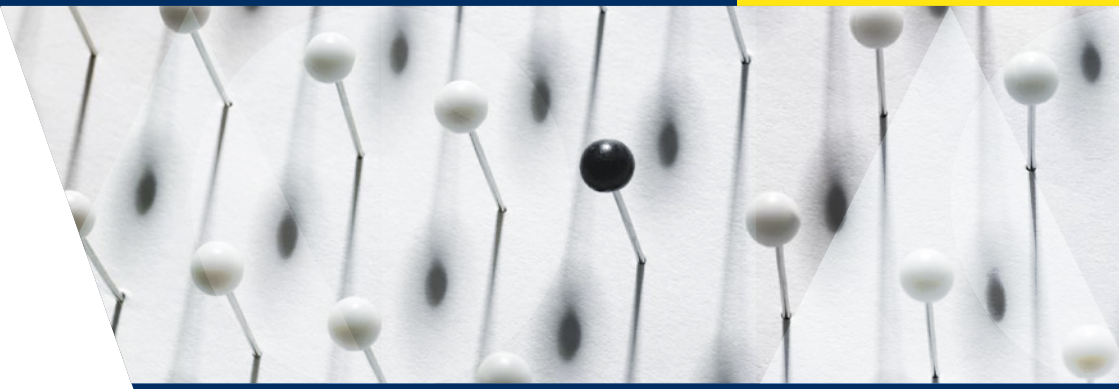
MANUEL



Manuel de droit européen en matière de protection des données

Édition 2018

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

EDPS

Le manuscrit de ce manuel a été achevé en avril 2018.

Des versions actualisées seront publiées sur le site web de la FRA à l'adresse : fra.europa.eu, sur le site web du Conseil de l'Europe à l'adresse : coe.int/dataprotection, sur le site web de la Cour européenne des droits de l'homme dans le menu « Jurisprudence » à l'adresse : echr.coe.int, et sur le site web du Contrôleur européen de la protection des données à l'adresse : edps.europa.eu.

Crédit photo (couverture & intérieur) : © iStockphoto

Luxembourg : Office des publications de l'Union européenne, 2019

CdE:	ISBN 978-92-871-9850-1		
FRA – print:	ISBN 978-92-9491-902-1	doi:10.2811/079264	TK-05-17-225-FR-C
FRA – web:	ISBN 978-92-9491-900-7	doi:10.2811/091298	TK-05-17-225-FR-N

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

EDPS

Manuel de droit européen en matière de protection des données

Édition 2018

Avant-propos

Nos sociétés sont de plus en plus numérisées. Compte tenu de ce nouvel état de fait, le rythme des évolutions technologiques et la façon dont sont traitées les données à caractère personnel nous affectent tous, au quotidien et à bien des égards. Les cadres juridiques de l'Union européenne (UE) et du Conseil de l'Europe, qui sont garants de la protection de la vie privée et des données à caractère personnel, ont récemment fait l'objet d'une révision.

L'Europe est à l'avant-garde de la protection des données au niveau mondial. Les normes de l'UE en matière de protection des données reposent sur la Convention 108 du Conseil de l'Europe, sur les instruments de l'UE – y compris le Règlement général sur la protection des données et la Directive relative à la protection des données destinées aux autorités policières et judiciaires pénales – ainsi que sur la jurisprudence de la Cour européenne des droits de l'homme et de la Cour de justice de l'Union européenne dans ce domaine.

Les réformes en matière de protection des données menées par l'UE et le Conseil de l'Europe sont vastes, et parfois complexes. Elles présentent de nombreux avantages et ont une incidence sur les particuliers et les entreprises. Ce manuel vise à sensibiliser le public et à améliorer les connaissances sur les règles en matière de protection des données, notamment celles des juristes non spécialisés qui sont confrontés aux questions de protection des données dans l'exercice de leurs fonctions.

Il a été élaboré par l'Agence des droits fondamentaux de l'Union européenne (FRA), avec le concours du Conseil de l'Europe (en association avec le greffe de la Cour européenne des droits de l'homme) et du Contrôleur européen de la protection des données. Version actualisée de l'édition 2014, ce manuel fait partie d'une série de manuels juridiques co-produits par la FRA et le Conseil de l'Europe.

Nous adressons nos remerciements aux autorités compétentes en matière de protection des données de Belgique, d'Estonie, de France, de Géorgie, de Hongrie, d'Irlande, d'Italie, de Monaco, de Suisse et du Royaume-Uni pour leurs précieux commentaires sur la version préliminaire du manuel. Par ailleurs, nous remercions l'unité « Protection des données » de la Commission européenne et son unité « Protection et flux de données internationaux ». Nous remercions également la Cour de justice de l'Union européenne pour son soutien documentaire durant les travaux préparatoires de ce manuel. Nous tenons enfin à remercier la Commission Nationale

de l'Informatique et des Libertés, en France, ainsi que la Commission de Contrôle des Informations Nominatives, de la Principauté de Monaco, pour leur soutien dans la révision de la version française du présent manuel.

Christos Giakoumopoulos	**Giovanni Buttarelli**	**Michael O'Flaherty**
Directeur général des Droits de l'Homme et État de droit du Conseil de l'Europe	Contrôleur européen de la protection des données	Directeur de l'Agence des droits fondamentaux de l'Union européenne

Table des matières

Abréviations et acronymes

ACC	Autorité de contrôle conjointe
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). Le Protocole d'amendement (STCE nº 223) à la Convention 108 (Convention 108 modernisée) a été adopté par le Comité des Ministres du Conseil de l'Europe à l'occasion de sa 128e session tenue à Elsinore, Danemark (les 17 et 18 mai 2018). L'usage dans le texte de « Convention 108 modernisée » fait référence à la Convention telle que modifiée par le Protocole STCE nº 223.
CouEDH	Cour européenne des droits de l'homme
C-SIS	Système central d'information Schengen
DPD	Délégué à la protection des données
DUDH	Déclaration universelle des droits de l'homme
EEE	Espace économique européen
EFSA	Autorité européenne de sécurité des aliments
ENISA	Agence européenne chargée de la sécurité des réseaux et de l'information
ENU	Unité nationale Europol
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
GCC	Groupe de coordination du contrôle
GPS	Système de positionnement mondial
GRC	Gestion de la relation client
ICCPR	Pacte international relatif aux droits civils et politiques
IP	Protocole internet
ISP	Fournisseur de services internet
JO	Journal officiel
MAE	Mandat d'arrêt européen
N-SIS	Système national d'information Schengen
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
RGPD	Règlement général sur la protection des données
SEPA	Espace unique de paiement en euros
SID	Système d'information des douanes
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
TIC	Technologies de l'information et de la communication
TUE	Traité sur l'Union européenne
UE	Union européenne
VIS	Système d'information sur les visas

Comment utiliser ce manuel ?

Le présent manuel détaille les normes légales relatives à la protection des données établies par l'Union européenne (UE) et le Conseil de l'Europe (CdE). Il a été conçu pour aider les praticiens du droit qui ne sont pas spécialisés dans le domaine de la protection des données et s'adresse ainsi tant aux avocats, aux juges et aux autres praticiens du droit qu'aux personnes travaillant pour d'autres organisations, telles que des organisations non gouvernementales (ONG), qui peuvent être confrontées à des problèmes juridiques en relation avec la protection des données.

Il s'agit d'un premier document de référence sur le droit de l'UE dans ce domaine, sur la Convention européenne des droits de l'homme (CEDH) ainsi que sur la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (la « Convention 108 ») et d'autres instruments du CdE.

Chaque chapitre commence par un tableau récapitulant les dispositions légales applicables aux thématiques abordées dans celui-ci. Les tableaux couvrent à la fois le droit de l'Union et celui du CdE et reprennent des extraits choisis de la jurisprudence de la Cour européenne des droits de l'homme (CouEDH) et de la Cour de justice de l'Union européenne (CJUE). Sont ensuite présentés par problématique les textes pertinents de ces deux juridictions européennes, dans la mesure où ils s'appliquent aux sujets spécifiques traités. Le lecteur peut ainsi se rendre compte des points de convergence et de divergence entre les deux systèmes juridiques. Cela devrait également aider le lecteur à trouver les informations essentielles concernant sa situation, en particulier s'il est soumis uniquement au droit du CdE. Dans certains chapitres, lorsque cela contribue à une présentation concise du contenu, l'ordre des sujets dans les tableaux peut légèrement s'écarter de celui suivi dans le chapitre proprement dit. Le manuel présente également un aperçu du cadre juridique des Nations Unies.

Les praticiens du droit des États qui ne sont pas membres de l'UE mais membres du Conseil de l'Europe, et donc parties à la CEDH et à la Convention 108, peuvent accéder aux informations pertinentes pour leur pays en consultant directement les sections se rapportant au Conseil de l'Europe. Les praticiens d'États non membres de l'UE doivent également garder à l'esprit que depuis l'adoption du Règlement général sur la protection des données de l'UE, les règles de l'UE en matière de protection des données s'appliquent aux organisations et autres entités qui ne sont pas établies

dans l'Union si elles traitent des données à caractère personnel et proposent des produits et des services à des personnes concernées dans l'Union ou surveillent le comportement de ces personnes.

Les praticiens du droit des États membres de l'UE devront consulter les deux sections, étant donné que ces États sont liés par les deux ordres juridiques. Il est à noter que la réforme et la modernisation des règles relatives à la protection des données en Europe, entreprises tant dans le cadre du Conseil de l'Europe (Convention 108 modernisée telle que modifiée par le Protocole STCE nº 223) que de l'UE (adoption du Règlement général sur la protection des données et de la Directive 2016/680/UE), ont été menées en parallèle. Les législateurs des deux systèmes juridiques ont veillé avec le plus grand soin à assurer la cohérence et la compatibilité entre les deux cadres juridiques. Les réformes ont donc conduit à une harmonisation plus poussée entre la législation du CdE et de l'UE en matière de protection des données. Pour les lecteurs qui souhaitent de plus amples informations sur une question particulière, une liste de références plus spécialisées se trouve dans la section « Lectures complémentaires » du manuel. Pour plus d'informations sur les dispositions de la Convention 108 et de son Protocole additionnel de 2001, qui reste en vigueur jusqu'à ce que le protocole d'amendement ne le soit, veuillez consulter l'édition 2014 de ce manuel.

Le droit du CdE est présenté sous la forme de brèves références à des affaires de la CouEDH. Celles-ci ont été sélectionnées parmi la multitude d'arrêts et de décisions de la CouEDH concernant des aspects de la protection des données.

Le droit pertinent de l'Union est constitué de mesures législatives qui ont été adoptées, des dispositions pertinentes des traités et de la Charte des droits fondamentaux de l'Union européenne, telles qu'elles ont été interprétées par la CJUE dans sa jurisprudence. De plus, le manuel contient des avis et lignes directrices adoptés par le Groupe de travail « Article 29 », l'organe consultatif chargé au titre de la Directive sur la protection des données de fournir un avis d'expert aux États membres de l'UE et qui sera remplacé par le Comité européen de la protection des données à partir du 25 mai 2018. Les avis du Contrôleur européen de la protection des données apportent également des informations importantes sur l'interprétation du droit de l'Union et sont donc repris dans ce manuel.

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

en ligne. La jurisprudence de la CJUE concerne l'ancienne Directive sur la protection des données. Cependant, les interprétations de la CJUE restent applicables aux droits et obligations correspondants prévus par le Règlement général sur la protection des données.

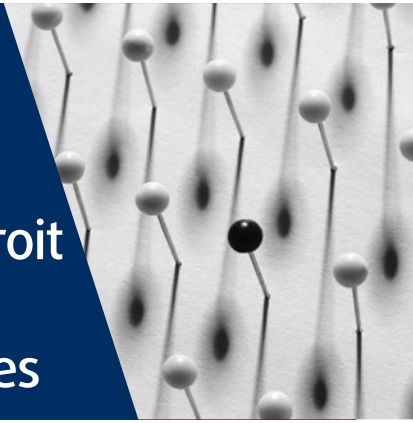
En outre, des exemples concrets et des scénarios construits sur des hypothèses sont présentés dans les encadrés sur fond bleu. Ces exemples illustrent l'application pratique des règles européennes en matière de protection des données, en particulier lorsqu'il n'existe pas de jurisprudence spécifique de la CouEDH ou de la CJUE. D'autres encadrés, sur fond gris, présentent des exemples extraits de sources autres que la jurisprudence de la CouEDH et de la CJUE, comme la législation et les avis publiés par le Groupe de travail « Article 29 ».

Le manuel commence par une brève description du rôle des deux systèmes juridiques tels qu'établis par la CEDH et le droit de l'UE (chapitre 1). Les chapitres 2 à 10 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 ;
- contrôle indépendant ;
- droits des personnes concernées et contrôle de leur application ;
- transferts et flux transfrontières de données à caractère personnel ;
- protection des données dans le contexte de la police et de la justice pénale ;
- autres règles européennes en matière de protection des données dans des domaines spécifiques ;
- défis modernes pour la protection des données à caractère personnel.

1

Contexte et genèse du droit européen en matière de protection des données



UE	Questions traitées	CdE
Droit à la protection des données		
Traité sur le fonctionnement de l'Union européenne, art. 16 Charte des droits fondamentaux de l'Union européenne, art. 8 (droit à la protection des données à caractère personnel) 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 (en vigueur jusqu'en mai 2018) Décision-cadre 2000/977/JAI relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, JO 2008 L 350 (en vigueur jusqu'en mai 2018) Règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données), JO 2016 L 119		CEDH, art. 8 (droit au respect de la vie privée et familiale, du domicile et de la correspondance) Convention modernisée pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108 modernisée)

UE	Questions traitées	CdE
Directive (UE) 2016/680 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, JO 2016 L 119 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 »), JO 2002 L 201 Règlement (CE) nº 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 sur la protection des données par les institutions de l'UE), JO 2001 L 8		
Limitations du droit à la protection des données à caractère personnel		
Charte des droits fondamentaux, art. 52, para. 1 Règlement général sur la protection des données (RGPD), art. 23 CJUE, affaires jointes C-92/09 et C-93/09, *Volker und Markus Schecke GbR et Hartmut Eifert c. Land Hessen* [GC], 2010		CEDH, art. 8, para. 2 Convention 108 modernisée, art. 11 CouEDH, *S. et Marper c. Royaume-Uni* [GC], nº 30562/04 et 30566/04, 2008
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* [GC], 2010	En général	
CJUE, C-73/07, *Tietosuojavaltuutettu c. Satakunnan Markkinapörssi Oy et Satamedia Oy* [GC], 2008 CJUE, C-131/12, *Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 2014	Liberté d'expression	CouEDH, *Axel Springer AG c. Allemagne* [GC], nº 39954/08, 2012 CouEDH, *Mosley c. Royaume-Uni*, nº 48009/08, 2011 CouEDH, *Bohlen c. Allemagne*, nº 53495/09, 2015

UE	Questions traitées	CdE
CJUE, C-28/08 P, *Commission européenne c. The Bavarian Lager Co. Ltd* [GC], 2010 CJUE, C-615/13 P, *ClientEarth, PAN Europe c. EFSA*, 2015	Accès aux documents	CouEDH, *Magyar Helsinki Bizottság c. Hongrie* [GC], nº 18030/11, 2016
RGPD, art. 90	Secret professionnel	CouEDH, *Pruteanu c. Roumanie*, nº 30181/05, 2015
RGPD, art. 91	Liberté de religion ou de conviction	
	Liberté des arts et des sciences	CouEDH, *Vereinigung bildender Künstler c. Autriche*, nº 68345/01, 2007
CJUE, C-275/06, *Productores de Música de España (Promusicae) c. Telefónica de España SAU* [GC], 2008	Protection de la propriété	
CJUE, C-131/12, *Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 2014 CJUE, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce c. Salvatore Manni*, 2017	Droits économiques	

1.1. Le droit à la protection des données à caractère personnel

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 et, à ce jour, le seul acte juridiquement contraignant au niveau international qui traite de la protection des données. La modernisation de la Convention a été menée à bien et s'est achevée avec l'adoption du Protocole d'amendement STCE nº 223.

- Dans le droit de l'UE, la protection des données à caractère personnel est reconnue comme un droit fondamental à part entière. Ce droit est consacré dans l'article 16 du Traité sur le fonctionnement de l'Union européenne (TFUE) et l'article 8 de la Charte des droits fondamentaux de l'UE.
- Dans le droit de l'UE, la protection des données a été réglementée pour la première fois par la Directive sur la protection des données en 1995.
- Compte tenu de la rapidité des développements technologiques, l'UE a adopté une nouvelle législation en 2016 afin d'adapter les règles relatives à la protection des données à l'ère du numérique. Le Règlement général sur la protection des données est entré en vigueur en mai 2018 et abroge la Directive sur la protection des données.
- Parallèlement au Règlement général sur la protection des données, l'UE a adopté une législation sur le traitement de données à caractère personnel par les autorités nationales à des fins répressives. La Directive (UE) 2016/680 établit les règles et principes de la protection des données qui régissent le traitement de données à caractère personnel 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.

