pénales, ou au sujet de personnes qui représentent une menace pour la sécurité publique. La juridiction de renvoi a demandé si le traitement de données à caractère personnel effectué dans un registre tel que le registre central des étrangers, auquel aucune autre autorité publique n'a accès, était compatible avec le droit de l'UE, dans la mesure où il n'existait aucun registre similaire pour les ressortissants allemands.

La CJUE a tout d'abord retenu que, conformément à l'article 7, point e), de la directive, des données à caractère personnel ne peuvent faire légalement l'objet d'un traitement que si cela est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique.

Selon la Cour, « eu égard à l'objectif consistant à assurer un niveau de protection équivalent dans tous les États membres, la notion de nécessité telle

131 Recommandation profilage, art. 3.4, point b).

132 Voir également la directive relative à la protection des données, considérant 32.

133 CJUE, C-524/06, *Huber c. Bundesrepublik Deutschland*, 16 décembre 2008.

qu'elle résulte de l'article 7, sous e), de la directive 95/46 (...) ne saurait avoir un contenu variable en fonction des États membres. Partant, il s'agit d'une notion autonome du droit communautaire qui doit recevoir une interprétation de nature à répondre pleinement à l'objet de cette directive tel que défini à l'article 1er, paragraphe 1, de celleci[134] ».

La Cour a relevé que le droit de séjour d'un citoyen de l'Union sur le territoire d'un État membre dont il n'est pas ressortissant n'est pas inconditionnel, mais qu'il peut être assorti des limitations et des conditions prévues par le traité et par les dispositions prises pour son application. Partant, si l'utilisation par un État membre d'un registre tel que l'AZR visant à soutenir les autorités en charge de l'application de la loi sur le droit de séjour est, en principe, légitime, un tel registre ne peut contenir d'autres informations que celles qui sont nécessaires à cette fin. La Cour a conclu qu'un tel système de traitement de données à caractère personnel ne pouvait être conforme au droit de l'UE que s'il contenait uniquement les données nécessaires à l'application de cette réglementation et si son caractère centralisé permettait une application plus efficace de cette réglementation. Il appartenait à la juridiction nationale de vérifier si ces conditions étaient satisfaites en l'espèce. Dans l'hypothèse négative, la conservation et le traitement de données à caractère personnel dans le cadre d'un registre tel que l'AZR à des fins statistiques ne sauraient, sur quelque fondement que ce soit, être considérés comme nécessaires au sens de l'article 7, point e), de la directive 95/46/CE[135].

Enfin, s'agissant de la question de l'utilisation des données contenues dans le registre aux fins de lutte contre la criminalité, la Cour a retenu que cet objectif implique « nécessairement la poursuite des crimes et des délits commis, indépendamment de la nationalité de leurs auteurs ». Le registre en cause ne contenait pas de données à caractère personnel concernant des ressortissants de l'État membre concerné et cette différence de traitement constituait une discrimination interdite par l'article 18 du TFUE. Par conséquent, cet article, tel qu'interprété par la Cour, « s'oppose à l'instauration par un État membre d'un système de traitement de données à caractère personnel spécifique aux citoyens de l'Union non-ressortissants de cet État membre dans l'objectif de lutter contre la criminalité[136] ».

134 *Ibid.*, para. 52.

135 *Ibid.*, paras. 54, 58, 59, 66, 67 et 68.

136 *Ibid.*, paras. 78 et 81.

L'utilisation de données à caractère personnel par des autorités agissant dans le domaine public est également soumise à l'article 8 de la **CEDH**.

Intérêt légitime poursuivi par le responsable du traitement ou par un tiers

Les personnes concernées ne sont pas les seules à avoir un intérêt légitime. L'article 7, point f), de la **directive relative à la protection des données,** dispose qu'un traitement de données à caractère personnel peut légalement être effectué s'il « est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée, qui appellent une protection (...) ».

Dans l'arrêt suivant, la CJUE a explicitement statué sur l'article 7, point f), de la directive :

Exemple : dans l'affaire *ASNEF et FECEMD*[137], la CJUE a précisé que le législateur national n'est pas autorisé à ajouter des conditions supplémentaires à celles prévues par l'article 7, point f), de la directive relative au traitement licite de données. La Cour a fait référence à une clause du droit espagnol en matière de protection des données selon laquelle d'autres parties privées ne peuvent invoquer un intérêt légitime au traitement de données à caractère personnel que si les informations figuraient déjà dans des sources publiques.

La Cour a dans un premier temps relevé que la directive 95/46 vise à rendre équivalent dans tous les États membres le niveau de protection des droits et libertés des personnes à l'égard du traitement de données à caractère personnel. Le rapprochement des législations nationales applicables en la matière ne doit pas conduire à affaiblir la protection qu'elles assurent, mais doit, au contraire, avoir pour objectif de garantir un niveau élevé de protection dans l'Union[138]. Par conséquent, la CJUE a considéré qu'« il découle de l'objectif consistant à assurer un niveau de protection équivalent dans tous les États membres que l'article 7 de la directive 95/46 prévoit une liste exhaustive et limitative des

137 CJUE, affaires jointes C-468/10 et C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) c. Administración del Estado*, 24 novembre 2011.

138 *Ibid.*, para. 28. Voir directive relative à la protection des données, considérants 8 et 10.

cas dans lesquels un traitement de données à caractère personnel peut être considéré comme étant licite ». En outre, « les États membres ne sauraient ni ajouter de nouveaux principes relatifs à la légitimation des traitements de données à caractère personnel à l'article 7 de la directive 95/46, ni prévoir des exigences supplémentaires qui viendraient modifier la portée de l'un des six principes prévus à cet article[139] ». La Cour a reconnu que « s'agissant de la pondération nécessaire en vertu de l'article 7, sous f), de la directive 95/46, il est possible de prendre en considération le fait que la gravité de l'atteinte aux droits fondamentaux de la personne concernée par ledit traitement peut varier en fonction du fait de savoir si les données en cause figurent déjà, ou non, dans des sources accessibles au public ».

Toutefois, « l'article 7, sous f), de cette directive s'oppose à ce qu'un État membre exclue de façon catégorique et généralisée la possibilité pour certaines catégories de données à caractère personnel d'être traitées, sans permettre une pondération des droits et intérêts opposés en cause dans un cas particulier ».

Au vu de ces considérations, la Cour a conclu que « l'article 7, sous f), de la directive 95/46 doit être interprété comme s'opposant à toute réglementation nationale qui, en l'absence du consentement de la personne concernée, exige, pour autoriser le traitement de ses données à caractère personnel nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable de ce traitement ou par le ou les tiers auxquels ces données sont communiquées, outre le respect des droits et libertés fondamentaux de cette dernière, que lesdites données figurent dans des sources accessibles au public, ce qui excluant de façon catégorique et généralisée tout traitement de données ne figurant pas dans de telles sources[140] ».

Les **recommandations du CdE** contiennent des formulations similaires. La recommandation sur le profilage reconnaît le traitement des données à caractère personnel aux fins de profilage comme légitime, s'il est nécessaire pour les intérêts légitimes de tiers, « à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée[141] ».

139 CJUE, affaires jointes C-468/10 et C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) c. Administración del Estado*, 24 novembre 2011, paras. 30 et 32.

140 *Ibid.*, paras. 40, 44, 48 et 49.

141 Recommandation profilage, art. 3.4, point b).

4.1.2. Règles relatives au traitement licite de données sensibles

Le **droit du CdE** laisse au droit national la tâche d'énoncer la protection appropriée pour l'utilisation de données sensibles, tandis que le **droit de l'UE**, à l'article 8 de la directive relative à la protection des données, prévoit un système détaillé pour le traitement de catégories de données qui révèlent : l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale et les données relatives à la santé ou à la vie sexuelle. Le traitement de données sensibles est en principe interdit[142]. Il existe toutefois une liste exhaustive d'exceptions à cette interdiction, qui figure à l'article 8, paragraphes 2 et 3 de la directive. Ces exceptions incluent le consentement explicite de la personne concernée, l'intérêt vital de la personne concernée, l'intérêt légitime de tiers et l'intérêt public.

Contrairement au traitement de données non sensibles, une relation contractuelle avec la personne concernée n'est pas considérée comme une base générale du traitement légitime de données sensibles. Par conséquent, si des données sensibles doivent être traitées dans le contexte d'un contrat avec la personne concernée, l'utilisation de ces données requiert le consentement explicite distinct de la personne concernée, en plus de l'acceptation de la conclusion d'un contrat. Une demande explicite de la personne concernée pour des produits ou services qui révèlent forcément des données sensibles devrait toutefois être considérée comme équivalente à un consentement explicite.

> Exemple : si un passager d'une compagnie aérienne, dans le contexte de la réservation d'un vol, demande que la compagnie aérienne fournisse un fauteuil roulant et de la nourriture casher, la compagnie aérienne est autorisée à utiliser ces données même si le passager n'a pas signé de clause de consentement supplémentaire stipulant qu'il acceptait l'utilisation de ses données révélant des informations sur sa santé et ses convictions religieuses.

Consentement explicite de la personne concernée

La première condition du traitement licite de données, peu importe qu'elles soient sensibles ou non, est le consentement de la personne concernée. Dans le cas de

142 Directive relative à la protection des données, art. 8, para. 1.

données sensibles, ce consentement doit être explicite. Le droit national peut toutefois disposer que le consentement à l'utilisation de données sensibles n'est pas une base légale suffisante pour autoriser leur traitement[143], par exemple lorsque, dans des cas exceptionnels, le traitement implique des risques inhabituels pour la personne concernée.

Dans un cas particulier, le consentement même implicite est reconnu comme une base légale du traitement de données sensibles : l'article 8, paragraphe 2, point e), de la directive, dispose que le traitement n'est pas interdit s'il porte sur des données manifestement rendues publiques par la personne concernée. Cet article suppose évidemment que l'action de la personne concernée consistant à rendre ses données publiques doit être interprétée comme impliquant un consentement de la personne concernée à l'utilisation des données qui la concernent.

Intérêt vital de la personne concernée

Comme pour les données non sensibles, des données sensibles peuvent faire l'objet d'un traitement au motif de l'intérêt vital de la personne concernée[144].

Pour que le traitement de données sensibles soit légitime sur ce fondement, il doit avoir été impossible de laisser le choix de la décision à la personne concernée, par exemple parce qu'elle était inconsciente ou absente et ne pouvait être jointe.

Intérêts légitimes de tiers

Comme pour les données non sensibles, les intérêts légitimes de tiers peuvent servir de base au traitement de données sensibles. Pour les données sensibles, et conformément à l'article 8, paragraphe 2, de la directive relative à la protection des données, cela ne vaut cependant que pour les cas suivants :

- quand le traitement est nécessaire à la défense des intérêts vitaux d'une autre personne[145] dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement ;

143 *Ibid.*, art. 8, para. 2, point a).

144 *Ibid.*, art. 8, para. 2, point c).

145 *Ibid.*

- quand des données sensibles sont pertinentes dans le domaine du droit du travail, telles que des données relatives à la santé, notamment dans le contexte d'un lieu de travail particulièrement dangereux, ou des données relatives à des convictions religieuses, comme dans le cadre de vacances[146] ;

- lorsque des fondations, associations ou autres organismes à but non lucratif et à finalité politique, philosophique, religieuse ou syndicale, traitent des données sur leurs membres, leurs sponsors ou les parties intéressées (ces données sont sensibles parce qu'il est probable qu'elles révéleront des convictions religieuses ou politiques de personnes concernées)[147] ;

- lorsque des données sensibles sont utilisées dans le contexte de procédures judiciaires devant un tribunal ou une autorité administrative pour la constatation, l'exercice ou la défense d'un droit en justice[148].

- De plus, conformément à l'article 8, paragraphe 3, de la directive relative à la protection des données, lorsque des données relatives à la santé sont utilisées à des fins d'examen ou de traitement médical par des prestataires de soins de santé, la gestion de ces services est incluse dans cette exception. À titre de garantie spéciale, une personne n'est reconnue « prestataire de soins de santé » que si elle est soumise à des obligations professionnelles spécifiques de confidentialité.

Intérêt public

En outre, conformément à l'article 8, paragraphe 4, de la directive relative à la protection des données, des États membres peuvent introduire d'autres finalités pour lesquelles des données sensibles peuvent être traitées, pour autant que :

- le traitement de données soit un motif d'intérêt public important ;

- il soit prévu par la législation nationale ou sur décision de l'autorité de contrôle ; et

146 *Ibid.*, art. 8, para. 2, point b).

147 *Ibid.*, art. 8, para. 2, point d).

148 *Ibid.*, art. 8, para. 2, point e).

- le droit national ou la décision de l'autorité de contrôle contiennent les garanties nécessaires pour protéger efficacement les intérêts des personnes concernées[149].

Un exemple majeur est celui des dossiers médicaux électroniques, qui seront bientôt mis en place dans de nombreux États membres. Ces dossiers permettent que des données relatives à la santé, collectées par des prestataires de soins de santé au cours du traitement d'un patient, soient mises à la disposition d'autres prestataires de soins de santé de ce patient à une grande échelle, habituellement à l'échelle du pays.

Le groupe de travail Article 29 a conclu que la mise en place de tels dossiers ne pourrait pas intervenir dans le cadre des règles juridiques actuelles relatives au traitement de données concernant des patients sur le fondement de l'article 8, paragraphe 3, de la directive relative à la protection des données. À supposer toutefois que l'existence de tels dossiers médicaux électroniques constitue un intérêt public important, elle pourrait être fondée sur l'article 8, paragraphe 4, de la directive, nécessitant une base légale explicite pour leur mise en place qui contienne également les garanties nécessaires pour assurer le fonctionnement du système en toute sécurité[150].

149 *Ibid.*, art. 8, para. 4.

150 Groupe de travail Article 29 (2007), *Document de travail sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME)*, WP 131, Bruxelles, 15 février 2007.

4.2. Règles relatives à la sécurité du traitement

Points clés

- Les règles relatives à la sécurité du traitement impliquent une obligation pour le responsable du traitement et le sous-traitant de prendre des mesures techniques et organisationnelles appropriées pour empêcher toute ingérence non autorisée dans des traitements de données.
- Le niveau de sécurité des données nécessaire est déterminé par :
  - les caractéristiques de sécurité existant sur le marché pour tout type particulier de traitement ;
  - les coûts ; et
  - la nature sensible ou non des données traitées.
- Le traitement de données en toute sécurité est également garanti par l'obligation générale imposée à tous, responsables du traitement ou sous-traitants, de veiller à préserver la confidentialité des données.

L'obligation des responsables du traitement et des sous-traitants de mettre en place des mesures adéquates garantissant la sécurité des données est donc énoncée dans le **droit du CdE en matière de protection des données** et dans le **droit de l'UE en matière de protection des données**.

4.2.1. Éléments de la sécurité des données

Conformément aux dispositions pertinentes du **droit de l'UE** :

> *« Les États membres prévoient que le responsable du traitement doit mettre en œuvre 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*[151] *».*

151 Directive relative à la protection des données, art. 17, para. 1.

Il existe une disposition similaire dans le **droit du CdE** :

> *« Des mesures de sécurité appropriées sont prises pour la protection des données à caractère personnel enregistrées dans des fichiers automatisés contre la destruction accidentelle ou non autorisée, ou la perte accidentelle, ainsi que contre l'accès, la modification ou la diffusion non autorisés*[152] *».*

Il existe aussi souvent des normes industrielles, nationales et internationales qui ont été développées pour la sécurité du traitement de données. Le label européen de protection de la vie privée (EuroPriSe), par exemple, est un projet eTEN (réseaux transeuropéens de télécommunications) de l'UE qui a étudié les possibilités de certification de produits, en particulier de logiciels, comme conformes au droit européen en matière de protection des données. L'Agence européenne pour la sécurité des réseaux et de l'information (ENISA) a été créée pour améliorer la capacité de l'UE, des États membres de l'UE et de la communauté professionnelle à prévenir, traiter et répondre aux problèmes de sécurité des réseaux et de l'information[153]. L'ENISA publie régulièrement des analyses de menaces de sécurité et des conseils sur la façon d'y répondre.

La sécurité des données n'est pas obtenue simplement par la mise en place du bon équipement (matériel et logiciel). Elle requiert également des règles organisationnelles internes appropriées, qui idéalement, doivent couvrir les points suivants :

- information régulière de tous les salariés sur les règles relatives à la sécurité des données et sur leurs obligations en vertu du droit en matière de protection des données, en particulier leurs obligations de confidentialité ;

- répartition claire des responsabilités et définition claire des compétences en matière de traitement des données, en particulier concernant les décisions de traitement de données à caractère personnel et de transfert de données à des tiers ;

- utilisation de données à caractère personnel selon les instructions de la personne compétente ou selon des règles générales définies ;

152 Convention 108, art. 7.

153 Règlement (CE) n °460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information, JO 2004 L 77.

- protection de l'accès aux sites, au matériel et aux logiciels du responsable du traitement ou du sous-traitant, y compris contrôle des autorisations d'accès ;

- garantie de ce que les autorisations d'accès à des données à caractère personnel ont été délivrées par la personne compétente et requièrent une documentation en bonne et due forme ;

- protocoles automatisés en matière d'accès à des données à caractère personnel par des moyens électroniques et des contrôles réguliers de ces protocoles par le bureau de contrôle interne ;

- documentation consciencieuse pour d'autres formes de diffusion que l'accès automatisé aux données afin de pouvoir démontrer l'absence de toute transmission illégale de données.

Offrir aux membres du personnel une formation et un enseignement adéquats en matière de sécurité des données est également un aspect important des précautions efficaces en matière de sécurité. Des procédures de vérification doivent également être en place pour garantir que des mesures appropriées existent non seulement sur le papier, mais sont également mises en œuvre et fonctionnent en pratique (notamment audits internes et externes).

Des mesures visant à améliorer le niveau de sécurité d'un responsable du traitement ou d'un soustraitant incluent des instruments tels que des délégués à la protection des données à caractère personnel, une formation des salariés à la sécurité, des audits réguliers, des tests de pénétration et des labels de qualité.

Exemple : dans l'affaire *I. c. Finlande*[154], la requérante n'avait pas été en mesure de prouver que son dossier médical avait fait l'objet d'un accès illégitime par des salariés de l'hôpital dans lequel elle travaillait. Son allégation de violation du droit à la protection de ses données avait donc été rejetée par les juridictions nationales. La CouEDH a conclu à une violation de l'article 8 de la CEDH car le système des dossiers médicaux de l'hôpital était tel qu'il n'était pas possible de vérifier rétroactivement l'utilisation des dossiers des patients, parce qu'il ne révélait que les cinq consultations les plus récentes et parce que cette information était supprimée une fois le dossier replacé dans les archives. Pour la CouEDH, la non-conformité du système d'archivage et de consultation des

154 CouEDH, *I. c. Finlande*, n° 20511/03, 17 juillet 2008.

dossiers au sein de l'hôpital avec les exigences légales du droit national était un élément déterminant auquel les juridictions nationales n'avaient pas accordé suffisamment de poids.

Notification de violation de données

Un nouvel instrument pour répondre aux violations de la sécurité des données a été introduit dans le droit en matière de protection des données de plusieurs pays européens : l'obligation pour les prestataires de services de communications électroniques de notifier les violations de données aux victimes potentielles et aux autorités de contrôle. Pour les prestataires de services de télécommunications, le droit de l'UE en fait une obligation[155]. La finalité des notifications de violation de données aux personnes concernées est d'éviter un préjudice : la notification de violations de données et de leurs conséquences possibles minimise le risque d'effets négatifs sur les personnes concernées. En cas de négligence grave, les prestataires peuvent aussi être verbalisés.

Il sera nécessaire de mettre en place des procédures internes, à l'avance, pour la gestion efficace et le signalement de violations de sécurité, dans la mesure où, selon la législation nationale, le calendrier de l'obligation de signalement aux personnes concernées et/ou à l'autorité de contrôle est généralement plutôt limité.

4.2.2. Confidentialité

Dans le droit de l'UE, le traitement de données en toute sécurité est également garanti par l'obligation générale imposée à tous, responsables du traitement ou sous-traitants, de veiller à préserver la confidentialité des données.

155 Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (*directive vie privée et communications électroniques*), JO 2002 L 201, art. 4, para. 3, tel que modifié par la directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques ; voir également directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et règlement (CE) n° 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs, JO 2009 L 337.

Exemple : un salarié d'une compagnie d'assurance reçoit un appel téléphonique sur son lieu de travail de la part d'une personne qui se présente comme un client et demande des informations sur son contrat d'assurance.

L'obligation de préserver la confidentialité des données des clients impose au salarié d'appliquer des mesures de sécurité minimales avant de divulguer des données à caractère personnel. Ceci pourrait être fait, par exemple, en proposant de rappeler à un numéro de téléphone figurant dans le dossier du client.

L'article 16 de la directive relative à la protection des données concerne uniquement la confidentialité dans le cadre d'une relation entre le responsable du traitement et le sous-traitant. La question de savoir si des responsables de traitement doivent préserver la confidentialité des données, au sens qu'ils ne peuvent pas les divulguer à des tiers, est traitée dans les articles 7 et 8 de la directive.

L'obligation de confidentialité ne s'étend pas aux situations dans lesquelles des données sont portées à la connaissance d'une personne en sa qualité de particulier, et non de salarié d'un responsable du traitement ou d'un sous-traitant. Dans ce cas, l'article 16 de la directive relative à la protection des données ne s'applique pas puisque, en réalité, l'utilisation de données à caractère personnel par des particuliers n'entre absolument pas dans le cadre de la directive dès lors que cette utilisation relève du champ d'application de l'« exemption domestique[156] ». L'exemption domestique est l'utilisation de données à caractère personnel « par une personne physique dans le cadre d'une activité purement personnelle ou domestique[157] ». Depuis la décision de la CJUE dans l'affaire *Bodil Lindqvist*[158], cette exemption doit toutefois être interprétée de façon restreinte, en particulier à l'égard de la diffusion de données. L'exemption domestique ne s'étend notamment pas à la publication de données à caractère personnel à un nombre illimité de destinataires sur Internet (pour plus d'informations sur l'affaire, se reporter aux Sections 2.1.2, 2.2, 2.3.1 et 6.1).

Dans le droit du CdE, l'obligation de confidentialité est sous-entendue dans la notion de sécurité des données figurant à l'article 7 de la Convention 108, consacré à la sécurité des données.

156 Directive relative à la protection des données, art. 3, para. 2, deuxième tiret.

157 *Ibid.*

158 CJUE, C-101/01, *Bodil Lindqvist*, 6 novembre 2003.

Pour les sous-traitants, la confidentialité signifie qu'ils ne peuvent utiliser les données à caractère personnel qui leur sont confiées par le responsable du traitement que dans la mesure où ils respectent les instructions de ce dernier. Pour les salariés d'un responsable du traitement ou d'un sous-traitant, la confidentialité requiert qu'ils n'utilisent des données à caractère personnel que selon les instructions de leurs supérieurs compétents.

L'obligation de confidentialité doit figurer dans tout contrat conclu entre des responsables du traitement et leurs sous-traitants. En outre, les responsables du traitement et les sous-traitants devront prendre des mesures spécifiques pour imposer à leurs salariés une obligation légale de confidentialité, habituellement obtenue par l'insertion de clauses de confidentialité dans le contrat de travail du salarié.

Le non-respect d'obligations professionnelles de confidentialité est puni par le droit pénal de nombreux États membres de l'UE et États contractants de la Convention 108.

4.3. Règles relatives à la transparence du traitement

Points clés

- Avant de commencer le traitement de données à caractère personnel, le responsable du traitement doit, au minimum, informer les personnes concernées de l'identité du responsable du traitement et de la finalité du traitement des données, à moins que la personne concernée ne dispose déjà de ces informations.
- Lorsque les données sont collectées auprès de tiers, l'obligation d'information ne s'applique pas si :
  - le traitement des données est prévu par la loi ; ou
  - la fourniture d'informations se révèle impossible ou impliquerait des efforts disproportionnés.
- Avant de commencer le traitement de données à caractère personnel, le responsable du traitement doit également :
  - notifier l'autorité de contrôle des traitements envisagés ; ou
  - faire en sorte que le traitement soit documenté en interne par un délégué indépendant à la protection des données à caractère personnel, si le droit national prévoit une telle procédure.

Le principe du traitement loyal requiert une transparence du traitement. À cette fin, le **droit du CdE** dispose que toute personne doit être capable d'établir l'existence de fichiers automatisés, leur finalité et le responsable du traitement compétent[159]. La façon d'y parvenir est laissée au législateur national. Le **droit de l'UE** est plus spécifique, garantissant une transparence pour la personne concernée au moyen de l'obligation du responsable du traitement d'informer la personne concernée et par voie de notification pour le grand public.

Les deux ordres juridiques prévoient des exceptions et restrictions aux obligations de transparence du responsable du traitement dans le droit national dès lors qu'une telle restriction constitue une mesure nécessaire pour garantir certains intérêts publics ou la protection de la personne concernée ou des droits et libertés de tiers, tant que cela est nécessaire dans une société démocratique[160]. De telles exceptions peuvent, par exemple, être nécessaires dans le contexte d'une enquête sur un crime, mais peuvent aussi être justifiées dans d'autres circonstances.

4.3.1. Information

Conformément au droit du CdE et de l'UE, les responsables du traitement sont tenus d'informer à l'avance la personne concernée du traitement envisagé[161]. Cette obligation ne dépend pas d'une demande de la personne concernée, mais doit être honorée de façon proactive par le responsable du traitement, peu importe que la personne concernée se montre intéressée par l'information.

Contenu de l'information

L'information doit inclure la finalité du traitement, ainsi que l'identité et les coordonnées du responsable du traitement[162]. La directive relative à la protection des données requiert de transmettre des informations complémentaires « dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont collectées, ces informations supplémentaires sont nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données ». Les articles 10 et 11 de la directive définissent notamment les grandes lignes des catégories de données traitées et les destinataires de ces données, ainsi que l'existence du droit d'accès

159 Convention 108, art. 8, point a).

160 *Ibid.*, art. 9, para. 2 ; et directive relative à la protection des données, art. 13, para. 1.

161 Convention 108, art. 8, point a) ; et directive relative à la protection des données, art. 10 et 11.

162 Convention 108, art. 8, point a) ; et directive relative à la protection des données, art. 10, points a) et b).

aux données et du droit de rectification de celles-ci. Lorsque des données sont collectées auprès des personnes concernées, l'information doit préciser si les réponses aux questions sont obligatoires ou volontaires, ainsi que les possibles conséquences d'une absence de réponse[163].

Du point de vue du **droit du CdE**, la transmission d'une telle information peut être considérée comme une bonne pratique dans le cadre du principe de la loyauté du traitement des données et, dans cette mesure, fait également partie du droit du CdE.

Le principe de la loyauté du traitement requiert que l'information soit facilement compréhensible par les personnes concernées. Il convient d'utiliser un langage adapté aux destinataires. Le niveau et le type de langage utilisés devraient être différents selon que l'on s'adresse à un public d'adultes ou d'enfants, au grand public ou à des universitaires experts.

Certaines personnes concernées voudront être informées brièvement sur la façon dont leurs données sont traitées et la raison de ce traitement, tandis que d'autres demanderont des explications détaillées. Le groupe de travail Article 29 s'est penché sur la question de savoir comment équilibrer cet aspect d'une information équitable et il milite en faveur de l'idée d'avis stratifiés[164], permettant à la personne concernée de décider du niveau de détail qu'elle souhaite obtenir.

Moment de remise des informations

La directive relative à la protection des données contient des dispositions légèrement différentes concernant le moment auquel les informations doivent être remises selon que les données ont été collectées auprès de la personne concernée (article 10) ou auprès d'un tiers (article 11). Lorsque les données sont collectées auprès de la personne concernée, l'information doit être remise, au plus tard, à la date de la collecte. Lorsque les données sont collectées auprès de tiers, l'information doit être remise, au plus tard, au moment où le responsable du traitement enregistre les données ou avant que les données ne soient communiquées à un tiers pour la première fois.

163 Directive relative à la protection des données, art. 10, point c).

164 Groupe de travail Article 29 (2004), Avis 10/2004 sur « Dispositions davantage harmonisées en matière d'informations », WP 100, Bruxelles, 25 novembre 2004.

Exceptions à l'obligation d'informer

Dans le droit de l'UE, il existe une exception générale à l'obligation d'informer la personne concernée lorsque celle-ci dispose déjà de l'information[165]. Il s'agit des situations dans lesquelles la personne concernée sait déjà, selon les circonstances de l'affaire, que ses données vont faire l'objet d'un traitement pour une certaine finalité par un certain responsable du traitement.

L'article 11 de la directive, qui porte sur l'obligation d'informer une personne concernée lorsque les données n'ont pas été obtenues auprès d'elle, dispose également qu'une telle obligation n'existe pas, en particulier pour un traitement à finalité statistique ou de recherche historique ou scientifique, lorsque :

- l'information s'avère impossible ;
- impliquerait des efforts disproportionnés ; ou
- si la législation prévoit expressément l'enregistrement ou la communication des données[166].

Seul l'article 11, paragraphe 2, de la directive relative à la protection des données dispose que des personnes concernées ne doivent pas être informées de traitements dès lors que ceux-ci sont prévus par la loi. Compte tenu de l'hypothèse juridique générale selon laquelle nul n'est censé ignorer la loi, on pourrait affirmer que, lorsque des données sont collectées auprès d'une personne concernée conformément à l'article 10 de la directive, la personne concernée dispose déjà de l'information. Mais dans la mesure où la connaissance de la loi n'est qu'une hypothèse, le principe de loyauté du traitement nécessiterait, conformément à l'article 10, que la personne concernée soit informée même si le traitement est prévu par la loi, d'autant plus que cette information n'est pas particulièrement compliquée lorsque des données sont collectées directement auprès de la personne concernée.