1.1.1. Le droit au respect de la vie privée et le droit à la protection des données à caractère personnel : une brève introduction

Le droit au respect de la vie privée et le droit à la protection des données à caractère personnel, bien qu'étroitement liés, sont des droits distincts. Le droit à la protection de la sphère privée – appelé droit au respect de la vie privée dans le droit européen – est apparu pour la première fois comme un des droits fondamentaux protégés de la personne dans le droit international des droits de l'homme par le biais de la Déclaration universelle des droits de l'homme (DUDH) de 1948. Peu après l'adoption de la DUDH, l'Europe a également affirmé ce droit dans la Convention européenne des droits de l'homme (CEDH), un traité établi en 1950 et juridiquement contraignant pour ses Parties contractantes. La CEDH dispose que toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. Toute ingérence d'une autorité publique dans l'exercice de ce droit est prohibée à moins que cette ingérence ne soit prévue par la loi, poursuive des intérêts publics importants et légitimes et soit nécessaire dans une société démocratique.

La DUDH et la CEDH ont été adoptées bien avant le développement des ordinateurs et d'internet et l'émergence de la société de l'information. Ces développements ont apporté des avantages considérables aux individus et à la société en améliorant la

qualité de vie, le rendement et la productivité. En même temps, ils présentent de nouveaux risques pour le droit au respect de la vie privée. Pour répondre à la nécessité de disposer de règles spécifiques pour la collecte et l'utilisation de données personnelles, un nouveau concept de vie privée est apparu, connu dans certaines juridictions sous l'appellation « protection des renseignements personnels » et dans d'autres sous le nom de « droit à l'autodétermination informationnelle »[1]. Ce concept a conduit à l'élaboration de réglementations spécifiques qui prévoient la protection des données à caractère personnel.

En Europe, la protection des données est apparue dans les années 1970 avec l'adoption d'une législation – par certains États – visant à contrôler le traitement d'informations personnelles par les autorités publiques et les grandes entreprises[2]. Des instruments destinés à la protection des données ont ensuite été élaborés au niveau européen[3] et, au fil des années, la protection des données est devenue un concept à part entière qui n'est plus englobé dans le droit au respect de la vie privée. Dans l'ordre juridique de l'UE, la protection des données est reconnue comme un droit fondamental, distinct du droit fondamental au respect de la vie privée. Cette séparation pose la question de la relation et des différences entre ces deux droits.

Le droit au respect de la vie privée et le droit à la protection des données à caractère personnel sont étroitement liés. Tous deux tendent à protéger des valeurs similaires, à savoir l'autonomie et la dignité humaine des individus, en leur accordant une sphère privée dans laquelle ils peuvent librement développer leur personnalité, penser et se forger des opinions. Ils constituent donc une condition préalable essentielle à l'exercice d'autres libertés fondamentales, telles que la liberté d'expression, la liberté de réunion et d'association pacifiques et la liberté de religion.

---

1 La Cour constitutionnelle fédérale allemande a affirmé un droit à l'autodétermination informationnelle dans un arrêt de 1983 rendu dans l'affaire *Volkszählungsurteil*, BVerfGE Bd. 65, S. 1ff. La Cour a considéré que l'autodétermination informationnelle découle du droit fondamental au respect de la personnalité, protégé par la Constitution allemande. Dans un arrêt de 2017, la CouEDH a reconnu que l'article 8 de la CEDH « consacre donc le droit à une forme d'auto-détermination informationnelle ». Voir CouEDH, *Satakunnan Markkinapörssi Oy et Satamedia Oy c. Finlande* [GC], nº 931/13, 27 juin 2017, para. 137.

2 Le Land allemand de Hesse a adopté le premier texte légal sur la protection des données en 1970, lequel n'était applicable que dans ce territoire. En 1973, la Suède a adopté la première loi nationale au monde sur la protection des données. À la fin des années 1980, plusieurs États européens (France, Allemagne, Pays-Bas et Royaume-Uni) avaient eux aussi adopté une législation en la matière.

3 La Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108) a été adoptée en 1981. Quant à l'UE, elle a adopté son premier instrument complet de protection des données en 1995 : la Directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Ces deux droits diffèrent par leur formulation et leur portée. Le droit au respect de la vie privée consiste en une interdiction générale de toute ingérence, sous réserve de certaines conditions d'intérêt public de nature à justifier une ingérence dans certains cas. La protection des données à caractère personnel est considérée comme un droit moderne et actif[4], qui met en place un système de contrôles et de mises en balance afin de protéger les individus chaque fois que leurs données à caractère personnel sont traitées. Le traitement doit être conforme aux critères essentiels de la protection des données à caractère personnel, à savoir un contrôle indépendant et le respect des droits de la personne concernée[5].

Non seulement l'article 8 de la Charte des droits fondamentaux de l'Union européenne (« la Charte ») consacre le droit à la protection des données à caractère personnel, mais il énonce également les valeurs fondamentales qui y sont associées. Il dispose que les données à caractère personnel doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne doit avoir le droit d'accéder aux données la concernant et d'en obtenir la rectification et le respect de ce droit doit être soumis au contrôle d'une autorité indépendante.

Le droit à la protection des données à caractère personnel entre en jeu chaque fois que des données à caractère personnel sont traitées ; il est donc plus large que le droit au respect de la vie privée. Tout traitement de données à caractère personnel fait l'objet d'une protection adéquate. La protection des données concerne tout type de données à caractère personnel et de traitement, indépendamment de leur rapport avec la vie privée et de leur incidence sur celle-ci. Le traitement de données à caractère personnel peut également enfreindre le droit au respect de la vie privée, comme le montrent les exemples ci-dessous. Il n'est néanmoins pas nécessaire de démontrer une violation de la vie privée pour que les règles relatives à la protection des données s'appliquent.

Le droit au respect de la vie privée concerne les cas où un intérêt privé, ou la « vie privée » d'une personne, a été compromis. Ainsi qu'on le verra tout au long de ce manuel, le concept de « vie privée » a été interprété au sens large dans la

4 L'avocat général Sharpston a décrit l'affaire comme impliquant deux droits distincts : le droit « classique » à la protection de la vie privée et un droit plus « moderne », le droit à la protection des données. Voir CJUE, affaires jointes C-92/09 et C-93/02, *Volker und Markus Schecke GbR c. Land Hessen, Conclusions de l'avocat général Sharpston*, 17 juin 2010, point 71.

5 Hustinx, P., Discours et articles du CEPD, *Le droit de l'Union européenne sur la protection des données : la révision de la directive 95/46/CE et la proposition de règlement général sur la protection des données*, juillet 2013.

jurisprudence comme couvrant des situations intimes, des informations sensibles ou confidentielles, des informations susceptibles de porter préjudice à la perception qu'a le public d'une personne, et même des aspects de la vie professionnelle et du comportement public d'une personne. Toutefois, l'appréciation de la question de savoir s'il y a ou s'il y a eu ingérence dans la « vie privée » dépend du contexte et des circonstances factuelles de chaque cas.

En revanche, toute opération supposant le traitement de données à caractère personnel pourrait tomber sous le coup des règles relatives à la protection des données et ouvrir le droit à la protection des données à caractère personnel. Ainsi, lorsqu'un employeur enregistre des informations sur les noms et les rémunérations versées à des salariés, le simple fait d'enregistrer ces informations ne peut être considéré comme une ingérence dans la vie privée. On pourrait toutefois invoquer une telle ingérence si, par exemple, l'employeur transférait les données personnelles des salariés à des tiers. Les employeurs doivent, en tout état de cause, respecter les règles relatives à la protection des données, étant donné que l'enregistrement des données des salariés constitue un traitement des données.

Exemple : dans l'affaire *Digital Rights Ireland*[6], la CJUE a été appelée à se prononcer sur la validité de la Directive 2006/24/CE à la lumière des droits fondamentaux à la protection des données à caractère personnel et au respect de la vie privée consacrés par la Charte des droits fondamentaux de l'UE. La directive imposait aux fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communication de conserver les données de télécommunications des citoyens pendant un maximum de deux ans afin de garantir que ces données restaient disponibles à des fins de prévention, d'enquêtes et de poursuites d'infractions pénales graves. La mesure concernait uniquement les données relatives au trafic, les données de localisation et les données nécessaires à l'identification de l'abonné ou de l'utilisateur. Elle ne s'appliquait pas au contenu des communications électroniques.

La CJUE a considéré que la directive était constitutive d'une ingérence dans le droit fondamental à la protection des données à caractère personnel « puisqu'elle prévoit un traitement des données à caractère

6 CJUE, affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources et autres* et *Kärntner Landesregierung et autres* [GC], 8 avril 2014.

personnel »[7]. Elle a en outre considéré que la directive interférait avec le droit au respect de la vie privée[8]. Prises dans leur ensemble, ces données à caractère personnel conservées en application de la directive, auxquelles les autorités compétentes pouvaient avoir accès, étaient susceptibles de permettre de tirer « des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci »[9]. L'ingérence dans ces deux droits était large et particulièrement grave.

La CJUE a déclaré la Directive 2006/24/CE invalide, en concluant que même si elle poursuivait un but légitime, l'ingérence dans les droits à la protection des données à caractère personnel et au respect de la vie privée était grave et ne se limitait pas à ce qui était strictement nécessaire.

1.1.2. Cadre juridique international : Nations Unies

Le cadre des Nations Unies ne reconnaît pas la protection des données à caractère personnel comme un droit fondamental, bien que le droit à la vie privée soit un droit fondamental inscrit de longue date dans l'ordre juridique international. Le droit à la protection de la sphère privée d'une personne contre une immixtion de tiers, en particulier de l'État, a été introduit pour la première fois dans un instrument international à l'article 12 de la DUDH sur le respect de la vie privée et familiale[10]. Bien qu'il s'agisse d'une déclaration non contraignante, la DUDH occupe une place de choix en tant qu'acte fondateur du droit international des droits de l'homme et a influencé l'élaboration d'autres instruments des droits de l'homme en Europe. Le Pacte international relatif aux droits civils et politiques (ICCPR), est entré en vigueur en 1976. Il proclame que nul ne peut faire l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation. L'ICCPR est un traité international par lequel ses 169 Parties contractantes s'engagent à respecter et à garantir l'exercice des droits civils de la personne, notamment le respect de la vie privée.

7 *Ibid.*, point 36.

8 *Ibid.*, points 32 à 35.

9 *Ibid.*, point 27.

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

Depuis 2013, les Nations Unies ont adopté deux résolutions concernant des questions liées à la vie privée, intitulées « Le droit à la vie privée à l'ère numérique »[11] en réponse à l'essor des nouvelles technologies et aux révélations sur la surveillance de masse mise en place dans certains États (« les révélations Snowden »). Elles condamnent fermement la surveillance de masse et mettent en évidence l'effet qu'une telle surveillance peut avoir sur les droits fondamentaux au respect de la vie privée et à la liberté d'expression ainsi que sur le fonctionnement d'une société démocratique et dynamique. En dépit de leur caractère non contraignant, ces résolutions ont déclenché un important débat politique à haut niveau à l'échelle internationale sur la vie privée, les nouvelles technologies et la surveillance. Elles ont également mené à la création d'un poste de Rapporteur spécial sur le droit à la vie privée, chargé de promouvoir et de protéger ce droit. Il a pour tâches spécifiques de collecter des informations sur les pratiques et les expériences nationales en matière de respect de la vie privée et sur les défis créés par les nouvelles technologies, d'échanger et de promouvoir les meilleures pratiques et de recenser les obstacles potentiels.

Alors que des résolutions antérieures insistaient sur les effets négatifs de la surveillance de masse et sur la responsabilité des États en matière de limitation des pouvoirs des services de renseignement, les résolutions plus récentes traduisent un progrès majeur dans le débat sur la vie privée aux Nations Unies[12]. Les résolutions adoptées en 2016 et 2017 réaffirment la nécessité de limiter les pouvoirs des services de renseignement et de condamner la surveillance de masse. Il y est toutefois affirmé expressément que « le renforcement de la capacité des entreprises de collecter, de traiter et d'utiliser les données personnelles représente un risque pour l'exercice du droit à la vie privée à l'ère du numérique ». Dès lors, outre la responsabilité des pouvoirs publics, les résolutions pointent également du doigt la responsabilité du secteur privé en matière de respect des droits de l'homme et appellent les entreprises à informer les utilisateurs de la collecte, de l'utilisation, du partage et de la conservation de données personnelles et à mettre en place des politiques de traitement transparentes.

11 Voir ONU, Assemblée générale, Résolution sur le droit à la vie privée à l'ère numérique, A/RES/68/167, New York, 18 décembre 2013 ; et ONU, Assemblée générale, Projet révisé de résolution sur le droit à la vie privée à l'ère numérique, A/C.3/69/L.26/Rev.1, New York, 19 novembre 2014.

12 ONU, Assemblée générale, Projet révisé de résolution sur le droit à la vie privée à l'ère numérique, A/C.3/71/L.39/Rev.1, New York, 16 novembre 2016 ; ONU, Conseil des droits de l'homme, Le droit à la vie privée à l'ère numérique, A/HRC/34/L.7/Rev.1, 22 mars 2017.

1.1.3. 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 CEDH en 1950, laquelle est entrée en vigueur en 1953.

Les Parties contractantes ont l'obligation internationale de respecter la CEDH. Tous les États membres du CdE ont désormais transposé ou donné effet à la CEDH dans leur droit national, de sorte qu'ils sont tenus d'agir conformément aux dispositions de la Convention. Les Parties contractantes doivent respecter les droits garantis dans la Convention dans le cadre de l'exercice de toute activité ou pouvoir. Cela inclut les activités menées pour assurer la sécurité nationale. Des arrêts marquants de la Cour européenne des droits de l'homme (CouEDH) ont porté sur des activités des États dans les domaines sensibles du droit et de la pratique en matière de sécurité nationale[13]. La Cour n'a pas hésité à affirmer que les activités de surveillance sont constitutives d'une ingérence dans le respect de la vie privée[14].

La CouEDH a été créée à Strasbourg (France) en 1959 pour garantir que les Parties contractantes respectent leurs obligations au titre de la CEDH. La CouEDH veille à ce que les États respectent leurs obligations au titre de la Convention en examinant les plaintes de particuliers, de groupes de particuliers, d'ONG ou de personnes morales invoquant des violations à la Convention. La CouEDH peut aussi examiner des affaires inter-États soumises par un ou plusieurs États membres du CdE contre un autre État membre.

Depuis 2018, le Conseil de l'Europe compte 47 États membres, dont 28 sont également des États membres de l'UE. Un requérant devant la CouEDH ne doit pas être ressortissant d'une des Parties contractantes, mais les violations invoquées doivent s'être produites dans le territoire relevant de la compétence de l'une des Parties contractantes.

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

13 Voir par exemple : CouEDH, *Klass et autres c. Allemagne*, nº 5029/71, 6 septembre 1978 ; CouEDH, *Rotaru c. Roumanie* [GC], nº 28341/95, 4 mai 2000 ; et CouEDH, *Szabó et Vissy c. Hongrie*, nº 37138/14, 12 janvier 2016.

14 *Ibid.*

familiale, du domicile et de la correspondance, et énonce les conditions dans lesquelles des restrictions à ce droit sont admises[15].

La CouEDH a examiné de nombreuses situations soulevant la question de la protection des données, notamment l'interception de communications[16], diverses formes de surveillance à la fois par le secteur privé et public[17] et la protection contre la conservation de données à caractère personnel par des autorités publiques[18]. Le respect de la vie privée n'est pas un droit absolu, car l'exercice de ce droit pourrait compromettre d'autres droits, comme la liberté d'expression et l'accès à l'information et inversement. C'est pourquoi la Cour s'efforce de trouver un équilibre entre les différents droits concernés. Non seulement elle a précisé que l'article 8 de la CEDH impose aux États de s'abstenir de toute action susceptible de violer ce droit de la Convention, mais elle 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[19]. Les chapitres correspondants détaillent un grand nombre de ces affaires.

1.1.4. 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 pour 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, lesquelles font référence à l'article 8 de la CEDH[20]. En 1981, une Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

15 Conseil de l'Europe, Convention européenne des droits de l'homme, STCE nº 005, 1950.

16 Voir par exemple : CouEDH, *Malone c. Royaume-Uni*, nº 8691/79, 2 août 1984 ; CouEDH, *Copland c. Royaume-Uni*, nº 62617/00, 3 avril 2007 ; ou CouEDH, *Mustafa Sezgin Tanrıkulu c. Turquie*, nº 27473/06, 18 juillet 2017.

17 Voir par exemple : CouEDH, *Klass et autres c. Allemagne*, nº 5029/71, 6 septembre 1978 ; CouEDH, *Uzun c. Allemagne*, nº 35623/05, 2 septembre 2010.

18 Voir par exemple : CouEDH, *Roman Zakharov c. Russie* [GC], nº 47143/06, 4 décembre 2015 ; CouEDH, *Szabó et Vissy c. Hongrie*, nº 37138/14, 12 janvier 2016.

19 Voir par exemple : CouEDH, *I c. Finlande*, nº 20511/03, 17 juillet 2008 ; CouEDH, *K.U. c. Finlande*, nº 2872/02, 2 décembre 2008.