S'agissant du droit du CdE, la Convention 108 prévoit explicitement des exceptions à son article 8. Encore une fois, les exceptions énoncées aux articles 10 et 11 de la directive relative à la protection des données peuvent être vues comme des exemples de bonne pratique pour les exceptions de l'article 9 de la Convention 108.

165 Directive relative à la protection des données, art. 10 et art. 11, para. 1.

166 *Ibid.*, considérant 40 et art. 11, para. 2.

Différents modes d'information

La façon idéale d'informer serait de s'adresser à chaque personne concernée, par oral ou par écrit. Si les données sont collectées auprès de la personne concernée, l'information devrait aller de pair avec la collecte. Mais lorsque des données sont collectées auprès de tiers, compte tenu notamment des difficultés pratiques évidentes à joindre les personnes concernées personnellement, l'information peut aussi être fournie par publication appropriée.

L'une des façons les plus efficaces de remettre l'information sera d'intégrer des clauses d'information correspondantes sur le site internet du responsable du traitement, sous forme de politique de vie privée du site internet, par exemple. Cependant, une partie significative de la population n'utilise pas Internet et la politique d'information d'une entreprise ou d'une autorité publique devrait en tenir compte.

4.3.2. Notification

Le droit national peut imposer aux responsables du traitement de notifier l'autorité de contrôle compétente de leurs traitements avant toute publication. Le droit national pourrait aussi prévoir que les responsables du traitement aient recours à un délégué à la protection des données à caractère personnel chargé, en particulier, de tenir un registre des traitements effectués par le responsable du traitement[167]. Ce registre interne doit être mis à la disposition du public sur demande.

Exemple : une notification, ainsi qu'une documentation émanant d'un délégué interne à la protection des données à caractère personnel, doit décrire les principales caractéristiques du traitement de données en question. Cela englobe des informations sur le responsable du traitement, la finalité du traitement, la base légale du traitement, les catégories de données traitées, les probables destinataires tiers et la possibilité ou non de flux transfrontières de données et, si oui, lesquels.

La publication de notifications par l'autorité de contrôle doit prendre la forme d'un registre spécial. Pour atteindre cet objectif, l'accès à ce registre doit être facile et gratuit. Il en va de même de la documentation tenue par le délégué à la protection des données à caractère personnel d'un responsable du traitement.

167 *Ibid.*, art. 18, para. 2, deuxième tiret.

Des exceptions aux obligations de notification de l'autorité de contrôle compétente ou de recours à un délégué interne à la protection des données peuvent être prévues par le droit national pour les traitements dont il est peu probable qu'ils présentent un risque particulier pour les personnes concernées, ainsi que prévu par l'article 18, paragraphe 2, de la directive relative à la protection des données[168].

4.4. Règles relatives à la promotion de la conformité

Points clés

- Développant le principe de la responsabilité, la directive relative à la protection des données mentionne plusieurs instruments de promotion de la conformité :
  - contrôle préalable des traitements envisagés par l'autorité de contrôle nationale ;
  - délégués à la protection des données à caractère personnel apportant au responsable du traitement une expertise spéciale en matière de protection des données ;
  - codes de conduite précisant les règles existantes en matière de protection des données pour l'application dans une branche d'une entreprise, en particulier d'une entreprise commerciale.
- Le droit du CdE propose des instruments similaires de promotion de la conformité dans sa recommandation profilage.

4.4.1. Contrôle préalable

Conformément à l'article 20 de la directive relative à la protection des données, l'autorité de contrôle doit vérifier les traitements qui peuvent présenter des risques particuliers au regard des droits et libertés des personnes concernées, en raison de leur finalité ou de leurs circonstances, avant le début du traitement. Le droit national détermine les traitements qui doivent faire l'objet d'un contrôle préalable. Un tel contrôle peut entraîner l'interdiction de traitements ou un ordre de modification de caractéristiques dans la conception proposée du traitement. L'article 20 de la directive vise à éviter qu'un traitement inutilement risqué ne débute, puisque l'autorité de contrôle est habilitée à interdire un tel traitement. La condition préalable à l'efficacité de ce mécanisme est que l'autorité de contrôle soit effectivement notifiée.

168 *Ibid.*, art. 18, para. 2, premier tiret.

Pour garantir que les responsables du traitement remplissent leur obligation de notification, les autorités de contrôle auront besoin de pouvoirs coercitifs, tels que la capacité à verbaliser les responsables du traitement.

Exemple : si une entreprise réalise des traitements qui, selon le droit national, sont soumis à un contrôle préalable, cette entreprise doit remettre la documentation sur le traitement envisagé à l'autorité de contrôle. L'entreprise n'est pas autorisée à commencer les traitements avant d'avoir reçu une réponse positive de l'autorité de contrôle.

Dans certains États membres, le droit national prévoit que des traitements peuvent commencer en l'absence de réaction de l'autorité de contrôle dans un certain délai, par exemple sous trois mois.

4.4.2. Délégués à la protection des données à caractère personnel

La directive relative à la protection des données permet au droit national de prévoir que les responsables de traitement nomment un détaché aux fonctions de délégué à la protection des données à caractère personnel[169], l'objectif étant de garantir que les droits et libertés des personnes concernées ne soient pas affectés négativement par les traitements[170].

Exemple : en Allemagne, conformément à l'article 4f, paragraphe 1, de la loi fédérale relative à la protection des données (*Bundesdatenschutzgesetz*), les entreprises privées sont tenues de nommer un délégué interne à la protection des données à caractère personnel dès lors qu'elles affectent de façon permanente dix personnes ou plus au traitement automatisé de données à caractère personnel.

La capacité à atteindre cet objectif requiert une certaine indépendance de la part du délégué au sein de la structure du responsable du traitement, ainsi que cela est explicitement soulevé dans la directive. Des droits du travail forts visant à prévenir toute éventualité, telle qu'un licenciement injustifié, seraient aussi nécessaires pour soutenir le fonctionnement efficace du poste de délégué.

169 *Ibid.*, art. 18, para. 2, deuxième tiret.

170 *Ibid.*

Pour promouvoir la conformité au droit national en matière de protection des données, le concept des délégués internes à la protection des données à caractère personnel a également été adopté dans certaines recommandations du CdE[171].

4.4.3. Codes de conduite

Pour promouvoir la conformité, les secteurs commerciaux et autres peuvent rédiger des règles détaillées régissant leurs activités de traitement classiques, codifiant des bonnes pratiques. L'expertise des membres du secteur privilégiera des solutions pratiques et, par conséquent, susceptibles d'être mises en œuvre. Par conséquent, les États membres (ainsi que la Commission européenne) sont encouragés à promouvoir l'élaboration de codes de conduite destinés à contribuer, en fonction de la spécificité des secteurs, à la bonne application des dispositions nationales prises par les États membres en application de la directive[172].

Pour garantir que ces codes de conduite soient conformes aux dispositions nationales adoptées en vertu de la directive relative à la protection des données, les États membres doivent établir une procédure d'évaluation des codes. Cette procédure requiert normalement la participation de l'autorité nationale, d'associations professionnelles et d'autres organisations représentant différentes catégories de responsables du traitement[173].

Les projets de codes communautaires, ainsi que les modifications ou prorogations de codes existants, peuvent être soumis au groupe de travail Article 29 pour évaluation. Après approbation par le groupe de travail, la Commission européenne peut assurer une publicité appropriée aux codes ainsi approuvés[174].

Exemple : la Fédération européenne de Marketing Direct (FEDMA) a développé un code de pratique européen concernant l'utilisation de données à caractère personnel dans le domaine du marketing direct. Le code a été soumis avec succès au groupe de travail Article 29. Une annexe, consacrée aux communications de marketing électroniques, a été ajoutée au code en 2010[175].

171 Voir, par exemple, recommandation profilage, art. 8.3.

172 Directive relative à la protection des données, art. 27, para. 1.

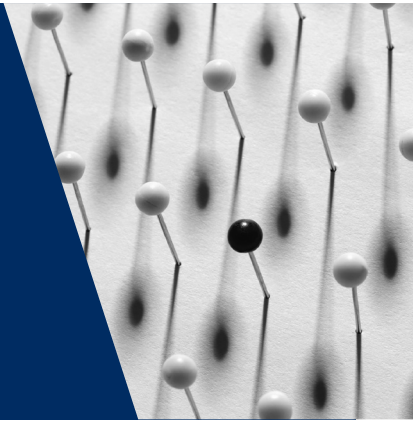
173 *Ibid.*, art. 27, para. 2.

174 *Ibid.*, art. 27, para. 3.

175 Groupe de travail Article 29 (2010), Avis 4/2010 sur le code de conduite européen de la FEDMA relatif à l'exploitation de données à caractère personnel dans le cadre d'opérations de marketing direct, WP 174, Bruxelles, 13 juillet 2010.

5

Les droits des personnes concernées et leur application



UE	Questions traitées	CdE
Droit d'accès		
Directive relative à la protection des données, article 12 CJUE, C-553/07, *College van burgemeester en wethouders van Rotterdam c. M.E.E.*, 7 mai 2009	**Droit d'accès à ses propres données**	Convention 108, article 8, point b)
	Droit de rectification, d'effacement (suppression) ou de verrouillage	Convention 108, article 8, point c) CouEDH, *Cemalettin Canli c. Turquie*, n° 22427/04, 18 novembre 2008 CouEDH, *SegerstedtWiberg et autres c. Suède*, n° 62332/00, 6 juin 2006 CouEDH, *Ciubotaru c. Moldavie*, n° 27138/04, 27 avril 2010
Droit d'opposition		
Directive relative à la protection des données, article 14, paragraphe 1, point a)	**Droit d'opposition en raison de la situation particulière de la personne concernée**	Recommandation profilage, article 5.3
Directive relative à la protection des données, article 14, paragraphe 1, point b)	**Droit d'opposition à une utilisation ultérieure de données à des fins de marketing**	Recommandation sur le marketing direct, article 4.1

Directive relative à la protection des données, article 15	**Droit d'opposition à des décisions automatisées**	Recommandation profilage, article 5.5
Contrôle indépendant		
Charte, article 8, paragraphe 3 Directive relative à la protection des données, article 28 Institutions européennes, règlement relatif à la protection des données, chapitre V Règlement relatif à la protection des données CJUE, C-518/07, *Commission européenne c. République fédérale d'Allemagne*, 9 mars 2010 CJUE, C-614/10, *Commission européenne c. République d'Autriche*, 16 octobre 2012 CJUE, C-288/12, *Commission européenne c. Hongrie*, 8 avril 2014	**Autorités nationales de contrôle**	Convention 108, protocole additionnel, article 1
Voies de recours et sanctions		
Directive relative à la protection des données, article 12	**Demande au responsable du traitement**	Convention 108, article 8, point b)
Directive relative à la protection des données, article 28, paragraphe 4 Institutions européennes, règlement relatif à la protection des données, article 32, paragraphe 2	**Plaintes déposées par une autorité de contrôle**	Convention 108, protocole additionnel, article 1, paragraphe 2, point b)
Charte, article 47	**Juridictions (en général)**	CEDH, article 13
Directive relative à la protection des données, article 28, paragraphe 3	**Juridictions nationales**	Convention 108, protocole additionnel, article 1, point 4
TFUE, article 263, paragraphe 4 Institutions européennes, règlement relatif à la protection des données, article 32, paragraphe 1 TFUE, article 267	**CJUE**	
	CouEDH	CEDH, article 34
Voies de recours et sanctions		
Charte, article 47 Directive relative à la protection des données, articles 22 et 23 CJUE, C-14/83, *Sabine von Colson et Elisabeth Kamann c. Land Nordrhein-Westfalen*, 10 avril 1984	**Infractions au droit national en matière de protection des données**	CEDH, article 13 (uniquement pour les États membres du CdE) Convention 108, article 10 CouEDH, *K.U. c. Finlande*, n °2872/02, 2 mars 2008

CJUE, C-152/84, *M.H. Marshall c. Southampton and SouthWest Hampshire Area Health Authority*, 26 février 1986		CouEDH, *Biriuk c. Lituanie*, n° 23373/03, 25 novembre 2008
Institutions européennes, règlement relatif à la protection des données, articles 34 et 49 CJUE, C-28/08 P, *Commission européenne c. The Bavarian Lager Co. Ltd*, 29 juin 2010	**Infractions au droit de l'UE par des institutions et organes communautaires**	

L'efficacité des règles juridiques en général et des droits des personnes concernées en particulier dépend en grande partie de l'existence de mécanismes appropriés pour les appliquer. Dans le droit européen en matière de protection des données, le droit national doit donner à la personne concernée les moyens de protéger ses données. Le droit national doit également prévoir l'établissement d'autorités de contrôle indépendantes pour aider les personnes concernées dans l'exercice de leurs droits et contrôler les traitements de données à caractère personnel. En outre, le droit à un recours effectif, tel que garanti par la CEDH et la Charte, impose que des recours judiciaires soient ouverts à tous.

5.1. Les droits des personnes concernées

Points clés

- Toute personne a le droit, en vertu de la législation nationale, d'obtenir du responsable du traitement la confirmation que celui-ci traite ou non ses données.
- Les personnes concernées ont le droit, en vertu de la législation nationale :
  - d'avoir accès à leurs données auprès de tout responsable du traitement qui traite de telles données ;
  - de faire rectifier (ou verrouiller, le cas échéant) leurs données par le responsable du traitement qui les traite, si les données sont inexactes ;
  - de faire supprimer ou verrouiller leurs données, le cas échéant, par le responsable du traitement si celui-ci traite leurs données illégalement.
- En outre, les personnes concernées ont le droit de s'opposer à des responsables de traitement concernant :
  - des décisions automatisées (prises à l'aide de données à caractère personnel traitées uniquement par des moyens automatisés) ;
  - le traitement de leurs données s'il aboutit à des résultats disproportionnés ;
  - l'utilisation de leurs données à des fins de marketing direct.

5.1.1. Droit d'accès

Dans le droit de l'UE, l'article 12 de la directive relative à la protection des données contient les éléments du droit d'accès des personnes concernées, y compris le droit d'obtenir du responsable du traitement « la confirmation que des données la concernant sont ou ne sont pas traitées, ainsi que des informations portant au moins sur les finalités du traitement, les catégories de données sur lesquelles il porte et les destinataires ou les catégories de destinataires auxquels les données sont communiquées » et « la rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme à la présente directive, notamment en raison du caractère incomplet ou inexact des données ».

Dans le droit du CdE, les mêmes droits existent et doivent être prévus par la législation nationale (article 8 de la Convention 108). Plusieurs recommandations du CdE utilisent le terme « accès », décrivent les différents aspects du droit d'accès et proposent de les transposer dans le droit national comme exposé au paragraphe ci-dessus.

Conformément à l'article 9 de la Convention 108, et à l'article 13 de la directive relative à la protection des données, l'obligation des responsables du traitement de répondre à une demande d'accès d'une personne concernée peut être limitée en raison des intérêts légitimes prépondérants de tiers. De tels intérêts peuvent inclure des intérêts publics tels que la sécurité nationale, la sécurité publique et la poursuite d'infractions pénales, ainsi que des intérêts privés qui priment sur les intérêts relatifs à la protection des données. Toute exception ou limitation doit être nécessaire dans une société démocratique et proportionnée au but recherché. Dans des cas très exceptionnels, par exemple en raison d'indications médicales, la protection de la personne concernée elle-même peut nécessiter une limitation de la transparence ; cela concerne en particulier la limitation du droit d'accès de toute personne concernée.

Lorsque des données sont traitées uniquement à des fins de recherche scientifique ou statistique, la directive relative à la protection des données permet la limitation des droits d'accès par la législation nationale ; à condition toutefois qu'il existe des garanties juridiques adéquates. En particulier, il convient de garantir qu'aucune mesure ou décision se rapportant à des personnes désignées ne sera prise dans le contexte du traitement des données et qu'« il n'existe manifestement aucun risque

d'atteinte à la vie privée de la personne concernée »[176]. L'article 9, paragraphe 3, de la Convention 108 contient des dispositions similaires.

Le droit d'accès à ses propres données

Dans le droit du CdE, le droit d'accès à ses propres données est explicitement reconnu par l'article 8 de la Convention 108. La CouEDH a maintes fois rappelé qu'il existe un droit d'accès aux informations concernant ses propres données détenues ou utilisées par des tiers et que ce droit découle de la nécessité du respect de la vie privée[177]. Dans l'affaire *Leander*[178], la CouEDH a conclu que le droit d'accès à des données à caractère personnel enregistrées par des autorités publiques peut toutefois être limité dans certaines circonstances.

Dans le droit de l'UE, le droit d'accès à ses propres données est explicitement reconnu par l'article 12 de la directive relative à la protection des données et, en tant que droit fondamental, à l'article 8, paragraphe 2, de la Charte.

L'article 12, point a), de la directive, dispose que les États membres doivent garantir à chaque personne concernée un droit d'accès à ses propres données à caractère personnel et un droit d'information. En particulier, chaque personne concernée a le droit d'obtenir du responsable du traitement la confirmation que les données la concernant sont ou ne sont pas traitées, ainsi que les informations portant au moins sur les éléments suivants :

- les finalités du traitement ;
- les catégories de données concernées ;
- les données faisant l'objet des traitements ;
- les destinataires ou les catégories de destinataires auxquels les données sont communiquées ;

176 Directive relative à la protection des données, art. 13, para. 2.

177 CouEDH, *Gaskin c. Royaume-Uni*, n° 10454/83, 7 juillet 1989 ; CouEDH, *Odièvre c. France* [GC], n° 42326/98, 13 février 2003 ; CouEDH, *K.H. et autres c. Slovaquie*, n° 32881/04, 28 avril 2009 ; CouEDH, *Godelli c. Italie*, n° 33783/09, 25 septembre 2012.

178 CouEDH, *Leander c. Suède*, n° 9248/81, 11 juillet 1985.

- toute information disponible sur l'origine des données faisant l'objet des traitements ;

- lorsque les décisions sont automatisées, la logique qui sous-tend tout traitement automatisé de données.

Le législateur national peut prévoir des informations supplémentaires devant être remises par le responsable du traitement, par exemple la citation de la base légale autorisant le traitement des données.

> Exemple : toute personne accédant à ses données à caractère personnel peut déterminer si les données sont exactes ou non. Il est donc indispensable que la personne concernée soit informée des catégories de données traitées, ainsi que du contenu des données. Par conséquent, il suffit pour un responsable du traitement qu'il indique simplement à la personne concernée qu'il traite son nom, son adresse, sa date de naissance et ses centres d'intérêt. Le responsable du traitement doit également indiquer à la personne concernée qu'il traite « le nom : N.N. ; une adresse : 1040 Vienne, Schwarzenbergplatz 11, Autriche ; la date de naissance : 10/10/1974 ; et les centres d'intérêt (selon la déclaration de la personne concernée) : musique classique ». Le dernier élément contient en plus des informations sur l'origine des données.

L'information de la personne concernée sur les données faisant l'objet de traitements et la communication de toutes les informations disponibles quant à leur origine doivent intervenir sous forme intelligible, ce qui signifie que le responsable du traitement peut devoir expliquer plus en détail à la personne concernée l'objet du traitement. Par exemple, se contenter de citer des abréviations techniques ou des termes médicaux en réponse à une demande d'accès ne sera généralement pas suffisant, même si l'enregistrement ne porte que sur de tels termes ou abréviations.

L'information sur l'origine des données traitées par le responsable du traitement doit être donnée dans la réponse à la demande d'accès, pour autant que l'information soit disponible. Cette disposition doit être comprise à la lumière des principes de la loyauté et de la responsabilité. Un responsable du traitement ne peut pas détruire des informations sur l'origine des données pour s'exonérer de l'obligation de les divulguer, de même qu'il ne peut ignorer les besoins usuels classiques et reconnus de documentation dans le domaine de ses activités. Ne conserver aucune

documentation sur l'origine des données traitées ne satisfera généralement pas l'obligation du responsable du traitement au titre du droit d'accès.

En cas d'évaluations automatisées, la logique générale de l'évaluation devra être expliquée, y compris les critères particuliers qui ont été pris en considération dans l'évaluation de la personne concernée.

La directive ne précise pas clairement si le droit d'accès à des informations concerne le passé et, si oui, quelle période dans le passé. À cet égard, comme souligné dans la jurisprudence de la CJUE, le droit d'accès à ses propres données ne peut être restreint indûment par des limites dans le temps. Les personnes concernées doivent aussi avoir une possibilité raisonnable d'obtenir des informations sur d'anciens traitements.

Exemple : dans l'affaire *Rijkeboer*[179], la CJUE était invitée à déterminer si, conformément à l'article 12, point a), de la directive, le droit d'un individu d'accéder à des informations sur les destinataires ou catégories de destinataires de données à caractère personnel, et sur le contenu des données communiquées, pouvait être limité à un an avant la demande d'accès.

Pour déterminer si l'article 12, point a), de la directive, autorise une telle limitation dans le temps, la Cour a décidé d'interpréter cet article à la lumière des finalités de la directive. La Cour a tout d'abord relevé que le droit d'accès est nécessaire pour permettre à la personne concernée d'obtenir que le responsable du traitement rectifie, efface ou verrouille ses données (article 12, point b)) ou qu'il signale aux tiers auxquels les données ont été communiquées, ces rectifications, effacement et verrouillage (article 12, point c)). Le droit d'accès est également nécessaire pour permettre à la personne concernée d'exercer le droit d'opposition au traitement de ses données à caractère personnel (article 14) ou le droit de recours en cas de dommage subi (articles 22 et 23).

Pour assurer l'effet utile des dispositions susvisées, la Cour a considéré que « ce droit doit nécessairement concerner le passé. En effet, si tel n'était pas le cas, la personne intéressée ne serait pas en mesure d'exercer de manière efficace son droit de faire rectifier, effacer ou verrouiller les données présumées illicites ou

179 CJUE, C-553/07, *College van burgemeester en wethouders van Rotterdam c. M. E. E. Rijkeboer*, 7 mai 2009.

incorrectes ainsi que d'introduire un recours juridictionnel et d'obtenir la réparation du préjudice subi ».

Le droit à la rectification, à l'effacement et au verrouillage de données

« Toute personne doit pouvoir bénéficier du droit d'accès aux données la concernant qui font l'objet d'un traitement, afin de s'assurer notamment de leur exactitude et de la licéité de leur traitement[180] ». Conformément à ces principes, les personnes concernées doivent avoir le droit, en vertu de la législation nationale, d'obtenir du responsable du traitement la rectification, l'effacement ou le verrouillage de leurs données si elles estiment que leur traitement n'est pas conforme à la disposition de la directive, en particulier en raison de la nature inexacte ou incomplète des données[181].

Exemple : dans l'affaire *Cemalettin Canli c. Turquie*[182], la CouEDH a constaté une violation de l'article 8 de la CEDH dans un rapport de police mal rédigé dans le cadre d'une procédure pénale.

Le requérant avait par deux fois été impliqué dans une procédure pénale en raison de son appartenance alléguée à des organisations illégales mais n'avait jamais été condamné. Lorsque le requérant a de nouveau été arrêté et inculpé pour un autre crime, la police a soumis à la juridiction pénale un rapport intitulé « *formulaire d'information sur des infractions complémentaires* » dans lequel le requérant était présenté comme membre de deux organisations illégales. La demande du requérant visant à modifier le rapport et les dossiers de la police n'a pas été acceptée. La CouEDH a retenu que les informations figurant dans le rapport de police relevaient du champ de l'article 8 de la CEDH, puisque des informations publiques peuvent aussi relever du domaine de la « vie privée » dès lors qu'elles sont systématiquement collectées et enregistrées dans des fichiers tenus par les autorités. De plus, le rapport de police était incorrect et son élaboration et sa présentation à la juridiction pénale n'étaient pas prévues par la loi. La CouEDH a donc conclu à une violation de l'article 8.

180 Directive relative à la protection des données, considérant 41.

181 *Ibid.*, art. 12, point b).

182 CouEDH, *Cemalettin Canli c. Turquie*, n° 22427/04, 18 novembre 2008, paras. 33, 42 et 43 ; CouEDH, *Dalea c. France*, n° 964/07, 2 février 2010.

Exemple : dans l'affaire *Segerstedt-Wiberg et autres c. Suède*[183], les requérants étaient affiliés à certains partis politiques libéraux et communistes. Ils pensaient que des informations à leur sujet avaient été saisies dans des dossiers policiers de sécurité. La CouEDH a pu établir que l'enregistrement des données en cause avait une base légale et poursuivait un but légitime. À l'égard de certains requérants, la CouEDH a retenu que la conservation continue des données constituait une ingérence disproportionnée dans leur vie privée. Par exemple, dans le cas de M. Schmid, les autorités avaient conservé une information selon laquelle il aurait prôné la résistance violente aux contrôles de police lors de manifestations en 1969. La CouEDH a jugé que cette information ne pouvait pas poursuivre un intérêt pertinent pour la sécurité nationale, en particulier compte tenu de sa nature historique. La CouEDH a conclu à une violation de l'article 8 de la CEDH à l'égard de quatre des cinq requérants.

Dans certaines affaires, il suffira que la personne concernée demande simplement la rectification de l'orthographe d'un nom, un changement d'adresse ou de numéro de téléphone, par exemple. Si, toutefois, de telles demandes sont liées à des questions juridiques, telles que l'identité légale de la personne concernée ou le lieu de résidence visant à obtenir la notification de documents légaux, des demandes de rectification pourraient ne pas suffire et le responsable du traitement pourrait être habilité à exiger une preuve de la prétendue inexactitude. De telles demandes ne sauraient placer une charge de la preuve déraisonnable sur la personne concernée et, par conséquent, empêcher les personnes concernées d'obtenir la rectification de leurs données. La CouEDH a constaté des violations de l'article 8 de la CEDH dans plusieurs affaires dans lesquelles le requérant n'avait pas été en mesure de contester l'exactitude des informations conservées dans des registres secrets[184].

Exemple : dans l'affaire *Ciubotaru c. Moldavie*[185], le requérant n'avait pas été en mesure de faire remplacer son origine ethnique enregistrée dans des dossiers officiels en tant que « moldave », par « roumaine », au motif qu'il n'avait pas motivé sa demande de modification. La CouEDH a jugé acceptable que les États réclament des preuves objectives lors de l'enregistrement de l'identité ethnique d'une personne. Lorsqu'une telle demande est basée sur des motifs purement subjectifs et non étayés, les autorités peuvent refuser. Toutefois, la

183 CouEDH, *Segerstedt-Wiberg et autres c. Suède*, n° 62332/00, 6 juin 2006, paras. 89 et 90 ; voir également, par exemple, CouEDH, *M.K. c. France*, n° 19522/09, 18 avril 2013.

184 CouEDH, *Rotaru c. Roumanie*, n° 28341/95, 4 mai 2000.

185 CouEDH, *Ciubotaru c. Moldavie*, n° 27138/04, 27 avril 2010, paras. 51 et 59.

demande du requérant avait d'autres fondements que la simple perception subjective de sa propre origine ethnique ; il avait pu démontrer des liens objectivement vérifiables avec le groupe ethnique des Roumains, tels que la langue, le nom, la compréhension et autres. Selon le droit national, le requérant était cependant tenu d'apporter la preuve de ce que ses parents avaient appartenu au groupe ethnique des Roumains. Compte tenu des réalités historiques de la Moldavie, une telle exigence a créé un obstacle insurmontable à l'enregistrement d'une identité ethnique autre que celle enregistrée au sujet de ses parents par les autorités soviétiques. En empêchant le requérant d'obtenir l'examen de sa demande à la lumière de preuves objectivement vérifiables, l'État n'a pas honoré son obligation positive de garantir le respect effectif de la vie privée. La CouEDH a conclu à une violation de l'article 8 de la CEDH.

Lors d'un procès civil ou d'une procédure devant une autorité publique visant à déterminer si des données sont correctes, la personne concernée peut demander qu'une mention ou une note soit inscrite dans son dossier personnel afin de souligner le fait qu'elle en conteste l'exactitude et qu'une décision officielle est pendante. Pendant cette période, le responsable du traitement des données ne doit pas présenter les données comme certaines ou finales, en particulier à des tiers.

La demande d'une personne concernée souhaitant obtenir l'effacement ou la suppression de données repose souvent sur l'allégation de l'absence de base légitime pour le traitement. De telles allégations surviennent souvent lorsque le consentement a été retiré ou quand certaines données ne sont plus nécessaires pour remplir la finalité de la collecte des données. La charge de la preuve de la légitimité du traitement des données pèse sur le responsable du traitement, puisque c'est lui qui doit en répondre. Conformément au principe de la responsabilité, le responsable du traitement doit être en mesure de démontrer à tout moment qu'il existe une base légale solide à son traitement de données, faute de quoi le traitement doit être interrompu.

Si le traitement de données est contesté au motif que les données sont incorrectes ou font l'objet d'un traitement illicite, la personne concernée peut, conformément au principe de loyauté du traitement, exiger que les données en cause soient verrouillées. Cela signifie que les données ne sont pas supprimées, mais que le responsable du traitement doit s'abstenir de les utiliser pendant la période de verrouillage. Cela serait particulièrement nécessaire dans les cas où l'utilisation continue de données inexactes ou détenues illégitimement pourrait porter préjudice à la personne concernée. Le droit national devrait fournir plus d'informations sur le moment où

l'obligation de verrouiller l'utilisation de données peut survenir et sur la façon dont elle devrait être exercée.

Les personnes concernées ont également le droit d'obtenir du responsable du traitement qu'il informe les tiers de tout verrouillage, toute rectification ou tout effacement s'ils ont reçu des données avant ces traitements. Dans la mesure où la communication des données aurait dû être documentée par le responsable du traitement, il devrait être possible d'identifier les destinataires des données et d'en demander la suppression. Mais si les données ont été publiées entre-temps, sur Internet par exemple, il peut s'avérer impossible d'obtenir leur suppression dans tous les cas, puisque les destinataires des données ne peuvent être identifiés. Conformément à la directive relative à la protection des données, contacter des destinataires de données en vue de leur rectification, suppression ou verrouillage est obligatoire « si cela ne s'avère pas impossible ou ne suppose pas un effort disproportionné[186] ».

5.1.2. Droit d'opposition

Le droit d'opposition inclut le droit d'opposition à des décisions individuelles automatisées, le droit d'opposition en raison de la situation particulière de la personne concernée et le droit d'opposition à toute future utilisation des données à des fins de prospection (« marketing direct »).

Le droit d'opposition à des décisions individuelles automatisées

Les décisions automatisées sont des décisions prises à l'aide de données à caractère personnel traitées uniquement par des moyens automatisés. S'il est probable que de telles décisions aient un impact considérable sur les vies des individus parce qu'elles portent, par exemple, sur leur solvabilité, leur rendement professionnel, leur comportement ou leur fiabilité, une protection spéciale est nécessaire pour éviter toutes conséquences inappropriées. La directive relative à la protection des données dispose que les décisions automatisées ne devraient pas trancher des questions importantes pour des individus et impose que la personne ait le droit de revoir la décision automatisée[187].

Exemple : la notation de crédit est une illustration pratique important du processus de décision automatisée. Pour déterminer rapidement la solvabilité d'un

186 Directive relative à la protection des données, art. 12, point c), dernière moitié de la phrase.

187 *Ibid.*, art. 15, para. 1.

futur client, certaines données, telles que la situation professionnelle et familiale, sont collectées auprès du client et associées à des données sur la personne obtenues auprès d'autres sources, telles que des systèmes d'information sur le crédit. Ces données sont saisies automatiquement dans un algorithme de notation, qui calcule une valeur globale représentant la fiabilité du client potentiel. L'employé de la société peut ainsi décider en quelques secondes si la personne concernée constitue un client acceptable.

Néanmoins, selon la directive, les États membres doivent prévoir qu'une personne peut être soumise à une décision individuelle automatisée si les intérêts de la personne concernée ne sont pas en jeu, parce que la décision était en faveur de celle-ci, ou sont sauvegardés par d'autres moyens[188]. Le **droit du CdE** prévoit aussi un droit d'opposition à des décisions automatisées, ainsi qu'il ressort de la recommandation profilage[189].

Le droit d'opposition en raison de la situation particulière de la personne concernée

Il n'existe pas de droit général pour les personnes concernées de s'opposer au traitement de leurs données[190]. L'article 14, point a), de la directive relative à la protection des données reconnaît cependant à la personne concernée le droit de s'opposer au traitement de ses données pour des raisons prépondérantes et légitimes tenant à sa situation particulière. Un droit similaire a été reconnu dans la recommandation profilage du CdE[191]. De telles dispositions visent à trouver le bon équilibre entre le droit à la protection des données de la personne concernée et les droits légitimes de tiers au traitement de ces données.

Exemple : une banque enregistre pendant sept ans des données sur ses clients qui ne remboursent pas correctement leur prêt. Un client dont les données sont enregistrées dans cette base de données sollicite un autre prêt. La base de données est consultée, une évaluation de la situation financière est réalisée et le client se voit refuser le prêt. Le client peut toutefois s'opposer à l'enregistrement

188 *Ibid.*, art. 15, para. 2.

189 Recommandation profilage, art. 5, para. 5.

190 Voir également CouEDH, *M.S. c. Suède*, n° 20837/92, 27 août 1997, dans laquelle des données médicales avaient été communiquées sans consentement ou possibilité d'opposition ; CouEDH, *Leander c. Suède*, n° 9248/81, 26 mars 1987 ; ou CouEDH, *Mosley c. Royaume-Uni*, n° 48009/08, 10 mai 2011.

191 Recommandation profilage, art. 5, para. 3.

de données à caractère personnel dans la base de données et demander la suppression des données s'il peut prouver que le retard de paiement était simplement le résultat d'une erreur qui avait été corrigée dès qu'il en avait eu connaissance.

L'effet d'une opposition réussie est que les données en question ne peuvent plus être traitées par le responsable du traitement. Des traitements réalisés sur les données de la personne concernée avant l'opposition restent cependant légitimes.

Le droit d'opposition à une utilisation ultérieure de données à des fins de prospection

L'article 14, point b), de la directive relative à la protection des données prévoit un droit spécifique d'opposition à l'utilisation de ses propres données aux fins de prospection. Un tel droit est également énoncé dans la recommandation du CdE sur le marketing direct[192]. Ce type d'opposition est destiné à être soulevé avant que les données ne soient communiquées à des tiers à des fins de prospection. La personne concernée doit donc avoir la possibilité de s'y opposer avant le transfert des données.

5.2. Contrôle indépendant

Points clés

- Pour garantir la protection effective des données, il appartient au droit national d'établir des autorités de contrôle indépendant.
- Les autorités de contrôle nationales agissent en toute indépendance, qui est garantie par le droit fondateur et reflétée dans la structure organisationnelle spécifique de l'autorité de contrôle.
- Les autorités de contrôle ont des missions spécifiques, parmi lesquelles :
  - surveiller et promouvoir la protection des données au niveau national ;
  - conseiller les personnes concernées et les responsables du traitement, ainsi que le gouvernement et le grand public ;

192 CdE, Comité des Ministres (1985), recommandation Rec (85) 20 aux États membres relative à la protection des données à caractère personnel utilisés à des fins de marketing direct, 25 octobre 1985, art. 4, para. 1.

- entendre les réclamations et aider la personne concernée en cas de violations alléguées au droit à la protection des données ;
- contrôler les responsables du traitement et les sous-traitants ;
- intervenir si nécessaire en
  - avertissant, admonestant, voire en verbalisant les responsables du traitement et sous-traitants,
  - ordonnant la correction, le verrouillage ou la suppression de données,
  - imposant une interdiction de traitement ;
- soumettre l'affaire aux tribunaux.

La directive relative à la protection des données requiert un contrôle indépendant comme mécanisme important garantissant la protection effective des données. La directive a introduit un instrument d'application de la protection des données qui n'apparaissait initialement pas dans la Convention 108 ou les lignes directrices sur la vie privée de l'OCDE.

Le contrôle indépendant s'étant révélé indispensable pour le développement d'une protection effective des données, une nouvelle disposition des lignes directrices sur la vie privée de l'OCDE, dans leur version révisée, adoptée en 2013, appelle les États membres à « procéder à la mise en place et assurer le fonctionnement d'autorités chargées de la protection de la vie privée qui soient dotées de la gouvernance, des ressources et de l'expertise technique nécessaires pour exercer leurs pouvoirs efficacement et prendre leurs décisions de manière objective, impartiale et cohérente[193] ».

Dans le droit du CdE, le protocole additionnel à la Convention 108 a rendu obligatoire la création d'autorités de contrôle. Cet acte énonce à l'article 1 le cadre légal des autorités de contrôle indépendantes que les États contractants doivent mettre en place dans leur droit national. Il utilise des formulations similaires pour décrire les missions et les pouvoirs de ces autorités à celles figurant dans la directive relative à la protection des données. En principe, les autorités de contrôle devraient donc fonctionner de la même façon dans le droit de l'UE et dans celui du CdE.

193 OCDE (2013), Lignes directrices sur la protection de la vie privée et les flux transfrontières de données de caractère personnel, art. 19, point c).

Dans le droit de l'UE, les compétences et la structure organisationnelle des autorités de contrôle ont tout d'abord été présentées à l'article 28, paragraphe 1, de la directive relative à la protection des données. Le règlement relatif à la protection des données des institutions communautaires[194] crée le Contrôleur européen de la protection des données (CEPD) comme autorité de contrôle du traitement des données par les organes et institutions communautaires. Lorsqu'il présente les rôles et responsabilités de l'autorité de contrôle, le règlement se fonde sur l'expérience acquise depuis la promulgation de la directive relative à la protection des données.

L'indépendance des autorités de protection des données est garantie par l'article 16, paragraphe 2, du TFUE et l'article 8, paragraphe 3, de la Charte. Ce dernier prévoit spécifiquement le contrôle par une autorité indépendante comme un élément essentiel du droit fondamental à la protection des données. En outre, la directive relative à la protection des données impose aux États membres de créer des autorités de contrôle chargées de surveiller l'application de la directive en toute indépendance[195]. Non seulement la législation afférente à la création d'un organe de contrôle doit contenir des dispositions garantissant spécifiquement son indépendance, mais la structure organisationnelle particulière de l'autorité doit démontrer cette'indépendance.

En 2010, la CJUE avait traité pour la première fois la question de l'étendue de l'exigence d'indépendance des autorités de contrôle de la protection des données[196]. Les exemples ci-dessous illustrent sa position.

Exemple : dans l'affaire *Commission c. Allemagne*[197], la Commission européenne a demandé à la CJUE de déclarer que l'Allemagne avait incorrectement transposé l'exigence d'une action « en toute indépendance » des autorités de contrôle chargées de garantir la protection des données et, partant, manqué à ses obligations découlant de l'article 28, paragraphe 1, de la directive relative

194 Règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données, JO 2001 L 8, art. 41 à 48.

195 Directive relative à la protection des données, art. 28, para. 1, dernière phrase ; Convention 108, protocole additionnel, art. 1, para. 3.

196 Voir FRA (2010), *Les droits fondamentaux : défis et réussites en 2010*, Rapport annuel, p. 59. La FRA avait traité cette question de façon très détaillée dans son rapport sur *La protection des données à caractère personnel dans l'Union européenne : le rôle des autorités nationales chargées de la protection des données*, publié en mai 2010.

197 CJUE, C-518/07, *Commission européenne c. République fédérale d'Allemagne*, 9 mars 2010, para. 27.

à la protection des données. Selon la Commission, le problème provenait du fait que l'Allemagne avait placé sous la tutelle de l'État les autorités de contrôle compétentes en matière de traitement des données à caractère personnel par le secteur non public dans les différents Länder.

Selon la Cour, l'appréciation du bien-fondé du recours dépendait de la portée de l'exigence d'indépendance contenue dans cet article et, partant, de l'interprétation de cette disposition.

La Cour a souligné que les mots « en toute indépendance » de l'article 28, paragraphe 1, de la directive, devaient être interprétés en se fondant sur le libellé même de cette disposition ainsi que sur les objectifs et l'économie de la directive relative à la protection des données[198]. La Cour a souligné que les autorités de contrôle étaient « les gardiennes » des droits liés au traitement de données à caractère personnel garantis dans la directive, et que leur institution dans les États membres était considérée « comme un élément essentiel de la protection des personnes à l'égard du traitement des données à caractère personnel[199] ». La Cour a conclu que « 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[200] ».

La CJUE a également retenu que la signification des termes « en toute indépendance » devait être interprétée à la lumière de l'indépendance du CEPD, telle que définie dans le règlement relatif à la protection des données des institutions communautaires. Elle a souligné que l'article 44, paragraphe 2, dudit règlement, « explicite la notion d'indépendance en ajoutant que, dans l'accomplissement de sa mission, le CEPD ne sollicite ni n'accepte d'instructions de quiconque ». Cela exclut la supervision par l'État d'une autorité de contrôle indépendante chargée de la protection des données[201].

Par conséquent, la CJUE a considéré que les institutions allemandes chargées de la protection des données au niveau des Länder n'étaient pas suffisamment

198 *Ibid.*, paras. 17 et 29.

199 *Ibid.*, para. 23.

200 *Ibid.*, para. 25.

201 *Ibid.*, para. 27.

indépendantes pour contrôler le traitement de données à caractère personnel par des organes non publics, au motif qu'elles étaient soumises à la tutelle de l'État.

Exemple : dans l'affaire *Commission c. Autriche*[202], la CJUE a mis en évidence des problèmes similaires concernant la position de certains membres et du personnel de l'autorité autrichienne de protection des données (commission de protection des données, « DSK »). Dans cette affaire, la Cour a conclu que le droit autrichien empêchait l'autorité autrichienne de protection des données d'exercer ses fonctions en toute indépendance au sens de la directive relative à la protection des données. L'indépendance de l'autorité autrichienne de protection des données n'était pas suffisamment garantie dans la mesure où la main d'œuvre de la DSK était fournie par le chancelier fédéral, lequel supervisait également la DSK et avait le droit d'être informé à tout moment sur son travail.

Exemple, dans l'affaire *Commission c. Hongrie*[203], la CJUE a souligné que « *l'exigence [...] selon laquelle il convient de garantir que chaque autorité de contrôle exerce en toute indépendance les missions dont elle est investie implique l'obligation pour l'État membre concerné de respecter la durée du mandat d'une telle autorité jusqu'à son terme initialement prévu* » et a considéré que « *en mettant fin de manière anticipée au mandat de l'autorité de contrôle de la protection des données à caractère personnel, la Hongrie a manqué aux obligations qui lui incombent en vertu de la directive 95/46/CE* [...] ».

Certaines autorités de contrôle se voient attribuer des pouvoirs et capacités par le droit national, parmi lesquels[204] :

- conseiller les responsables du traitement et personnes concernées sur toutes les questions relatives à la protection des données ;
- enquêter sur des traitements et intervenir en conséquence ;
- donner des avertissements ou admonestations aux responsables du traitement ;
- ordonner la rectification, le verrouillage, l'effacement ou la destruction des données ;

202 CJUE, C-614/10, *Commission européenne c. République d'Autriche*, 16 octobre 2012, paras. 59 et 63.

203 CJUE, C-288/12, *Commission européenne c. Hongrie*, 8 avril 2014, paras. 50 et 67.

204 Directive relative à la protection des données, art. 28 ; voir également Convention 108, protocole additionnel, art. 1.

- imposer une interdiction temporaire ou définitive de traitement ;
- soumettre l'affaire aux tribunaux.

Pour pouvoir exercer ses fonctions, une autorité de contrôle doit avoir accès à l'ensemble des données à caractère personnel et aux informations nécessaires à une enquête, ainsi qu'à tous les locaux dans lesquels un responsable du traitement conserve des informations pertinentes.

Il existe des différences considérables entre les juridictions nationales quant aux procédures et aux effets juridiques des constatations d'une autorité de contrôle. Elles peuvent aller de recommandations de type médiateur à des décisions immédiatement exécutables. Par conséquent, lorsqu'il s'agit d'analyser l'efficacité des voies de recours ouvertes dans une juridiction, les instruments de recours doivent être appréciés dans leur contexte.

5.3. Voies de recours et sanctions

Points clés

- Conformément à la Convention 108, ainsi qu'à la directive relative à la protection des données, la législation nationale doit prévoir des voies de recours et sanctions appropriées contre des infractions au droit à la protection des données.
  - Dans le droit de l'UE, le droit à un recours effectif requiert que la législation nationale prévoie des recours judiciaires contre des infractions au droit à la protection des données, qu'il soit possible de se rapprocher d'une autorité de contrôle ou non.
  - Le droit national doit prévoir des sanctions effectives, équivalentes, proportionnées et dissuasives.
- Avant de saisir les tribunaux, il convient tout d'abord de se tourner vers un responsable du traitement. Le caractère obligatoire ou non de la prise de contact avec une autorité de contrôle avant de saisir un tribunal est laissé au législateur national.
- Les personnes concernées peuvent saisir la CouEDH de violations du droit en matière de protection des données, en dernier recours et sous certaines conditions.
- En outre, les personnes concernées peuvent saisir la CJUE, mais uniquement dans des cas très limités.

Les droits conférés par la législation en matière de protection des données peuvent uniquement être exercés par la personne dont les droits sont en jeu ; c'est-à-dire une personne qui soit, ou au moins affirme être, la personne concernée. Ces personnes peuvent être représentées dans l'exercice de leurs droits par des personnes satisfaisant aux exigences nécessaires en vertu de la législation nationale. Les mineurs doivent être représentés par leurs parents ou tuteurs. Devant les autorités de contrôle, une personne peut aussi être représentée par des associations dont le but légal est de promouvoir le droit à la protection des données.

5.3.1. Demandes au responsable du traitement

Les droits visés à la Section 3.2 doivent tout d'abord être exercés vis-à-vis du responsable du traitement. Il est inutile de s'adresser directement à l'autorité nationale de contrôle ou à un tribunal, puisque l'autorité ne pourrait que conseiller de contacter d'abord le responsable du traitement et le tribunal jugerait toute demande irrecevable. Les conditions de forme d'une demande légalement pertinente à un responsable du traitement, en particulier la question de savoir si elle doit prendre la forme d'une demande écrite, doivent être réglées par le droit national.

L'entité qui a été contactée en qualité de responsable du traitement doit réagir à la demande, même si elle n'est pas le responsable du traitement. En tout état de cause, une réponse doit être remise à la personne concernée dans le délai imparti par la législation nationale, même s'il s'agit uniquement de dire qu'aucune donnée n'est traitée au sujet du demandeur. Conformément aux dispositions de l'article 12, point a), de la directive relative à la protection des données, et de l'article 8, point b), de la Convention 108, cette demande doit être traitée « sans délai excessif ». Le droit national devrait donc prévoir une période de réponse qui soit suffisamment courte, mais qui permette tout de même au responsable du traitement de répondre correctement à la demande.

Avant de répondre à la demande, l'entité contactée en qualité de responsable du traitement doit établir l'identité du demandeur afin de déterminer s'il est véritablement la personne qu'il prétend être et afin d'éviter ainsi un manquement grave à la confidentialité. Lorsque les exigences relatives à l'établissement de l'identité ne sont pas particulièrement réglementées dans le droit national, elles doivent faire l'objet d'une décision du responsable du traitement. Le principe de la loyauté du traitement impose cependant que les responsables du traitement ne prévoient pas de conditions trop difficiles pour reconnaître l'identification (et l'authenticité de la requête, comme évoqué dans la Section 2.1.1).

Le droit national doit également trancher la question de savoir si les responsables du traitement, avant de répondre à des demandes, peuvent imposer le règlement de frais au demandeur : l'article 12, point a), de la directive, et l'article 8, point b), de la Convention 108, disposent que la réponse à des demandes d'accès doit être donnée « sans (...) frais excessifs ». Dans de nombreux pays européens, le droit national dispose que les réponses à des demandes en vertu du droit en matière de protection des données doivent être apportées gratuitement, tant qu'elles n'impliquent pas d'effort excessif ou déraisonnable ; en contrepartie, le droit national protège généralement les responsables du traitement contre les abus du droit à obtenir une réponse à des demandes.

Si la personne, l'institution ou l'organe approché en qualité de responsable du traitement ne conteste pas être le responsable du traitement, il est tenu, dans le délai prescrit par le droit national :

- d'accéder à la demande et d'indiquer au demandeur la façon dont il s'est conformé à la demande ; ou

- d'indiquer au demandeur la raison pour laquelle sa demande ne sera pas acceptée.

5.3.2. Plaintes déposées par l'autorité de contrôle

Toute personne ayant déposé une demande d'accès ou s'étant opposée à un traitement ne recevant pas de réponse opportune et satisfaisante peut soumettre une demande d'assistance à l'autorité nationale de contrôle de la protection des données. Dans le cadre de la procédure devant l'autorité de contrôle, il convient de préciser si la personne, l'institution ou l'organe contacté par le demandeur était effectivement tenu de répondre à la demande et si la réponse a été correcte et suffisante. La personne concernée doit être informée par l'autorité de contrôle de l'issue de la procédure[205]. Les effets juridiques des résultats de la procédure devant des autorités de contrôle nationales dépendent du droit national : les décisions de l'autorité peuvent-elles être légalement exécutées, c'est-à-dire sont-elles exécutables par une autorité officielle, ou est-il nécessaire de faire appel à un tribunal si le responsable du traitement ne suit pas les décisions (avis, avertissement, etc.) de l'autorité de contrôle ?

205 Directive relative à la protection des données, art. 28, para. 4.

Si le droit à la protection des données garanti par l'article 16 du TFUE a été violé par des institutions ou organes communautaires, la personne concernée peut former une réclamation auprès du CEPD[206], l'autorité indépendante de contrôle de la protection des données aux termes du règlement relatif à la protection des données des institutions communautaires définissant les devoirs et pouvoirs du CEPD. En l'absence de réponse du CEPD dans un délai de six mois, la réclamation est présumée rejetée.

Il doit également être possible de former un recours devant les tribunaux contre des décisions rendues par des autorités nationales de contrôle. Cela vaut pour la personne concernée comme pour le responsable du traitement, puisqu'il était également partie à la procédure devant une autorité de contrôle.

Exemple : le 24 juillet 2013, l'*Information Commissioner* britannique a rendu une décision demandant à la police du Hertfordshire de cesser l'utilisation d'un système de localisation de plaques d'immatriculation jugé illégal. Les données collectées par des caméras étaient enregistrées à la fois dans les bases de données de la police locale et dans une base de données centrale. Les photos des plaques d'immatriculation étaient conservées pendant deux ans et les photos des véhicules pendant 90 jours. Il a été retenu qu'une utilisation aussi prolongée de caméras et d'autres formes de surveillance n'était pas proportionnée au problème que l'on tentait de résoudre.

5.3.3. Plainte déposée devant un tribunal

Conformément à la directive relative à la protection des données, toute personne ayant adressé une demande à un responsable du traitement en vertu du droit en matière de protection des données et qui n'est pas satisfaite de la réponse du responsable du traitement doit être habilitée à former une réclamation devant une juridiction nationale[207].

Le caractère obligatoire ou non de la prise de contact préalable avec une autorité de contrôle, avant de saisir un tribunal, est laissé au législateur national. Dans la plupart des cas, toutefois, il sera avantageux pour les personnes exerçant leur droit à la

206 Règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données, JO 2001 L 8.

207 Directive relative à la protection des données, art. 22.

protection des données de contacter d'abord l'autorité de contrôle, dans la mesure où le traitement de demandes d'assistance ne devrait pas être bureaucratique et devrait être gratuit. L'expertise documentée dans la décision de l'autorité de contrôle (avis, avertissement, etc.) peut aussi aider la personne concernée à faire valoir ses droits devant les tribunaux.

Dans le droit du CdE, des violations du droit à la protection des données, prétendument intervenues au niveau national d'un État contractant à la CEDH et constituant en même temps une violation de l'article 8 de la CEDH, peuvent également être invoquées devant la CouEDH après l'épuisement de toutes les voies de recours nationales disponibles. Invoquer une violation de l'article 8 de la CEDH devant la CouEDH doit également satisfaire à d'autres critères de recevabilité (articles 34 à 37 de la CEDH)[208].

Bien que les demandes à la CouEDH puissent être directement dirigées contre des États contractants, elles peuvent aussi porter indirectement sur des actions ou omissions de particuliers, pour autant qu'un État contractant n'ait pas honoré ses obligations positives en vertu de la CEDH et n'ait pas apporté de protection suffisante contre des violations du droit à la protection des données dans le droit national.

Exemple : dans l'affaire *K.U. c. Finlande*[209], le requérant, un mineur, s'est plaint qu'une publicité à connotation sexuelle avait été postée à son sujet sur un site de rencontres en ligne. L'identité de la personne ayant posté l'information n'avait pas été révélée par le fournisseur de services en raison des obligations de confidentialité imposées par le droit finlandais. Le requérant affirmait que le droit finlandais ne prévoyait pas de protection suffisante contre de telles actions d'un particulier plaçant des informations compromettantes sur autrui (le requérant) sur Internet. La CouEDH a retenu que les États sont non seulement tenus de s'abstenir de toute ingérence arbitraire dans la vie privée des individus, mais qu'ils peuvent également être soumis à des obligations positives impliquant « l'adoption de mesures visant au respect de la vie privée jusque dans les relations des individus entre eux ». Dans le cas du requérant, sa protection pratique et effective nécessitait que des mesures effectives soient prises pour identifier et poursuivre l'auteur. Or, l'État ne proposait pas une telle protection et la CouEDH a conclu à une violation de l'article 8 de la CEDH.

208 CEDH, art. 34 à 37, disponibles à l'adresse : www.echr.coe.int/Pages/home.aspx?p=caselaw/analysis&c=#n1347458601286_pointer.

209 CouEDH, *K.U. c. Finlande*, n °2872/02, 2 mars 2009.

Exemple : dans l'affaire *Köpke c. Allemagne*[210], la requérante était soupçonnée de vol sur son lieu de travail et avait donc fait l'objet d'une surveillance vidéo secrète. La CouEDH a conclu que rien n'indiquait que les autorités nationales aient omis de trouver un juste équilibre, dans la limite de leur marge d'appréciation, entre le droit de la requérante au respect de sa vie privée en vertu de l'article 8, et l'intérêt de son employeur à la protection des droits à la propriété, d'une part, et l'intérêt du grand public à la bonne administration de la justice, d'autre part. Le recours a donc été déclaré irrecevable.

Si la CouEDH retient qu'un État contractant a violé l'un quelconque des droits protégés par la CEDH, l'État contractant est tenu d'exécuter la décision de la CouEDH. Les mesures d'exécution doivent d'abord mettre fin à la violation et remédier, autant que possible, à ses conséquences négatives pour le requérant. L'exécution de décisions peut aussi nécessiter des mesures d'ordre général empêchant des violations similaires à celles constatées par la Cour, que ce soit par la voie d'amendements législatifs, de la jurisprudence ou d'autres mesures.

Lorsque la CouEDH constate une violation de la CEDH, l'article 41 de la CEDH dispose qu'elle peut accorder une satisfaction juste au requérant aux dépens de l'État contractant.

Dans le droit de l'UE[211], les victimes d'infractions au droit national en matière de protection des données, qui transpose le droit européen en la matière, peuvent parfois saisir la CJUE de leur affaire. Il existe deux scénarios possibles sur la façon dont la réclamation d'une personne concernée tirée d'une infraction à son droit à la protection des données peut aboutir à une procédure devant la CJUE.

Dans le premier scénario, la personne concernée doit être la victime directe d'un acte administratif ou réglementaire de l'UE qui enfreint son droit à la protection des données. Selon l'article 263, paragraphe 4, du TFUE :

> *« Toute personne physique ou morale peut former (...) un recours contre les actes dont elle est le destinataire ou qui la concernent directement et individuellement, ainsi que contre les actes réglementaires qui la concernent directement et qui ne comportent pas de mesures d'exécution. »*

210 CouEDH, *Köpke c. Allemagne* (déc.), n° 420/07, 5 octobre 2010.

211 UE (2007), Traité de Lisbonne modifiant le traité sur l'Union européenne et le traité instituant la Communauté européenne, signé à Lisbonne, 13 décembre 2007, JO 2007 C 306. Voir également les versions consolidées du Traité sur l'Union européenne, JO 2012 C 326, et du TFUE, JO 2012 C 326.

Par conséquent, les victimes du traitement illicite de leurs données par un organe communautaire peuvent saisir directement le Tribunal de la CJUE, organe compétent pour statuer sur des affaires relevant du règlement relatif à la protection des données des institutions communautaires. Une personne peut également saisir directement la CJUE si sa situation juridique est directement affectée par une disposition légale communautaire.

Le second scénario concerne la compétence de la CJUE (Cour de justice) pour rendre des décisions préjudicielles conformément à l'article 267 du TFUE.

Les personnes concernées peuvent, dans le cadre de procédures nationales, demander à la juridiction nationale d'interroger la Cour de justice sur l'interprétation des traités de l'UE et sur l'interprétation et la validité d'actes des institutions, organes, offices ou agences communautaires. Les explications apportées sont appelées des « décisions préjudicielles ». Il ne s'agit pas d'une voie de recours directe pour le plaignant, mais cela permet aux juridictions nationales de garantir qu'elles interprètent correctement le droit européen.

Si une partie à la procédure devant les juridictions nationales demande le renvoi d'une question devant la CJUE, seules les juridictions nationales agissant en dernier recours, dont les décisions sont finales, sont tenues de s'y conformer.

Exemple : dans l'affaire *Kärntner Landesregierung et autres*[212], la Cour constitutionnelle autrichienne a soumis des questions à la CJUE concernant la validité des articles 3 à 9 de la Directive 2006/24/CE (*directive relative à la conservation des données, invalidée le 8 avril 2014*) au regard des articles 7, 9 et 11 de la Charte, ainsi que la question de savoir si certaines dispositions de la loi fédérale autrichienne sur les télécommunications, transposant la directive relative à la conservation des données, étaient ou non compatibles avec certains aspects de la directive relative à la protection des données et du règlement relatif à la protection des données.