20 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.

(Convention 108)[21], a été ouverte à la signature. La Convention 108 était, et reste aujourd'hui, le seul instrument international juridiquement contraignant 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, y compris 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 le traitement de données à caractère personnel, et vise en même temps à réguler les flux transfrontières de données à caractère personnel. S'agissant 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. Cela signifie que les données ne devraient pas être utilisées 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 sur le traitement de données à caractère personnel et les obligations en matière de sécurité des données, 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.

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 énoncés dans la Convention ne sont possibles que si des intérêts supérieurs, tels que la sécurité de l'État ou la sûreté publique, entrent en jeu. De plus, la Convention prévoit une libre circulation des données à caractère personnel entre les Parties contractantes et impose certaines restrictions à cette circulation vers des États dont la réglementation ne prévoit pas une protection équivalente.

Il est à noter que la Convention 108 est contraignante pour les États qui l'ont ratifiée. Elle n'est pas soumise au contrôle juridictionnel de la CouEDH, mais elle a été prise en compte dans la jurisprudence de cette dernière dans le contexte de l'article 8 de la CEDH. Au fil du temps, la Cour a déclaré que la protection des données à caractère personnel constitue un élément important du droit au respect de la vie privée

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

(article 8) et les principes de la Convention 108 l'ont guidée dans la détermination de l'existence ou de l'absence d'une ingérence dans ce droit fondamental[22].

Afin de développer plus avant les principes généraux et les règles énoncés dans la Convention 108, le Comité des Ministres du CdE a adopté plusieurs recommandations, qui ne sont pas juridiquement contraignantes. Celles-ci ont influencé l'évolution du droit de la protection des données en Europe. Ainsi, pendant des années, le seul instrument fournissant des orientations sur l'utilisation des données à caractère personnel dans le secteur de la police en Europe a été la Recommandation relative à la police[23]. Les principes contenus dans cette recommandation, tels que les moyens de conserver les fichiers de données et la nécessité d'appliquer des règles claires concernant les personnes autorisées à accéder à ces fichiers, ont été développés et se reflètent dans la législation ultérieure de l'UE[24]. Des recommandations plus récentes visent à relever les défis de l'ère du numérique, par exemple en ce qui concerne le traitement de données dans le cadre de l'emploi (voir chapitre 9).

Tous les États membres de l'UE ont ratifié la Convention 108. En 1999, des amendements de la Convention 108 ont été proposés pour permettre à l'UE d'y adhérer[25]. En 2001, un Protocole additionnel à la Convention 108 a été adopté. Il a introduit des dispositions sur les flux transfrontières de données vers des pays qui ne sont pas Parties à la Convention, appelés « pays tiers », et sur la création obligatoire d'autorités nationales de contrôle de la protection des données[26].

La Convention 108 est ouverte à l'adhésion d'États non membres du CdE. La capacité de la Convention à constituer une norme universelle et son ouverture servent de base à la promotion de la protection des données au niveau mondial. À ce jour, 51 pays sont Parties à la Convention 108. Ils incluent tous les États membres du

22 Voir par exemple : CouEDH, *Z c. Finlande*, nº 22009/93, 25 février 1997.

23 CdE, Comité des Ministres (1987), Recommandation Rec(87)15 aux États membres visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, 17 septembre 1987.

24 Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JO L 281, 23 novembre 1995.

25 CdE, Amendements à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STCE nº 108), adoptés par le Comité des Ministres, à Strasbourg, le 15 juin 1999.

26 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 nº 181, 2001. Avec la modernisation de la Convention 108, ce protocole n'est plus appliqué car ses dispositions ont été mises à jour et intégrées dans la Convention 108 modernisée.

CdE (47 pays). L'Uruguay est le premier pays non européen à y avoir adhéré en août 2013, suivi par Maurice, le Sénégal et la Tunisie, en 2016 et 2017.

La Convention a récemment fait l'objet d'une modernisation. Une consultation publique a eu lieu en 2011 et a confirmé les deux principaux objectifs de ce travail : renforcer la protection de la vie privée dans le domaine numérique et consolider le mécanisme de suivi de la Convention. Le processus de modernisation a été axé sur ces objectifs et s'est achevé avec l'adoption d'un Protocole d'amendement de la Convention 108 (Protocole STCE nº 223). Le travail a été mené parallèlement à d'autres réformes des instruments internationaux de protection des données et en même temps que la réforme des règles de l'UE en la matière, lancée en 2012. Les législateurs du Conseil de l'Europe et de l'UE ont veillé avec le plus grand soin à assurer la cohérence et la compatibilité entre les deux cadres juridiques. La modernisation préserve le caractère général et flexible de la Convention et renforce son potentiel d'instrument universel pour le droit de la protection des données. Des principes importants y sont réaffirmés et consolidés et elle offre de nouveaux droits aux individus tout en accroissant simultanément les responsabilités des entités qui traitent les données à caractère personnel et en renforçant la responsabilité. Par exemple, les individus dont les données personnelles sont traitées ont le droit de connaître la logique de ce traitement et de s'y opposer. Pour lutter contre le recours accru au profilage en ligne, la Convention instaure également le droit de l'individu à ne pas se soumettre à des décisions reposant uniquement sur un traitement automatisé sans que son avis soit pris en compte. L'application effective des règles de la protection des données par des autorités de contrôle indépendantes dans les Parties contractantes est considérée comme essentielle à la mise en œuvre pratique de la Convention. À cet effet, la Convention modernisée insiste sur le fait que les autorités de contrôle doivent être investies de pouvoirs et de fonctions réels et jouir d'une véritable indépendance dans l'exercice de leur mission.

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

Le droit de l'UE se compose du droit primaire 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 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 le « droit dérivé de l'UE ».

Protection des données dans le droit primaire de l'UE

Les traités originaux des Communautés européennes ne contenaient pas de référence aux droits de l'homme ou à leur protection, étant donné qu'au départ, la Communauté économique européenne était envisagée comme une organisation régionale axée sur l'intégration économique et la création d'un marché commun. Le principe d'attribution est un principe fondamental sous-tendant la création et le développement des Communautés européennes, qui est toujours d'application aujourd'hui. Selon ce principe, l'UE n'agit que dans les limites des compétences qui lui ont été conférées par les États membres, telles qu'elles sont définies dans les traités de l'UE. À la différence du Conseil de l'Europe, les traités de l'UE ne prévoient aucune compétence explicite en matière de droits fondamentaux.

À mesure qu'elle était saisie d'affaires invoquant des violations des droits de l'homme dans des domaines relevant de la compétence du droit de l'UE, la CJUE a développé une importante interprétation des traités. Afin de protéger les 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, la CEDH en particulier. La CJUE a déclaré qu'elle garantirait la conformité du droit de l'UE à ces principes.

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, l'Union a adopté en 2000 la Charte des droits fondamentaux de l'Union européenne. Celle-ci 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 n'étant au départ qu'un document politique, la Charte est depuis devenue un instrument juridiquement contraignant[27] du droit primaire de l'UE (voir l'article 6, paragraphe 1, du TUE) lors de l'entrée en vigueur du Traité de Lisbonne le 1er décembre 2009[28]. Les dispositions de la Charte s'adressent aux institutions et

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

28 Voir versions consolidées des Communautés européennes (2012), Traité sur l'Union européenne, JO 2012 C 326, et Traité sur le fonctionnement de l'Union européenne (2012), TFUE, JO 2012 C 326.

organes de l'UE et leur imposent de respecter les droits qui y sont énumérés dans l'exercice de leurs fonctions. Les dispositions de la Charte lient également les États membres dans la mise en œuvre du droit de l'UE.

Non seulement la Charte garantit le droit au respect de la vie privée et familiale (article 7), mais elle établit également le droit à la protection des données (article 8). Elle élève explicitement cette protection au niveau d'un droit fondamental dans le droit de l'UE. Les institutions et organes de l'UE doivent garantir ce droit, comme les États membres lorsqu'ils transposent le droit de l'Union (article 51 de la Charte). Formulé plusieurs années 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, non seulement la Charte mentionne explicitement un droit à la protection des données à l'article 8, paragraphe 1, mais elle 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, requiert que le contrôle de la mise en œuvre de ces principes soit exercé par une autorité indépendante.

L'adoption du Traité de Lisbonne est un jalon dans le développement du droit de la protection des données, non seulement parce qu'il a élevé la Charte au rang d'instrument juridique contraignant du droit primaire, mais également parce qu'il établit le droit à la protection des données à caractère personnel. Ce droit est spécifiquement prévu à l'article 16 du TFUE, dans la section du traité consacrée aux principes généraux de l'UE. L'article 16 crée également une nouvelle base juridique, en rendant l'UE compétente pour légiférer sur les questions relatives à la protection des données. Il s'agit là d'un développement important car les règles de l'UE en matière de protection des données – en particulier la Directive relative à la protection des données – reposaient à l'origine sur la base juridique du marché intérieur et sur la nécessité de rapprocher les législations nationales afin de ne pas entraver la libre circulation des données au sein de l'UE. L'article 16 du TFUE offre désormais une base juridique autonome à une approche moderne et exhaustive de la protection des données, couvrant tous les domaines de compétence de l'UE, y compris la coopération policière et judiciaire en matière pénale. L'article 16 du TFUE affirme également que le respect des règles relatives à la protection des données adoptées conformément à son contenu est soumis au contrôle d'autorités indépendantes. Il a servi de base juridique pour l'adoption d'une réforme complète des règles relatives à la protection des données en 2016, composée du Règlement général sur la protection des données et de la Directive relative à la protection des données pour les autorités policières et judiciaires en matière pénale (voir ci-dessous).

Le Règlement général sur la protection des données

De 1995 à mai 2018, le principal instrument juridique de l'UE en matière de protection des données était 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 caractères personnel et à la libre circulation de ces données (Directive relative à la protection des données)[29]. Elle a été adoptée en 1995, à un moment où plusieurs États membres avaient déjà adopté des législations nationales de protection des données[30] et répondait à la nécessité d'harmoniser ces législations afin d'assurer un niveau élevé de protection et la libre circulation des données à caractère personnel entre les États membres. La libre circulation des marchandises, des capitaux et des personnes au sein du marché interne requérait la libre circulation des données, celle-ci ne pouvait être réalisée qu'à condition que les États membres puissent s'appuyer sur un niveau uniforme élevé de protection des données.

La Directive relative à la protection des données reflétait les principes de protection déjà contenus dans les législations nationales et dans la Convention 108, tout en les étoffant souvent. Elle s'appuie sur la possibilité, prévue à l'article 11 de la Convention 108, d'ajouter des instruments de protection. En particulier, l'introduction dans la directive d'un contrôle indépendant servant d'instrument pour améliorer le respect des règles de protection des données s'est révélée être une contribution majeure au bon fonctionnement du droit européen de la protection des données. Cet élément a donc été intégré au droit du CdE en 2001 au moyen du Protocole additionnel à la Convention 108. Ceci illustre l'interaction étroite et l'influence positive que ces deux instruments exercent l'un sur l'autre au fil des ans.

La Directive relative à la protection des données a établi un système détaillé et exhaustif de protection des données dans l'UE. Toutefois, conformément au système juridique de l'UE, les directives ne sont pas directement applicables et doivent être transposées dans le droit national des États membres. Inévitablement, les États membres disposent d'une marge de pouvoir discrétionnaire dans la transposition des dispositions de la directive. Bien que l'objectif de la directive ait été de parvenir

29 Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JO 1995 L 281.

30 Le Land allemand de Hesse a adopté le premier texte légal au monde sur la protection des données en 1970, laquelle n'était applicable que sur son territoire. La Suède a adopté la *Datalagen* en 1973 ; l'Allemagne a adopté la *Bundesdatenschutzgesetz* en 1976 et la France a adopté la loi relative à l'informatique, aux fichiers et aux libertés en 1977. Au Royaume-Uni, le *Data Protection Act* a été adopté en 1984. Enfin, les Pays-Bas ont adopté la *Wet Persoonregistraties* en 1989.

à une harmonisation complète[31] (et à une protection complète), dans la pratique, elle a été transposée différemment selon les États membres. Il en a résulté la mise en place de règles différentes de protection des données dans l'UE, avec des définitions et des règles interprétées différemment en droit national selon les pays. Les niveaux d'application et la sévérité des sanctions différaient également d'un État membre à l'autre. Enfin, des changements importants sont intervenus dans les technologies de l'information depuis la rédaction de la directive au milieu des années 1990. Tous ces éléments mis en ensemble ont abouti à la réforme du droit européen de la protection des données.

Après des années d'intenses discussions, la réforme a conduit à l'adoption du Règlement général sur la protection des données (RGPD) en avril 2016. Les débats concernant la nécessité de moderniser les règles de l'UE sur la protection des données ont débuté en 2009, avec le lancement par la Commission d'une consultation publique sur le futur cadre juridique du droit fondamental à la protection des données à caractère personnel. La proposition de règlement a été publiée par la Commission en janvier 2012, marquant le point de départ d'un long processus législatif de négociations entre le Parlement européen et le Conseil de l'UE. Après son adoption, le Règlement général sur la protection des données prévoyait une période de transition de deux ans. Il est devenu pleinement applicable le 25 mai 2018, date à laquelle la Directive relative à la protection des données a été abrogée.

L'adoption du RGPD en 2016 a modernisé la législation de l'UE en matière de protection des données, en la rendant apte à protéger les droits fondamentaux dans le cadre des défis économiques et sociaux de l'ère du numérique. Le RGPD préserve et développe les principes de base et les droits de la personne concernée établis par la Directive relative à la protection des données. Il introduit en outre de nouvelles obligations en imposant aux organisations de mettre en place une protection des données dès la conception et par défaut, de désigner un délégué à la protection des données dans certaines circonstances, de se conformer à un nouveau droit à la portabilité des données et de respecter le principe de la responsabilité. En vertu du droit de l'Union, les règlements sont directement applicables et il n'y a pas lieu de les transposer en droit national. Le Règlement général sur la protection des données établit donc un ensemble unique de règles de protection des données pour l'ensemble de l'UE. Il donne naissance à un cadre cohérent de règles relatives à la protection des données dans toute l'UE, créant un environnement de sécurité juridique

31 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, point 29.

dont peuvent bénéficier les opérateurs économiques et les personnes physiques en leur qualité de « personnes concernées ».

Toutefois, bien que le RGPD soit directement applicable, les États membres sont censés actualiser leur législation nationale existante en la matière afin de l'aligner pleinement sur le règlement, tout en laissant une marge d'appréciation pour des dispositions spécifiques, comme le prévoit le considérant 10. Les principaux principes et règles énoncés dans le règlement et les droits forts que celui-ci confère aux personnes physiques constituent une partie importante du manuel et sont présentés dans les chapitres qui suivent. Le règlement énonce des règles exhaustives sur la portée territoriale. Il s'applique aux entreprises établies dans l'UE ainsi qu'aux responsables du traitement et sous-traitants non établis dans l'UE qui proposent des biens ou des services à des personnes physiques dans l'UE ou surveillent leur comportement. Étant donné que plusieurs entreprises technologiques étrangères détiennent une part essentielle du marché européen et ont des millions de clients dans l'UE, il est important que ces organisations soient soumises aux règles européennes en matière de protection des données afin de garantir la protection des personnes physiques et d'établir des conditions équitables.

La protection des données en matière répressive : la Directive 2016/680

La Directive abrogée relative à la protection des données prévoyait un système complet de protection des données. Celui-ci a été renforcé par l'adoption du Règlement général sur la protection des données. Quoique complet, le champ d'application de la Directive abrogée relative à la protection des données était limité aux activités relevant du marché intérieur et à celles des autorités publiques autres que les autorités répressives. L'adoption d'instruments spécifiques a donc été nécessaire pour parvenir à la clarté et à l'équilibre nécessaires entre la protection des données et d'autres intérêts légitimes et pour relever des défis particulièrement importants dans des secteurs particuliers. C'est notamment le cas des règles régissant le traitement des données à caractère personnel par des autorités répressives.

Le premier instrument juridique de l'UE réglementant cet aspect a été 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. Ses règles s'appliquaient uniquement aux données policières et judiciaires échangées entre des États membres. Le traitement national de données à caractère personnel par des autorités répressives était exclu de son champ d'application.

La Directive (UE) 2016/680 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[32], appelée également « Directive relative à la protection des données pour les autorités policières et judiciaires en matière pénale », a remédié à cette situation. Adoptée parallèlement au RGPD, la directive a abrogé la Décision-cadre 2008/977/JAI et a établi un système exhaustif de protection des données à caractère personnel dans le domaine répressif, tout en reconnaissant les spécificités du traitement des données liées à la sécurité publique. Alors que le Règlement général sur la protection des données énonce des règles générales en vue de protéger les personnes physiques à l'égard du traitement de leurs données à caractère personnel et de garantir la libre circulation de ces données dans l'UE, la directive établit des règles spécifiques pour la protection des données dans le domaine de la coopération judiciaire en matière pénale et de la coopération policière. Lorsqu'une autorité compétente traitera des données à caractère personnel à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, la Directive 2016/680 s'appliquera. Lorsqu'une autorité compétente traitera des données à caractère personnel à d'autres fins que celles précitées, le régime général établi par le RGPD s'appliquera. À la différence du champ d'application de son prédécesseur (Décision-cadre 2008/977/JAI du Conseil), celui de la Directive 2016/680 s'étend au traitement national des données à caractère personnel par les autorités répressives et n'est pas limité aux échanges de ces données entre les États membres. En outre, la directive vise à trouver un équilibre entre les droits des personnes physiques et les objectifs légitimes du traitement lié à la sécurité.