M. Seitlinger, l'un des requérants devant la Cour constitutionnelle, a indiqué utiliser le téléphone, l'iInternet et le courriel pour un usage à la fois professionnel et personnel. Par conséquent, les informations qu'il envoyait et recevait passaient sur les réseaux de télécommunications publics. La loi autrichienne sur

212 CJEU, affaires jointes C 293/12 et C 594/12, *Digital Rights Ireland et Seitlinger et autres*, 8 avril 2014.

les télécommunications de 2003 imposait à son fournisseur de service de collecter et d'enregistrer des données sur son utilisation du réseau. M. Seitlinger avait réalisé que cette collecte et cette sauvegarde de ses données à caractère personnel n'étaient absolument pas nécessaires aux fins techniques de transmettre les informations d'un point A à un point B sur le réseau. En outre, la collecte et la sauvegarde de ces données n'étaient absolument pas nécessaires à des fins de facturation. M. Seitlinger n'avait certainement pas consenti à une telle utilisation de ses données à caractère personnel. La seule raison pour la collecte et la sauvegarde de toutes ces données supplémentaires était la loi autrichienne sur les télécommunications de 2003.

M. Seitlinger a donc engagé une action devant la Cour constitutionnelle autrichienne, soutenant que les obligations réglementaires imposées à son fournisseur de services étaient contraires aux droits fondamentaux que lui conférait l'article 8 de la Charte.

La CJUE statue uniquement sur les éléments constitutifs de la demande de décision préjudicielle qui lui est adressée. La juridiction nationale reste compétente pour statuer sur l'affaire initiale.

En principe, la Cour de justice doit répondre aux questions qui lui sont posées. Elle ne peut pas refuser de rendre une décision préjudicielle au motif que cette réponse ne serait ni pertinente, ni opportune par rapport à l'affaire initiale. Elle peut toutefois refuser si la question ne relève pas de son domaine de compétence.

Enfin, si un droit à la protection des données garanti par l'article 16 du TFUE, est violé par une institution ou un organe communautaire dans le cadre du traitement de données à caractère personnel, la personne concernée peut soumettre l'affaire au Tribunal de la CJUE (article 32, paragraphes 1 et 4, du règlement relatif à la protection des données des institutions communautaires). Il en va de même pour les décisions du CEPD concernant de telles infractions (article 32, paragraphe 3, du règlement relatif à la protection des données des institutions communautaires).

Tandis que le Tribunal de la CJUE est compétent pour statuer sur les questions concernant le règlement relatif à la protection des données des institutions communautaires, si une personne, agissant en qualité de membre du personnel d'une institution ou d'un organe communautaire, cherche à obtenir réparation, cette personne doit cependant s'adresser au tribunal de la fonction publique de l'UE.

Exemple : l'affaire *Commission européenne c. The Bavarian Lager Co. Ltd*[213] illustre les voies de recours existantes contre des activités ou décisions d'institutions ou organes communautaires en matière de protection des données.

Bavarian Lager a demandé à la Commission européenne l'accès au procès-verbal complet d'une réunion organisée par la Commission, qui aurait été consacrée à des questions juridiques pertinentes pour la société. La Commission a refusé la demande d'accès de la société au motif d'intérêts prépondérants l'emportant sur la protection des données[214]. Bavarian Lager a formé un recours contre cette décision devant la CJUE, en application de l'article 32 du règlement relatif à la protection des données des institutions communautaires ; plus précisément, le recours a été formé devant le tribunal de première instance (prédécesseur du Tribunal). Dans sa décision dans l'affaire T-194/04, *Bavarian Lager c. Commission*, le tribunal de première instance a annulé la décision de la Commission rejetant la demande d'accès. La Commission européenne a fait appel de cette décision devant la Cour de justice de la CJUE. La Cour de justice (en grande chambre) a annulé l'arrêt du tribunal de première instance et confirmé le rejet de la demande d'accès de la Commission européenne.

5.3.4. Sanctions

Dans le droit du CdE, l'article 10 de la Convention 108 dispose que des sanctions et recours appropriés doivent être établis par chaque Partie concernant les violations aux dispositions du droit interne donnant effet aux principes de base pour la protection des données énoncés dans la Convention 108[215]. Dans le droit de l'UE, l'article 24 de la directive relative à la protection des données dispose que les États membres « prennent les mesures appropriées pour assurer la pleine application des dispositions de la présente directive et déterminent notamment les sanctions à appliquer en cas de violation des dispositions prises (...) ».

Les deux actes laissent aux États membres une large marge d'appréciation dans le choix des sanctions et recours appropriés. Aucun acte légal ne donne de conseils

213 CJUE, C-28/08 P, *Commission européenne c. The Bavarian Lager Co. Ltd*, 29 juin 2010.

214 Pour une analyse de l'argument, voir : CEPD (2011), *Accès du public aux documents contenant des données à caractère personnel après l'arrêt rendu dans l'affaire* Bavarian Lager, Bruxelles, CEPD, disponible à l'adresse : www.secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_EN.pdf

215 CouEDH, *I. c. Finlande*, n° 20511/03, 17 juillet 2008 ; CouEDH, *K.U. c. Finlande*, n° 2872/02, 2 décembre 2008.

particuliers sur la nature ou le type de sanctions appropriées, ni d'exemples correspondants.

Toutefois :

> *« Bien que les États membres de l'UE jouissent d'une marge d'appréciation pour déterminer quelles mesures sont les plus appropriées pour la sauvegarde des droits que les justiciables tirent du droit de l'UE, conformément au principe de coopération loyale visé à l'article 4, paragraphe 3, du TUE, les exigences minimales d'efficacité, d'équivalence, de proportionnalité et de dissuasion doivent être respectés*[216] *».*

La CJUE a régulièrement maintenu que le droit national n'était pas totalement libre de déterminer les sanctions.

Exemple : dans l'affaire *Von Colson et Kamann c. Land Nordrhein-Westfalen*[217], la CJUE a souligné que tous les États membres destinataires d'une directive étaient tenus d'adopter, dans leurs systèmes juridiques nationaux, toutes les mesures nécessaires pour garantir qu'elle soit pleinement effective, conformément aux objectifs poursuivis. La Cour a retenu que, bien qu'il appartienne aux États membres de choisir les façons et moyens de garantir la mise en œuvre d'une directive, cette liberté n'affecte pas l'obligation qui leur est imposée. En particulier, un recours juridique effectif doit permettre à l'individu de poursuivre et exécuter le droit en question dans toute sa mesure. Pour obtenir une protection véritable et efficace, les voies de recours doivent déclencher des procédures pénales et/ou des mesures de compensation dissuasives, assorties de possibles sanctions.

S'agissant des sanctions contre des infractions au droit européen par des institutions ou organes communautaires, en raison du champ particulier du règlement relatif à la protection des données des institutions communautaires, des sanctions ne sont envisagées que sous la forme d'une action disciplinaire. Conformément à l'article 49 du règlement, « tout manquement aux obligations auxquelles un

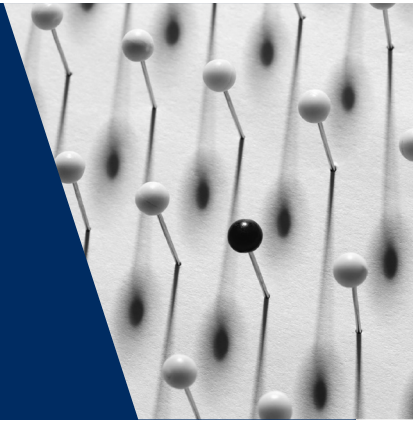
216 FRA (2012), *Avis de l'Agence des droits fondamentaux de l'Union européenne concernant le programme de réforme des règles en matière de protection des données à caractère personnel*, 2/2012, Vienne, 1er octobre 2012, p. 27.

217 CJUE, C-14/83, *Sabine von Kolson et Elisabeth Kamann c. Land Nordrhein-Westfalen*, 10 avril 1984.

fonctionnaire ou un autre agent des Communautés européennes est tenu en vertu du présent règlement, commis intentionnellement ou par négligence, l'expose à une sanction disciplinaire (...) ».

6

Flux transfrontaliers de données



UE	Questions traitées	CdE
Flux transfrontaliers de données		
Directive relative à la protection des données, article 25, paragraphe 1 CJUE, C-101/01, *Bodil Lindqvist*, 6 novembre 2003	**Définition**	Convention 108, protocole additionnel, article 2, paragraphe 1
Libre circulation des données		
Directive relative à la protection des données, article 1, paragraphe 2	**Entre les États membres de l'UE**	
	Entre les États contractants de la Convention 108	Convention 108, article 12, paragraphe 2
Directive relative à la protection des données, article 25	**Vers des pays tiers présentant un niveau adéquat de protection des données**	Convention 108, protocole additionnel, article 2, paragraphe 1
Directive relative à la protection des données, article 26, paragraphe 1	**Vers des pays tiers dans des cas particuliers**	Convention 108, protocole additionnel, article 2, paragraphe 2, point a)
Circulation restreinte de données vers des pays tiers		
Directive relative à la protection des données, article 26, paragraphe 2 Directive relative à la protection des données, article 26, paragraphe 4	**Clauses contractuelles**	Convention 108, protocole additionnel, article 2, paragraphe 2, point b) Guide relatif à la préparation de clauses contractuelles

Directive relative à la protection des données, article 26, paragraphe 2	Règles d'entreprise contraignantes	
Exemples : Accord PNR UE/États-Unis Accord SWIFT UE/États-Unis	Accords internationaux spéciaux	

La directive relative à la protection des données prévoit non seulement la libre circulation des données entre les États membres, mais contient également des dispositions relatives aux exigences afférentes au transfert de données à caractère personnel vers des pays tiers en dehors de l'UE. Le CdE a également reconnu l'importance de la mise en œuvre de règles pour les flux transfrontières de données vers des pays tiers et a adopté le protocole additionnel à la Convention 108 en 2001. Ce protocole reprend les principales règles relatives aux flux transfrontières de données des parties à la Convention et des États membres de l'UE.

6.1. Nature des flux transfrontaliers de données

Point clé

- Le flux transfrontalier de données est le transfert de données à caractère personnel vers un destinataire qui est soumis à une juridiction étrangère.

L'article 2, paragraphe 1, du protocole additionnel à la Convention 108 décrit le flux transfrontières de données comme le transfert de données à caractère personnel vers un destinataire qui est soumis à une juridiction étrangère. L'article 25, paragraphe 1, de la directive relative à la protection des données règle « le transfert vers un pays tiers de données à caractère personnel faisant l'objet d'un traitement, ou destinées à faire l'objet d'un traitement après leur transfert (...) ». Un tel transfert de données n'est autorisé que conformément aux règles énoncées à l'article 2 du protocole additionnel à la Convention 108, ainsi que, pour les États membres de l'UE, aux articles 25 et 26 de la directive relative à la protection des données.

Exemple : dans l'affaire *Bodil Lindqvist*[218], la CJUE a retenu que « l'opération consistant à faire référence, sur une page internet, à diverses personnes, et

218 CJUE, C-101/01, *Bodil Lindqvist*, 6 novembre 2003, paras. 27, 68 et 69.

à les identifier soit par leur nom, soit par d'autres moyens, par exemple leur numéro de téléphone ou des informations relatives à leurs conditions de travail et à leurs passe-temps, constitue un "traitement de données à caractère personnel, automatisé en tout ou en partie", au sens de l'article 3, paragraphe 1, de la directive 95/46 ».

La Cour a ensuite souligné que la directive énonce également des règles spécifiques visant à permettre aux États membres de contrôler le transfert de données à caractère personnel vers des pays tiers.

Toutefois, compte tenu, d'une part, du niveau de développement d'Internet à la date d'élaboration de la directive et, d'autre part, de l'absence dans la directive de critères applicables à l'utilisation d'Internet, « on ne saurait présumer que le législateur communautaire avait l'intention d'inclure dans la notion de "transfert vers un pays tiers de données" une telle inscription (...) de données sur une page internet, même si celles-ci sont ainsi rendues accessibles aux personnes de pays tiers possédant les moyens techniques d'y accéder ».

Toutefois, si la directive « était interprété(e) en ce sens qu'il existe un "transfert vers un pays tiers de données" chaque fois que des données à caractère personnel sont chargées sur une page internet, ce transfert serait nécessairement un transfert vers tous les pays tiers où existent les moyens techniques nécessaires pour accéder à Internet. Le régime spécial prévu par [la directive] deviendrait donc nécessairement, en ce qui concerne les opérations sur Internet, un régime d'application générale. En effet, dès que la Commission constaterait (...) qu'un seul pays tiers n'assure pas un niveau de protection adéquat, les États membres seraient obligés d'empêcher toute mise sur Internet de données à caractère personnel ».

Le principe selon lequel la simple publication de données (à caractère personnel) n'est pas considérée comme un flux transfrontalier de données s'applique aussi aux registres publics en ligne ou aux médias de masse, tels que les journaux (électroniques) et la télévision. Seule une communication s'adressant directement à des destinataires particuliers peut être qualifiée de « flux transfrontalier de données ».

6.2. Libre circulation de données entre des États membres ou entre des États contractants

Point clé

- Le transfert de données à caractère personnel vers un autre État membre de l'Espace économique européen ou vers un autre État contractant à la Convention 108 doit être exempt de toutes restrictions.

Conformément à l'article 12, paragraphe 2, de la Convention 108, **aux termes du droit du CdE**, il doit exister une libre circulation des données à caractère personnel entre les parties à la Convention. Le droit national ne peut restreindre l'exportation de données à caractère personnel vers un État contractant, sauf si :

- la nature particulière des données le nécessite[219] ; ou
- la restriction est nécessaire pour éviter de contourner les dispositions légales nationales relatives aux flux transfrontières de données vers des pays tiers[220].

Dans le droit de l'UE, des restrictions ou interdictions de la libre circulation des données entre les États membres pour des raisons de protection des données sont interdites par l'article 1, paragraphe 2, de la directive relative à la protection des données. La zone de la libre circulation des données a été étendue par l'Accord sur l'espace économique européen (EEE)[221] qui intègre l'Islande, le Liechtenstein et la Norvège au marché intérieur.

Exemple : si un affilié d'un groupe international de sociétés, établi dans plusieurs États membres de l'UE, parmi lesquels la Slovénie et la France, transfère des données à caractère personnel de la Slovénie vers la France, ce flux de données ne doit pas être restreint ou interdit par le droit national slovène.

219 Convention 108, art. 12, para. 3, point a).

220 *Ibid.*, art. 12, para. 3, point b).

221 Décision du Conseil et de la Commission du 13 décembre 1993 relative à la conclusion de l'accord sur l'Espace économique européen entre les Communautés européennes, leurs États membres et la république d'Autriche, la république de Finlande, la république d'Islande, la principauté de Liechtenstein, le royaume de Norvège, le royaume de Suède et la Confédération suisse, JO 1994 L 1.

Mais si le même affilié slovène souhaite transférer les mêmes données à caractère personnel vers la société-mère aux États-Unis, l'exportateur de données slovène doit suivre la procédure prévue par le droit slovène en matière de flux transfrontaliers de données vers des pays tiers sans niveau de protection des données adéquate, à moins que la société-mère n'ait adhéré aux principes de la « sphère de sécurité » relatifs à la protection de la vie privée, un code de conduite volontaire sur la fourniture d'un niveau adéquat de protection des données (voir Section 6.3.1).

Les flux transfrontaliers de données vers des États membres de l'EEE à des fins ne relevant pas du marché intérieur, notamment pour des enquêtes criminelles, ne sont toutefois pas soumis aux dispositions de la directive relative à la protection des données et, par conséquent, ne sont pas couverts par le principe de la libre circulation des données. S'agissant du droit du CdE, tous les domaines sont inclus dans le champ de la Convention 108 et du protocole additionnel à la Convention 108, bien que les États contractants puissent prévoir des exceptions. Tous les membres de l'EEE sont également parties à la Convention 108.

6.3. Libre circulation des données vers des pays tiers

Points clés

- Le transfert de données à caractère personnel vers des pays tiers est exempt de toutes restrictions en vertu du droit national en matière de protection des données si :
  - l'adéquation de la protection des données sur le territoire du destinataire a été établie ; ou
  - cela est nécessaire dans les intérêts spécifiques de la personne concernée ou les intérêts légitimes prépondérants de tiers, en particulier des intérêts publics importants.
- L'adéquation de la protection des données dans un pays tiers signifie que les principes majeurs de la protection des données soient effectivement mis en œuvre dans le droit interne de ce pays.
- Dans le droit de l'UE, l'adéquation de la protection des données dans un pays tiers est appréciée par la Commission européenne. Dans le droit du CdE, il appartient au législateur interne de définir et d'apprécier l'adéquation.

6.3.1. Libre circulation des données en raison d'une protection adéquate

Le **droit du CdE** permet au droit interne d'autoriser la libre circulation de données vers des États non contractants si l'État ou l'organisation destinataire assure un niveau adéquat de protection pour le transfert de données envisagé[222]. Le législateur interne décide de l'appréciation du niveau de protection des données dans un pays étranger et désigne la personne chargée de cette appréciation.

Dans le droit de l'UE, la libre circulation des données vers des pays tiers offrant un niveau adéquat de protection des données est prévue à l'article 25, paragraphe 1, de la directive relative à la protection des données. L'exigence d'adéquation, plutôt que d'équivalence, permet de satisfaire différents modes de mise en œuvre de la protection des données. Conformément à l'article 25, paragraphe 6, de la directive, la Commission européenne est compétente pour apprécier le niveau de protection dans des pays étrangers par la voie d'attestations du niveau adéquat de la protection et de consultations sur l'appréciation avec le groupe de travail Article 29 qui a contribué de façon majeure à l'interprétation des articles 25 et 26[223].

Une attestation de niveau adéquat de la protection délivrée par la Commission européenne a force obligatoire. Si la Commission européenne publie une attestation de niveau adéquat de la protection pour un certain pays au *Journal officiel de l'Union européenne*, tous les pays membres de l'EEE et leurs organes sont tenus de suivre la décision, ce qui signifie que les données peuvent circuler vers ce pays sans procédures de vérification ou d'autorisation devant des autorités nationales[224].

La Commission européenne peut également évaluer certaines parties du système juridique d'un pays ou se limiter à des sujets particuliers. Par exemple, la Commission a attesté du niveau adéquat de protection pour le seul droit commercial privé

222 Convention 108, protocole additionnel, art. 2, para. 1.

223 Voir, par exemple, groupe de travail Article 29 (2003), Document de travail : Transferts de données personnelles vers des pays tiers : Application de l'article 26 (2) de la directive de l'UE relative à la protection des données et aux règles d'entreprise contraignantes applicables aux transferts internationaux de données, WP 74, Bruxelles, 3 juin 2003 ; et groupe de travail Article 29 (2005), Document de travail relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995, WP 114, Bruxelles, 25 novembre 2005.

224 Une liste actualisée des pays ayant reçu une attestation de niveau adéquat de la protection est disponible en anglais sur le site Internet de la Commission européenne, direction générale de la Justice, à l'adresse : http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.

du Canada[225]. Il existe également plusieurs attestations de niveau adéquat de protection pour des transferts basés sur des accords entre l'UE et des pays étrangers. Ces décisions portent exclusivement sur un type spécifique de transfert de données, tel que la transmission de dossiers passagers par des compagnies aériennes à des autorités étrangères de contrôle aux frontières lorsque la compagnie aérienne vole depuis l'UE vers certaines destinations étrangères (voir Section 6.4.3). Une pratique plus récente de transfert de données basée sur des accords spéciaux entre l'UE et des pays tiers abandonne généralement les attestations de niveau adéquat de protection, supposant que l'accord lui-même offre un niveau de protection adéquat des données[226].

L'une des décisions les plus importantes en matière d'adéquation ne porte en réalité par sur un ensemble de dispositions légales[227]. Elle concerne plutôt des règles, telles qu'un code de conduite, appelées principes de la « sphère de sécurité » relatifs à la protection de la vie privée. Ces principes ont été élaborés entre l'Union européenne et les États-Unis pour les sociétés commerciales américaines. L'adhésion à ces principes est obtenue par un engagement volontaire proclamé devant le ministère américain du Commerce et documenté dans une liste publiée par ce ministère. Dans la mesure où l'un des éléments importants de l'adéquation est l'efficacité de la mise en œuvre de la protection des données, l'accord sur les principes de la sphère de sécurité prévoit également un certain contrôle par l'État : seules peuvent adhérer aux principes les sociétés qui sont soumises au contrôle de la *Federal Trade Commission* américaine.

225 Commission européenne (2002), décision 2002/2/CE du 20 décembre 2001 constatant, conformément à la directive 95/46/CE du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par la loi canadienne sur la protection des renseignements personnels et les documents électroniques, JO 2002 L 2.

226 Par exemple, l'accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation des données des dossiers passagers et leur transfert au ministère américain de la sécurité intérieure, JO 2012 L 215, p. 5–14 ou l'accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données de messagerie financière de l'Union européenne aux États-Unis aux fins du programme de surveillance du financement du terrorisme, JO 2010 L 8, p. 11–16.

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

6.3.2. Libre circulation des données dans des cas particuliers

Dans le droit du CdE, l'article 2, paragraphe 2, du protocole additionnel à la Convention 108 permet le transfert de données à caractère personnel à des pays tiers ne disposant pas de protection adéquate des données dès lors que le transfert est prévu par le droit national et qu'il est nécessaire pour :

- les intérêts spécifiques de la personne concernée ; ou
- les intérêts légitimes prépondérants de tiers, en particulier des intérêts publics importants.

Dans le droit de l'UE, l'article 26, paragraphe 1, de la directive relative à la protection des données contient des dispositions similaires à celles du protocole additionnel à la Convention 108.

Conformément à la directive, les intérêts des personnes concernées peuvent justifier la libre circulation de données vers un pays tiers si :

- la personne concernée a donné son consentement de manière non équivoque à l'exportation des données ;
- la personne concernée conclut (ou s'apprête à conclure) un contrat nécessitant clairement que les données soient transférées à un destinataire à l'étranger ;
- un contrat entre un responsable du traitement et un tiers a été conclu dans l'intérêt de la personne concernée ;
- le transfert est nécessaire pour protéger l'intérêt vital de la personne concernée ; ou
- pour le transfert de données depuis des registres publics ; il s'agit d'un exemple d'intérêts prépondérants du grand public de pouvoir accéder à des informations conservées dans des registres publics.

Les intérêts légitimes de tiers peuvent justifier le flux transfrontalier de données[228] :

228 Directive relative à la protection des données, art. 26, para. 1, point d).

- en raison d'un intérêt public important, autre que des affaires de sécurité nationale ou publique, puisque celles-ci ne sont pas couvertes par la directive relative à la protection des données ; ou

- pour la constatation, l'exercice ou la défense d'un droit en justice.

Les affaires susvisées doivent être comprises comme des exceptions à la règle selon laquelle le transfert désinhibé de données vers d'autres pays nécessite un niveau de protection adéquat des données dans le pays destinataire. Les exceptions doivent toujours être interprétées de façon restrictive. C'est ce que le groupe de travail Article 29 a régulièrement souligné dans le contexte de l'article 26, paragraphe 1, de la directive relative à la protection des données, en particulier si le consentement est présenté comme la base du transfert de données[229]. Le groupe de travail Article 29 a conclu que les règles générales relatives à la signification légale du consentement s'appliquaient aussi à l'article 26, paragraphe 1, de la directive. Si, dans le contexte de rapports de travail, par exemple, on ne peut dire avec certitude si le consentement donné par le salarié était véritablement un consentement libre, des transferts de données ne peuvent être fondés sur l'article 26, paragraphe 1, point a), de la directive. Dans de telles situations, l'article 26, paragraphe 2, qui impose aux autorités nationales de protection des données de délivrer une autorisation aux transferts de données, trouve application.

6.4. Circulation restreinte de données vers des pays tiers

Points clés

- Avant d'exporter des données vers des pays tiers ne garantissant pas un niveau adéquat de protection des données, le responsable du traitement peut être tenu de soumettre le flux de données envisagé à l'examen de l'autorité de contrôle.
- Le responsable du traitement qui souhaite exporter des données doit démontrer deux éléments lors de cet examen :
  - l'existence d'une base légale pour le transfert de données vers le destinataire ; et

229 Voir, en particulier, groupe de travail Article 29 (2005), Document de travail relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE, du 24 octobre 1995, WP 114, Bruxelles, 25 novembre 2005.

  - l'existence de mesures garantissant une protection adéquate des données sur le territoire du destinataire.
- Les mesures établissant une protection adéquate des données chez le destinataire peuvent comprendre :
  - des clauses contractuelles entre le responsable du traitement exportant les données et le destinataire étranger des données ; ou
  - des règles d'entreprise contraignantes, habituellement applicables à des transferts de données au sein d'un groupe multinational d'entreprises.
- Les transferts de données vers des autorités étrangères peuvent aussi être régis par un accord international spécial.

La directive relative à la protection des données et le protocole additionnel à la Convention 108 permettent au droit interne d'établir des régimes pour les flux transfrontières de données à destination de pays tiers qui ne garantissent pas un niveau adéquat de protection des données, dès lors que le responsable du traitement a conclu des accords spéciaux pour assurer des garanties adéquates de protection des données sur le territoire du destinataire et dès lors que le responsable du traitement peut en apporter la preuve à une autorité compétente. Cette exigence n'est explicitement mentionnée que dans le protocole additionnel à la Convention 108 ; toutefois, elle est aussi considérée comme la procédure classique par la directive relative à la protection des données.

6.4.1. Clauses contractuelles

Le **droit du CdE** comme le **droit de l'UE** mentionnent des clauses contractuelles entre le responsable du traitement exportant des données et le destinataire dans le pays tiers comme possibles moyens de préserver un niveau suffisant de protection des données dans le pays du destinataire.

Au **niveau de l'UE**, la Commission européenne, avec l'assistance du groupe de travail Article 29, a développé des clauses contractuelles types qui ont été officiellement certifiées par une décision de la Commission comme preuve d'une protection adéquate des données[230]. Dans la mesure où toutes les décisions de la Commission lient les États membres, les autorités nationales en charge de contrôler les flux transfrontaliers de données doivent reconnaître ces clauses contractuelles types dans leurs

230 Directive relative à la protection des données, art. 26, para. 4.

procédures[231]. Par conséquent, si le responsable du traitement qui exporte les données et le destinataire du pays tiers concluent et signent ces clauses, celles-ci constituent envers l'autorité de contrôle une preuve suffisante de l'existence de garanties adéquates.

L'existence de clauses contractuelles types dans le cadre juridique européen n'interdit pas aux responsables du traitement de formuler d'autres clauses contractuelles *ad hoc*. Celles-ci devraient cependant produire le même niveau de protection que celui apporté par les clauses contractuelles types. Les caractéristiques les plus importantes des clauses contractuelles types sont :

- une clause du tiers bénéficiaire qui permet aux personnes concernées d'exercer des droits contractuels même si elles ne sont pas parties au contrat ;

- le destinataire ou l'importateur des données acceptant de faire l'objet de la procédure de l'autorité nationale de contrôle du responsable du traitement exportant les données et/ou de tribunaux en cas de litige.

Il existe aujourd'hui deux ensembles de clauses types pour les transferts de responsable du traitement à responsable du traitement entre lesquels l'exportateur des données peut choisir[232]. Pour les transferts de responsable du traitement à sous-traitant, il n'existe qu'un ensemble de clauses contractuelles types[233].

Dans le contexte du **droit du CdE**, le Comité consultatif de la Convention 108 a élaboré un guide relatif à la préparation de clauses contractuelles[234].

231 TFUE, art. 288.

232 L'ensemble I figure à l'annexe de la Commission européenne (2001), décision 2001/497/CE de la Commission du 15 juin 2001 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu de la directive 95/46/CE, JO 2001 L 181 ; l'ensemble II figure à l'annexe de la Commission européenne (2004), décision 2004/915/CE de la Commission du 27 décembre 2004 modifiant la décision 2001/497/CE en ce qui concerne l'introduction d'un ensemble alternatif de clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers, JO 2004 L 385.

233 Commission européenne (2010), décision 2010/87 de la Commission du 5 février 2010 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE, du Parlement européen et du Conseil, JO 2010 L 39.

234 CdE, Comité consultatif de la Convention 108 (2002), *Guide relatif à la préparation de clauses contractuelles régissant la protection des données lors de communications de données à caractère personnel à des tiers non soumis à un niveau de protection des données adéquat.*

6.4.2. Règles d'entreprise contraignantes

Les règles d'entreprise contraignantes multilingues (REC) impliquent souvent plusieurs autorités européennes de protection des données à la fois[235]. Pour que des REC soient approuvées, le projet correspondant doit être envoyé avec les formulaires de demande standardisés à l'autorité chef de file[236]. L'autorité chef de file est identifiable sur le formulaire de demande standardisé. Cette autorité informe ensuite toutes les autorités de contrôle dans les pays membres de l'EEE dans lesquels des affiliés du groupe sont établis, bien que leur participation à la procédure d'évaluation des REC soit facultative. Même si elles n'ont pas valeur contraignante, toutes les autorités de protection des données concernées devraient intégrer le résultat de l'évaluation dans leurs procédures d'autorisation officielles.

6.4.3. Accords internationaux spéciaux

L'UE a conclu des accords spéciaux pour deux types de transferts de données :

Données des dossiers passagers (PNR)

Les données PNR sont collectées par des transporteurs aériens pendant le processus de réservation et comprennent les noms, adresses, informations sur la carte de crédit et numéros de sièges de passagers aériens. Conformément à la législation américaine, les compagnies aériennes sont tenues de communiquer ces données au ministère américain de la Sécurité intérieure avant le départ des passagers, que ce soit pour les vols à l'arrivée ou au départ des États-Unis.

235 Le contenu et la structure de règles d'entreprise contraignantes appropriées sont expliqués dans groupe de travail Article 29 (2008) Document de travail établissant un cadre pour la structure des règles d'entreprise contraignantes, WP 154, Bruxelles, 24 juin 2008 ; et dans groupe de travail Article 29 (2008), Document de travail établissant un tableau présentant les éléments et principes des règles d'entreprise contraignantes, WP 153, Bruxelles, 24 juin 2008.