À cet effet, la directive consacre le droit à la protection des données à caractère personnel et les principes de base qui devraient régir le traitement des données, en suivant de près les règles et principes énoncés dans le RGPD. Les droits des personnes physiques et les obligations faites aux responsables du traitement – par exemple, en ce qui concerne la sécurité des données, la protection des données dès la conception et par défaut et les notifications de violation des données – sont similaires aux droits et obligations formulés dans le RGPD. La directive tient également compte des grands défis technologiques émergents qui peuvent avoir des

32 Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, JO L 119 du 4 mai 2016.

effets particulièrement pénibles pour les personnes physiques, comme le recours des autorités répressives à des techniques de profilage et vise à y répondre. En principe, les décisions uniquement fondées sur le traitement automatisé des données, comme le profilage, doivent être interdites.[33] En outre, elles ne doivent pas être fondées sur des données sensibles. Ces principes sont soumis à quelques exceptions prévues par la directive. De plus, un tel traitement ne doit pas entraîner une discrimination à l'égard d'une personne[34].

Cette directive contient également des règles afin de garantir la responsabilité des responsables du traitement. Ceux-ci doivent désigner un délégué à la protection des données afin de contrôler le respect des règles de protection des données, d'informer et de conseiller l'entité et les salariés effectuant le traitement sur leurs obligations et de coopérer avec l'autorité de contrôle. Le traitement de données à caractère personnel dans le domaine de la police et de la justice pénale est désormais soumis au contrôle d'autorités indépendantes. Tant le régime général de la protection des données que le régime spécial prévu à des fins répressives et pénales doivent se conformer également aux exigences de la Charte des droits fondamentaux de l'UE.

Le régime spécial du traitement des données dans le cadre de la coopération policière et judiciaire institué par la Directive relative à la protection des données pour les autorités policières et judiciaires en matière pénale est décrit en détail au chapitre 8.

Directive « vie privée et communications électroniques »

L'établissement de règles spéciales de protection des données a également été jugé nécessaire dans le secteur des communications électroniques. Avec l'essor d'internet, de la téléphonie fixe et de la téléphonie mobile, il était important de veiller à ce que les droits au respect de la vie privée et à la confidentialité des utilisateurs soient respectés. La Directive 2002/58/CE[35] 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 ») énonce

33 Directive relative à la protection des données pour les autorités policières et judiciaires en matière pénale, art. 11, para. 1.

34 *Ibid.*, art. 11, paras. 2 et 3.

35 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 L 201 (Directive « vie privée et communications électroniques »).

les règles relatives à la sécurité des données à caractère personnel sur ces réseaux, à la notification des violations des données personnelles et à la confidentialité des communications.

En ce qui concerne la sécurité, les fournisseurs de services de communications électroniques doivent, entre autres choses, veiller à ce que l'accès aux données à caractère personnel soit limité exclusivement aux personnes autorisées et prendre des mesures afin d'éviter que ces données soient détruites, perdues ou endommagées accidentellement[36]. En cas de risque particulier de violation de la sécurité du réseau de communication public, les opérateurs doivent informer les abonnés du risque encouru[37]. Si, en dépit des mesures de sécurité mises en œuvre, une violation de la sécurité se produit, le fournisseur doit notifier la violation des données à caractère personnel à l'autorité nationale compétente chargée de la mise en œuvre et de l'application de la directive. Les fournisseurs sont parfois tenus de notifier également les violations de données à caractère personnel aux personnes physiques, à savoir lorsque la violation est de nature à affecter négativement les données les concernant ou leur vie privée[38]. La confidentialité des communications impose que les écoutes téléphoniques, le stockage ou tout type de surveillance ou d'interception de communications et de données relatives au trafic soient, en principe, interdits. La directive interdit également les communications non sollicitées (souvent appelées « spams »), à moins que les utilisateurs n'aient donné leur consentement, et elle contient des règles sur le stockage des « cookies » sur les ordinateurs et les appareils. Il ressort clairement de ces obligations négatives centrales que la confidentialité des communications est liée de manière significative à la protection du droit au respect de la vie privée consacré par l'article 7 de la Charte et du droit à la protection des données à caractère personnel garanti par l'article 8 de la Charte.

En janvier 2017, la Commission a publié une proposition de règlement concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques, dont le but est de remplacer la Directive « vie privée et communications électroniques ». La réforme vise à aligner les règles régissant les communications électroniques sur le nouveau régime de protection des données mis en place par le Règlement général sur la protection des données. Le nouveau règlement sera directement applicable dans toute l'Union ; toutes les personnes physiques jouiront du même niveau de protection de leurs communications

36 *Ibid.*, art. 4, para. 1.

37 *Ibid.*, art. 4, para. 2.

38 *Ibid.*, art. 4, para. 3.

électroniques, tandis que les opérateurs de services de télécommunication et les entreprises bénéficieront de la clarté des dispositions, de la sécurité juridique et de l'existence d'un ensemble harmonisé de règles applicables dans toute l'UE. Les règles proposées concernant la confidentialité des communications électroniques s'appliqueront également aux nouveaux acteurs qui fournissent des services de communication électronique non couverts par la Directive « vie privée et communications électroniques ». Cette dernière ne couvrait que les opérateurs de services de télécommunications traditionnels. Du fait de l'explosion de l'utilisation de services tels que Skype, WhatsApp, Facebook, Messenger et Viber pour envoyer des messages ou pour téléphoner, ces services « over-the-top » (OTT) relèveront désormais du champ d'application du règlement et devront se conformer à ses exigences en matière de protection des données, de respect de la vie privée et de sécurité. Au moment de la publication du présent manuel, un processus législatif relatif aux règles sur la vie privée et les communications électroniques était toujours en cours.

Règlement (CE) n° 45/2001

Étant donné que la Directive relative à la protection des données ne pouvait s'appliquer qu'aux États membres de l'UE, un instrument juridique supplémentaire était nécessaire pour protéger le traitement de données à caractère personnel effectué par les institutions et organes de l'UE. Le Règlement (CE) nº 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 sur la protection des données traitées par les institutions de l'UE) y pourvoit[39].

Le Règlement (CE) nº 45/2001 est calqué sur les principes du régime européen général de la protection des données et les applique aux traitements de données effectués par les institutions et organes de l'UE dans l'exercice de leurs fonctions. De plus, il instaure une autorité de contrôle indépendante chargée de surveiller l'application de ses dispositions, le Contrôleur européen de la protection des données (CEPD). Le CEPD est investi de pouvoirs de contrôle et a le devoir de contrôler le traitement des données à caractère personnel au sein des institutions et organes de l'UE, ainsi que d'entendre et d'enquêter sur les réclamations concernant des violations alléguées des règles relatives à la protection des données. Il fournit également des avis aux institutions et organes de l'UE sur toutes les questions en rapport

39 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.

avec la protection des données à caractère personnel, depuis les nouvelles propositions législatives jusqu'à la rédaction de règles internes relatives au traitement des données.

En janvier 2017, la Commission européenne a présenté une proposition de nouveau règlement relatif au traitement des données par les institutions de l'UE, qui abrogera le règlement actuel. Tout comme ce fut le cas de la réforme de la Directive « vie privée et communications électroniques », la réforme du Règlement (CE) nº 45/2001 modernisera et harmonisera ses dispositions avec le nouveau régime de protection des données mis en place par le Règlement général sur la protection des données.

Le rôle de la CJUE

La CJUE est compétente pour déterminer si un État membre a effectivement rempli ses obligations au titre du droit de l'UE en matière de protection des données et pour interpréter la législation de l'UE afin d'en assurer l'application effective et uniforme dans tous les États membres. Depuis l'adoption de la Directive relative à la protection des données en 1995, un corpus considérable de jurisprudence s'est constitué et a clarifié le champ d'application et la signification des principes applicables à la protection des données et du droit fondamental à la protection des données à caractère personnel consacré par l'article 8 de la Charte. Bien que la directive ait été abrogée et qu'un nouvel instrument juridique – le Règlement général sur la protection des données – soit entré en vigueur, cette jurisprudence préexistante demeure valable et pertinente aux fins de l'interprétation et de l'application des principes de la protection des données de l'UE, dans la mesure où les principes et concepts de base de la Directive relative à la protection des données ont été conservés dans le RGPD.

1.2. Limitations du droit à la protection des données à caractère personnel

Points clés

- Le droit à la protection des données n'est pas un droit absolu ; il peut être limité si nécessaire pour servir un objectif d'intérêt général ou protéger les droits et libertés d'autrui.

- Les conditions de limitation des droits au respect de la vie privée et à la protection des données à caractère personnel sont énumérées à l'article 8 de la CEDH et à l'article 52, paragraphe 1, de la Charte. Elles ont été développées et interprétées par la jurisprudence de la CouEDH et de la CJUE.
- En vertu du droit de protection des données du CdE, le traitement de données à caractère personnel constitue une ingérence licite dans le droit au respect de la vie privée et ne peut être exercé uniquement si :
  - elle est prévue par la loi ;
  - elle poursuit un but légitime ;
  - elle respecte le contenu essentiel des droits et libertés fondamentaux ;
  - elle est nécessaire et proportionnée dans une société démocratique pour atteindre un but légitime.
- L'ordre juridique de l'UE impose des conditions similaires aux limitations de l'exercice des droits fondamentaux protégés par la Charte. Toute limitation d'un droit fondamental, y compris la protection des données à caractère personnel, ne peut être licite que si :
  - elle est prévue par la loi ;
  - elle respecte le contenu essentiel du droit ;
  - elle est nécessaire, sous réserve du principe de proportionnalité ; et
  - elle poursuit un objectif d'intérêt général reconnu par l'Union ou répond au besoin de protection des droits d'autrui.

Le droit fondamental à la protection des données à caractère personnel prévu par l'article 8 de la Charte n'est pas une prérogative absolue, « mais doit être pris en considération par rapport à sa fonction dans la société »[40]. L'article 52, paragraphe 1, de la Charte reconnaît donc que des limitations peuvent être imposées à l'exercice de droits tels que ceux garantis par les articles 7 et 8 de la Charte, pour autant que ces limitations soient prévues par la loi, qu'elles respectent le contenu essentiel de ces droits et libertés et, sous réserve du principe de la proportionnalité, qu'elles soient nécessaires et poursuivent des objectifs d'intérêt général reconnus par l'UE ou répondent au besoin de protection des droits et libertés d'autrui[41]. De même, dans le système de la CEDH, la protection des données est garantie par l'article 8 et

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

41 *Ibid.*, point 50.

l'exercice de ce droit peut être limité, si nécessaire, pour poursuivre un but légitime. La présente section détaille les conditions d'ingérence au titre de la CEDH, telle qu'interprétée par la jurisprudence de la CouEDH, ainsi que les conditions des limitations licites au titre de l'article 52 de la Charte.

1.2.1. Exigences devant être remplies pour qu'une ingérence soit 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, protégé par l'article 8 de la CEDH[42]. Comme expliqué plus haut (voir section 1.1.1 et section 1.1.4), contrairement à l'ordre juridique de l'UE, la CEDH n'affirme pas la protection des données à caractère personnel comme un droit fondamental distinct, Mais il fait plutôt partie des droits protégés au titre du droit au respect de la vie privée. Par conséquent, toute opération impliquant le traitement de données à caractère personnel pourrait relever du champ d'application de l'article 8 de la CEDH. Pour déclencher l'article 8, il convient en premier lieu de déterminer s'il a été porté atteinte à un intérêt privé ou à la vie privée d'une personne. Dans sa jurisprudence, la CouEDH a traité la notion de « vie privée » comme un concept large, englobant même des aspects de la vie professionnelle et du comportement en public. Elle a également déclaré que la protection des données à caractère personnel constitue un élément important du droit au respect de la vie privée. Toutefois, en dépit de la large interprétation de la notion de vie privée, tous les types de traitement ne compromettraient pas, en soi, les droits protégés par l'article 8.

Lorsque la CouEDH considère que le traitement en question affecte le droit des personnes au respect de la vie privée, elle examine si l'ingérence est justifiée. Le droit au respect de la vie privée n'est pas un droit absolu, mais doit être mis en balance et concilié avec d'autres droits et intérêts légitimes, qu'ils appartiennent à d'autres personnes (intérêts privés) ou à la société dans son ensemble (intérêts publics).

Les conditions cumulatives dans lesquelles une ingérence pourrait être justifiée sont les suivantes :

42 CouEDH, *S. et Marper c. Royaume-Uni* [GC], n° 30562/04 et 30566/04, 8 décembre 2008, point 67.

Ingérence prévue par la loi

Selon la jurisprudence de la CouEDH, l'ingérence est prévue par la loi si elle repose sur une disposition du droit national qui présente certaines caractéristiques. La loi doit être « accessible au justiciable et prévisible »[43]. Une règle est prévisible « lorsqu'elle est rédigée avec assez de précision pour permettre à toute personne, en s'entourant au besoin de conseils éclairés, de régler sa conduite »[44]. Par ailleurs, « [l]e degré de précision requis de la "loi" à cet égard dépendra du sujet en question »[45].

Exemples : dans l'affaire *Rotaru c. Roumanie*[46], le requérant invoquait une violation de son droit au respect de la vie privée au motif que le service roumain de renseignements détenait et utilisait un fichier contenant ses informations personnelles. La CouEDH a estimé que le droit roumain autorisait la collecte, l'enregistrement et l'archivage, dans des dossiers secrets, d'informations importantes pour la sécurité nationale, sans poser de 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. La Cour a donc 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.

Dans l'affaire *Taylor-Sabori c. Royaume-Uni*[47], le requérant avait fait l'objet d'une surveillance policière. Utilisant un « clone » du messager de poche

43 CouEDH, *Amann c. Suisse* [GC], nº 27798/95, 16 février 2000, para. 50 ; voir aussi CouEDH, *Kopp c. Suisse*, nº 23224/94, 25 mars 1998, para. 55 ; CouEDH, *Iordachi et autres c. Moldova*, nº 25198/02, 10 février 2009, para. 50.

44 CouEDH, *Amann c. Suisse* [GC], nº 27798/95, 16 février 2000, para. 56 ; voir aussi CouEDH, *Malone c. Royaume-Uni*, nº 8691/79, 2 août 1984, para. 66 ; CouEDH, *Silver et autres c. Royaume-Uni*, nº 5947/72, 6205/73, 7052/75, 7061/75, 7107/75 et 7113/75, 25 mars 1983, para. 88.

45 CouEDH, *The Sunday Times c. Royaume-Uni*, nº 6538/74, 26 avril 1979, para. 49 ; voir aussi CouEDH, *Silver et autres c. Royaume-Uni*, nº 5947/72, 6205/73, 7052/75, 7061/75, 7107/75 et 7113/75, 25 mars 1983, para. 88.

46 CouEDH, *Rotaru c. Roumanie* [GC], nº 28341/95, 4 mai 2000, para. 57 ; voir aussi CouEDH, *Association for European Integration and Human Rights et Ekimdzhiev c. Bulgarie*, nº 62540/00, 28 juin 2007 ; CouEDH, *Shimovolos c. Russie*, nº 30194/09, 21 juin 2011 ; et CouEDH, *Vetter c. France*, nº 59842/00, 31 mai 2005.

47 CouEDH, *Taylor-Sabori c. Royaume-Uni*, nº 47114/99, 22 octobre 2002.

du requérant, la police avait pu intercepter des messages qui lui étaient adressés. Le requérant avait ensuite été arrêté et inculpé pour collusion en vue de la vente d'une substance réglementée. Certains éléments à charge du ministère public étaient des reproductions manuscrites récentes des messages du messager de poche 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'avait dès lors pas été effectuée dans des conditions « prévues par la loi ». La CouEDH a conclu à une violation de l'article 8 de la CEDH.

L'affaire *Vukota-Bojić c. Suisse*[48] concernait la surveillance secrète d'une allocataire de prestations sociales par des détectives privés recrutés par sa compagnie d'assurances. La CouEDH a considéré que, si la mesure de surveillance contestée dans la plainte avait été demandée par une compagnie d'assurances privée, c'est l'État qui avait donné à celle-ci le droit de verser des prestations dans le cadre de l'assurance médicale obligatoire et le pouvoir de prélever des cotisations. Un État ne peut se soustraire à sa responsabilité découlant de la Convention en déléguant ses obligations à des organisations privées ou à des particuliers. Le droit interne devait prévoir des garanties suffisantes contre les abus en ce qui concerne l'ingérence avec les droits découlant de l'article 8 de la CEDH pour que celle-ci soit « prévue par la loi ». En l'espèce, la CouEDH a conclu à une violation de l'article 8 de la CEDH au motif que le droit interne n'indiquait pas de manière suffisamment claire l'étendue et les modalités d'exercice du pouvoir discrétionnaire conféré aux compagnies d'assurances agissant en tant qu'autorités publiques dans le cadre de litiges en matière d'assurances, pour faire surveiller secrètement un assuré. En particulier, le droit interne ne comportait pas des garanties suffisantes contre les abus.

Poursuite d'un but légitime

Le but légitime peut être l'un des intérêts publics précités ou la protection des droits et libertés d'autrui. Les buts légitimes pouvant justifier une ingérence sont, selon l'article 8, paragraphe 2, de la CEDH, les intérêts de sécurité nationale, de sûreté publique, de bien-être économique du pays, de défense de l'ordre et de prévention

48 CouEDH, *Vukota-Bojić c. Suisse*, nº 61838/10, 18 octobre 2016, para. 77.

des infractions pénales, de protection de la santé ou de la morale et de protection des droits et libertés d'autrui.

> Exemple : dans l'affaire *Peck c. Royaume-Uni*[49], le requérant a tenté de se suicider dans la rue en se tailladant les poignets, sans savoir qu'une caméra de surveillance avait filmé toute la scène. Après le sauvetage du requérant par la police, qui regardait les caméras de surveillance, celle-ci a diffusé la séquence dans les médias, qui l'ont publiée sans masquer le visage du requérant. La CouEDH a conclu à 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 en particulier proportionnée au but légitime recherché »[50]. Lorsqu'elle apprécie si une mesure est nécessaire pour répondre à un besoin social urgent, la CouEDH examine sa pertinence et son adéquation par rapport à l'objectif poursuivi. À cet effet, elle peut prendre en compte le fait que l'ingérence vise à résoudre un problème qui, s'il n'y est pas répondu, pourrait avoir un effet préjudiciable sur la société, qu'il existe des preuves que l'ingérence peut atténuer cet effet négatif, ainsi que les points de vue sociétaux plus larges sur le problème en question.[51] Par exemple, la collecte et la conservation de données à caractère personnel par des services de sécurité sur des personnes physiques particulières ayant des liens avec des mouvements terroristes seraient une ingérence dans le droit à la vie privée des personnes, qui répond néanmoins à un besoin social important et urgent : la sécurité nationale et la lutte contre le terrorisme. Pour répondre au critère de nécessité, l'ingérence devra également être proportionnée. Selon la jurisprudence de la CouEDH, la proportionnalité est abordée dans le cadre du concept de nécessité. La proportionnalité requiert qu'une mesure d'ingérence dans l'exercice des droits protégés par la CEDH n'aille pas au-delà de ce qui est nécessaire pour atteindre le but légitime poursuivi. Les facteurs importants à prendre en compte

49 CouEDH, *Peck c. Royaume-Uni*, nº 44647/98, 28 janvier 2003, para. 85.

50 CouEDH, *Leander c. Suède*, nº 9248/81, 26 mars 1987, para. 58.

51 Groupe de travail « Article 29 » sur la protection des données (Groupe de travail « Article 29 ») (2014), *Avis sur l'application des notions de nécessité et de proportionnalité et la protection des données dans le secteur répressif*, WP 211, Bruxelles, 27 février 2014, p. 7 et 8.

lors de l'appréciation du critère de proportionnalité sont la portée de l'ingérence, notamment le nombre de personnes concernées, et les garanties ou les avertissements mis en place pour limiter sa portée ou ses effets négatifs sur les droits des individus[52].

Exemple : dans l'affaire *Khelili c. Suisse*[53], la police a découvert lors d'un contrôle que la requérante transportait des cartes de visite indiquant : « Gentille, jolie femme fin trentaine attend ami pour prendre un verre de temps en temps ou sortir. Tel. (...). ». Selon la requérante, suite à cette découverte, les policiers l'ont enregistrée dans leurs dossiers comme prostituée, 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 illicite paraissait 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 *S. et Marper c. Royaume-Uni*[54], les deux requérants ont été arrêtés et accusés d'infractions pénales. La police a relevé leurs empreintes digitales et des échantillons d'ADN, conformément à la loi sur la police et les preuves en matière pénale. Les requérants n'ont jamais été condamnés pour ces infractions : l'un a été acquitté et la procédure dirigée contre le second a été classée sans suite. Néanmoins, leurs empreintes digitales, leurs profils ADN et des échantillons cellulaires ont été conservés dans une base de données par la police et la législation nationale autorisait

52 *Ibid.*, p. 9 à 11.

53 CouEDH, *Khelili c. Suisse*, nº 16188/07, 18 octobre 2011.

54 CouEDH, *S. et Marper c. Royaume-Uni* [GC], nº 30562/04 et nº 30566/04, 4 décembre 2008.

leur conservation sans limite dans le temps. Alors que le Royaume-Uni a fait valoir que la conservation contribuait à l'identification des futurs délinquants et poursuivait donc le but légitime de prévenir et de détecter des infractions, la CouEDH a jugé que l'ingérence dans le droit au respect de la vie des requérants était injustifiée. Elle a rappelé que les principes de base de la protection des données imposent que la conservation de données à caractère personnel soit proportionnée par rapport à la finalité de la collecte et que les délais de conservation doivent être limités. La Cour a admis que l'extension de la base de données pour inclure les profils ADN non seulement des personnes condamnées, mais également de toutes les personnes soupçonnées mais non condamnées pouvait avoir contribué à la détection et à la prévention d'infractions pénales au Royaume-Uni. Toutefois, elle a été « frappée par le caractère général et indifférencié du pouvoir de conservation »[55].

La conservation d'échantillons cellulaires est particulièrement intrusive, compte tenu de la profusion d'informations génétiques et relatives à la santé qu'ils contiennent. Les empreintes digitales et des échantillons pouvaient être prélevés sur des personnes arrêtées et conservés indéfiniment dans la base de données de la police, quelles que soient la nature et la gravité de l'infraction, et même pour des délits mineurs non passibles d'emprisonnement. De plus, il n'existe que peu de possibilités pour un individu acquitté d'obtenir l'effacement des données de la base de données. Enfin, la CouEDH a accordé une attention particulière au fait qu'un requérant avait onze ans lorsqu'il a été arrêté. La conservation des données personnelles des mineurs non condamnés peut leur être particulièrement préjudiciable en raison de leur vulnérabilité et de l'importance que revêtent leur développement et leur intégration dans la société[56]. La Cour a conclu à l'unanimité que la conservation constituait une atteinte disproportionnée au droit des requérants au respect de leur vie privée et ne pouvait être considérée comme nécessaire dans une société démocratique.

Exemple : dans l'affaire *Leander c. Suède*[57], 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

55 *Ibid.*, para. 119.

56 *Ibid.*, para. 124.

57 CouEDH, *Leander c. Suède*, nº 9248/81, 26 mars 1987, paras. 59 et 67.

de sa nécessité dans une société démocratique. Les garanties spéciales prévues par la législation nationale dans le but de protéger les intérêts de la personne concernée (par exemple, les 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.

1.2.2. Conditions des limitations licites en vertu de la Charte des droits fondamentaux 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 une disposition consacrée aux limitations relatives à l'exercice des droits et libertés qu'elle reconnaît.

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 données à caractère personnel, tel que le traitement de données à caractère personnel, n'est admissible 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[58] ; 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.

La protection des données à caractère personnel étant un droit fondamental distinct et indépendant dans l'ordre juridique de l'UE, garanti par l'article 8 de la Charte, tout traitement de données à caractère personnel constitue, par essence, une ingérence dans ce droit. Il est indifférent que les données à caractère personnel concernent

58 Sur l'évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel, *voir :* CEPD (2017), *Guide pour l'évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel*, Bruxelles, 11 avril 2017.

la vie privée d'une personne, qu'elles soient sensibles ou que les personnes concernées aient subi un inconvénient quelconque. Pour être licite, l'ingérence doit remplir toutes les conditions énoncées à l'article 52, paragraphe 1, de la Charte.

Ingérence prévue par la loi

Les limitations du droit à la protection des données à caractère personnel doivent être prévues par la loi. Cette exigence implique que les limitations doivent avoir une base juridique dûment accessible et prévisible, formulée de façon suffisamment précise pour permettre aux individus de comprendre leurs obligations et d'adapter leur comportement. La base juridique doit également clairement définir la portée et les modalités de l'exercice du pouvoir par les autorités compétentes afin de protéger les individus contre toute ingérence arbitraire. Cette interprétation est similaire à l'exigence d'« ingérence licite » dans la jurisprudence de la CouEDH[59] et il a été affirmé que la signification de l'expression « prévue par la loi » utilisée dans la Charte devrait se voir attribuer une portée similaire à celle que revêt cette expression dans le contexte de la CEDH[60]. La jurisprudence de la CouEDH, et en particulier la notion de « qualité de la loi » qu'elle a développée au fil des ans, est un élément pertinent qui doit être pris en considération par la CJUE dans l'interprétation de la portée de l'article 52, paragraphe 1, de la Charte[61].

Respect du contenu essentiel du droit

Dans l'ordre juridique de l'UE, toute limitation des droits fondamentaux protégés par la Charte doit respecter le contenu essentiel de ces droits. En d'autres termes, les limitations qui sont si larges et intrusives qu'elles vident un droit fondamental de son contenu essentiel ne peuvent être justifiées. Si l'essence du droit est compromise, la limitation doit être considérée comme illicite, sans qu'il soit nécessaire d'apprécier plus avant si elle poursuit un objectif d'intérêt général et répond aux critères de nécessité et de proportionnalité.

59 CEPD (2017), Guide pour l'évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel, Bruxelles, 11 avril 2017, p. 4 ; voir aussi CJUE, *Avis 1/15 de la Cour (grande chambre)*, 26 juillet 2017.

60 CJUE, affaires jointes C-203/15 et C-698/15, *Tele2 Sverige AB c. Post- och telestyrelsen* et *Secretary of State for the Home Department c. Tom Watson, Peter Brice et Geoffrey Lewis*, conclusions de l'avocat général Saugmandsgaard Øe, présentées le 19 juillet 2016, point 140.

61 CJUE, C-70/10, *Scarlet Extended SA c. Société belge des auteurs compositeurs et éditeurs (SABAM)*, *conclusions de l'avocat général Cruz Villalón*, présentées le 14 avril 2011, point 100.

Exemple : l'affaire *Schrems*[62] concernait la protection des personnes physiques à l'égard du transfert de leurs données à caractère personnel vers des pays tiers, en l'espèce les États-Unis. M. Schrems, un ressortissant autrichien utilisateur de Facebook depuis plusieurs années, a introduit une plainte auprès de l'autorité irlandaise de contrôle de la protection des données afin de dénoncer le transfert de ses données personnelles de la filiale irlandaise de Facebook à Facebook Inc. et aux serveurs situés aux États-Unis, où elles font l'objet d'un traitement. Il a fait valoir que, à la lumière des révélations faites en 2013 par M. Snowden, un lanceur d'alerte américain, sur les activités de surveillance des services américains de renseignement, la loi et les pratiques des États-Unis n'offraient pas une protection suffisante aux données à caractère personnel transférées vers le territoire américain. M. Snowden avait révélé que la National Security Agency procédait directement à des écoutes sur les serveurs d'entreprises comme Facebook et pouvait lire le contenu de discussions instantanées et de messages privés.

Les transferts de données vers les États-Unis reposaient sur une décision d'adéquation, adoptée par la Commission en 2000 et autorisant les transferts vers des entreprises américaines qui avaient déclaré qu'elles protégeraient les données à caractère personnel transférées de l'UE et se conformeraient au principe dit de la « sphère de sécurité ». Lorsque la CJUE a été saisie de l'affaire, elle a examiné la validité de la décision de la Commission à la lumière de la Charte. Elle a rappelé que la protection des droits fondamentaux exige que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci s'opèrent dans les limites du strict nécessaire. La CJUE a estimé qu'une réglementation permettant aux autorités publiques d'accéder de manière généralisée au contenu de communications électroniques doit être considérée « comme portant atteinte au contenu essentiel du droit fondamental au respect de la vie privée, tel que garanti par l'article 7 de la Charte ». Ce droit serait privé de toute signification si les pouvoirs publics américains étaient autorisés à accéder à des communications de manière généralisée, sans aucune justification objective fondée sur des raisons de sécurité nationale ou de prévention de la criminalité, liées spécifiquement aux individus concernés, et sans que ces pratiques de surveillance soient assorties de garanties adéquates contre les abus de pouvoir.

62 CJUE, C-362/14, *Maximillian Schrems c. Data Protection Commissioner* [GC], 6 octobre 2015.

La CJUE a, par ailleurs, fait valoir qu'« une réglementation ne prévoyant aucune possibilité pour le justiciable d'exercer des voies de droit afin d'avoir accès à des données à caractère personnel le concernant, ou d'obtenir la rectification ou la suppression de telles données » est incompatible avec le droit fondamental à une protection juridictionnelle effective (article 47 de la Charte). La Décision concernant la sphère de sécurité ne garantissait donc pas un niveau de protection des droits fondamentaux par les États-Unis équivalant à celui garanti au sein de l'UE au titre de la directive lue à la lumière de la Charte. La CJUE a donc annulé la décision[63].

Exemple : dans l'affaire *Digital Rights Ireland*[64], la CJUE a examiné la compatibilité de la Directive 2006/24/CE (Directive relative à la conservation des données) avec les articles 7 et 8 de la Charte. La directive obligeait les fournisseurs de services de communications électroniques à conserver les données de trafic et de localisation pendant six mois au moins et 24 mois au plus et autorisait les autorités nationales compétentes à accéder à ces données à des fins de prévention, de recherche, de détection et de poursuite d'infractions pénales graves. La directive ne permettait pas de conserver le contenu des communications électroniques. La CJUE a fait valoir que les données que les fournisseurs devaient conserver en application de la directive incluaient les données nécessaires pour tracer et identifier la source et la destination d'une communication, la date, l'heure et la durée de celle-ci, le numéro appelant, les numéros appelés et les adresses IP. Ces données, « prises dans leur ensemble, étaient susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci ».

63 La décision de la Cour d'annuler la Décision 520/2000/CE de la Commission était également fondée sur d'autres motifs, qui seront examinés dans d'autres chapitres de ce manuel. La CJUE a notamment considéré que la décision limitait illicitement les pouvoirs des autorités nationales de contrôle de la protection des données. De plus, dans le système de la sphère de sécurité, il n'existe pas de voies de recours juridictionnelles pour les personnes qui souhaitent accéder aux données à caractère personnel les concernant et/ou obtenir leur rectification ou leur effacement. Il a donc également été porté atteinte à l'essence du droit fondamental à une protection juridictionnelle effective, consacré par l'article 47 de la Charte.

64 CJUE, affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources et autres* et *Kärntner Landesregierung et autres* [GC], 8 avril 2014.

Par conséquent, la conservation de données à caractère personnel au titre de la directive constituait une ingérence particulièrement grave dans l'exercice des droits au respect de la vie privée et à la protection des données à caractère personnel. La CJUE a toutefois conclu que l'ingérence n'avait pas porté atteinte à l'essence de ces droits. S'agissant du droit au respect de la vie privée, son essence n'avait pas été affectée parce que la directive ne permettait pas de connaître le contenu des communications électroniques en tant que tel. De même, il n'a pas été porté atteinte au droit à la protection des données à caractère personnel, étant donné que la directive imposait aux fournisseurs de services de communications électroniques de respecter certains principes de la protection des données et de la sécurité des données et de mettre en œuvre des mesures techniques et organisationnelles à cet effet.

Nécessité et proportionnalité

L'article 52, paragraphe 1, de la Charte dispose que, dans le respect du principe de la proportionnalité, des limitations à l'exercice des droits et libertés fondamentaux reconnus par celle-ci ne peuvent être spécifiées que si elles sont nécessaires.

Une limitation peut être **nécessaire** s'il existe une nécessité d'adopter des mesures pour atteindre l'objectif d'intérêt public poursuivi ; cependant, la nécessité, telle qu'elle est interprétée par la CJUE, implique également que les mesures adoptées soient moins intrusives que d'autres options pour atteindre le même but. Pour ce qui concerne les limitations des droits au respect de la vie privée et à la protection des données à caractère personnel, la CJUE applique un strict critère de nécessité selon lequel « les dérogations et les limitations doivent s'opérer dans les limites du strict nécessaire ». Si une limitation est jugée strictement nécessaire, il convient également d'en apprécier la proportionnalité.

On entend par **proportionnalité** le fait que les avantages résultant de la limitation devraient l'emporter sur les inconvénients que celle-ci entraîne pour l'exercice des droits fondamentaux concernés[65]. Afin de réduire les inconvénients et les risques pour l'exercice des droits au respect de la vie privée et à la protection des données, il importe que les limitations contiennent des garanties adéquates.