236 Groupe de travail Article 29 (2007), Recommandation 1/2007 sur l'application type pour l'approbation des règles d'entreprise contraignantes applicables au transfert des données à caractère personnel, WP 133, Bruxelles, 10 janvier 2007.

Afin d'assurer une protection adéquate des données PNR, et en conformité avec les dispositions de la directive 95/46/CE, un « paquet PNR »[237] comprenant l'adéquation du traitement des données effectué par le ministère de la Sécurité intérieure des États-Unis (*Department of Homeland Security United States,* DHS) a été adopté en 2004.

Après l'annulation du paquet PNR par la Cour de justice,[238] deux accords séparés ont été signés ayant comme objectif, tout d'abord, de fournir une base juridique pour la divulgation des données PNR aux autorités américaines; et ensuite, d'assurer la protection adéquate des données dans le pays destinataire.

Le premier accord sur la façon dont les données sont partagées et gérées entre les pays de l'UE et les États-Unis, signé en 2007 présentait plusieurs défauts et a été remplacé en 2012 par un nouvel accord visant à mieux garantir la sécurité juridique.[239] Le nouvel accord apporte des améliorations significatives. Il restreint et clarifie les finalités pour lesquelles les informations peuvent être utilisées, telles que les formes graves de criminalité transnationale et le terrorisme et il établit la période pendant laquelle les données PNR peuvent être enregistrées : ainsi, toutes les données doivent être rendues anonymes à l'issue d'un délai de six mois. Si des données sont utilisées à mauvais escient, les personnes concernées ont un droit de recours administratif et judiciaire conformément au droit américain. Tout individu a également le droit d'accéder à ses propres données PNR et d'obtenir leur rectification par le ministère américain de la Sécurité intérieure, y compris avec possibilité d'effacement si les informations sont incorrectes.

L'accord, qui a pris effet le 1er juillet 2012, restera en vigueur pendant sept ans, jusqu'en 2019.

237 Décision du Conseil 2004/496/EC du 17 mai 2004 concernant la conclusion d'un accord entre la Communauté européenne et les États-Unis d'Amérique sur le traitement et le transfert de données PNR par des transporteurs aériens au bureau des douanes et de la protection des frontières du ministère américain de la sécurité intérieure et décision de la Commission 2004/535/CE du 14 mai 2004 relative au niveau de protection adéquat des données à caractère personnel contenues dans les dossiers des passagers aériens transférés au Bureau des douanes et de la protection des frontières des États-Unis d'Amérique.

238 CJUE, affaires jointes C-317/04 et C-318/04, *Parlement européen c. Conseil de l'UE*, 30 Mai 2006, para. 57, 58 et 59, dans lequel la Cour a statué que la décision d'adéquation et l'accord relatif au traitement des données sont exclus du champ d'application de la directive.

239 Décision 2012/472/UE du Conseil du 26 avril 2012 relative à la conclusion de l'accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation des données des dossiers passagers et leur transfert au ministère américain de la sécurité intérieure, JO 2012 L 215/4. Le texte de l'accord est joint à cette décision, JO 2012 L 215, p. 5–14.

En décembre 2011, le Conseil de l'Union européenne a approuvé la conclusion d'un nouvel accord entre l'Union européenne et l'Australie concernant le traitement et le transfert de données PNR[240]. L'accord entre l'Union européenne et l'Australie sur les données PNR constitue une nouvelle étape du programme de l'UE, qui comprend des lignes directrices globales en matière de PNR[241], la mise en place d'un système PNR pour l'UE[242] et la négociation d'accords avec des pays tiers[243].

Données de messagerie financière

La Société de télécommunications interbancaires mondiales (SWIFT) basée en Belgique, qui est le responsable du traitement de la plupart des transferts mondiaux d'argent à partir de banques européennes, opérait avec un « centre jumeau » situé aux États-Unis. Celle-ci a reçu une demande de communication de données de la part du ministère américain des finances aux fins d'une enquête liée au terrorisme.[244]

Du point de vue de l'UE, il n'existait pas de base légale suffisante pour communiquer ces données européennes importantes, qui n'étaient accessibles aux États-Unis que

240 Décision 2012/981/UE du Conseil du 13 décembre 2011 relative à la conclusion de l'accord entre l'Union européenne et l'Australie sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au service australien des douanes et de la protection des frontières, JO 2012 L 186/3. Le texte de l'accord, qui remplace un précédent accord de 2008, est joint à cette décision, JO 2012 L 186, p. 4–16.

241 Voir, en particulier, Communication de la Commission du 21 septembre 2010 relative à la démarche globale en matière de transfert des données des dossiers passagers (PNR) aux pays tiers, COM(2010) 492 final, Bruxelles, 21 septembre 2010, voir également Groupe de Travail « Article 29 » Avis 7/2010 sur la communication de la Commission européenne relative à la démarche globale en matière de transfert des données des dossiers passagers (PNR) aux pays tiers, WP 178, Bruxelles, 12 novembre 2010.

242 Proposition de directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, COM(2011) 32 final, Bruxelles, 2 février 2011. En avril 2011, le Parlement européen a demandé à la FRA de remettre un avis sur cette proposition et sur sa conformité avec la Charte des droits fondamentaux de l'Union européenne. Voir : FRA (2011), *Avis 1/2011 – Données des dossiers passagers*, Vienne, 14 juin 2011.

243 L'UE négocie actuellement un nouvel accord PNR avec le Canada, qui remplacera l'accord de 2006 actuellement en vigueur.

244 Voir, dans ce contexte, groupe de travail Article 29 (2011), Opinion 14/2011 sur les questions de protection des données relatives à la prévention du blanchiment de capitaux et du financement du terrorisme, WP 186, Bruxelles, 13 juin 2011 ; groupe de travail Article 29 (2006), Avis 10/2006 sur le traitement des données à caractère personnel par la Société de télécommunications interbancaires mondiales (SWIFT), WP 128, Bruxelles, 22 novembre 2006 ; Commission belge de la protection de la vie privée (2008), *« Contrôle et procédure de recommandation initiés à l'égard de la société SWIFT scrl »*, décision, 9 décembre 2008.

parce que l'un des centres de traitement de données et de service de SWIFT était implanté aux États-Unis.

Un accord spécial entre l'UE et les États-Unis, appelé « accord SWIFT », avait été conclu en 2010 pour apporter la base légale nécessaire et garantir une protection adéquate des données[245].

Conformément à cet accord, les données financières conservées par SWIFT continuent d'être communiquées au ministère américain des Finances pour la prévention ou la détection du terrorisme ou de son financement, ainsi que pour les enquêtes ou les poursuites en la matière. Le ministère américain des Finances peut demander à obtenir des données financières de la part de SWIFT dès lors que la demande :

- identifie aussi clairement que possible les données financières ;
- justifie clairement la nécessité de transmettre les données ;
- est adaptée aussi strictement que possible afin de minimiser le volume de données demandées ;
- ne vise pas à obtenir des données liées à l'Espace unique de paiement en euros (SEPA).

Europol doit recevoir une copie de chaque demande du ministère américain des Finances et vérifier si les principes de l'accord SWIFT sont respectés[246]. S'ils le sont, la société SWIFT est tenue de remettre directement les données financières au ministère américain des Finances. Le ministère doit alors enregistrer les données financières dans un environnement physique sécurisé de sorte que seuls des analystes enquêtant sur le terrorisme ou son financement puissent y accéder et les données financières ne doivent pas être interconnectées avec une quelconque autre base de données. De manière générale, les données financières reçues de SWIFT doivent être supprimées au plus tard cinq ans après leur réception. Les données financières

245 Décision 2010/412/UE du Conseil du 13 juillet 2010 relative à la conclusion de l'accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données de messagerie financière de l'Union européenne aux États-Unis aux fins du programme de surveillance du financement du terrorisme, JO 2010 L 195, p. 3 et 4. Le texte de l'accord est joint à cette décision, JO 2010 L 195, p. 5–14.

246 L'autorité de contrôle commune d'Europol a effectué des vérifications sur les activités menées par Europol dans ce domaine, dont les résultats sont disponibles à l'adresse : http://europoljsb.consilium.europa.eu/reports/inspection-report.aspx?lang=en.

qui sont pertinentes pour des enquêtes ou poursuites particulières peuvent être conservées aussi longtemps qu'elles sont nécessaires pour les enquêtes ou poursuites en question.

Le ministère américain des Finances peut transférer des informations issues des données reçues de SWIFT à des organismes chargés de l'application de la loi, de sécurité publique ou de lutte contre le terrorisme, aux États-Unis ou à l'étranger, exclusivement pour la prévention ou la détection du terrorisme et de son financement ou pour les enquêtes ou poursuites en la matière. Lorsque le transfert sortant de données financières implique un citoyen ou un résident d'un État membre de l'UE, tout partage des données avec les autorités d'un pays tiers requiert le consentement préalable des autorités compétentes de l'État membre concerné. Des exceptions sont possibles lorsque le partage des données est essentiel pour prévenir un danger grave et immédiat pour la sécurité publique.

Des observateurs indépendants, notamment une personne nommée par la Commission européenne, contrôlent la conformité avec les principes de l'accord SWIFT.

Les personnes concernées ont le droit d'obtenir confirmation de l'autorité européenne de protection des données compétente du respect de leur droit à la protection des données à caractère personnel. Les personnes concernées ont également le droit à la correction, à l'effacement ou au verrouillage de leurs données collectées et enregistrées par le ministère américain des finances dans le cadre de l'accord SWIFT. Toutefois, les droits d'accès des personnes concernées peuvent faire l'objet de certaines limitations légales. Lorsqu'un accès est refusé, la personne concernée doit être informée par écrit du refus et de son droit à former un recours administratif ou judiciaire aux États-Unis.

L'accord SWIFT est valable pendant cinq ans jusqu'en août 2015. Il se prolongera automatiquement pour des périodes successives d'un an, sauf si l'une des parties informe l'autre, au moins six mois à l'avance, de son intention de ne pas prolonger l'accord.

7

Protection des données dans le contexte de la police et de la justice pénale

UE	Questions traitées	CdE
	En général	Convention 108
	Police	Recommandation relative à la police
		CouEDH, *B.B. c. France*, n °5335/06, 17 décembre 2009
		CouEDH, *S. et Marper c. Royaume-Uni*, n° 30562/04 et 30566/04, 4 décembre 2008
		CouEDH, *Vetter c. France*, n° 59842/00, 31 mai 2005
	Cybercriminalité	Convention sur la cybercriminalité
Protection des données dans le contexte de la coopération policière et judiciaire transfrontalière		
Décision cadre relative à la protection des données	En général	Convention 108 Recommandation relative à la police
Décision Prüm	Pour les données spéciales : empreintes digitales, ADN, hooliganisme, etc.	Convention 108 Recommandation relative à la police
Décision Europol Décision Eurojust Règlement Frontex	Par des agences spéciales	Convention 108 Recommandation sur les données de police
Décision Schengen II Règlement VIS Règlement Eurodac Décision SID	Par des systèmes spéciaux d'information communs	Convention 108 Recommandation relative à la police
		CouEDH, *Dalea c. France*, n° 964/07, 2 février 2010

Pour trouver un équilibre entre les intérêts individuels à la protection des données et les intérêts de la société à la collecte des données dans le but de lutter contre la criminalité et de garantir la sécurité nationale et la sûreté publique, le CdE et l'UE ont adopté certains actes juridiques.

7.1. Droit du CdE en matière de protection des données dans le domaine de la police et de la justice pénale

Points clés

- La Convention 108 et la recommandation du CdE relative à la police couvrent la protection des données dans tous les domaines d'action de la police.
- La Convention sur la cybercriminalité (*Convention de Budapest*) est un acte juridique international ayant force obligatoire consacré aux crimes commis contre et à l'aide de réseaux électronique.

Au niveau européen, la Convention 108 couvre tous les domaines du traitement des données à caractère personnel et ses dispositions visent à réglementer de manière générale le traitement des données à caractère personnel. Par conséquent, la Convention 108 s'applique à la protection des données dans le domaine de la police et de la justice pénale, bien que les États contractants puissent en limiter l'application.

Les missions légales des autorités de police et de justice pénale requièrent souvent le traitement de données à caractère personnel pouvant avoir des conséquences graves pour les individus concernés. La recommandation sur les données de police adoptée par le CdE en 1987 conseille les États contractants sur la façon dont ils doivent donner effet aux principes de la Convention 108 dans le contexte du traitement de données à caractère personnel par des autorités de police[247].

247 CdE, Comité des Ministres (1987), recommandation Rec (87) 15 aux États membres visant à réglementer l'utilisation des données à caractère personnel dans le secteur de la police, 17 septembre 1987.

7.1.1. La recommandation relative à la police

La CouEDH a systématiquement reconnu que l'enregistrement et la conservation de données à caractère personnel par des autorités de police ou de sécurité nationale constituait une atteinte à l'article 8, paragraphe 1, de la CEDH. De nombreux arrêts de la CouEDH portent sur la justification de telles atteintes[248].

Exemple : dans l'affaire *B.B. c. France*[249], la CouEDH a retenu que l'inclusion d'un délinquant sexuel condamné dans une base de données judiciaire nationale relevait de l'article 8 de la CEDH. Toutefois, dans la mesure où des garanties suffisantes en matière de protection des données avaient été établies (droit de la personne concernée de demander l'effacement des données, durée limitée de conservation des données et accès restreint aux données), un juste équilibre avait été trouvé entre les intérêts privés et publics antagonistes en jeu. La CouEDH a exclu la violation de l'article 8 de la CEDH.

Exemple : dans l'affaire *S. et Marper c. Royaume-Uni*[250], les deux requérants avaient été inculpés pour des infractions pénales, mais pas condamnés. La police avait néanmoins enregistré et conservé leurs empreintes digitales, profils ADN et échantillons biologiques. La conservation illimitée de données biométriques était autorisée par la loi dans les cas où une personne était suspectée d'une infraction pénale et même si, par la suite, le suspect était acquitté ou les charges étaient abandonnées. La CouEDH a retenu que la conservation générale et aveugle de données à caractère personnel, non limitée dans le temps, dans des cas où les personnes n'avaient que peu de possibilités de demander une suppression, constituait une ingérence disproportionnée dans le droit du requérant au respect de la vie privée. La CouEDH a conclu à une violation de l'article 8 de la CEDH.

De nombreux autres arrêts de la CouEDH portent sur la justification d'une ingérence par surveillance dans le droit à la protection des données.

248 Voir, par exemple, CouEDH, *Leander c. Suède*, n° 9248/81, 26 mars 1987 ; CouEDH, *M. M. c. Royaume-Uni*, n° 24029/07, 13 novembre 2012 ; CouEDH, *M.K. c. France*, n° 19522/09, 18 avril 2013.

249 CouEDH, *B.B. c. France*, n °5335/06, 17 décembre 2009.

250 CouEDH, *S. et Marper c. Royaume-Uni*, n° 30562/04 et 30566/04, 4 décembre 2008, paras. 119 et 125.

Exemple : dans l'affaire *Allan c. Royaume-Uni*[251], les autorités avaient secrètement enregistré les conversations privées d'un prisonnier avec un ami dans une partie de la prison réservée aux visites et avec un co-accusé dans une cellule. La CouEDH a considéré que les appareils d'enregistrement audio et vidéo dans la cellule du requérant, dans la partie de la prison réservée aux visites et sur un codétenu, constituaient une ingérence dans le droit à la vie privée du requérant. Dans la mesure où, à l'époque, aucun système réglementaire ne régissait l'utilisation d'appareils d'enregistrement cachés par la police, l'ingérence n'était pas prévue par la loi. La CouEDH a conclu à une violation de l'article 8 de la CEDH.

Exemple : dans l'affaire *Klass et autres c. Allemagne*[252], les requérants affirmaient que plusieurs actes législatifs allemands autorisant une surveillance secrète de leurs courriels, courrier et télécommunications constituaient une violation de l'article 8 de la CEDH, notamment parce que la personne concernée n'avait pas été informée des mesures de surveillance et ne pourrait pas saisir les tribunaux à l'issue de telles mesures. La CouEDH a retenu qu'une menace de surveillance constitue forcément une ingérence dans la liberté de communication entre des utilisateurs des services de postes et télécommunications. Mais elle a par ailleurs constaté qu'il existait des garanties suffisantes contre les abus. Le législateur allemand avait eu raison de considérer que de telles mesures étaient nécessaires dans une société démocratique, dans l'intérêt de la sécurité nationale et pour la défense de l'ordre et la prévention des infractions pénales. La CouEDH a exclu la violation de l'article 8 de la CEDH.

Dans la mesure où le traitement de données par des autorités de police peut avoir un impact significatif sur les personnes concernées, il est particulièrement nécessaire de disposer de règles détaillées relatives à la protection des données pour la tenue de bases de données en la matière. La recommandation du CdE relative à la police devait répondre à la question en donnant des conseils sur la façon dont des données devaient être collectées pour le travail de la police ; sur la façon dont les fichiers de données devaient être conservés dans ce domaine ; sur les personnes qui pouvaient être autorisées à accéder à ces fichiers, y compris les conditions de transfert de données à des autorités de police étrangères ; sur la façon dont les personnes concernées devaient pouvoir exercer leur droit à la protection des données ; et sur la façon dont le contrôle par des autorités indépendantes devait se mettre

251 CouEDH, *Allan c. Royaume-Uni*, n° 48539/99, 5 novembre 2002.

252 CouEDH, *Klass et autres c. Allemagne*, n° 5029/71, 6 septembre 1978.

en place. L'obligation d'offrir une sécurité adéquate des données est également envisagée.

La recommandation ne prévoit pas de collecte ouverte et aveugle de données par les autorités de police. Elle limite la collecte de données à caractère personnel par les autorités de police aux données nécessaires pour la prévention d'un réel danger ou la suppression d'une infraction pénale spécifique. Toute collecte supplémentaire de données devra reposer sur une législation nationale spécifique. Le traitement de données sensibles devrait être limité à l'absolue nécessité dans le contexte d'une enquête particulière.

Lorsque des données à caractère personnel sont collectées à l'insu de la personne concernée, celle-ci devrait être informée de la collecte dès qu'une telle divulgation ne peut plus nuire à l'enquête. La collecte de données par surveillance technique ou tout autre moyen automatisé devrait aussi reposer sur des dispositions légales spécifiques.

Exemple : dans l'affaire *Vetter c. France*[253], des témoins anonymes accusaient le requérant d'un homicide. Le requérant se rendant souvent chez un ami, la police y avait installé des dispositifs d'écoute sans l'autorisation du juge chargé de l'enquête. Sur la base des conversations enregistrées, le requérant a été arrêté et poursuivi pour homicide. Il a demandé que l'enregistrement soit déclaré irrecevable, affirmant notamment qu'il n'était pas prévu par la loi. Pour la CouEDH, la question était de savoir si l'utilisation des dispositifs d'écoute était ou non « prévue par la loi ». L'écoute de locaux privés ne relève manifestement pas du champ d'application des articles 100 et suivants du code de procédure pénale car ces dispositions portent sur l'interception de lignes téléphoniques. L'article 81 du code n'indique pas clairement l'étendue ou le mode d'exercice du pouvoir discrétionnaire des autorités dans l'autorisation du contrôle de conversations privées. Par conséquent, le requérant n'a pas bénéficié du degré minimum de protection garanti aux citoyens en vertu de l'état de droit dans une société démocratique. La CouEDH a conclu à une violation de l'article 8 de la CEDH.

La recommandation conclut que, lors de l'enregistrement de données à caractère personnel, des distinctions claires doivent être opérées entre : les données

253 CouEDH, *Vetter c. France*, n °59842/00, 31 mai 2005.

administratives et les données de police ; les différents types de personnes concernées, tels que suspects, condamnés, victimes et témoins ; et les données considérées comme irréfutables et celles basées sur des suspicions ou spéculations.

La finalité des données de police devrait être strictement limitée, ce qui a des conséquences sur la communication des données de police à des tiers : le transfert ou la communication de ces données dans le secteur de la police devrait dépendre de la question de savoir s'il existe un intérêt légitime au partage des informations. Le transfert ou la communication de ces données en dehors du secteur de la police ne devrait être autorisé que s'il existe une obligation ou autorisation légale claire. Le transfert ou la communication international devrait être limité aux autorités de police étrangères et basé sur des dispositions légales spéciales, si possible des accords internationaux, sauf s'il est nécessaire pour la prévention d'un danger grave et immédiat.

Le traitement de données par la police doit faire l'objet d'un contrôle indépendant afin de garantir sa conformité avec le droit national en matière de protection des données. Les personnes concernées doivent jouir de tous les droits d'accès prévus par la Convention 108. Lorsque les droits d'accès des personnes concernées ont été restreints conformément à l'article 9 de la Convention 108 dans l'intérêt de l'efficacité des enquêtes de police, la personne concernée doit avoir le droit, en vertu de la législation nationale, de former un recours devant l'autorité nationale de contrôle de la protection des données ou devant tout autre organe indépendant.

7.1.2. La Convention de Budapest sur la cybercriminalité

Les activités criminelles utilisant et affectant de plus en plus les systèmes électroniques de traitement des données, de nouvelles dispositions légales pénales sont nécessaires pour relever ce défi. Le CdE a donc adopté un acte juridique international, la Convention sur la cybercriminalité (également appelée « Convention de Budapest ») pour traiter la question des crimes commis contre et à l'aide de réseaux électroniques[254]. Cette convention est ouverte à l'adhésion de pays non membres du CdE et, mi-2013, quatre États hors CdE (l'Australie, la République dominicaine, le Japon et les États-Unis) étaient parties à la convention et 12 autres non membres l'avaient signée ou avaient été invités à y adhérer.

254 Conseil de l'Europe, Comité des Ministres (2001), Convention sur la cybercriminalité, STCE n° 185, Budapest, 23 novembre 2001, entrée en vigueur le 1er juillet 2004.

La Convention sur la cybercriminalité reste le traité international le plus influent concernant les manquements à la loi qui interviennent sur Internet ou sur d'autres réseaux d'information. Elle impose aux parties de mettre à jour et d'harmoniser leur législation pénale contre le piratage et d'autres atteintes à la sécurité, y compris les atteintes au droit d'auteur, la fraude par ordinateur, la pornographie infantile et d'autres cyber-activités illicites. La Convention prévoit également des facultés à caractère procédural couvrant la recherche sur des réseaux informatiques et l'interception de communications dans le contexte de la lutte contre la cybercriminalité. Enfin, elle permet une coopération internationale effective. Un protocole additionnel à la Convention porte sur l'incrimination de la propagande raciste et xénophobe sur des réseaux informatiques.

Si la Convention n'est pas véritablement un outil de promotion de la protection des données, elle criminalise des activités qui entraîneront probablement la violation du droit d'une personne concernée à la protection de ses données. Elle oblige également les parties contractantes à prévoir, lors de la mise en œuvre de la Convention, une protection adéquate des droits de l'homme et des libertés, y compris des droits garantis par la CEDH, tels que le droit à la protection des données[255].

7.2. Droit de l'UE en matière de protection des données dans le domaine de la police et de la justice pénale

Points clés

- Au niveau de l'UE, la protection des données dans le secteur de la police et de la justice pénale est uniquement réglementée dans le contexte de la coopération transfrontalière des autorités de police et de justice.
- Il existe des régimes spéciaux de protection des données pour l'Office européen de police (Europol) et l'unité de coopération judiciaire de l'UE (Eurojust), organes communautaires qui encouragent et contribuent à l'application de la loi au-delà des frontières.
- Il existe également des régimes spéciaux de protection des données pour les systèmes d'information conjoints qui sont établis au niveau européen pour l'échange transfrontalier d'informations entre les autorités de police et de justice compétentes. Citons à titre d'exemples importants Schengen II, le Système d'information sur les visas (VIS) et Eurodac, un système centralisé contenant les données d'empreinte digitales de pays tiers demandant l'asile dans un État membre de l'UE.

255 *Ibid.*, art. 15, para. 1.

La directive relative à la protection des données ne s'applique pas au domaine de la police et de la justice pénale. La Section 7.2.1 décrit les actes juridiques les plus importants dans ce domaine.

7.2.1. La décision cadre relative à la protection des données

La décision cadre 2008/977/JAI du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale (*décision cadre relative à la protection des données*)[256] vise à protéger les données à caractère personnel des personnes physiques dont les données à caractère personnel sont traitées à des fins de prévention et de détection d'infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales. Des autorités compétentes travaillant dans le domaine de la police et de la justice pénale agissent pour le compte des États membres ou de l'UE. Ces autorités sont des agences ou organes communautaires, ainsi que des autorités des États membres[257]. L'applicabilité de la décision cadre est limitée à garantir la protection des données dans la coopération transfrontière entre ces autorités et ne s'étend pas à la sécurité nationale.

La décision cadre relative à la protection des données repose dans une large mesure sur les principes et définitions contenus dans la Convention 108 et la directive relative à la protection des données.

Les données peuvent uniquement être utilisées par une autorité compétente et pour les finalités pour lesquelles elles ont été transmises ou mises à disposition. L'État membre destinataire doit respecter toutes les restrictions applicables à l'échange de données prévues par la législation de l'État membre qui transmet les données. L'utilisation de données par l'État destinataire pour d'autres finalités est cependant autorisée sous certaines conditions. La journalisation et la documentation des transmissions est une mission spécifique des autorités compétentes pour contribuer à la clarification des responsabilités découlant de réclamations. Le transfert sortant de données, reçues dans le cadre d'une coopération transfrontalière, à destination de

256 Conseil de l'Union européenne (2008), décision cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale (décision cadre relative à la protection des données), JO 2008 L 350.

257 *Ibid.*, art. 2, point h).

tiers requiert le consentement de l'État membre dont proviennent les données, bien qu'il existe des exceptions dans les situations d'urgence.

Les autorités compétentes doivent prendre les mesures de sécurité nécessaires pour protéger les données à caractère personnel contre toute forme de traitement illicite.

Chaque État membre doit s'assurer qu'une ou plusieurs autorités nationales indépendantes de contrôle sont chargées de conseiller et de surveiller la mise en œuvre des dispositions prises en application de la décision cadre relative à la protection des données. Elles peuvent aussi être saisies par toute personne d'une demande relative à la protection de ses droits et libertés à l'égard du traitement de données à caractère personnel par les autorités compétentes.

La personne concernée a le droit d'être informée du traitement de ses données à caractère personnel et elle dispose d'un droit d'accès, de rectification, d'effacement ou de verrouillage. Lorsque l'exercice de ces droits est refusé pour des raisons prépondérantes, la personne concernée doit avoir un droit de recours devant l'autorité nationale de contrôle compétente et/ou devant un tribunal. Si une personne subit un préjudice en raison de violations du droit national transposant la décision cadre relative à la protection des données, cette personne peut obtenir réparation de la part du responsable du traitement[258]. De manière générale, les personnes concernées doivent avoir accès à un recours juridictionnel pour toute violation de leurs droits garantis par la législation nationale transposant la décision cadre relative à la protection des données[259].

La Commission européenne a proposé une réforme, composée d'un règlement général sur la protection des données[260] et d'une directive générale sur la protection des données[261]. Cette nouvelle directive remplacera l'actuelle décision cadre relative

258 *Ibid.*, art. 19.

259 *Ibid.*, art. 20.

260 Commission européenne (2012), *Proposition de règlement du Parlement européen et du Conseil 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 (règlement général sur la protection des données)*, COM(2012) 11 final, Bruxelles, 25 janvier 2012.

261 Commission européenne (2012), *Proposition de directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, ou d'exécution de sanctions pénales, et à la libre circulation de ces données (directive générale relative à la protection des données)*, COM(2012) 10 final, Bruxelles, 25 janvier 2012.

à la protection des données et appliquera des principes et règles d'ordre général à la coopération policière et judiciaire en matière pénale.

7.2.2. Actes juridiques plus spécifiques en matière de protection des données dans la coopération transfrontalière des services de police et des autorités chargées de l'application de la loi

En plus de la décision cadre relative à la protection des données, l'échange d'informations détenues par des États membres dans des domaines spécifiques est réglementé par un certain nombre d'actes juridiques, tels que la décision cadre 2009/315/JAI du Conseil concernant l'organisation et le contenu des échanges d'informations extraites du casier judiciaire entre les États membres et la décision du Conseil relative aux modalités de coopération entre les cellules de renseignement financier des États membres en ce qui concerne l'échange d'informations[262].

Il est important de noter que la coopération transfrontalière[263] entre les autorités compétentes implique de plus en plus l'échange de données d'immigration. Ce domaine de la loi ne relève pas des affaires de police et de justice pénale, mais il est pertinent, à de nombreux égards, pour le travail des autorités de police et de justice. Il en va de même des données relatives aux biens importés dans l'UE ou exportés depuis l'UE. La suppression des contrôles aux frontières intérieures au sein de l'UE a renforcé le risque de fraude, imposant aux États membres d'intensifier la coopération, notamment en améliorant les échanges transfrontaliers d'informations, pour détecter et poursuivre plus efficacement les violations de la législation douanière nationale et européenne.

262 Conseil de l'Union européenne (2009), décision cadre 2009/315/JAI du Conseil du 26 février 2009 concernant l'organisation et le contenu des échanges d'informations extraites du casier judiciaire entre les États membres, JO 2009 L 93 ; Conseil de l'Union européenne (2000), décision 2000/642/JAI du Conseil du 17 octobre 2000 relative aux modalités de coopération entre les cellules de renseignement financier des États membres en ce qui concerne l'échange d'informations, JO 2000 L 271.