65 CEPD (2017), *Guide pour l'évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel*, p. 5.

Exemple : dans l'affaire *Volker und Markus Schecke*[66], la CJUE a conclu qu'en imposant la publication de données à caractère personnel de toutes les personnes physiques bénéficiaires d'une aide au titre de certains fonds agricoles sans opérer de distinction sur la base de critères pertinents, tels que les périodes pendant lesquelles elles ont perçu de telles aides, la fréquence ou encore le type et l'importance de celles-ci, le Conseil et la Commission ont excédé les limites qu'impose le respect du principe de proportionnalité.

La CJUE a donc conclu à la nécessité de déclarer invalides certaines dispositions du Règlement (CE) nº 1290/2005 du Conseil et de déclarer le Règlement (CE) nº 259/2008 invalide dans son intégralité[67].

Exemple : dans l'affaire *Digital Rights Ireland*[68], la CJUE a considéré que l'ingérence dans l'exercice du droit au respect de la vie privée causée par la Directive relative à la conservation des données ne portait pas atteinte à l'essence de ce droit, dans la mesure où elle interdisait la conservation du contenu des communications électroniques. Elle a toutefois conclu que la directive était incompatible avec les articles 7 et 8 de la Charte et l'a déclarée invalide. Étant donné que les données de trafic et de localisation, agrégées et considérées dans leur ensemble, pouvaient être analysées et donner une image détaillée de la vie privée d'individus, elle constituait une ingérence grave dans ce droit. La CJUE a tenu compte du fait que la directive imposait la conservation de toutes les données relatives au trafic de téléphonie fixe, de téléphonie mobile, d'accès à internet, de courrier électronique par internet et de téléphonie par internet, en s'appliquant à tous les moyens de communication électronique, dont l'usage est très répandu dans la vie quotidienne des gens. Dans la pratique, cela constituait une ingérence qui touchait toute la population européenne. Compte tenu de l'ampleur et de la gravité de cette ingérence, l'objectif de lutte contre la criminalité grave ne saurait à lui seul justifier la conservation des données de trafic et de

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

67 Règlement (CE) nº 1290/2005 du Conseil du 21 juin 2005 relatif au financement de la politique agricole commune, JO 2005 L 209 ; Règlement (CE) nº 259/2008 de la Commission du 18 mars 2008 portant modalités d'application du règlement (CE) nº 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 (FEDER), JO 2008 L 76.

68 CJUE, affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources et autres* et Kärntner Landesregierung *et autres* [GC], 8 avril 2014, point 39.

localisation, selon la CJUE. En outre, la directive n'a pas fixé de critères objectifs garantissant que l'accès des autorités nationales compétentes aux données conservées soit limité à ce qui est strictement nécessaire. De plus, elle ne contenait pas de conditions matérielles et procédurales régissant l'accès et l'utilisation des données conservées par les autorités nationales, qui n'étaient pas soumises à un contrôle préalable par un juge ou un autre organisme indépendant.

La CJUE est parvenue à une conclusion similaire dans les affaires jointes *Tele2 Sverige AB c. Post- och telestyrelsen* et *Secretary of State for the Home Department c. Tom Watson et autres*[69]. Ces affaires concernaient la conservation des données de trafic et de localisation de « tous les abonnés et utilisateurs inscrits et [visaient] tous les moyens de communication électronique ainsi que l'ensemble des données relatives au trafic » sans « aucune différenciation, limitation ou exception en fonction de l'objectif poursuivi »[70]. En l'espèce, la conservation des données s'appliquait indépendamment du fait qu'une personne ait ou non, directement ou indirectement, un lien avec des infractions pénales graves ou que ses communications soient ou non pertinentes pour la sécurité nationale. Compte tenu de l'absence de lien entre les données conservées et une menace pour la sécurité publique ou des restrictions concernant une période temporelle ou une zone géographique, la CJUE a conclu que la réglementation nationale excédait les limites du strict nécessaire aux fins de la lutte contre la criminalité[71].

Dans son *Guide pour l'évaluation de la nécessité*, le Contrôleur européen de la protection des données suit une approche similaire[72]. Ce guide vise à aider à déterminer si les mesures proposées sont conformes au droit de l'Union en matière de protection des données. Il a été conçu dans le but de mieux équiper les décideurs politiques et les législateurs de l'Union chargés d'élaborer ou d'étudier des mesures qui prévoient le traitement de données à caractère personnel et limitent le droit à la protection de ces données et d'autres droits et libertés énoncés dans la Charte.

69 CJUE, affaires jointes C-203/15 et C-698/15, *Tele2 Sverige AB c. Post- och telestyrelsen* et *Secretary of State for the Home Department c. Tom Watson et autres* [GC], 21 décembre 2016, points 105 et 106.

70 *Ibid.*, point 105.

71 *Ibid.*, point 107.

72 CEPD (2017), *Guide pour l'évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel*, Bruxelles, 11 avril 2017.

Objectifs d'intérêt général

Pour être justifiée, toute limitation de l'exercice des droits reconnus par la Charte doit aussi répondre effectivement aux objectifs d'intérêt général reconnus par l'Union ou à la nécessité de protéger les droits et libertés d'autrui. En ce qui concerne la nécessité de protéger les droits et libertés d'autrui, le droit à la protection des données à caractère personnel interagit souvent avec d'autres droits fondamentaux. La section 1.3 analyse en détail ces interactions. Quant aux objectifs d'intérêt général, ils incluent les objectifs généraux de l'UE énoncés à l'article 3 du Traité sur l'Union européenne (TUE), tels que la promotion de la paix et du bien-être de ses citoyens, la justice et la promotion sociales et la création d'un espace de liberté, de sécurité et de justice au sein duquel est assurée la libre circulation des personnes, en liaison avec des mesures appropriées en matière de prévention de la criminalité et de lutte contre ce phénomène, ainsi que d'autres objectifs et intérêts protégés par des dispositions spécifiques des traités[73]. Le RGPD précise l'article 52, paragraphe 1, de la Charte à cet égard. L'article 23, paragraphe 1, du règlement énumère une série d'objectifs d'intérêt général considérés comme légitimes pour limiter les droits des personnes physiques, pour autant que la limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée. La sécurité et la défense nationales, la prévention d'infractions pénales, la protection d'intérêts économiques et financiers importants de l'UE ou d'un État membre, la santé publique et la sécurité sociale comptent au nombre des objectifs d'intérêt public mentionnés dans cette disposition.

Il est important de définir et d'expliquer l'objectif d'intérêt général poursuivi par la limitation de manière suffisamment détaillée, car la nécessité de celle-ci sera appréciée sur la base de ces explications. Une description claire et détaillée de l'objectif poursuivi par la limitation et des mesures proposées est essentielle pour permettre d'apprécier si elle est nécessaire[74]. L'objectif poursuivi, la nécessité et la proportionnalité de la limitation sont étroitement liés.

> Exemple : l'affaire *Schwarz c. Stadt Bochum*[75] concernait des limitations du droit au respect de la vie privée et du droit à la protection des données à caractère personnel découlant du prélèvement et de la conservation

73 Explications relatives à la Charte des droits fondamentaux (2007/C 303/02), JO 2007 C 303, p. 17 à 35.

74 CEPD (2017), *Guide pour l'évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel*, Bruxelles, 11 avril 2017, p. 4.

75 CJUE, C-291/12, *Michael Schwarz c. Stadt Bochum*, 17 octobre 2013.

d'empreintes digitales lorsque les autorités des États membres délivrent des passeports[76]. Le requérant a sollicité la délivrance d'un passeport auprès de la ville de Bochum (Stadt Bochum), mais a refusé que ses empreintes digitales soient relevées ; à la suite de cela, la ville de Bochum a rejeté sa demande de passeport. Le requérant a ensuite introduit un recours devant une juridiction allemande pour qu'un passeport lui soit délivré sans que ses empreintes digitales ne soient relevées. La juridiction allemande a saisi la CJUE et lui a demandé s'il fallait considérer comme valide l'article 1er, paragraphe 2, du Règlement nº 2252/2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres.

La CJUE a souligné que les empreintes digitales **sont des données à caractère personnel**, étant donné qu'elles contiennent objectivement des informations uniques sur des personnes physiques et permettent leur identification précise, alors que la collecte et la conservation des empreintes digitales constituent un traitement. Ce traitement, qui est régi par l'article 1er, paragraphe 2, du Règlement nº 2252/2004, constitue une menace pour les droits au respect de la vie privée et à la protection des données à caractère personnel[77]. L'article 52, paragraphe 1, de la Charte admet toutefois des limitations à l'exercice de ces droits, pour autant que ces limitations soient prévues par la loi, qu'elles respectent le contenu essentiel de ces droits et que, dans le respect du principe de proportionnalité, elles soient nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui.

En l'espèce, la CJUE a commencé par faire valoir que la limitation découlant de la collecte et de la conservation des empreintes digitales lors de la délivrance de passeports doit être considérée comme étant **prévue par la loi**, dès lors que l'article 1er, paragraphe 2, du Règlement nº 2252/2004 prévoit ces opérations. Deuxièmement, ce règlement a été conçu pour prévenir la falsification des passeports et empêcher leur utilisation frauduleuse. Par conséquent, l'article 1er, paragraphe 2, vise à prévenir, entre autres, l'entrée illégale de personnes sur le territoire de l'UE et poursuit donc un objectif d'intérêt général reconnu par l'Union. Troisièmement, il ne ressort pas des éléments dont dispose la Cour – et il n'a d'ailleurs pas été allégué – que les

76 *Ibid.*, points 33 à 36.

77 *Ibid.*, points 27 à 30.

limitations apportées à l'exercice de ces droits en l'espèce ne respecteraient pas le contenu essentiel de ces droits. Quatrièmement, la conservation des empreintes digitales sur un support de stockage hautement sécurisé, prévue par cette disposition, requiert une sophistication technique. Cette conservation est susceptible de réduire le risque de falsification des passeports et de faciliter la tâche des autorités chargées d'examiner l'authenticité de ceux-ci aux frontières de l'UE. Il n'est pas déterminant que la méthode ne soit pas totalement fiable. En effet, bien qu'elle n'exclue pas complètement les acceptations de personnes non autorisées, il suffit qu'elle réduise dans une mesure significative le risque de telles acceptations. Au regard des considérations qui précèdent, la CJUE a conclu que le prélèvement et la conservation des empreintes digitales, visés à l'article 1er, paragraphe 2, du Règlement nº 2252/2004, sont appropriés pour atteindre les buts poursuivis par ce règlement et, partant, l'objectif d'empêcher l'entrée illégale de personnes sur le territoire de l'Union[78].

La CJUE a ensuite apprécié le caractère **nécessaire** de ce traitement, observant que l'opération faisant l'objet du litige consistait simplement à relever l'empreinte de deux doigts, lesquels sont d'ailleurs normalement exposés à la vue d'autrui, de sorte qu'il ne s'agit pas d'une opération revêtant un caractère intime. Celle-ci n'entraîne pas non plus un désagrément physique ou psychique particulier pour l'intéressé, pas davantage que lorsqu'une photo de son visage est enregistrée. Il y a lieu de relever également que la seule alternative réelle au prélèvement des empreintes digitales évoquée au cours de la procédure devant la Cour consiste dans la saisie d'une image de l'iris de l'œil. Or, rien dans le dossier soumis à la Cour n'indique que ce dernier procédé soit moins attentatoire aux droits reconnus par les articles 7 et 8 de la Charte que le prélèvement des empreintes digitales. En outre, en ce qui concerne l'efficacité de ces deux dernières méthodes, il est constant que la maturité technologique de celle fondée sur la reconnaissance de l'iris n'est pas encore aussi avancée que la technologie de reconnaissance des empreintes digitales, qu'elle est actuellement significativement plus onéreuse que celle de la comparaison des empreintes digitales et, de ce fait, moins adaptée à une utilisation généralisée. Dans ces conditions, il y a lieu de constater que n'ont pas été portées à la connaissance de la Cour deux mesures susceptibles de contribuer, de manière suffisamment efficace, au but de protéger des passeports contre leur utilisation frauduleuse, tout en portant des atteintes

78 *Ibid.*, points 35 à 45.

moins importantes aux droits reconnus par les articles 7 et 8 de la Charte que celles résultant de la méthode fondée sur les empreintes digitales[79].

La CJUE a fait valoir que l'article 4, paragraphe 3, du Règlement nº 2252/2004 précise expressément que les empreintes digitales ne peuvent être utilisées que dans le seul but de vérifier l'authenticité du passeport et l'identité de son titulaire, tandis que l'article 1er, paragraphe 2, dudit règlement ne prévoit pas le stockage des empreintes digitales excepté dans le passeport, lequel demeure la propriété exclusive de son seul titulaire. Le règlement n'envisage aucune base juridique pour le stockage centralisé des données collectées sur son fondement ou pour l'utilisation de ces dernières à d'autres fins que celle d'empêcher l'entrée illégale de personnes sur le territoire de l'Union[80]. Eu égard aux considérations qui précèdent, la CJUE a conclu que l'examen de la question posée par la juridiction de renvoi n'a pas révélé d'éléments de nature à affecter la validité de l'article 1er, paragraphe 2, du Règlement nº 2252/2004.

Relation entre la Charte et la CEDH

En dépit de leurs libellés différents, les conditions applicables aux limitations licites à l'exercice des droits prévues par l'article 52, paragraphe 1, de la Charte rappellent l'article 8, paragraphe 2, de la CEDH sur le droit au respect de la vie privée. Dans leur jurisprudence, la CJUE et la CouEDH renvoient souvent à leurs arrêts respectifs dans le cadre du dialogue constant qu'entretiennent les deux juridictions en vue de parvenir à une interprétation harmonieuse des règles relatives à la protection des données. Selon l'article 52, paragraphe 3, de la Charte, « [d]ans la mesure où la présente Charte contient des droits correspondant à des droits garantis par la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, leur sens et leur portée sont les mêmes que ceux que leur confère ladite convention ». L'article 8 de la Charte ne correspond toutefois pas directement à un article de la CEDH[81]. L'article 52, paragraphe 3, de la Charte traite du contenu et de la portée des droits protégés par chaque ordre juridique plutôt que des conditions de leur limitation. Cependant, vu le contexte plus large du dialogue et de la coopération entre les deux juridictions, la CJUE peut tenir compte, dans ses analyses, des

79 CJUE, C-291/12, *Michael Schwarz c. Stadt Bochum*, 17 octobre 2013, points 46 à 53.

80 *Ibid.*, points 56 à 61.

81 CEPD (2017), *Guide pour l'évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel*, Bruxelles, 11 avril 2017, p. 6.

critères de limitation licite énoncés à l'article 8 de la CEDH, tel qu'interprété par la CouEDH. Le scénario inverse par lequel la CouEDH peut faire référence aux conditions de limitation licite au titre de la Charte est également possible. En tout état de cause, il convient également de tenir compte du fait qu'il n'existe pas dans la CEDH d'équivalent parfait de l'article 8 de la Charte qui fasse référence à la protection des données à caractère personnel, et en particulier aux droits de la personne concernée, aux motifs légitimes du traitement et au contrôle par une autorité indépendante. Certains éléments de l'article 8 de la Charte peuvent être fondés sur la jurisprudence de la CouEDH concernant l'article 8 de la CEDH et la Convention 108[82]. Ce lien garantit que la CJUE et la CouEDH s'inspirent mutuellement en ce qui concerne les questions qui se rapportent à la protection des données.

1.3. Interaction avec d'autres droits et intérêts légitimes

Points clés

- Le droit à la protection des données interagit souvent avec d'autres droits, comme la liberté d'expression et la liberté de recevoir et de transmettre des informations.
- Cette interaction est souvent ambivalente : s'il existe des situations dans lesquelles le droit à la protection des données à caractère personnel crée des tensions avec un droit spécifique, il en existe d'autres où le droit à la protection des données à caractère personnel garantit effectivement le respect du même droit spécifique. C'est notamment le cas de la liberté d'expression, étant donné que le secret professionnel est un élément du droit au respect de la vie privée.
- Le besoin de protéger les droits et libertés d'autrui est l'un des critères utilisés pour évaluer la limitation licite du droit à la protection des données à caractère personnel.
- Lorsque différents droits sont concernés, les juridictions doivent les mettre en balance afin de les concilier.
- Le Règlement général sur la protection des données exige des États membres qu'ils concilient le droit à la protection des données à caractère personnel avec la liberté d'expression et d'information.
- Les États membres peuvent également adopter des règles spécifiques en droit national afin de concilier le droit à la protection des données à caractère personnel avec l'accès du public aux documents officiels et les obligations de secret professionnel.

82 Explications relatives à la Charte des droits fondamentaux (2007/C 303/02), p. 8.

Le droit à la protection des données à caractère personnel n'est pas un droit absolu et les conditions de la limitation licite de celui-ci ont été détaillées ci-dessus. L'un des critères applicables aux limitations licites des droits, reconnu par le droit de l'Union et du CdE, est le caractère nécessaire de l'ingérence dans la protection des données afin de protéger les droits et libertés d'autrui. Lorsque la protection des données interagit avec d'autres droits, la CouEDH et la CJUE ont toutes deux déclaré à maintes reprises qu'il est nécessaire de mettre en balance le droit à la protection des données avec d'autres droits aux fins de l'application et de l'interprétation de l'article 8 de la CEDH et de l'article 8 de la Charte[83]. Plusieurs exemples importants illustrent la manière dont cette mise en balance est réalisée.