263 Commission européenne (2012), Communication de la Commission au Parlement européen et au Conseil – Renforcer la coopération dans le domaine de la répression au sein de l'UE : le modèle européen d'échange d'informations (EIXM), COM(2012) 735 final, Bruxelles, 7 décembre 2012.

La décision Prüm

Un exemple important de coopération transfrontalière institutionnalisée par l'échange de données détenues au niveau national est la décision 2008/615/JAI du Conseil relative à l'approfondissement de la coopération transfrontière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontière (*décision Prüm*), qui a transposé le traité de Prüm dans le droit communautaire en 2008[264]. Le traité de Prüm était un accord international de coopération policière signé en 2005 par l'Autriche, la Belgique, la France, l'Allemagne, le Luxembourg, les Pays-Bas et l'Espagne[265].

L'objectif de la décision Prüm est d'aider les États membres à améliorer le partage d'informations dans le but de prévenir et de combattre la criminalité dans trois domaines : terrorisme, criminalité transfrontalière et migration irrégulière. À cette fin, la décision prévoit des dispositions concernant :

- l'accès automatisé aux profils ADN, données d'empreintes digitales et certaines données nationales relatives à l'immatriculation des véhicules ;
- la transmission de données en relation avec des événements majeurs à dimension transfrontalière ;
- la transmission d'informations pour prévenir des infractions terroristes ;
- d'autres mesures d'approfondissement de la coopération policière transfrontalière.

Les bases de données mises à disposition dans le cadre de la décision Prüm sont entièrement régies par le droit national, mais l'échange de données est également régi par la décision et, plus récemment, par la décision cadre relative à la protection des données. Les organes compétents pour le contrôle de ces flux de données sont les autorités nationales de contrôle de la protection des données.

264 Conseil de l'Union européenne (2008), décision 2008/615/JAI du Conseil du 23 juin 2008 relative à l'approfondissement de la coopération transfrontière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontière, JO 2008 L 210.

265 Convention entre le Royaume de Belgique, la République fédérale d'Allemagne, le Royaume d'Espagne, la République française, le Grand-Duché de Luxembourg, le Royaume des Pays-Bas et la République d'Autriche relatif à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme, la criminalité transfrontalière et la migration illégale ; disponible en anglais à l'adresse : http://register.consilium.europa.eu/pdf/en/05/st10/st10900.en05.pdf.

7.2.3. Protection des données à Europol et Eurojust

Europol

Europol, l'Office européen de police, est situé à la Haye et dispose d'unités nationales Europol (UNE) dans chaque État membre. Europol a été créé en 1998 ; son statut légal actuel d'institution communautaire repose sur la décision du Conseil portant création de l'Office européen de police (*décision Europol*)[266]. L'objectif d'Europol est de contribuer à la prévention du crime organisé, du terrorisme et d'autres formes de criminalité grave, ainsi qu'aux enquêtes en la matière - selon la liste figurant en annexe à la décision Europol - affectant au moins deux États membres.

Pour atteindre ses objectifs, Europol a créé le système d'information Europol qui fournit une base de données aux États membres leur permettant d'échanger des renseignements et informations en matière criminelle par l'intermédiaire de leurs UNE. Le système d'information Europol peut être utilisé pour fournir des données portant sur : des personnes suspectées ou condamnées pour une infraction pénale relevant de la compétence d'Europol ou des personnes à l'égard desquelles il existe des éléments de fait indiquant qu'elles s'apprêtent à commettre de telles infractions. Europol et les UNE peuvent saisir et récupérer des données directement dans le système d'information Europol. Seule la partie ayant saisi les données dans le système peut les modifier, les corriger ou les supprimer.

Si nécessaire pour l'exécution de ses missions, Europol peut sauvegarder, modifier et utiliser des données concernant des infractions pénales dans des fichiers de travail à des fins d'analyse. Les fichiers de travail à des fins d'analyse sont créés dans le but d'assembler, de traiter ou d'utiliser des données afin de contribuer à des enquêtes pénales concrètes menées par Europol conjointement avec des États membres de l'UE.

Suite à de récents développements, le Centre européen de lutte contre la cybercriminalité a été créé à Europol le 1er janvier 2013[267]. Le Centre sert de plate-forme

266 Conseil de l'Union européenne (2009), décision du Conseil du 6 avril 2009 portant création de l'Office européen de police, (Europol), JO 2009 L 121.Voir également proposition de règlement de la Constitution qui institue donc le cadre juridique nécessaire à la création d'un nouvel Europol, qui succédera à l'agence Europol créée par la décision 2009/371/JAI du Conseil du 6 avril 2009 portant création de l'Office européen de police (Europol) et au CEPOL institué par la décision 2005/681/JAI du Conseil du 20 septembre 2005 instituant le Collège européen de police (CEPOL), COM(2013) 173 final.

267 Voir également CEPD (2012), *Avis du Contrôleur européen de la protection des données relatif à la communication de la Commission européenne au Conseil et au Parlement européen concernant l'établissement d'un Centre européen de lutte contre la cybercriminalité*, Bruxelles, 29 juin 2012.

communautaire d'information sur la cybercriminalité, contribuant à accélérer les réactions en cas de criminalité en ligne, développant et déployant des capacités numériques en matière de criminalistique et fournissant des bonnes pratiques en matière d'enquêtes pénales. Le Centre se concentre sur :

- les cybercrimes commis par des groupes organisés dans le but de générer d'importants bénéfices, telle que la fraude en ligne ;
- les cybercrimes lourds de conséquences pour leurs victimes, tels que l'exploitation sexuelle des enfants en ligne ;
- les cybercrimes perturbant les systèmes critiques de l'UE en matière d'infrastructure et d'information.

Le système de protection des données régissant les activités d'Europol est amélioré. La décision Europol dispose en son article 27 que les principes énoncés dans la Convention 108 et la recommandation sur les données de police concernant le traitement de données automatisées et non automatisées trouvent application. La transmission de données entre Europol et les États membres doit également satisfaire aux règles prévues par la décision cadre relative à la protection des données.

Pour garantir la conformité à la législation applicable en matière de protection des données et, en particulier, pour garantir que le traitement de données à caractère personnel ne viole pas les droits de l'individu, l'Autorité de contrôle commune (ACC) indépendante d'Europol examine et contrôle les activités d'Europol[268]. Chaque individu a un droit d'accès à toutes données à caractère personnel qu'Europol peut détenir à son sujet, en plus d'un droit de demander que ces données à caractère personnel soient vérifiées, rectifiées ou supprimées. Toute personne qui n'est pas satisfaite d'une décision d'Europol concernant l'exercice de ces droits peut former un recours devant le comité des recours de l'ACC.

Si un préjudice est survenu en raison d'erreurs de droit ou de fait dans les données enregistrées ou traitées à Europol, la partie lésée peut uniquement former un recours devant le tribunal compétent de l'État membre dans lequel le préjudice est survenu[269]. Europol remboursera l'État membre si le préjudice résulte d'un manquement d'Europol à se conformer à ses obligations légales.

268 Décision Europol, art. 34.

269 *Ibid.*, art. 52.

Eurojust

Eurojust, constitué en 2002, est un organe communautaire basé à La Haye chargé de promouvoir la coopération judiciaire dans les enquêtes et poursuites relatives à la criminalité grave touchant au moins deux États membres[270]. Eurojust est compétent pour :

- stimuler et améliorer la coordination des enquêtes et poursuites entre les autorités compétentes des divers États membres ;
- faciliter l'exécution des demandes et décisions en relation avec la coopération judiciaire.

Les fonctions d'Eurojust sont exercées par des membres nationaux. Chaque État membre délègue un juge ou un membre du ministère public à Eurojust, dont le statut est soumis au droit national et qui se voit confier les compétences nécessaires pour remplir les missions requises pour favoriser et améliorer la coopération judiciaire. En outre, les membres nationaux agissent conjointement sous forme de collège pour exercer des missions spéciales d'Eurojust.

Eurojust peut traiter des données à caractère personnel pour autant que cela soit nécessaire à la réalisation de ses objectifs. Un tel traitement est toutefois limité à des informations spécifiques relatives aux personnes qui sont suspectées d'avoir commis une infraction pénale relevant de la compétence d'Eurojust, d'y avoir participé ou d'avoir été condamné à ce titre. Eurojust peut également traiter certaines informations relatives à des témoins ou victimes d'infractions pénales relevant de sa compétence[271]. Dans des circonstances exceptionnelles, Eurojust peut, pendant une durée limitée, traiter des données à caractère personnel plus vastes en lien avec les circonstances d'une infraction dès lors que ces données sont immédiatement pertinentes pour une enquête en cours. Dans les limites de ses compétences, Eurojust

270 Conseil de l'Union européenne (2002), décision 2002/187/JAI Conseil du 28 février 2002 instituant Eurojust afin de renforcer la lutte contre les formes graves de criminalité, JO 2002 L 63 ; Conseil de l'Union européenne (2003), décision 2003/659/JAI du Conseil du 18 juin 2003 modifiant la décision 2002/187/JAI instituant Eurojust afin de renforcer la lutte contre les formes graves de criminalité, JO 2003 L 44 ; Conseil de l'Union européenne (2009), décision 2009/426/JAI du Conseil du 16 décembre 2008 sur le renforcement d'Eurojust et modifiant la décision 2002/187/JAI instituant Eurojust afin de renforcer la lutte contre les formes graves de criminalité, JO 2009 L 138 (décisions Eurojust).

271 Version consolidée de la décision 2002/187/JAI du Conseil, telle que modifiée par la décision 2003/659/JAI du Conseil et par la décision 2009/426/JAI du Conseil, art. 15, para. 2.

peut coopérer avec d'autres institutions, organes et agences communautaires et échanger des données à caractère personnel avec ceux-ci. Eurojust peut également coopérer et échanger des données à caractère personnel avec des pays et organisations tiers.

S'agissant de la protection des données, Eurojust doit garantir un niveau de protection au moins équivalent aux principes de la Convention 108 du Conseil de l'Europe et à ses amendements ultérieurs. Des règles et limitations particulières doivent être respectées en cas d'échange de données ; elles sont mises en place dans des accords de coopération ou des arrangements de travail conformément aux décisions Eurojust du Conseil et aux règles Eurojust relatives à la protection des données[272].

Une ACC indépendante a été établie à Eurojust, ayant pour mission de contrôler le traitement des données à caractère personnel par Eurojust. Des individus peuvent former un recours devant l'ACC s'ils ne sont pas satisfaits de la réponse d'Eurojust à une demande d'accès, de rectification, de verrouillage ou d'effacement de données à caractère personnel. Quand Eurojust traite des données à caractère personnel de façon illicite, Eurojust répond de tout préjudice causé à la personne concernée conformément à la législation nationale de l'État membre dans lequel son siège est situé, les Pays-Bas.

7.2.4. Protection des données dans les systèmes d'information conjoints au niveau de l'UE

En plus de l'échange de données entre les États membres et de la création d'autorités européennes spécialisées dans la lutte contre la criminalité transfrontalière, plusieurs systèmes d'information conjoints ont été établis au niveau de l'UE pour faire office de plate-forme d'échange de données entre les autorités nationales et européennes compétentes à des fins répressives spécifiques, y compris pour le droit en matière d'immigration et le droit douanier. Certains de ces systèmes sont nés d'accords multilatéraux qui ont ensuite été remplacés par des actes légaux et systèmes européens, tels que le système d'information Schengen, le système d'information sur les visas, Eurodac, Eurosur ou le système d'information douanier.

272 Dispositions du règlement intérieur d'Eurojust relatives au traitement et à la protection des données à caractère personnel, JO 2005 C 68/01, 19 mars 2005, p. 1.

L'Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle (euLISA)[273], créée en 2012, est responsable de la gestion opérationnelle à long terme du système d'information Schengen 2e génération (SIS II), du système d'information sur les visas (VIS) et d'Eurodac. La tâche principale de l'eu-LISA est de garantir l'exploitation efficace, sécurisée et continue des systèmes de technologies de l'information. Elle est également chargée de l'adoption des mesures nécessaires pour garantir la sécurité des systèmes et celle des données.

Le système d'information Schengen

En 1985, plusieurs États membres des anciennes Communautés européennes ont conclu l'accord entre les États de l'Union économique Benelux, de la République fédérale d'Allemagne et de la République française relatif à la suppression graduelle des contrôles aux frontières communes (*accord de Schengen*), visant à créer une zone de libre circulation des personnes, non entravée par des contrôles aux frontières sur le territoire de Schengen[274]. Pour contrebalancer la menace contre la sécurité publique qui pouvait résulter de l'ouverture des frontières, des contrôles renforcés aux frontières extérieures de la zone de Schengen ont été mis en place, ainsi qu'une coopération étroite entre les autorités nationales de police et de justice.

En conséquence de l'adhésion de nouveaux États à l'accord de Schengen, le système de Schengen a finalement été intégré au cadre juridique de l'UE par le traité d'Amsterdam[275]. Cette décision a été mise en œuvre en 1999. La version la plus récente du système d'information de Schengen, le « SIS II », est entrée en vigueur le 9 avril 2013. Il couvre désormais tous les États membres de l'UE ainsi que l'Islande, le Liechtenstein, la Norvège et la Suisse[276]. Europol et Eurojust ont accès au SIS II.

273 Règlement (UE) n° 1077/2011 du Parlement européen et du Conseil du 25 octobre 2011 portant création d'une agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice, JO 2011 L 286.

274 Accord entre les États de l'Union économique Benelux, de la République fédérale d'Allemagne et de la République française relatif à la suppression graduelle des contrôles aux frontières communes, JO 2000 L 239.

275 Communautés européennes (1997), Traité d'Amsterdam modifiant le traité sur l'Union européenne, les traités instituant les Communautés européennes et certains actes connexes, JO 1997 C 340.

276 Règlement (CE) n° 1987/2006 du Parlement européen et du Conseil du 20 décembre 2006 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération, (*SIS II*), JO 2006 L 381 ; et Conseil de l'Union européenne (2007), décision 2007/533/JHA du Conseil du 12 juin 2007 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération, (SIS II), JO 2007 L 205.

Le SIS II est composé d'un système central (CS-SIS), d'un système national (N-SIS) dans chaque État membre et d'une infrastructure de communication entre le système central et les systèmes nationaux. Le CS-SIS contient certaines données saisies par les États membres sur des personnes et des objets. Le CS-SIS est utilisé par les autorités nationales de contrôle aux frontières, de police, de douane, de visa et de justice dans l'ensemble de l'espace Schengen. Chaque État membre exploite une forme nationale du CS-SIS, appelé « système d'information Schengen national » (N-SIS), qui est constamment mis à jour, actualisant ainsi le CS-SIS. Le N-SIS est consulté et émet une alerte quand :

- la personne n'a pas le droit d'entrer ou de séjourner sur le territoire de Schengen ;
- la personne ou l'objet est recherché par des autorités judiciaires ou par celles chargées de l'application de la loi ;
- la personne a été signalée comme disparue ; ou
- des biens, tels que des billets de banque, voitures, camionnettes, armes à feu et documents d'identité, ont été signalés comme volés ou perdus.

En cas d'alerte, des activités de suivi sont initiées par l'intermédiaire des systèmes d'information Schengen nationaux.

Le SIS II contient de nouvelles fonctionnalités, telles que la possibilité de saisir : des données biométriques, notamment empreintes digitales et photos ; ou de nouvelles catégories d'alertes, telles que bateaux, aéronefs, conteneurs ou moyens de paiement volés ; des alertes améliorées sur les personnes et objets ; et des copies de mandats d'arrêt européens (MAE) sur des personnes recherchées pour arrestation, remise ou extradition.

La décision 2007/533/JAI du Conseil sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (décision SIS II) intègre la Convention 108 : « Les données à caractère personnel traitées en application de la présente décision sont protégées conformément à la Convention 108 du Conseil de l'Europe »[277]. Lorsque l'utilisation de données à caractère personnel

277 Conseil de l'Union européenne (2007), décision 2007/533/JAI du Conseil du 12 juin 2007 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération, JO 2007 L 205, art. 57.

par des autorités nationales de police intervient en application de la décision Schengen II, les dispositions de la Convention 108 et de la recommandation sur les données de police doivent être transposées dans le droit national.

L'autorité de contrôle nationale compétente de chaque État membre supervise le N-SIS national. En particulier, il lui appartient de contrôler la qualité des données que l'État membre saisit dans le CS-SIS via le N-SIS. L'autorité nationale de contrôle doit veiller à la réalisation d'un audit des traitements de données au sein du N-SIS national au moins tous les quatre ans. Les autorités nationales de contrôle et le CEPD coopèrent et assurent un contrôle coordonné du N-SIS tandis que le CEPD est en charge du contrôle du CS-SIS. Dans un souci de transparence, un rapport conjoint d'activité est envoyé au Parlement européen, au Conseil et à l'eu-LISA tous les deux ans.

Les droits d'accès des individus concernant le SIS II peuvent être exercés dans tout État membre puisque chaque N-SIS est une copie conforme du CS-SIS.

Exemple : dans l'affaire *Dalea c. France*[278], le requérant s'est vu refuser un visa touristique pour la France, les autorités françaises ayant indiqué dans le système d'information Schengen que son entrée devait être refusée. Le requérant a cherché en vain à accéder à ses données et à en obtenir la rectification ou la suppression devant la Commission nationale de l'informatique et des libertés et, en dernier recours, devant le Conseil d'État. La CouEDH a considéré que le signalement du requérant dans le système d'information Schengen était prévu par la loi et poursuivait le but légitime de protéger la sécurité nationale. Le requérant n'ayant pas montré en quoi il avait effectivement subi un préjudice du fait de son impossibilité d'entrer dans l'espace Schengen, et puisqu'il existait des mesures suffisantes pour le protéger contre des décisions arbitraires, l'ingérence dans son droit au respect de la vie privée était proportionnée. Le recours du requérant au titre de l'article 8 a donc été déclaré irrecevable.

Le système d'information sur les visas

Le système d'information sur les visas (VIS), également exploité par l'eu-LISA, a été développé pour soutenir la mise en œuvre d'une politique européenne commune

278 CouEDH, *Dalea c. France*, n° 964/07, 2 février 2010.

des visas[279]. Le VIS permet aux États Schengen d'échanger des données sur les visas par l'intermédiaire d'un système qui connecte les consulats des États Schengen situés dans des pays non membres de l'UE avec les points externes de passage des frontières de tous les États Schengen. Le VIS traite les données concernant les demandes de visas de court séjour en vue de visites ou de transit dans l'espace Schengen. Le VIS permet aux autorités aux frontières de vérifier, à l'aide de données biométriques, si la personne qui présente un visa est son véritable titulaire et d'identifier les personnes sans documents ou porteuses de documents frauduleux.

Conformément au règlement (CE) n° 767/2008 du Parlement européen et du Conseil concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour (*règlement VIS*), seules des données relatives au demandeur, à ses visas, photographies, empreintes digitales, liens vers des demandes précédentes et dossiers de candidature de personnes l'accompagnant, peuvent être enregistrées dans le VIS[280]. L'accès au VIS pour saisir, modifier ou supprimer des données est exclusivement restreint aux autorités en charge des visas des États membres, tandis que l'accès pour consulter les données est accordé aux autorités en charge des visas et aux autorités compétentes pour les contrôles aux points externes de passage aux frontières, les contrôles d'immigration et les demandes d'asile. Sous certaines conditions, les autorités de police nationales compétentes et Europol peuvent demander l'accès à des données saisies dans le VIS dans le but de prévenir et de détecter des actes de terrorisme et infractions pénales ou d'enquêter en la matière[281].

279 Conseil de l'Union européenne (2004), décision du Conseil du 8 juin 2004 portant création du système d'information sur les visas (VIS), JO 2004 L 213 ; règlement (CE) n° 767/2008 du Parlement européen et du Conseil du 9 juillet 2008 concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour, JO 2008 L 218 (*règlement VIS*) ; Conseil de l'Union européenne (2008), décision 2008/633/JAI du Conseil du 23 juin 2008 concernant l'accès en consultation au système d'information sur les visas (VIS) par les autorités désignées des États membres et par l'Office européen de police (Europol) aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière, JO 2008 L 218.

280 Art. 5 du règlement (CE) n° 767/2008 du Parlement européen et du Conseil du 9 juillet 2008 concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour (*règlement VIS*), JO 2008 L 218.

281 Conseil de l'Union européenne (2008), décision 2008/633/JAI du Conseil du 23 juin 2008 concernant l'accès en consultation au système d'information sur les visas (VIS) par les autorités désignées des États membres et par l'Office européen de police (Europol) aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière, JO 2008 L 218.

Eurodac

Le nom Eurodac fait référence aux empreintes digitales. Il s'agit d'un système centralisé contenant des données sur les empreintes digitales de ressortissants de pays tiers faisant une demande d'asile dans un État membre de l'UE[282]. Le système existe depuis janvier 2003 et sa finalité est de contribuer à déterminer à quel l'État membre il appartient d'examiner une demande d'asile particulière en vertu du règlement (CE) n° 343/2003 du Conseil établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande d'asile présentée dans l'un des États membres par un ressortissant d'un pays tiers (*règlement Dublin II*)[283]. Les données à caractère personnel figurant dans Eurodac peuvent uniquement être utilisées aux fins de faciliter l'application du règlement Dublin II ; toute autre utilisation fera l'objet de sanctions.

Eurodac est composé d'une unité centrale, exploitée par l'eu-LISA, pour l'enregistrement et la comparaison des empreintes digitales, et d'un système de transmission électronique de données entre les États membres et la base de données centrale. Les États membres prennent et transmettent les empreintes digitales de chaque ressortissant de pays tiers ou de chaque apatride, âgé de 14 ans au moins, qui demande l'asile sur leur territoire ou qui est appréhendé pour avoir passé leur frontière extérieure sans autorisation. Les États membres peuvent également prendre et transmettre les empreintes digitales de chaque ressortissant de pays tiers ou chaque apatride qui séjourne sur leur territoire sans permission.

Les données relatives aux empreintes digitales sont uniquement enregistrées dans la base de données Eurodac sous forme pseudonymisée. En cas de correspondance, le pseudonyme, ainsi que le nom du premier État membre ayant transmis les données relatives aux empreintes digitales, est divulgué au second État membre. Ce second État membre contacte ensuite le premier État membre puisque, conformément au règlement Dublin II, le premier État membre est responsable du traitement de la demande d'asile.

282 Règlement (CE) n° 2725/2000 du 11 décembre 2000 concernant la création du système « Eurodac » pour la comparaison des empreintes digitales aux fins de l'application efficace de la convention de Dublin, JO 2000 L 316 ; règlement (CE) n° 407/2002 du Conseil du 28 février 2002 fixant certaines modalités d'application du règlement (CE) n° 2725/2000 concernant la création du système « Eurodac » pour la comparaison des empreintes digitales aux fins de l'application efficace de la convention de Dublin, JO 2002 L 62 (règlements Eurodac).

283 Règlement (CE) n° 343/2003 du Conseil du 18 février 2003 établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande d'asile présentée dans l'un des États membres par un ressortissant d'un pays tiers, JO 2003 L 50 (règlement Dublin II).

Les données à caractère personnel enregistrées dans Eurodac portant sur des demandeurs d'asile sont conservées pendant 10 ans à compter de la date à laquelle les empreintes digitales ont été prises, à moins que la personne concernée n'obtienne la citoyenneté d'un État membre de l'UE. Dans ce cas, les données doivent être immédiatement effacées. Les données concernant des ressortissants étrangers appréhendés pour avoir passé la frontière extérieure sans autorisation sont conservées pendant deux ans. Ces données doivent être effacées dès que la personne concernée reçoit un permis de séjour, quitte le territoire de l'UE ou obtient la citoyenneté d'un État membre.

En plus de tous les États membres de l'UE, l'Islande, la Norvège, le Liechtenstein et la Suisse appliquent également Eurodac sur la base d'accords internationaux.

Eurosur

Le système européen de surveillance des frontières (*Eurosur*)[284] est destiné à améliorer le contrôle des frontières extérieures de Schengen par la détection, la prévention et la lutte contre l'immigration irrégulière et la criminalité transfrontalière. Il sert à améliorer l'échange d'informations et la coopération opérationnelle entre les centres de coordination nationale et Frontex, l'agence européenne en charge du développement et de l'application du nouveau concept de gestion intégrée des frontières[285]. Ses objectifs généraux sont :

- réduire le nombre de migrants illégaux entrant clandestinement dans l'UE ;
- réduire le nombre de décès de migrants illégaux en sauvant plus de vies en mer ;
- accroître la sécurité interne de l'UE dans son ensemble en contribuant à la prévention de la criminalité transfrontalière[286].

284 Règlement (CE) n °1052/2013 du Parlement européen et du Conseil du 22 octobre 2013 portant création du système européen de surveillance des frontières (Eurosur), JO 2013 L 295.

285 Règlement (UE) n° 1168/2011 du Parlement européen et du Conseil du 25 octobre 2011 modifiant le règlement (CE) n° 2007/2004 du Conseil portant création d'une Agence européenne pour la gestion de la coopération opérationnelle aux frontières extérieures des États membres de l'Union européenne, JO 2011 L 394 (règlement Frontex).

286 Voir également : Commission européenne (2008), *Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions : Examen de la création d'un système européen de surveillance des frontières (Eurosur)*, COM(2008) 68 final, Bruxelles, 13 février 2008 ; Commission européenne (2011), *Analyse d'impact accompagnant la proposition de règlement du Parlement européen et du Conseil portant création du système européen de surveillance des frontières (Eurosur), document de travail des services de la Commission*, SEC(2011) 1536 final, Bruxelles,12 décembre 2011, p. 18.

Il a commencé sa mission le 2 décembre 2013 dans tous les États membres ayant des frontières extérieures et il la débutera le 1er décembre 2014 dans les autres. Le règlement s'appliquera à la surveillance des frontières terrestres, marines extérieures et aériennes des États membres.

Système d'information douanier

Un autre système important d'information conjoint établi au niveau de l'UE est le système d'information douanier (SID)[287]. Dans le cadre de la création du marché intérieur, tous les contrôles et toutes les formalités à l'égard des produits circulant sur le territoire européen ont été abolis, entraînant un risque accru de fraude. Ce risque a été contrebalancé par le renforcement de la coopération entre les administrations douanières des États membres. La finalité du SID est d'aider les États membres à prévenir des atteintes graves aux législations douanières et agricoles nationales et européennes, ainsi qu'à enquêter et poursuivre en la matière.

Les informations contenues dans le SID comprennent des données à caractère personnel en référence aux produits, moyens de transport, entreprises, personnes, biens et espèces conservés, saisis ou confisqués. Ces informations peuvent uniquement être utilisées dans le but de repérer, de signaler et de réaliser des inspections particulières ou des analyses stratégiques ou opérationnelles concernant des personnes suspectées d'avoir enfreint des dispositions douanières.

L'accès au SID est accordé aux autorités douanières, fiscales, agricoles, de santé publique et policières nationales, ainsi qu'à Europol et Eurojust.

Le traitement de données à caractère personnel doit être conforme aux règles spécifiques établies par le Règlement n° 515/97 et la Convention SID[288], ainsi qu'aux dispositions de la directive relative à la protection des données, du règlement relatif à la protection des données des institutions communautaires, de la Convention 108 et de la recommandation sur les données de police. Le CEPD

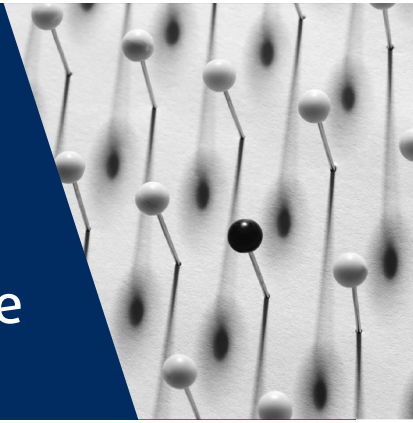
287 Conseil de l'Union européenne (1995), acte du Conseil du 26 juillet 1995 établissant la convention sur l'emploi de l'informatique dans le domaine des douanes, JO 1995 C 316, modifié par Conseil de l'Union européenne (2009), décision 2009/917/JAI du Conseil du 30 novembre 2009 sur l'emploi de l'informatique dans le domaine des douanes, JO 2009 L 323 (*décision SID*), Règlement (CE) n° 515/97 du Conseil du 13 mars 1997 relatif à l'assistance mutuelle entre les autorités administratives des États membres et à la collaboration entre celles-ci et la Commission en vue d'assurer la bonne application des réglementations douanière et agricole.

288 *Ibid.*

est chargé du contrôle de la conformité du SID au Règlement (CE) n° 45/2001 et convoque au moins une fois par an une réunion avec toutes les autorités de protection des données compétentes en matière de contrôle du SID.

8

Autres lois européennes spécifiques en matière de protection des données



UE	Questions traitées	CdE
Directive relative à la protection des données Directive vie privée et communications électroniques	**Communications électroniques**	Convention 108 Recommandation sur les services de télécommunications
Directive relative à la protection des données, article 8, paragraphe 2, point b)	**Relations de travail**	Convention 108 Recommandation en matière d'emploi
		CouEDH, *Copland c. Royaume-Uni*, n° 62617/00, 3 avril 2007
Directive relative à la protection des données, article 8, paragraphe 3	**Données médicales**	Convention 108 Recommandation sur les données médicales
		CouEDH, *Z. c. Finlande*, n °22009/93, 25 février 1997
Directive relative aux essais cliniques	**Essais cliniques**	
Directive relative à la protection des données, article 6, paragraphe 1, points b) et e), et article 13, paragraphe 2	**Statistiques**	Convention 108 Recommandation sur les données statistiques
Règlement (CE) n° 223/2009 relatif aux statistiques européennes CJUE, C-524/06, *Huber c. Bundesrepublik Deutschland*, 16 décembre 2008	**Statistiques officielles**	Convention 108 Recommandation sur les données statistiques

Directive 2004/39/CE concernant les marchés d'instruments financiers Règlement (UE) n° 648/2012 sur les produits dérivés de gré à gré, les contreparties centrales et les référentiels centraux Règlement (CE) n° 1060/2009 sur les agences de notation de crédit Directive 2007/64/CE concernant les services de paiement dans le marché intérieur	**Données financières**	Convention 108 Recommandation 90 (19) sur la protection des données à caractère personnel utilisées à des fins de paiement et autres opérations connexes CouEDH, *Michaud c. France*, n °12323/11, 6 décembre 2012

Dans plusieurs cas, des actes juridiques spéciaux ont été adoptés au niveau européen ; ils appliquent de façon plus détaillée les règles générales de la Convention 108 ou de la directive relative à la protection des données, à des situations spécifiques.

8.1. Communications électroniques

Points clés

- Des règles spécifiques relatives à la protection des données dans le domaine des télécommunications, eu égard notamment aux services téléphoniques, sont contenues dans la recommandation du CdE de 1995.
- Le traitement de données à caractère personnel relatives à la fourniture de services de communication au niveau européen est réglementé dans la directive vie privée et communications électroniques.
- La confidentialité des communications électroniques porte non seulement sur le contenu d'une communication, mais aussi sur les données relatives au trafic (par exemple qui a communiqué avec qui, quand et pendant combien de temps) et sur les données de lieu (par exemple l'endroit depuis lequel les données ont été communiquées).

Les réseaux de communication ont un plus grand potentiel d'ingérence injustifiée dans la sphère personnelle des utilisateurs, puisqu'ils offrent les moyens techniques d'écouter et d'étudier des communications intervenant sur de tels réseaux. Par conséquent, des règlements spéciaux en matière de protection des données ont été jugés nécessaires pour répondre aux risques particuliers pour les utilisateurs de services de communication.

En 1995, le CdE a publié une recommandation pour la protection des données dans le domaine des télécommunications, eu égard notamment aux services téléphoniques[289]. Conformément à cette recommandation, les finalités de la collecte et du traitement de données à caractère personnel dans le contexte des télécommunications devraient être limitées à : la connexion d'un utilisateur au réseau, permettant le service de télécommunication particulier, la facturation, la vérification, la garantie du fonctionnement technique optimal et le développement du réseau et du service.

Une attention particulière a également été accordée à l'utilisation de réseaux de communication pour l'envoi de messages de prospection. De manière générale, aucun message de prospection ne peut être adressé à tout abonné ayant expressément demandé à ne pas recevoir de messages publicitaires. Des appareils d'appel automatisés pour la transmission de messages publicitaires préenregistrés ne peuvent être utilisés que si un abonné a donné son consentement exprès. Le droit national doit prévoir des règles détaillées dans ce domaine.

S'agissant du **cadre juridique européen,** après une première tentative en 1997, la directive sur la vie privée et les communications électroniques (*directive vie privée et communications électroniques*) a été adoptée en 2002 et amendée en 2009, afin de compléter et préciser les dispositions de la directive relative à la protection des données pour le secteur des télécommunications[290]. L'application de la directive vie privée et communications électroniques est limitée aux services de communication sur des réseaux électroniques publics.

La directive vie privée et communications électroniques distingue trois catégories principales de données générées lors d'une communication :

289 CdE, Comité des Ministres (1995), recommandation Rec (95) 4 sur la protection des données à caractère personnel dans le domaine des services de télécommunication, eu égard notamment aux services téléphoniques, 7 février 1995.

290 Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, JO 2002 L 201 (*directive vie privée et communications électroniques*), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques ; directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et règlement (CE) n° 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs, JO 2009 L 337.

- les données qui constituent le contenu des messages envoyés pendant la communication ; ces données sont strictement confidentielles ;

- les données nécessaires à l'établissement et au maintien de la communication, appelées données relatives au trafic, telles que les informations sur les partenaires de communication, le moment et la durée de la communication ;

- les données relatives au trafic regroupent des données spécifiquement liées à l'emplacement du dispositif de communication, appelées données de localisation ; ces données portent également sur l'emplacement *des utilisateurs* des dispositifs de communication et elles sont particulièrement pertinentes pour les utilisateurs d'appareils mobiles.

Les données relatives au trafic peuvent uniquement être utilisées par le fournisseur de services à des fins de facturation et pour la prestation technique du service. Avec le consentement de la personne concernée, toutefois, ces données peuvent être divulguées à d'autres responsables du traitement offrant des services à valeur ajoutée, notamment donnant des informations concernant la localisation de l'utilisateur par rapport à la prochaine station de métro ou pharmacie, ou les prévisions météo de l'endroit où il se trouve.

Conformément à l'article 15 de la directive vie privée et communications électroniques, tout autre accès à des données relatives à des communications sur des réseaux électroniques, tel qu'un accès dans le but d'enquêter sur des crimes, doit satisfaire aux exigences d'ingérence justifiée dans le droit à la protection des données tel qu'il est énoncé à l'article 8, paragraphe 2, de la CEDH et confirmé aux articles 8 et 52 de la Charte.

Les amendements de 2009 à la directive vie privée et communications électroniques[291] ont introduit les éléments suivants :

- Les restrictions concernant l'envoi de courriels à des fins de prospection ont été étendues aux services de mini-messagerie, aux services de messagerie

291 Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) n° 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs, JO 2009 L 337.

multimédia et aux autres types d'applications similaires ; les courriels de prospection sont interdits, sauf si un consentement préalable a été obtenu. À défaut d'un tel consentement, seuls des clients antérieurs peuvent être contactés par des courriels de prospection s'ils ont communiqué leur adresse électronique et ne s'y opposent pas.

- Une obligation a été imposée aux États membres d'offrir des recours juridictionnels contre des violations à l'interdiction de communications non sollicitées[292].

- La mise en place de cookies, logiciels contrôlant et enregistrant les actions de l'utilisateur d'un ordinateur, n'est plus permise sans le consentement de l'utilisateur. La législation nationale doit réglementer plus en détail la façon dont le consentement devrait être exprimé et obtenu pour garantir une protection suffisante[293].

L'autorité de contrôle compétente doit être informée immédiatement de toute violation de données suite à un accès non autorisé, à une perte ou à une destruction de données. Les abonnés doivent être informés chaque fois qu'ils peuvent subir un préjudice en conséquence d'une violation de données[294].

La directive relative à la conservation des données[295], invalidée le 8 avril 2014, imposait aux prestataires de services de communication de veiller à la disponibilité des données relatives au trafic, en particulier pour lutter contre les formes graves de criminalité, pendant une période comprise entre six mois minimum et 24 mois maximum, que le prestataire ait encore eu besoin de ces données à des fins de facturation ou pour la fourniture technique du service ou non.

Les États membres de l'UE désignent des autorités publiques indépendantes chargées de contrôler la sécurité des données conservées.

---

292 Voir la directive modifiée, art. 13.

293 Voir *ibid.*, art. 5 ; voir également groupe de travail Article 29 (2012), Avis 04/2012 sur l'exemption de l'obligation de consentement pour certains cookies, WP 194, Bruxelles, 7 juin 2012.

294 Voir également groupe de travail Article 29 (2011), Document de travail 01/2011 concernant le cadre juridique relatif aux violations de données à caractère personnel actuellement en vigueur dans l'UE et présentant des recommandations quant aux actions à entreprendre à l'avenir, WP 184, Bruxelles, 5 avril 2011.

295 Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE, JO 2006 L 105, invalidée le 8 avril 2014.

La conservation de données relatives à des télécommunications constitue manifestement une ingérence dans le droit à la protection des données.[296] La question de savoir si cette ingérence est justifiée a été contestée dans le cadre de plusieurs procédures en justice dans des États membres de l'UE.[297]

> Exemple : dans les affaires *Digital Rights* et *Seitlinger et autres*[298], la CJUE a jugé que la directive relative à la conservation des données était invalide. Selon la Cour, « cette directive comporte une ingérence dans ces droits fondamentaux d'une vaste ampleur et d'une gravité particulière dans l'ordre juridique de l'Union sans qu'une telle ingérence soit précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au strict nécessaire. »

Une question fondamentale dans le contexte des communications électroniques est l'ingérence par les autorités publiques. Les moyens de surveillance ou d'interception des communications, tels que les dispositifs d'écoute, ne sont autorisés que s'ils sont prévus par la loi et s'ils constituent une mesure nécessaire dans une société démocratique, dans l'intérêt : de la protection de la sécurité nationale, de la sûreté publique, des intérêts monétaires de l'État ou de la suppression d'infractions pénales ; ou de la protection de la personne concernée ou des droits et libertés d'autrui.

Exemple : dans l'affaire *Malone c. Royaume-Uni*[299], le requérant avait été inculpé d'un certain nombre d'infractions liées au recel de biens volés. Pendant son procès, il est apparu qu'une conversation téléphonique du requérant avait été interceptée en vertu d'un mandat délivré par le Secrétaire d'État pour le ministère de l'Intérieur. Même si le mode d'interception de la communication du requérant était légal au regard du droit interne, la CouEDH a retenu qu'il n'existait pas de base légale concernant l'étendue et les modalités d'exercice du pouvoir d'appréciation attribué aux

296 CEPD (2011), *Avis du 31 mai 2011 sur le rapport d'évaluation de la Commission au Conseil et au Parlement européen concernant la directive sur la conservation des données (directive 2006/24/CE)*, 31 mai 2011.

297 Allemagne, Tribunal constitutionnel fédéral (*Bundesverfassungsgericht*), 1 BvR 256/08, 2 mars 2010 ; Roumanie, Cour constitutionnelle fédérale (*Curtea Constituțională a României*), n° 1258, 8 octobre 2009 ; République tchèque, Cour constitutionnelle (*Ústavní soud České republiky*), 94/2011 Coll., 22 mars 2011.

298 CJUE, affaires jointes C293/12 et C594/12, *Digital Rights Ireland et Seitlinger et autres*, 8 avril 2014, para. 65.

299 CouEDH, *Malone c. Royaume-Uni*, n° 8691/79, 26 avril 1985.

autorités publiques dans ce domaine et que l'ingérence résultant de l'existence de la pratique en question n'était donc pas « prévue par la loi ». La CouEDH a conclu à une violation de l'article 8 de la CEDH.

8.2. Données sur l'emploi

Points clés

- La recommandation du CdE sur les données sur l'emploi prévoit des règles spécifiques pour la protection des données dans les relations de travail.
- Dans la directive relative à la protection des données, les relations du travail sont spécifiquement mentionnées dans le contexte du traitement de données sensibles.
- La validité du consentement, qui doit avoir été donné librement, comme base légale du traitement de données sur des salariés peut être discutable compte tenu du déséquilibre économique entre l'employeur et les salariés. Les circonstances du consentement doivent être appréciées avec prudence.

Il n'existe pas de cadre juridique spécifique dans l'UE régissant le traitement de données dans le contexte de l'emploi. Dans la directive relative à la protection des données, les relations de travail sont spécifiquement mentionnées à l'article 8, paragraphe 2, consacré au traitement de données sensibles. S'agissant du CdE, la recommandation sur les données sur l'emploi a été publiée en 1989 et fait actuellement l'objet d'une mise à jour[300].

Une étude des problèmes les plus courants en matière de protection des données spécifiques au domaine de l'emploi figure dans un document de travail du groupe de travail Article 29[301]. Le groupe de travail a analysé l'importance du consentement comme base légale du traitement de données sur l'emploi[302]. Le groupe de travail a constaté que le déséquilibre économique entre l'employeur demandant un consen-

300 Conseil de l'Europe, Comité des Ministres (1989), recommandation Rec (89) 2 aux États membres relative à la protection des données à caractère personnel utilisées à des fins d'emploi, 18 janvier 1989. Voir également Comité consultatif de la Convention 108, *Étude sur la recommandation R(89)2 relative à la protection des données à caractère personnel utilisées à des fins d'emploi et propositions de révision de ladite recommandation*, 9 septembre 2011.

301 Groupe de travail Article 29 (2001), *Avis 8/2001 sur le traitement des données à caractère personnel dans le contexte professionnel*, WP 48, Bruxelles, 13 septembre 2001.

302 Groupe de travail Article 29 (2005), *Document de travail relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995*, WP 114, Bruxelles, 25 novembre 2005.

tement et le salarié donnant un consentement aura souvent pour effet de remettre en question la liberté du consentement. Les circonstances dans lesquelles le consentement est demandé devraient donc être examinées avec soin lors de l'appréciation de la validité du consentement dans le contexte professionnel.

Un problème courant en matière de protection des données dans l'environnement de travail classique actuel est l'étendue légitime du contrôle des communications électronique des salariés sur le lieu du travail. On entend souvent que ce problème peut facilement être résolu par l'interdiction de l'utilisation privée des systèmes de communication au travail. Mais une telle interdiction générale pourrait être disproportionnée et irréaliste. L'arrêt suivant de la CouEDH est particulièrement intéressant à cet égard :

> Exemple : dans l'affaire *Copland c. Royaume-Uni*[303], l'utilisation du téléphone, du courriel et d'Internet par une employée de collège avait été secrètement surveillée pour déterminer si elle faisait une utilisation abusive des équipements du collège à des fins personnelles. La CouEDH a considéré que les appels téléphoniques passés depuis les locaux professionnels étaient couverts par les notions de vie privée et de correspondance. Par conséquent, ces appels et courriels passés et envoyés depuis le travail, ainsi que les informations obtenues par la surveillance de l'utilisation privée d'Internet, étaient protégés par l'article 8 de la CEDH. Il n'existait aucune disposition réglementant les circonstances dans lesquelles des employeurs peuvent surveiller l'utilisation du téléphone, du courriel et d'Internet par leurs salariés. Partant, l'ingérence n'était pas prévue par loi. La CouEDH a donc conclu à une violation de l'article 8 de la CEDH.

Conformément à la recommandation du CdE sur l'emploi, les données à caractère personnel collectées à des fins d'emploi doivent être obtenues directement auprès du salarié concerné.

Les données à caractère personnel collectées à des fins de recrutement doivent être limitées aux informations nécessaires pour évaluer l'adéquation des candidats et leur potentiel professionnel.

La recommandation mentionne aussi spécifiquement les données d'appréciation (« *judgmental data* ») liées aux performances ou au potentiel de salariés individuels. Les données d'appréciation doivent être basées sur des évaluations justes

303 CouEDH, *Copland c. Royaume-Uni*, n° 62617/00, 3 avril 2007.

et honnêtes et ne doivent pas être formulées de façon injurieuse. C'est ce qu'imposent les principes de la loyauté du traitement des données et de l'exactitude des données.

Un aspect spécifique du droit en matière de protection des données dans le rapport employeur/salarié est le rôle des représentants des salariés. Ces représentants ne peuvent recevoir les données à caractère personnel de salariés que si cela est nécessaire pour leur permettre de défendre leurs intérêts.

Les données à caractère personnel sensibles collectées à des fins d'emploi ne peuvent être traitées que dans des cas particuliers et selon les garanties énoncées par le droit national. Les employeurs ne peuvent interroger des salariés ou candidats sur leur état de santé ou les soumettre à un examen médical que si cela est nécessaire pour : déterminer leur adéquation au poste ; satisfaire aux exigences de la médecine préventive ; ou permettre le versement de prestations sociales. Aucune donnée relative à la santé ne peut être collectée auprès d'autres sources que le salarié concerné, sauf s'il a donné son consentement exprès et informé ou sauf si la législation nationale le prévoit.

Conformément à la recommandation sur l'emploi, les salariés doivent être informés de la finalité du traitement de leurs données à caractère personnel, du type de données à caractère personnel enregistrées, des entités auxquelles les données sont communiquées régulièrement, ainsi que de la finalité et de la base légale de ces communications. En outre, les employeurs doivent informer leurs salariés à l'avance de l'introduction ou l'adaptation de systèmes automatisés pour le traitement de données à caractère personnel ou pour le contrôle des déplacements ou de la productivité des salariés.

Les salariés doivent avoir un droit d'accès à leurs données sur l'emploi, ainsi qu'un droit de rectification et d'effacement. Si des données d'appréciation sont traitées, les salariés doivent également avoir le droit de contester le jugement de valeur. Ces droits peuvent cependant être temporairement limités aux fins d'enquêtes internes. Si un salarié se voit refuser l'accès à des données à caractère personnel, leur rectification ou leur effacement, la législation nationale doit prévoir des procédures appropriées pour contester un tel refus.

8.3. Données médicales

Point clé

- Les données médicales sont des données sensibles qui bénéficient donc d'une protection particulière.

Les données à caractère personnel concernant l'état de santé de la personne concernée sont qualifiées de données sensibles à l'article 8, paragraphe 1, de la directive relative à la protection des données, et à l'article 6 de la Convention 108. En outre, les données médicales sont soumises à un régime plus strict que les données non sensibles en ce qui concerne leur traitement.

Exemple : dans l'affaire *Z. c. Finlande*[304], l'ex-mari de la requérante, qui était séropositif, avait commis un certain nombre d'infractions sexuelles. Par la suite, il avait été condamné pour homicide involontaire au motif qu'il avait sciemment exposé des victimes au risque d'une infection par le VIH. La juridiction nationale a ordonné que l'ensemble de l'arrêt et des pièces versées au dossier de l'affaire reste confidentiel pendant dix ans, malgré les demandes de la requérante visant à allonger cette période de confidentialité. Sa demande a été refusée par la Cour d'appel, laquelle avait rendu un arrêt contenant les noms complets de la requérante et de son ex-mari. La CouEDH a retenu que l'ingérence n'était pas nécessaire dans une société démocratique, au motif que la protection des données médicales est fondamentale au regard du droit au respect de la vie privée et de la vie familiale, en particulier s'agissant d'informations concernant une infection par le VIH, compte tenu de la stigmatisation associée à cette maladie dans de nombreuses sociétés. Par conséquent, la CouEDH a conclu qu'autoriser l'accès à l'identité et à l'état de santé de la requérante, tels que décrits dans l'arrêt de la Cour d'appel, après une période limitée à dix ans après le rendu de l'arrêt, constituerait une violation de l'article 8 de la CEDH.

L'article 8, paragraphe 3, de la directive relative à la protection des données permet le traitement de données médicales lorsque cela est nécessaire aux fins de

304 CouEDH, *Z. c. Finlande*, n °22009/93, 25 février 1997, paras. 94 et 112 ; voir également CouEDH, *M.S. c. Suède*, n° 20837/92, 27 août 1997 ; CouEDH, *L.L. c. France*, n° 7508/02, 10 octobre 2006 ; CouEDH, *I. c. Finlande*, n° 20511/03, 17 juillet 2008 ; CouEDH, *K.H. et autres c. Slovaquie*, n° 32881/04, 28 avril 2009 ; CouEDH, *Szuluk c. Royaume-Uni*, n° 36936/05, 2 juin 2009.

la médecine préventive, de diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de services de santé. Le traitement peut toutefois être autorisé s'il est effectué par un praticien de la santé soumis au secret professionnel ou par une autre personne également soumise à une obligation de secret équivalente[305].

La recommandation du CdE sur les données médicales de 1997 applique de façon plus détaillée les principes de la Convention 108 au traitement de données dans le domaine médical[306]. Les règles proposées sont conformes à celles de la directive relative à la protection des données s'agissant des finalités légitimes du traitement de données médicales, des obligations nécessaires au secret professionnel pour les personnes utilisant des données médicales et des droits des personnes concernées à la transparence ainsi qu'à l'accès, à la rectification et à la suppression des données. De plus, les données médicales qui font l'objet d'un traitement licite par des professionnels des services de santé ne peuvent être transférées à des autorités répressives à moins qu'il n'existe des garanties suffisantes empêchant toute divulgation incompatible avec le respect de la vie privée garanti par l'article 8 de la CEDH[307].

En outre, la recommandation sur les données médicales contient des dispositions spéciales relatives aux données médicales des enfants in utero et des personnes handicapées, ainsi que sur le traitement des données génétiques. La recherche scientifique est explicitement reconnue comme une raison de conserver des données plus longtemps que nécessaire, bien que cela requiert généralement une anonymisation. L'article 12 de la recommandation sur les données médicales propose des règles détaillées pour les situations dans lesquelles des chercheurs ont besoin de données à caractère personnel et où des données anonymisées sont insuffisantes.

La pseudonymisation peut être un moyen approprié de satisfaire les besoins scientifiques tout en protégeant les intérêts des patients concernés. Le concept de la pseudonymisation dans le contexte de la protection des données est expliqué plus en détail dans la Section 2.1.3.

305 Voir également CouEDH, *Biriuk c. Lituanie*, n° 23373/03, 25 novembre 2008.

306 CdE, Comité des Ministres (1997), recommandation Rec (97) 5 aux États membres relative à la protection des données médicales, 13 février 1997.

307 CouEDH, *Avilkina et autres c. Russie*, n° 1585/09, 6 juin 2013, para. 53 (non final).

Une discussion approfondie s'est déroulée au niveau national et européen sur des initiatives visant à enregistrer des données sur le traitement médical d'un patient dans un dossier médical électronique[308]. Un aspect particulier de l'existence de systèmes nationaux de dossiers médicaux électroniques est leur disponibilité au-delà des frontières : un sujet particulièrement intéressant au sein de l'UE dans le contexte des soins de santé transfrontaliers[309].

Un autre domaine de discussion autour des nouvelles dispositions est celui des essais cliniques, en d'autres termes l'essai de nouveaux médicaments dans un environnement de recherche documenté ; là encore, ce sujet a des implications considérables en matière de protection des données. Les essais cliniques de produits médicaux à usage humain sont réglementés par la directive 2001/20/CE du Parlement européen et du Conseil du 4 avril 2001 concernant le rapprochement des dispositions législatives, réglementaires et administratives des États membres relatives à l'application de bonnes pratiques cliniques dans la conduite d'essais cliniques de médicaments à usage humain (*directive relative aux essais cliniques*)[310]. En décembre 2012, la Commission européenne a proposé un règlement visant à remplacer la directive relative aux essais cliniques pour uniformiser et améliorer l'efficacité des procédures d'essais[311].

Il existe de nombreuses autres initiatives législatives et de différente nature en cours d'examen au niveau communautaire concernant les données à caractère personnel dans le secteur de la santé[312].

308 Groupe de travail Article 29 (2007), *Document de travail sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME)*, WP 131, Bruxelles, 15 février 2007.

309 Directive 2011/24/CE du Parlement européen et du Conseil du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers, JO 2011 L 88.

310 Directive 2001/20/CE du Parlement européen et du Conseil du 4 avril 2001 concernant le rapprochement des dispositions législatives, réglementaires et administratives des États membres relatives à l'application de bonnes pratiques cliniques dans la conduite d'essais cliniques de médicaments à usage humain, JO 2001 L 121.

311 Commission européenne (2012), *Proposition de règlement du Parlement européen et du Conseil relatif aux essais cliniques de médicaments à usage humain et abrogeant la directive 2001/20/CE*, COM(2012) 369 final, Bruxelles, 17 juillet 2012.

312 CEPD (2013), *Avis du Contrôleur européen de la protection des données sur la communication de la Commission relative au « Plan d'action pour la santé en ligne 2012-2020 – des soins de santé innovants pour le XXIe siècle »*, Bruxelles, 27 mars 2013.

8.4. Traitement de données à des fins statistiques

Points clés

- Les données collectées à des fins statistiques ne peuvent pas être utilisées à d'autres fins.
- Les données collectées de façon légitime à toute autre fin peuvent également être utilisées à des fins statistiques, à condition que la législation nationale prévoie des garanties adéquates qui soient satisfaites par les utilisateurs. Dans cette perspective, notamment, l'anonymisation ou la pseudonymisation avant la transmission à des tiers devrait être envisagée.

Dans la directive relative à la protection des données, le traitement de données à des fins statistiques est mentionné dans le contexte d'exceptions possibles aux principes de la protection des données. Conformément à l'article 6, paragraphe 1, point b), de la directive, il est possible de renoncer au principe de la limitation des finalités dans le droit national en faveur de l'utilisation ultérieure de données à des fins statistiques, même si le droit national doit néanmoins prévoir toutes les garanties nécessaires. L'article 13, paragraphe 2, de la directive autorise le droit national à limiter les droits d'accès si les données sont traitées exclusivement à des fins statistiques ; là encore, des garanties adéquates doivent exister dans le droit national. Dans ce contexte, la directive relative à la protection des données prévoit une exigence spécifique selon laquelle les données acquises ou créées dans le cadre de recherches statistiques ne peuvent pas être utilisées pour des décisions concrètes sur des personnes concernées.

Bien que les données qui ont été collectées légalement par un responsable du traitement à toute fin puissent être réutilisées par ce responsable à ses propres fins statistiques (« statistiques secondaires »), les données devraient en fonction des circonstances être anonymisées ou pseudonymisées avant d'être transmises à un tiers à des fins statistiques, à moins que la personne concernée n'y ait consenti ou que cela soit spécifiquement prévu par le droit national. C'est ce qui découle de l'exigence de garanties appropriées prévue à l'article 6, paragraphe 1, point b), de la directive relative à la protection des données.

Les cas les plus importants d'utilisation de données à des fins statistiques sont les statistiques officielles, réalisées par les bureaux nationaux et européens de la

statistique sur la base des législations nationales et européennes relatives aux statistiques officielles. Conformément à ces législations, les citoyens et les entreprises sont généralement tenus de communiquer des données aux autorités statistiques. Les fonctionnaires qui travaillent dans des bureaux statistiques sont soumis à des obligations spéciales au secret professionnel qu'ils observent avec soin dans la mesure où elles sont essentielles au niveau de confiance élevé des citoyens, nécessaire si des données doivent être communiquées aux autorités de la statistique.

Le règlement (CE) n° 223/2009 relatif aux statistiques européennes (*règlement sur les statistiques européennes*) contient des règles essentielles pour la protection des données dans les statistiques officielles et, par conséquent, peut aussi être considéré comme pertinent pour des dispositions relatives aux statistiques officielles au niveau national[313]. Le règlement maintient le principe selon lequel les opérations de statistiques officielles requièrent une base légale suffisamment précise[314].

> Exemple : dans l'affaire *Huber c. Bundesrepublik Deutschland*[315], la CJUE a considéré que la collecte et l'enregistrement de données à caractère personnel par une autorité à des fins statistiques ne pouvaient justifier la légalité du traitement. Le droit encadrant le traitement de données à caractère personnel doit également satisfaire l'exigence de nécessité, ce qui n'était pas le cas en l'espèce.

Dans le contexte du CdE, la recommandation sur les données statistiques, publiée en 1997, couvre la réalisation de statistiques dans les secteurs public et privé[316]. Cette recommandation introduit des principes qui coïncident avec les règles principales de la directive relative à la protection des données décrites ci-dessus. Des règles plus détaillées concernent les points ci-après.

313 Règlement (CE) n° 223/2009 du Parlement européen et du Conseil du 11 mars 2009 relatif aux statistiques européennes et abrogeant le règlement (CE, Euratom) n° 1101/2008 relatif à la transmission à l'Office statistique des Communautés européennes d'informations statistiques couvertes par le secret, le règlement (CE) n° 322/97 du Conseil relatif à la statistique communautaire et la décision 89/382/CEE, Euratom du Conseil instituant un comité du programme statistique des Communautés européennes, JO 2009 L 87.

314 Ce principe doit être plus détaillé dans le Code de pratique d'Eurostat qui, conformément à l'art. 11 du règlement sur les statistiques européennes, doit apporter des conseils éthiques sur le mode de réalisation des statistiques officielles, y compris sur l'utilisation prévenante des données à caractère personnel ; disponible à l'adresse : http://epp.eurostat.ec.europa.eu/portal/page/portal/about_eurostat/introduction.

315 CJUE, C-524/06, *Huber c. Bundesrepublik Deutschland*, 16 décembre 2008 ; voir en particulier para. 68.

316 Conseil de l'Europe, Comité des Ministres (1997), recommandation Rec (97) 18 aux États membres relative à la protection des données à caractère personnel collectées et traitées à des fins statistiques, 30 septembre 1997.

Tandis que les données qui ont été collectées par un responsable du traitement à des fins statistiques ne peuvent pas être utilisées à quelque autre fin que ce soit, les données qui ont été collectées à des fins autres que statistiques peuvent faire l'objet d'une utilisation statistique par la suite. La recommandation sur les données statistiques autorise même la communication de données à des tiers si celle-ci poursuit une finalité purement statistique, auquel cas les parties doivent convenir et consigner par écrit l'étendue de l'utilisation ultérieure légitime à des fins statistiques. Dans la mesure où cette formalité ne saurait se substituer au consentement de la personne concernée, il convient de supposer qu'il doit exister des garanties appropriées supplémentaires énoncées par la législation nationale pour minimiser les risques d'utilisation abusive de données à caractère personnel, comme une obligation d'anonymiser ou de pseudonymiser les données avant leur transmission.