Outre la mise en balance réalisée par ces juridictions, les États peuvent, si nécessaire, adopter une législation en vue de concilier le droit à la protection des données à caractère personnel avec d'autres droits. Pour cette raison, le Règlement général sur la protection des données prévoit plusieurs domaines de dérogation nationale.

Pour ce qui concerne la liberté d'expression, le RGPD exige des États membres qu'ils concilient, par la loi, « le droit à la protection des données à caractère personnel au titre du présent règlement avec le droit à la liberté d'expression et d'information, y compris le traitement à des fins journalistiques et à des fins d'expression universitaire, artistique ou littéraire »[84]. Les États membres peuvent aussi adopter des lois en vue de concilier la protection des données avec l'accès du public aux documents officiels et les obligations de secret professionnel protégées en tant que forme du droit au respect de la vie privée[85].

1.3.1. Liberté d'expression

Le droit à la liberté d'expression est l'un des droits qui interagit le plus avec le droit à la protection des données.

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

83 CouEDH, *Von Hannover c. Allemagne (nº 2)* [GC], nº 40660/08 et nº 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, point 48 ; CJUE, C-275/06, *Productores de Música de España (Promusicae) c. Telefónica de España SAU* [GC], 29 janvier 2008, point 68.

84 Règlement général sur la protection des données (RGPD), art. 85.

85 *Ibid.*, art. 86 et 90.

recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontières ». Conformément à l'article 11 de la Charte et à l'article 10 de la CEDH, la liberté d'information protège non seulement le droit de fournir des informations, mais également celui d'en *recevoir*.

Les limitations à la liberté d'expression doivent respecter les critères prévus à l'article 52, paragraphe 1, de la Charte, décrits plus haut. De plus, l'article 11 correspond à l'article 10 de la CEDH. Selon l'article 52, paragraphe 3, de la Charte, dans la mesure où la Charte 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 ». Ces droits couvrent, notamment, le droit au respect de la vie privée et le droit à la protection des données à caractère personnel.

La relation entre la protection des données à caractère personnel et la liberté d'expression est régie par l'article 85 du Règlement général sur la protection des données, intitulé « Traitements et liberté d'expression et d'information ». Selon cet article, les États membres doivent concilier le droit à la protection des données à caractère personnel et le droit à la liberté d'expression et d'information. En particulier, des exemptions et dérogations à des chapitres spécifiques du RGPD sont prévues à des fins journalistiques et à des fins d'expression universitaire, artistique ou littéraire, dans la mesure où elles sont nécessaires pour concilier le droit à la protection des données à caractère personnel et la liberté d'expression et d'information.

Exemple : dans l'affaire *Tietosuojavaltuutettu c. Satakunnan Markkinapörssi Oy et Satamedia Oy*[86], il était demandé à la CJUE de définir les rapports entre la protection des données et la liberté de la presse[87]. La Cour devait examiner

86 CJUE, C-73/07, *Tietosuojavaltuutettu c. Satakunnan Markkinapörssi Oy et Satamedia Oy* [GC], 16 décembre 2008, points 56, 61 et 62.

87 L'affaire portait sur l'interprétation de l'article 9 de la directive relative à la protection des données – aujourd'hui remplacé par l'article 85 du RGPD – qui énonçait ce qui suit : « Les États membres prévoient, pour les traitements de données à caractère personnel effectués aux seules fins de journalisme ou d'expression artistique ou littéraire, des exemptions et dérogations au présent chapitre, au chapitre IV et au chapitre VI dans la seule mesure où elles s'avèrent nécessaires pour concilier le droit à la vie privée avec les règles régissant la liberté d'expression ».

la diffusion par Markkinapörssi et Satamedia de données fiscales concernant plus de 1,2 million de personnes physiques, obtenues légalement auprès de l'administration fiscale finlandaise. L'autorité finlandaise de contrôle de la protection des données avait rendu une décision imposant à l'entreprise de cesser de diffuser ces données. L'entreprise a contesté cette décision devant une juridiction nationale, qui a demandé à la CJUE des éclaircissements sur l'interprétation à donner à la Directive relative à la protection des données. 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 à des fins exclusivement journalistiques. 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 interpréter l'article 9 de la directive (sur le traitement de données à caractère personnel et la liberté d'expression). Elle 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, comme celle du journalisme, devaient être interprétées de manière large. Elle a ensuite observé que, pour obtenir une pondération équilibrée entre ces 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.

La CouEDH a examiné la même affaire, après que la juridiction nationale a décidé, sur le fondement des orientations données par la CJUE, que l'ordre de l'autorité de contrôle de cesser la publication de toutes les informations fiscales constituait une ingérence justifiée dans la liberté d'expression de l'entreprise. La CouEDH a confirmé cette approche[88]. Elle a conclu que, bien

88 CouEDH, *Satakunnan Markkinapörssi Oy et Satamedia Oy c. Finlande* [GC], nº 931/13, 27 juin 2017.

qu'il y ait ingérence dans le droit des entreprises à fournir des informations, l'ingérence était prévue par la loi, poursuivait un but légitime et était nécessaire dans une société démocratique.

La Cour a rappelé les critères énoncés dans la jurisprudence qui devraient guider les autorités nationales et la CouEDH elle-même, lors de la mise en balance de la liberté d'expression et du droit au respect de la vie privée. Dans le cas d'un discours politique ou d'un débat sur des questions d'intérêt général, il n'y a guère de place pour des restrictions au droit de recevoir et de fournir des informations, le public ayant le droit d'être informé, un « droit qui est essentiel dans une société démocratique »[89]. Cependant, des articles de presse ayant pour seul objet de satisfaire la curiosité d'un certain lectorat sur les détails de la vie privée d'une personne ne sauraient passer pour contribuer à un quelconque débat d'intérêt général. La dérogation aux règles relatives à la protection des données à des fins journalistiques a pour but de permettre aux journalistes d'accéder à des données, de les collecter et de les traiter afin d'être en mesure d'exercer leurs activités journalistiques. Il existait donc effectivement un intérêt général à donner accès aux grandes quantités de données fiscales concernées et à permettre aux sociétés requérantes de les collecter et de les traiter. En revanche, la Cour a conclu qu'il n'y avait pas d'intérêt général à ce que la presse diffuse en masse de telles données brutes, telles quelles, sans aucun apport analytique. Les informations fiscales peuvent avoir permis à des membres du public curieux de classer des personnes dans des catégories en fonction de leur situation économique et donc de satisfaire les attentes d'un public friand de détails quant à la vie privée d'autrui. Ceci ne peut donc être considéré comme une contribution à un débat d'intérêt général.

Exemple : dans l'affaire *Google Spain*[90], la CJUE a examiné la question de savoir si Google était tenu de supprimer des informations obsolètes sur les difficultés financières du requérant de sa liste des résultats de recherche. Lorsqu'une recherche était menée sur le moteur de recherche Google en utilisant le nom du requérant, les résultats fournissaient des liens vers de vieux articles de presse mentionnant ses liens avec une procédure de faillite. Le requérant a estimé que cela portait atteinte à ses droits au respect de

89 *Ibid.*, para. 169.

90 CJUE, C-131/12, *Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 13 mai 2014, points 81 à 83.

la vie privée et à la protection des données à caractère personnel, étant donné que la procédure avait pris fin des années plus tôt, ce qui ôtait toute pertinence à ces références.

La Cour a d'abord précisé que les moteurs de recherche sur internet et les résultats de recherche fournissant des données à caractère personnel permettent d'établir un profil détaillé de la personne concernée. Compte tenu de la numérisation croissante de la société, l'exigence que les données à caractère personnel soient exactes et que leur publication n'aille pas au-delà de ce qui est nécessaire, c'est-à-dire informer le public, est essentielle pour garantir un niveau élevé de protection des données aux personnes concernées. Le « responsable du traitement doit assurer, dans le cadre de ses responsabilités, de ses compétences et de ses possibilités, que ce traitement satisfait aux exigences » du droit de l'UE, pour que les garanties prévues par celui-ci puissent développer leur plein effet. Cela signifie que le droit d'effacement de données à caractère personnel lorsque le traitement n'est plus nécessaire ou est dépassé couvre également les moteurs de recherche, qui ont été considérés comme étant les responsables du traitement et pas simplement des sous-traitants (voir section 2.3.1).

Sur la question de savoir si Google était tenu de supprimer les liens relatifs au requérant, la CJUE a conclu que, dans certaines conditions, les personnes concernées ont le droit d'obtenir l'effacement de leurs données à caractère personnel des résultats de recherche d'un moteur de recherche sur internet. Ce droit peut être invoqué lorsque les informations relatives à une personne sont inexactes, inadéquates, non pertinentes ou excessives aux fins du traitement des données. La CJUE a reconnu que ce droit n'est pas absolu et qu'il doit être mis en balance avec d'autres droits, en particulier l'intérêt et le droit du public à avoir accès aux informations. Chaque demande d'effacement doit être appréciée au cas par cas afin de trouver un équilibre entre les droits fondamentaux à la protection des données à caractère personnel et au respect de la vie privée de la personne concernée, d'une part, et les intérêts légitimes de tous les utilisateurs d'internet, d'autre part. La Cour a fourni des orientations sur les facteurs à prendre en considération dans cet exercice de mise en balance. La nature de l'information en cause est un facteur particulièrement important. Si l'information est sensible pour la vie privée de la personne concernée et qu'il n'y a pas d'intérêt général à rendre cette information publique, la protection des données et le respect de la vie privée l'emporteront sur le droit du public d'avoir accès à cette information.

En revanche, s'il appert que la personne concernée est une personnalité publique ou que l'information est de nature à justifier l'octroi de l'accès du public à ces informations, l'ingérence avec les droits fondamentaux à la protection des données et au respect de la vie privée est justifié.

À la suite de cet arrêt, le Groupe de travail « Article 29 » a adopté des lignes directrices sur la mise en œuvre de l'arrêt rendu par la Cour. Celles-ci incluent une liste de critères communs que les autorités de contrôle doivent utiliser lorsqu'elles examinent des plaintes relatives à des demandes d'effacement émanant de particuliers et qui les guideront dans cet exercice de mise en balance des droits[91].

La CouEDH a rendu plusieurs arrêts qui font autorité sur la conciliation du droit à la protection des données avec le droit à la liberté d'expression.

Exemple : dans l'affaire *Axel Springer AG c. Allemagne*[92], 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 enfreignait 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 :

- l'événement auquel l'article publié est consacré est-il d'intérêt général ?
- la personne concernée est-elle une personne publique ?
- comment les informations ont-elles été obtenues et sont-elles fiables ?

La CouEDH a conclu que l'arrestation et la condamnation de l'acteur étaient un fait judiciaire public et revêtait donc un intérêt général, que l'acteur était suffisamment célèbre pour être qualifié de personne publique et que les informations avaient été fournies par le bureau du procureur et que leur exactitude n'était pas contestée par les parties. Par conséquent, les restrictions à la publication imposées à la société n'étaient pas

91 Groupe de travail « Article 29 » (2014), *Lignes directrices sur la mise en œuvre de l'arrêt de la CJUE sur « Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos (AEPD) et Mario Costeja González » (C-131/12)*, WP 225, Bruxelles, 26 novembre 2014.

92 CouEDH, *Axel Springer AG c. Allemagne* [GC], nº 39954/08, 7 février 2012, paras. 90 et 91.

raisonnablement proportionnées envers le 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 : l'affaire *Coudec et Hachette Filipacchi Associés c. France*[93] concernait la publication par un hebdomadaire français d'une interview de M^me^ Coste, qui prétendait que le Prince Albert de Monaco était le père de son fils. L'interview décrivait également la relation de M^me^ Coste avec le prince et la manière dont il avait réagi à la naissance de l'enfant et était accompagné de photographies du prince avec l'enfant. Le Prince Albert a intenté une action contre la société éditrice pour violation de son droit à la protection de la vie privée. Les juridictions françaises ont conclu que la publication de l'article avait causé un préjudice irréversible au Prince Albert et ont condamné la société éditrice au versement de dommages-intérêts et à la publication de la condamnation en couverture du magazine.

La société éditrice du magazine a porté l'affaire devant la CouEDH, en alléguant que l'arrêt des juridictions françaises constituait une ingérence injustifiée dans leur droit à la liberté d'expression. La CouEDH a dû mettre en balance le droit du Prince Albert au respect de la vie privée avec le droit à la liberté d'expression de la société éditrice et le droit du public à être informé. Le droit de M^me^ Coste de faire connaître son histoire au public et l'intérêt de l'enfant à faire établir officiellement une relation filiale étaient également des éléments importants à prendre en considération.

La CouEDH a conclu que la publication de l'interview constituait une immixtion dans la vie privée du prince et a ensuite examiné si celle-ci était nécessaire. Elle a considéré que la publication concernait une personne publique et une question d'intérêt général, étant donné que les citoyens monégasques avaient un intérêt à être informés de l'existence d'un enfant du prince car le devenir d'une monarchie héréditaire est « intrinsèquement lié à l'existence d'une descendance » et éveille donc l'intérêt du public[94]. La Cour a également observé que l'article avait permis à M^me^ Coste et à son enfant d'exercer leur droit à la liberté d'expression. Les juridictions nationales n'avaient pas dûment pris en compte les principes et critères établis par la jurisprudence de la CouEDH aux fins de la mise en balance du droit au respect de la vie

93 CouEDH, *Coudec et Hachette Filipacchi Associés c. France* [GC], nº 40454/07, 10 novembre 2015.

94 *Ibid.*, paras. 104 à 116.

privée et du droit à la liberté d'expression. Elle a conclu que la France avait violé l'article 10 de la CEDH sur la liberté d'expression.

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*[95], un hebdomadaire national avait publié des photographies intimes du requérant, une personnalité connue qui a ensuite intenté une action au civil contre la société éditrice et s'est vu octroyer des dommages-intérêts. En dépit de l'octroi d'une indemnisation financière, le requérant a affirmé avoir été victime d'une violation de son droit au respect de la vie privée, 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'obligation de notification préalable de la publication par le journal.

La CouEDH a fait valoir que bien que la divulgation de ce type d'information eut poursuivi généralement un but de divertissement et non d'éducation, elle bénéficiait 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 *Bohlen c. Allemagne*[96], le requérant, un chanteur et producteur artistique célèbre, avait publié une autobiographie et a ensuite été contraint d'en retirer certains passages à la suite de plusieurs décisions de justice. L'histoire a été largement couverte par les médias nationaux

95 CouEDH, *Mosley c. Royaume-Uni*, nº 48009/08, 10 mai 2011, paras. 129 et 130.

96 CouEDH, *Bohlen c. Allemagne*, nº 53495/09, 19 février 2015, paras. 45 à 60.

et une société du secteur du tabac a lancé une campagne publicitaire humoristique faisant référence à cet événement, en utilisant le prénom du requérant sans son consentement. Le requérant a vainement tenté d'obtenir un dédommagement de l'agence de publicité en invoquant une violation de ses droits au titre de l'article 8 de la CEDH. La CouEDH a rappelé les critères pertinents régissant la mise en balance du droit au respect de la vie privée et du droit à la liberté d'expression et a conclu à l'absence de violation de l'article 8. Le requérant était un personnage public et la publicité ne faisait pas référence aux détails de sa vie privée, mais à un événement public qui avait déjà été couvert par les médias et s'inscrivait dans un débat public. En outre, la publicité était humoristique et ne contenait rien de dégradant ou de négatif à l'égard du requérant.

Exemple : dans l'affaire *Biriuk c. Lituanie*[97], la requérante a soutenu devant la CouEDH que la Lituanie avait failli à son obligation d'assurer le respect de sa vie privée au motif que, bien qu'une atteinte grave à sa vie privée eût été commise par un grand quotidien, les juridictions nationales statuant sur l'affaire ne lui avaient accordé qu'un montant dérisoire à titre de dommages-intérêts. Lors de la détermination des dommages-intérêts pour préjudice moral, les tribunaux nationaux ont appliqué les dispositions du droit national sur la diffusion d'informations au public, qui plafonnait le montant de dommages-intérêts pour préjudice moral causé par la diffusion illicite au public par les médias d'informations sur la vie privée d'une personne. L'affaire concernait la publication par le principal quotidien lituanien d'un article publié en une sur la séropositivité de la requérante. L'article critiquait également le comportement de la requérante et mettait en cause ses mœurs.

La CouEDH a rappelé que la protection des données à caractère personnel et surtout des données médicales revêt une importance fondamentale pour le droit au respect de la vie privée au titre de la CEDH. La confidentialité des données relatives à la santé est particulièrement importante, étant donné que la divulgation de données médicales (la séropositivité de la requérante en l'espèce) peut affecter gravement la vie privée et familiale d'une personne, son emploi et son intégration dans la société. La Cour a attaché une importance particulière au fait que, selon l'article de presse, des membres du personnel médical de l'hôpital avaient fourni des informations sur la séropositivité de la requérante en violation flagrante de leur obligation de

97 CouEDH, *Biriuk c. Lituanie*, nº 23373/03, 25 novembre 2008.

secret médical. Il n'y a donc pas eu ingérence légitime dans le droit à la vie privée de la requérante.