Les professionnels chargés de recherches statistiques devraient être liés par des obligations spéciales au secret professionnel (comme c'est le cas pour les statistiques officielles) en vertu de la législation nationale. Cette obligation devrait également être étendue aux interviewers, dès lors qu'ils travaillent à la collecte des données provenant de personnes concernées ou d'autres personnes.

Si aucune enquête statistique utilisant des données à caractère personnel n'est prévue par la loi, les personnes concernées doivent consentir à l'utilisation de leurs données afin de rendre le traitement légitime, ou avoir au moins la possibilité de s'y opposer. Si des interviewers collectent des données à caractère personnel à des fins statistiques, les personnes concernées doivent être clairement informées du caractère obligatoire ou facultatif de la divulgation des données selon le droit national. Aucune donnée sensible ne peut être collectée de façon permettant l'identification d'un individu, sauf autorisation explicite du droit national.

Si une étude statistique ne peut pas être réalisée sans données anonymes et si des données à caractère personnel sont effectivement nécessaires, les données collectées à cette fin doivent être anonymisées dès que possible. À tout le moins, les résultats de l'enquête statistique ne doivent pas autoriser l'identification de personnes concernées, quelles qu'elles soient, à moins que cela ne présente manifestement aucun risque.

À l'issue de l'analyse statistique, les données à caractère personnel utilisées doivent être supprimées ou anonymisées. Dans ce cas, la recommandation sur les données statistiques propose que les données d'identification soient enregistrées séparément des autres données à caractère personnel. Cela signifie par exemple

que les données doivent être pseudonymisées et que la clé de cryptage ou la liste des synonymes d'identification doit être enregistrée séparément des données pseudonymisées.

8.5. Données financières

Points clés

- Bien que les données financières ne soient pas des données sensibles au sens de la Convention 108 ou de la directive relative à la protection des données, leur traitement requiert des garanties particulières pour assurer l'exactitude et la sécurité des données.
- Les systèmes de paiement électroniques nécessitent une protection intégrée des données, appelée « respect de la vie privée dès la conception » (« *privacy by design* »).
- Des problèmes particuliers de protection des données surviennent dans ce domaine du fait de la nécessité de mécanismes d'authentification appropriés.

Exemple : dans l'affaire *Michaud c. France*[317], le requérant, un avocat français, contestait l'obligation que lui imposait le droit français de signaler toute suspicion de blanchiment d'argent par ses clients. La CouEDH a relevé qu'imposer aux avocats de signaler aux autorités administratives des informations concernant un tiers, dont ils prennent connaissance dans le cadre d'échanges avec cette personne, constitue une ingérence dans le droit des avocats au respect de leur correspondance et de leur vie privée au titre de l'article 8 de la CEDH, ce concept couvrant aussi bien des activités de nature professionnelle que commerciale. Toutefois, l'ingérence était prévue par la loi et poursuivait un but légitime, à savoir la défense de l'ordre et la prévention des infractions pénales. Dans la mesure où les avocats ne sont soumis à l'obligation de signaler une suspicion que dans des circonstances très limitées, la CouEDH a jugé cette obligation proportionnée et à exclu la violation de l'article 8.

Une application du cadre légal général de la protection des données, tel qu'il est prévu dans la Convention 108, au contexte des paiements a été développée par

317 CouEDH, *Michaud c. France*, n° 12323/11, 6 décembre 2012 ; voir également CouEDH, *Niemietz c. Allemagne*, n° 13710/88, 16 décembre 1992, para. 29, et CouEDH, *Halford c. Royaume-Uni*, n° 20605/92, 25 juin 1997, para. 42.

la recommandation Rec (90) 19 du CdE de 1990[318]. Cette recommandation clarifie l'étendue de la collecte et de l'utilisation légales de données dans le contexte de paiements, en particulier à l'aide de cartes de paiement. Elle propose également aux législateurs nationaux des règles détaillées sur les limites de la communication de données de paiement à des tiers, les limites dans le temps de la conservation des données, la transparence, la sécurité des données et les flux de données transfrontières et, enfin, sur le contrôle et les voies de recours. Les solutions proposées correspondent au cadre communautaire général de protection des données qui a été prévu par la suite dans la directive relative à la protection des données.

Un certain nombre d'actes juridiques sont en cours de création pour réglementer les marchés d'instruments financiers et les activités des établissements de crédit et des sociétés de placement[319]. D'autres actes juridiques contribuent à lutter contre les délits d'initié et la manipulation de cours[320]. Les problèmes les plus critiques dans ces domaines qui ont un impact sur la protection des données sont :

- la conservation de registres des transactions financières ;
- le transfert de données à caractère personnel vers des pays tiers ;
- l'enregistrement de conversations téléphoniques ou communications électroniques, y compris le pouvoir des autorités compétentes de demander à consulter les enregistrements des échanges téléphoniques et de données ;

318 CdE, Comité des Ministres (1990), recommandation R (90) 19 sur la protection des données à caractère personnel utilisées à des fins de paiement et autres opérations connexes, 13 septembre 1990.

319 Commission européenne (2011), *Proposition de directive du Parlement européen et du Conseil concernant les marchés d'instruments financiers, abrogeant la directive 2004/39/CE du Parlement européen et du Conseil*, COM(2011) 656 final, Bruxelles, 20 octobre 2011 ; Commission européenne (2011), *Proposition de règlement du Parlement européen et du Conseil concernant les marchés d'instruments financiers et modifiant le règlement [EMIR] sur les produits dérivés négociés de gré à gré, les contreparties centrales et les référentiels centraux*, COM(2011) 652 final, Bruxelles, 20 octobre 2011 ; Commission européenne (2011), *Proposition de directive du Parlement européen et du Conseil concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement et modifiant la directive 2002/87/CE du Parlement européen et du Conseil relative à la surveillance complémentaire des établissements de crédit, des entreprises d'assurance et des entreprises d'investissement appartenant à un conglomérat financier*, COM(2011) 453 final, Bruxelles, 20 juillet 2011.

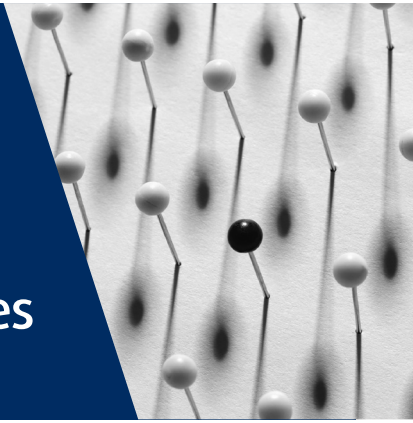
320 Commission européenne (2011), *Proposition de règlement du Parlement européen et du Conseil sur les opérations d'initiés et les manipulations de marché (abus de marché)*, COM(2011) 651 final, Bruxelles, 20 octobre 2011 ; Commission européenne (2011), *Proposition de directive du Parlement européen et du Conseil relative aux sanctions pénales applicables aux opérations d'initiés et aux manipulations de marché*, COM(2011) 654 final, Bruxelles, 20 octobre 2011.

- la divulgation d'informations personnelles, y compris la publication de sanctions ;
- les pouvoirs de contrôle et d'enquête des autorités compétentes, y compris les inspections sur site et la visite de locaux privés en vue de saisir des documents ;
- les mécanismes de signalement d'infractions, c'est-à-dire les systèmes de transmission d'informations ; et
- la coopération entre les autorités compétentes des États membres et l'Autorité européenne des marchés financiers (AEMF).

D'autres problèmes en la matière sont aussi traités de façon spécifique, notamment la collecte des données sur le statut financier des personnes concernées[321] ou le paiement transfrontalier par virements bancaires, qui entraîne inévitablement des flux de données à caractère personnel[322].

321 Règlement (CE) n° 1060/2009 du Parlement européen et du Conseil du 16 septembre 2009 sur les agences de notation de crédit, JO 2009 L 302 ; Commission européenne, *Proposition de règlement du Parlement européen et du Conseil modifiant le règlement (CE) n° 1060/2009 sur les agences de notation de crédit*, COM(2010) 289 final, Bruxelles, 2 juin 2010.

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



Lectures complémentaires

Chapitre 1

Araceli Mangas, M. (ed.) (2008), *Carta de los derechos fundamentales de la Unión Europea*, Bilbao, Fundación BBVA.

Berka, W. (2012), *Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit*, Vienne, Manzsche Verlags- und Universitätsbuchhandlung.

EDRi, *An introduction to data protection*, Bruxelles, www.edri.org/files/paper06_datap.pdf.

Frowein, J. et Peukert, W. (2009), *Europäische Menschenrechtskonvention*, Berlin, N. P. Engel Verlag.

Grabenwarter, C. et Pabel, K. (2012), *Europäische Menschenrechtskonvention*, Munich, C. H. Beck.

Harris, D., O'Boyle, M., Warbrick, C. et Bates, E. (2009), *Law of the European Convention on Human Rights*, Oxford, Oxford University Press.

Jarass, H. (2010), *Charta der Grundrechte der Europäischen Union*, Munich, C. H. Beck.

Mayer, J. (2011), *Charta der Grundrechte der Europäischen Union*, Baden-Baden, Nomos.

Mowbray, A. (2012), *Cases, materials, and commentary on the European Convention on Human Rights*, Oxford, Oxford University Press.

Nowak, M., Januszewski, K. et Hofstätter, T. (2012), *All human rights for all – Vienna manual on human rights*, Antwerp, intersentia N. V., Neuer Wissenschaftlicher Verlag.

Picharel, C. et Coutron, L. (2010), *Charte des droits fondamentaux de l'Union européenne et convention européenne des droits de l'homme*, Brussels, Emile Bruylant.

Simitis, S. (1997), 'Die EU-Datenschutz-Richtlinie – Stillstand oder Anreiz?', *Neue Juristische Wochenschrift*, n° 5, p. 281–288.

Warren, S. et Brandeis, L. (1890), 'The right to privacy', *Harvard Law Review,* Vol. 4, n° 5, p. 193–220, www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf

White, R. et Ovey, C. (2010), *The European Convention on Human Rights*, Oxford, Oxford University Press.

Chapitre 2

Carey, P. (2009), *Data protection: A practical guide to UK and EU law*, Oxford, Oxford University Press.

Delgado, L. (2008), *Vida privada y protección de datos en la Unión Europea*, Madrid, Dykinson S. L.

Desgens-Pasanau, G. (2012), *La protection des données à caractère personnel*, Paris, LexisNexis.

Di Martino, A. (2005), *Datenschutz im europäischen Recht*, Baden-Baden, Nomos.

Morgan, R. et Boardman, R. (2012), *Data protection strategy: Implementing data protection compliance*, London, Sweet & Maxwell.

Ohm, P. (2010), « Broken promises of privacy: Responding to the surprising failure of anonymization », *UCLA Law Review*, Vol. 57, n° 6, p. 1701–1777.

Tinnefeld, M., Buchner, B. et Petri, T. (2012), *Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in europäischer Sicht*, Munich, Oldenbourg Wissenschaftsverlag.

United Kingdom Information Commissioner's Office (2012), *Anonymisation: managing data protection risk. Code of practice*, www.ico.org.uk/for_organisations/data_protection/topic_guides/anonymisation.

Chapitres 3 à 5

Brühann, U. (2012), « Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr » dans : Grabitz, E., Hilf, M. et Nettesheim, M. (eds.), *Das Recht der Europäischen Union*, Band IV, A. 30, Munich, C. H. Beck.

Conde Ortiz, C. (2008), *La protección de datos personales*, Cadiz, Dykinson.

Coudray, L. (2010), *La protection des données personnelles dans l'Union européenne*, Sarrebruck, Éditions universitaires européennes.

Dammann, U. et Simitis, S. (1997), *EG-Datenschutzrichtlinie*, Baden-Baden, Nomos.

FRA (Agence des droits fondamentaux de l'Union européenne) (2010), *Developing indicators for the protection, respect and promotion of the rights of the child in the European Union,* Conference edition, Vienne, FRA.

FRA (2010), *La protection des données à caractère personnel dans l'Union européenne : le rôle des autorités nationales chargées de la protection des données – Renforcement de l'architecture des droits fondamentaux au sein de l'UE II*, Luxembourg, Office des publications de l'Union européenne (Office des publications).

FRA (2011), *L'accès à la justice en Europe : présentation des défis à relever et des opportunités à saisir*, Luxembourg, Office des publications.

Simitis, S. (2011), *Bundesdatenschutzgesetz*, Baden-Baden, Nomos.

United Kingdom Information Commissioner's Office, *Privacy Impact Assessment*, disponible à l'adresse : www.ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment.

Chapitre 6

Gutwirth, S., Poullet, Y., De Hert, P., De Terwangne, C. et Nouwt, S. (2009), *Reinventing data protection?*, Berlin, Springer.

Kuner, C. (2007), *European data protection law*, Oxford, Oxford University Press.

Kuner, C. (2013), *Transborder data flow regulation and data privacy law*, Oxford, Oxford University Press.

Chapitre 7

Europol (2012), *Data Protection at Europol*, Luxembourg, Office des publications, www.europol.europa.eu/sites/default/files/publications/europol_dpo_booklet_0.pdf.

Eurojust, *Data protection at Eurojust: A robust, effective and tailor-made regime*, La Haye, Eurojust.

Drewer, D., Ellermann, J. (2012), *Europol's data protection framework as an asset in the fight against cybercrime,* ERA Forum, Vol. 13, n° 3, p. 381–395.

Gutwirth, S., Poullet, Y. et De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. et Leenes, R. (2011), *Computers, privacy and data protection: An element of choice*, Dordrecht, Springer.

Konstadinides, T. (2011), *Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem*, *European Law Review*, Vol. 36, n° 5, p. 722–776.

Santos Vara, J. (2013), *The role of the European Parliament in the conclusion of the Transatlantic Agreements on the transfer of personal data after Lisbon*, Centre for the Law of External Relations, CLEER Working Papers 2013/2, www.asser.nl/upload/documents/20130226T013310-cleer_13-2_web.pdf.

Chapitre 8

Büllesbach, A., Gijrath, S., Poullet, Y. et Hacon, R. (2010), *Concise European IT law*, Amsterdam, Kluwer Law International.

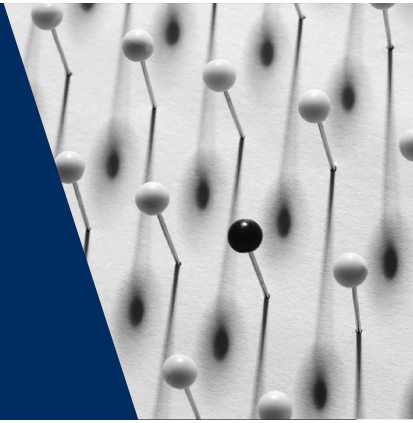
Gutwirth, S., Leenes, R., De Hert, P. et Poullet, Y. (2012), *European data protection: In good health?*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y. et De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. et Leenes, R. (2011), *Computers, privacy and data protection: An element of choice*, Dordrecht, Springer.

Konstadinides, T. (2011), Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem, *European Law Review*, Vol. 36, n° 5, p. 722-76.

Rosemary, J. et Hamilton, A. (2012), *Data protection law and practice*, London, Sweet & Maxwell.



Jurisprudence

Jurisprudence de la Cour européenne des droits de l'homme

Accès aux données à caractère personnel

Gaskin c. Royaume-Uni, n° 10454/83, 7 juillet 1989
Godelli c. Italie, n° 33783/09, 25 septembre 2012
K.H. et autres c. Slovaquie, n° 32881/04, 28 avril 2009
Leander c. Suède, n° 9248/81, 26 mars 1987
Odièvre c. France [GC], n° 42326/98, 13 février 2003

Mise en balance entre protection des données et liberté d'expression

Axel Springer AG c. Allemagne [GC], n° 39954/08, 7 février 2012
Von Hannover c. Allemagne, n° 59320/00, 24 juin 2004
Von Hannover c. Germany (n° 2) [GC], n° 40660/08 et 60641/08, 7 février 2012

Contestations en matière de protection des données en ligne

K.U. c. Finlande, n 2872/02, 2 décembre 2008

Correspondance

Amann c. Suisse [GC], n° 27798/95, 16 février 2000
Bernh Larsen Holding AS et autres c. Norvège, n° 24117/08, 14 mars 2013
Cemalettin Canli c. Turquie, n° 22427/04, 18 novembre 2008

Dalea c. France, n° 964/07, 2 février 2010
Gaskin c. Royaume-Uni, n° 10454/83, 7 juillet 1989
Haralambie c. Roumanie, n° 21737/03, 27 octobre 2009
Khelili c. Suisse, n° 16188/07, 18 octobre 2011
Leander c. Suède, n° 9248/81, 26 mars 1987
Malone c. Royaume-Uni, n° 8691/79, 26 avril 1985
McMichael c. Royaume-Uni, n° 16424/90, 24 février 1995
M.G. c. Royaume-Uni, n° 39393/98, 24 septembre 2002
Rotaru c. Roumanie [GC], n° 28341/95, 4 mai 2000
S. et Marper c. Royaume-Uni, n° 30562/04 et 30566/04, 4 décembre 2008
Shimovolos c. Russie, n° 30194/09, 21 juin 2011
Turek c. Slovaquie, n° 57986/00, 14 février 2006

Bases de données de casiers judiciaires

B.B. c. France, n 5335/06, 17 décembre 2009
M.M. c. Royaume-Uni, n° 24029/07, 13 novembre 2012

Bases de données ADN

S. et Marper c. Royaume-Uni, n° 30562/04 et 30566/04, 4 décembre 2008

Données GPS

Uzun c. Allemagne, n° 35623/05, 2 septembre 2010

Données relatives à la santé

Biriuk c. Lituanie, n° 23373/03, 25 novembre 2008
I. c. Finlande, n 20511/03, 17 juillet 2008
L.L. c. France, n 7508/02, 10 octobre 2006
M.S. c. Suède, n° 34209/96, 2 juillet 2002
Szuluk c. Royaume-Uni, n° 36936/05, 2 juin 2009
Z. c. Finlande, n 22009/93, 25 février 1997

Identité

Ciubotaru c. Moldavie, n° 27138/04, 27 avril 2010
Godelli c. Italie, n° 33783/09, 25 septembre 2012
Odièvre c. France [GC], n° 42326/98, 13 février 2003

Informations concernant des activités professionnelles

Michaud c. France, n 12323/11, 6 décembre 2012
Niemietz c. Allemagne, n° 13710/88, 16 décembre 1992

Interception de communications

Amann c. Suisse [GC], n° 27798/95, 16 février 2000
Copland c. Royaume-Uni, n° 62617/00, 3 avril 2007
Cotlet c. Roumanie, n° 38565/97, 3 juin 2003
Kruslin c. France, n 11801/85, 24 avril 1990
Lambert c. France, n 23618/94, 24 août 1998
Liberty et autres c. Royaume-Uni, n° 58243/00, 1er juillet 2008
Malone c. Royaume-Uni, n° 8691/79, 26 avril 1985
Halford c. Royaume-Uni, n° 20605/92, 25 juin 1997
Szuluk c. Royaume-Uni, n° 36936/05, 2 juin 2009

Obligations des responsables

B.B. c. France, n 5335/06, 17 décembre 2009
I. c. Finlande, n 20511/03, 17 juillet 2008
Mosley c. Royaume-Uni, n° 48009/08, 10 mai 2011

Photographies

Sciacca c. Italie, n° 50774/99, 11 janvier 2005
Von Hannover c. Allemagne, n° 59320/00, 24 juin 2004

Droit à l'oubli

Segerstedt-Wiberg et autres c. Suède, n° 62332/00, 6 juin 2006

Droit d'opposition

Leander c. Suède, n° 9248/81, 26 mars 1987
Mosley c. Royaume-Uni, n° 48009/08, 10 mai 2011
M.S. c. Suède, n° 34209/96, 2 juillet 2002
Rotaru c. Roumanie [GC], n° 28341/95, 4 mai 2000

Catégories sensibles de données

I. c. Finlande, n 20511/03, 17 juillet 2008

Michaud c. France, n 12323/11, 6 décembre 2012
S. et Marper c. Royaume-Uni, n° 30562/04 et 30566/04, 4 décembre 2008

Contrôle et exécution (rôle des différents acteurs, y compris autorités de protection des données)

I. c. Finlande, n 20511/03, 17 juillet 2008
K.U. c. Finlande, n 2872/02, 2 décembre 2008
Von Hannover c. Allemagne, n° 59320/00, 24 juin 2004
Von Hannover c. Germany (n° 2) [GC], n° 40660/08 et 60641/08, 7 février 2012

Méthodes de contrôle

Allan c. Royaume-Uni, n° 48539/99, 5 novembre 2002
Association « 21 Décembre 1989 » et autres c. Roumanie, n° 33810/07 et 18817/08, 24 mai 2011
Bykov c. Russie [GC], n° 4378/02, 10 mars 2009
Kennedy c. Royaume-Uni, n° 26839/05, 18 mai 2010
Klass et autres c. Allemagne, n° 5029/71, 6 septembre 1978
Rotaru c. Roumanie [GC], n° 28341/95, 4 mai 2000
Taylor-Sabori c. Royaume-Uni, n° 47114/99, 22 octobre 2002
Uzun c. Allemagne, n°35623/05, 2 septembre 2010
Vetter c. France, n 59842/00, 31 mai 2005

Vidéo-surveillance

Köpke c. Allemagne, n° 420/07, 5 octobre 2010
Peck c. Royaume-Uni, n° 44647/98, 28 janvier 2003

Échantillons vocaux

P.G. et J.H. c. Royaume-Uni, n° 44787/98, 25 septembre 2001
Wisse c. France, n 71611/01, 20 décembre 2005

Jurisprudence de la Cour de justice de l'Union européenne

Jurisprudence liée à la directive relative à la protection des données

Tietosuojavaltuutettu c. Satakunnan Markkinapörssi Oy et Satamedia Oy, C-73/07, 16 décembre 2008
[Concept des « activités journalistiques » au sens de l'article 9 de la directive relative à la protection des données]

Volker und Markus Schecke GbR et Hartmut Eifert c. Land Hessen, affaires jointes C-92/09 et C93/09, 9 novembre 2010
[Proportionnalité de l'obligation légale de publier des données à caractère personnel concernant les bénéficiaires de certains fonds agricoles européens]

Bodil Lindqvist, C-101/01, 6 novembre 2003
[Légitimité de la publication sur Internet par un particulier de données concernant la vie privée de tiers]

Google Spain, S.L., Google Inc. c. Agencia Española de Protección de Datos, Mario Costeja González, C-131/12, renvoi préjudiciel d'*Audiencia Nacional* (Espagne) formé le 9 mars 2012, 25 mai 2012, pendant
[Obligations des prestataires de moteurs de recherche de s'abstenir, à la demande de la personne concernée, de présenter des données à caractère personnel dans les résultats de recherche]

Commission européenne c. Royaume de Suède, C-270/11, 30 mai 2013
[Amende pour absence de mise en œuvre d'une directive]

Productores de Música de España (Promusicae) c. Telefónica de España SAU, C-275/06, 29 janvier 2008
[Obligation de fournisseurs d'accès à Internet de divulguer l'identité des utilisateurs de programmes d'échanges de fichiers KaZaA à une association de protection de la propriété intellectuelle]

Commission européenne c. Hongrie, C-288/12, 8 avril 2014
[Légitimité du renvoi de ses fonctions du contrôleur national de la protection des données]

Michael Schwarz c. Stadt Bochum, conclusions de l'avocat général, C-291/12, 13 juin 2013
[Violation du droit primaire de l'UE par le règlement (CE) 2252/2004 prévoyant l'enregistrement d'empreintes digitales sur les passeports]

SABAM c. Netlog N.V., C-360/10, 16 février 2012
[Obligation de prestataires de réseaux sociaux d'empêcher l'utilisation illicite d'œuvres musicales et audiovisuelles par des utilisateurs du réseau]

Rechnungshof c. Österreichischer Rundfunk et autres et Neukomm et Lauermann c. Österreichischer Rundfunk, affaires jointes C-465/00, C-138/01 et C-139/01, 20 mai 2003
[Proportionnalité de l'obligation légale de publier des données à caractère personnel sur les salaires d'employés de certaines catégories d'institutions liées au secteur public]

Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) et Federación de Comercio Electrónico y Marketing Directo (FECEMD) c. Administración del Estado, affaires jointes C-468/10 et C-469/10, 24 novembre 2011
[Mise en application correcte de l'article 7, point f), de la directive relative à la protection des données – « intérêts légitimes de tiers » – dans la législation nationale]

Commission européenne c. République fédérale d'Allemagne, C-518/07, 9 mars 2010
[Indépendance d'une autorité de contrôle nationale]

Huber c. Bundesrepublik Deutschland, C-524/06, 16 décembre 2008
[Légitimité de la détention de données concernant des étrangers dans un registre statistique]

Deutsche Telekom AG c. Bundesrepublik Deutschland, C-543/09, 5 mai 2011
[Nécessité du renouvellement du consentement]

College van burgemeester en wethouders van Rotterdam c. M.E.E, C-553/07, 7 mai 2009
[Droit d'accès de la personne concernée]

Digital Rights Ireland et Seitlinger et autres, affaires jointes C 293/12 et C 594/12, 8 avril 2014
[Violation du droit primaire de l'UE par la directive relative à la conservation des données]

Commission européenne c. République d'Autriche, C-614/10, 16 octobre 2012
[Indépendance d'une autorité de contrôle nationale]

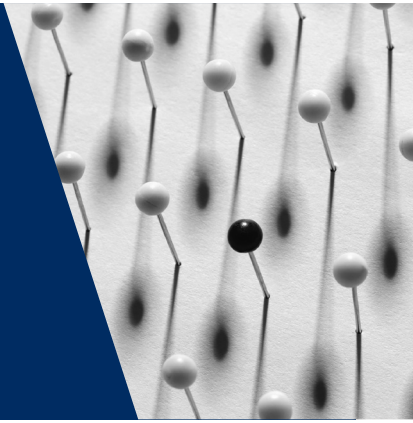
Jurisprudence liée au règlement relatif à la protection des données des institutions communautaires

Commission européenne c. The Bavarian Lager Co. Ltd, C-28/08 P, 29 juin 2010
[Accès aux documents]

Interporc Im- und Export GmbH c. Commission des Communautés européennes, C-41/00 P, 6 mars 2003
[Accès aux documents]

Dimitrios Pachtitis c. Commission européenne, F-35/08, 15 juin 2010
[Utilisation de données à caractère personnel dans le contexte d'un emploi dans des institutions communautaires]

V c. Parlement européen, F-46/09, 5 juillet 2011
[Utilisation de données à caractère personnel dans le contexte d'un emploi dans des institutions communautaires]



Liste de la jurisprudence

Jurisprudence de la Cour de justice de l'Union européenne

Jurisprudence de la Cour européenne des droits de l'homme

Case-law of national courts

Agence des droits fondamentaux de l'Union européenne
Conseil de l'Europe – Cour européenne des droits de l'homme

Manuel de droit européen en matière de protection des données

2014 – 215 p. – 14,8 x 21 cm

ISBN 978-92-871-9954-6 (CdE)
ISBN 978-92-9239-332-8 (FRA)
doi:10.2811/53800

De nombreuses informations sur l'Agence des droits fondamentaux de l'Union européenne sont disponibles sur le site internet de la FRA (fra.europa.eu).

Plus d'informations sur le Conseil de l'Europe sont disponibles sur le site internet du Conseil à: hub.coe.int.

D'autres informations sur la jurisprudence de la Cour européenne des droits de l'homme sont disponibles sur le site internet de la Cour: echr.coe.int. Le portail de recherche HUDOC donne accès aux arrêts et décisions en anglais et/ou en français, à des traductions dans d'autres langues, aux avis consultatifs et résumés juridiques, aux communiqués de presse et autres informations sur le travail de la Cour.

10.2811/53800 TK-01-13-772-FR-C

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

L'évolution rapide des technologies de l'information et de la communication souligne la nécessité croissante d'une solide protection des données à caractère personnel, un droit qui est garanti à la fois par les instruments de l'Union européenne (UE) et du Conseil de l'Europe (CdE). Les avancées technologiques étendent notamment les frontières de la surveillance, de l'interception des communications et de la conservation des données, ce qui place le droit à la protection des données face à des défis majeurs. Le présent manuel est conçu de façon à permettre aux praticiens du droit qui ne sont pas spécialisés en matière de protection des données de se familiariser avec ce domaine du droit. Il fournit une synthèse des cadres légaux applicables de l'UE et du CdE. Il explique la jurisprudence clé et résume les principaux arrêts de la Cour européenne des droits de l'homme et de la Cour de justice de l'Union européenne. En l'absence d'une telle jurisprudence, il présente des illustrations pratiques sur la base de scénarios hypothétiques. En un mot, le présent manuel vise à contribuer au plein respect du droit à la protection des données.

AGENCE DES DROITS FONDAMENTAUX DE L'UNION EUROPÉENNE
Schwarzenbergplatz 11 – 1040 Vienne – Autriche
Tél. +43 (1) 580 30-60 - Fax +43 (1) 580 30-693
fra.europa.eu – info@fra.europa.eu

COUR EUROPÉENNE DES DROITS DE L'HOMME
CONSEIL DE L'EUROPE
67075 Strasbourg Cedex - France
Tél. +33 (0) 3 88 41 20 00 - Fax +33 (0) 3 88 41 27 30
hub.coe.int - echr.coe.int - publishing@echr.coe.int

Office des publications
ISBN 978-92-871-9954-6 (CdE)
ISBN 978-92-9239-332-8 (FRA)
ISBN 978-92-9239-332-8
9 789292 393328