L'article a été publié par la presse et la liberté d'expression est également un droit fondamental garanti par la CEDH. Cependant, en examinant la question de savoir si l'existence d'un intérêt général justifiait la publication de ce type d'information sur la requérante, la Cour a conclu que l'objectif principal de la publication était d'augmenter les ventes du journal en satisfaisant la curiosité des lecteurs. Pareil objectif ne pouvait pas être considéré comme contribuant à un quelconque débat d'intérêt général pour la société. Dans un cas aussi « flagrant d'abus de la liberté de la presse », les restrictions sévères imposées par la loi pour réparer le préjudice subi et le montant dérisoire octroyé pour préjudice moral signifiaient que la Lituanie avait failli à son obligation positive de protéger le droit à la vie privée de la requérante. La Cour a conclu qu'il y avait eu violation de l'article 8 de la CEDH.

Le droit à la liberté d'expression et le droit à la protection des données à caractère personnel ne sont pas toujours contradictoires. Dans certains cas, la protection effective des données à caractère personnel garantit la liberté d'expression.

Exemple : dans l'affaire *Tele2 Sverige*, la CJUE a déclaré que l'ingérence causée par la Directive 2006/24 (Directive relative à la conservation des données) envers les droits fondamentaux consacrés aux articles 7 et 8 de la Charte était « d'une vaste ampleur et doit être considérée comme particulièrement grave. La circonstance que la conservation des données est effectuée sans que les abonnés ou les utilisateurs des services de communication électronique en soient informés est susceptible de générer dans l'esprit des personnes concernées le sentiment que leur vie privée fait l'objet d'une surveillance constante ». La Cour a également conclu que la conservation généralisée des données de trafic et de localisation pouvait avoir une incidence sur l'utilisation des communications électroniques et « en conséquence, sur l'exercice par ces derniers de leur liberté d'expression, garantie par l'article 11 de la Charte »[98]. En ce sens, en exigeant des garanties

98 CJUE, affaires jointes C-203/15 et C-698/15, *Tele2 Sverige AB c. Post- och telestyrelsen* et *Secretary of State for the Home Department* c. *Tom Watson et autres* [GC], 21 décembre 2016, points 37 et 101 ; CJUE, affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources et autres* et *Kärntner Landesregierung et autres* [GC], 8 avril 2014, point 28.

strictes que la conservation des données ne sera pas généralisée, les règles relatives à la protection des données contribuent en fait à l'exercice de la liberté d'expression.

S'agissant du droit de recevoir des informations, qui fait également partie de la liberté d'expression, on observe une prise de conscience croissante de l'importance de la transparence du gouvernement pour le fonctionnement d'une société démocratique. La transparence est un objectif d'intérêt général qui pourrait justifier une ingérence avec le droit à la protection des données, si elle est nécessaire et proportionnée, comme l'explique la section 1.2. Au cours des vingt dernières années, le droit d'accès aux documents détenus par des autorités publiques a donc été reconnu comme un droit important de tout citoyen de l'UE et de toute personne physique résidant dans un État membre ou de toute personne morale y ayant son siège.

Conformément au droit du CdE, les principes consacrés dans la Recommandation relative à l'accès aux documents publics, qui a servi de source d'inspiration aux auteurs de la Convention sur l'accès aux documents publics (Convention 205) peuvent être invoqués[99].

Dans le droit de l'UE, le droit d'accès aux documents est garanti par le Règlement nº 1049/2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission (Règlement sur l'accès aux documents)[100]. 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, organismes de l'Union, quel que soit leur support ».

Ce droit peut entrer en conflit avec le droit à la protection des données si l'accès à un document conduit à révéler des données à caractère personnel d'autrui. L'article 86 du Règlement général sur la protection des données prévoit clairement que les données à caractère personnel figurant dans des documents officiels détenus par une autorité publique ou par un organisme public peuvent être communiquées par ladite autorité ou ledit organisme conformément au droit de l'Union[101] ou au droit d'un État

99 CdE, Comité des Ministres (2002), Recommandation R (81) 19 et Recommandation Rec(2002)2 aux États membres sur l'accès aux documents publics, 21 février 2002 ; CdE, Convention sur l'accès aux documents publics, STCE nº 205, 18 juin 2009. Cette convention n'est pas encore entrée en vigueur.

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

101 Charte des droits fondamentaux, art. 42, TFUE, art. 15, para. 3 et Règlement nº 1049/2001.

membre afin de concilier le droit d'accès du public aux documents officiels et le droit à la protection des données à caractère personnel au titre du règlement.

Les demandes d'accès aux documents ou aux 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 *Volker und Markus Schecke et Hartmut Eifert c. Land Hessen*[102], la CJUE a été amenée à se prononcer sur la proportionnalité de la publication, imposée par la législation de l'UE, du nom des bénéficiaires de subventions agricoles de l'UE et des montants perçus. La publication visait à accroître la transparence et à contribuer au contrôle public de la bonne utilisation des fonds publics par l'administration. Plusieurs bénéficiaires ont contesté la proportionnalité de cette publication.

La CJUE, notant que le droit à la protection des données n'est pas une prérogative absolue, a fait valoir que la publication sur un site internet des données nominatives relatives aux bénéficiaires de deux fonds d'aide agricole de l'UE et des montants précis perçus par ceux-ci constitue une ingérence dans leur vie privée, en général, et dans la protection des données à caractère personnel les concernant, en particulier.

La CJUE a conclu que cette ingérence dans les droits garantis par les 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 savoir accroître la transparence de l'utilisation des fonds communautaires. La Cour a toutefois considéré que la publication des noms des personnes physiques bénéficiaires d'aides agricoles de l'UE provenant de ces deux fonds ainsi que des montants précis perçus par celles-ci constituait une mesure disproportionnée et n'était pas justifiée au regard de l'article 52, paragraphe 1, de la Charte. Elle a reconnu l'importance, dans une société démocratique, d'informer les contribuables de l'utilisation des fonds publics. Cependant, étant donné qu'« aucune prééminence automatique ne saurait être reconnue à l'objectif de transparence sur le droit à la protection des données à caractère personnel »[103], les institutions

102 CJUE, affaires jointes C-92/09 et C-93/09, *Volker und Markus Schecke GbR et Hartmut Eifert c. Land Hessen* [GC], 9 novembre 2010, points 47-52, 66, 67, 75, 86 et 92.

103 *Ibid*. point 85.

de l'UE étaient tenues de mettre en balance l'intérêt de l'Union à garantir la transparence et l'atteinte à l'exercice des droits au respect de la vie privée et à la protection des données que les bénéficiaires ont subie du fait de la publication.

La CJUE a considéré que les institutions de l'UE n'avaient pas correctement mené cet exercice de pondération, étant donné qu'il était possible d'envisager des mesures qui affecteraient moins négativement les droits fondamentaux des personnes physiques, tout en contribuant également efficacement à l'objectif de transparence poursuivi par la publication. À titre d'exemple, plutôt qu'une publication générale concernant tous les bénéficiaires et mentionnant leur nom et les montants précis perçus par chacun, une distinction pourrait être opérée selon des critères pertinents, tels que les périodes pendant lesquelles ils ont perçu l'aide, la fréquence ou encore le type et l'importance de celle-ci[104]. La CJUE a donc déclaré partiellement invalide la législation de l'UE relative à la publication d'informations concernant les bénéficiaires des fonds agricoles européens.

Exemple : dans l'affaire *Rechnungshof c. Österreichischer Rundfunk et autres*[105], la CJUE a examiné la compatibilité de certaines lois autrichiennes avec le droit de l'UE en matière de protection des données. La législation imposait qu'un organisme public collecte et transmette des données sur les revenus afin de publier le nom et les revenus des agents de diverses entités publiques dans un rapport annuel accessible au grand public. Certaines personnes ont refusé de communiquer leurs données en invoquant le droit à la protection des données.

Dans son avis, la CJUE a invoqué la protection des droits fondamentaux en tant que principe général du droit de l'Union et l'article 8 de la CEDH, rappelant que la Charte n'était pas contraignante à cette époque. Elle a déclaré que la collecte de données relatives aux revenus professionnels d'une personne physique, et en particulier leur communication à des tiers, relève du champ d'application du droit au respect de la vie privée et constitue une violation de ce droit. Cette ingérence pourrait être justifiée si elle avait été prévue par la loi, avait poursuivi un but légitime et avait été nécessaire

104 *Ibid.* point 89.

105 CJUE, C-465/00, C-138/01 et C-139/09, *Rechnungshof c. Österreichischer Rundfunk et autres* et *Christa Neukomm et Joseph Lauermann c. Österreichischer Rundfunk*, 20 mai 2003.

pour atteindre ce but dans une société démocratique. La Cour a relevé que la législation autrichienne poursuivait un but légitime, étant donné qu'elle visait à maintenir les salaires des salariés du secteur public dans des limites raisonnables, une considération également liée au bien-être économique du pays. Toutefois, l'intérêt de l'Autriche à garantir la meilleure utilisation des fonds publics devait être mis en balance avec la gravité de l'ingérence dans le droit au respect de la vie privée des personnes concernées.

Tout en laissant à la juridiction nationale le soin de déterminer si la publication des données relatives aux revenus des personnes physiques était nécessaire et proportionnée par rapport au but poursuivi par la législation, la CJUE a invité la juridiction nationale à examiner si pareil but n'aurait pas pu être atteint aussi efficacement par des moyens moins intrusifs. Un exemple serait la communication des données à caractère personnel uniquement aux organismes publics de contrôle plutôt qu'au grand public.

Dans des affaires ultérieures, il est devenu évident que la mise en balance de la protection des données et de l'accès aux documents requiert une analyse approfondie au cas par cas. Aucun de ces droits ne peut prévaloir automatiquement sur l'autre. La CJUE a eu l'occasion d'interpréter le droit à l'accès à des documents contenant des données à caractère personnel dans deux affaires.

Exemple : dans l'affaire *Commission européenne c. Bavarian Lager*[106], la CJUE a défini l'étendue de la protection des données à caractère personnel dans le contexte de l'accès aux documents des institutions de l'UE, ainsi que le rapport entre le Règlement nº 1049/2001 (Règlement relatif à l'accès aux documents) et le Règlement nº 45/2001 (Règlement relatif à la protection des données des institutions de l'UE). La société Bavarian Lager, créée en 1992, importait de la bière allemande en bouteille au Royaume-Uni, essentiellement pour des pubs et des bars. Elle a toutefois rencontré des difficultés parce que la législation britannique favorisait *de facto* les producteurs nationaux. En réponse à la plainte de Bavarian Lager, la Commission européenne a engagé 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 de l'Union. Bavarian Lager a ensuite demandé à la Commission, entre autres documents, une copie

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

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 une nouvelle demande 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 des institutions de l'UE.

N'étant pas satisfaite par cette position, Bavarian Lager a formé un recours devant le Tribunal de première instance. Celui-ci a annulé la décision de la Commission par son arrêt du 8 novembre 2007 (affaire T-194/04, *The Bavarian Lager Co. Ltd c. Commission des Communautés européennes*), considérant en particulier que la simple inscription des noms des personnes 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 formé par la Commission, la CJUE a annulé l'arrêt du Tribunal de première instance. La Cour 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 du Règlement relatif à la protection des données des institutions de l'UE deviennent intégralement applicables. La Cour 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 de consentement des cinq participants à cette réunion, la Commission s'est soumise à suffisance à son obligation de transparence 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 afin de démontrer la nécessité du transfert de ces données personnelles, la Commission n'a pas

pu mettre en balance les différents intérêts des parties en cause. Elle ne pouvait pas non plus vérifier s'il n'existait aucune raison de penser que ce transfert pourrait porter atteinte aux intérêts légitimes des personnes concernées », comme le prescrit le Règlement relatif à la protection des données des institutions de l'UE.

Exemple : dans l'affaire *Client Earth et PAN Europe c. EFSA*[107], la CJUE a examiné la question de savoir si la décision de l'Autorité européenne de sécurité des aliments (EFSA) de refuser à des demandeurs le plein accès à des documents était nécessaire pour protéger les droits au respect de la vie privée et à la protection des données des personnes concernées par les documents. Ces derniers portaient sur un projet de rapport d'orientation élaboré par un groupe de travail de l'EFSA en collaboration avec des experts externes sur la mise sur le marché de produits phytopharmaceutiques. Au départ, l'EFSA a accordé un accès partiel aux demandeurs et refusé l'accès à certaines versions de travail du projet de document d'orientation. Ensuite, elle a accordé l'accès à la version du projet incluant les observations individuelles des experts externes. Elle a toutefois occulté le nom des experts, en invoquant l'article 4, paragraphe 1, point b), du Règlement nº 45/2001 concernant le traitement de données à caractère personnel par les institutions et organes de l'UE et la nécessité de protéger la vie privée des experts externes. En première instance, le Tribunal de l'UE a confirmé la décision de l'EFSA.

Sur pourvoi formé par les requérantes, la CJUE a annulé l'arrêt rendu en première instance. Elle a conclu que, dans cette affaire, le transfert de données à caractère personnel était nécessaire pour s'assurer de l'impartialité de chacun des experts externes dans l'exercice de leur mandat de scientifiques et garantir la transparence du processus décisionnel de l'EFSA. Selon la Cour, l'EFSA n'a pas précisé en quoi la divulgation du nom des experts externes ayant formulé des observations spécifiques sur le projet d'orientation porterait préjudice aux intérêts légitimes des experts. Un argument général affirmant que la divulgation est de nature à porter atteinte à la vie privée n'est pas suffisant, s'il n'est pas étayé par des preuves spécifiques à chaque cas d'espèce.

107 CJUE, C-615/13 P, *ClientEarth, Pesticide Action Network Europe (PAN Europe) c. Autorité européenne de sécurité des aliments (EFSA), Commission européenne*, 16 juillet 2015.

Selon ces arrêts, une ingérence dans le droit à la protection des données dans le contexte 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[108].

Cette approche est similaire à celle suivie par la CouEDH à l'égard du respect de la vie privée et de l'accès aux documents, comme le montre l'arrêt suivant. Dans l'arrêt *Magyar Helsinki*, la CouEDH a déclaré que l'article 10 ne reconnaît pas un droit individuel d'accès aux informations détenues par une autorité publique et n'oblige pas le gouvernement à transmettre ces informations à l'individu. Toutefois, ce droit ou cette obligation pourrait naître : premièrement, lorsque la divulgation des informations est imposée par une décision judiciaire ayant acquis force de loi ; deuxièmement, lorsqu'un accès à l'information est indispensable à l'exercice du droit à la liberté d'expression d'un individu, en particulier la liberté de recevoir et de transmettre des informations, et lorsque le refus d'accès constituerait une ingérence dans ce droit[109]. La question de savoir si et dans quelle mesure le refus de donner accès à des informations constitue une ingérence dans l'exercice par un requérant du droit à la liberté d'expression doit s'apprécier au cas par cas et à la lumière des circonstances particulières de la cause, en particulier : i) le but de la demande d'information, ii) la nature des informations recherchées, iii) le rôle du requérant, et iv) le point de savoir si les informations sont déjà disponibles.

Exemple : dans l'affaire *Magyar Helsinki Bizottság c. Hongrie*[110], la requérante, une ONG de défense des droits de l'homme, a demandé des informations à la police concernant le travail d'avocats commis d'office afin de réaliser une étude sur le fonctionnement du système de commission d'office en Hongrie. La police a refusé de fournir les informations demandées, alléguant qu'elles constituaient des données à caractère personnel non soumises à l'obligation de divulgation. Sur la base des principes susvisés, la CouEDH a conclu qu'il y avait eu ingérence dans l'exercice d'un droit protégé par l'article 10. Plus précisément, la requérante souhaitait exercer le droit de communiquer des informations sur un sujet d'intérêt public, sollicitait l'accès aux informations à cette fin et les informations étaient nécessaires aux fins de l'exercice de

108 Voir, toutefois, le détail des délibérations dans 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.

109 CouEDH, *Magyar Helsinki Bizottság c. Hongrie* [GC], nº 18030/11, 8 novembre 2016, para. 148.

110 *Ibid.*, paras. 181 et 187 à 200.

son droit à la liberté d'expression. Les informations relatives à la commission d'office des avocats revêtaient un intérêt pour le public. Il n'y avait pas de raison de douter que l'étude en question renfermait des informations du type de celles que la requérante avait entrepris de communiquer au public et que celui-ci avait le droit de recevoir. La Cour a estimé établi que la requérante avait besoin d'accéder aux informations demandées pour accomplir cette tâche. Enfin, les informations en question étaient déjà disponibles.

La CouEDH a conclu que le refus de donner accès à des informations dans cette affaire avait porté atteinte à l'essence même de la liberté de recevoir des informations. En tirant cette conclusion, elle a notamment analysé la finalité des informations demandées et leur contribution à un important débat public, la nature des informations sollicitées et si elles présentaient un intérêt public, ainsi que le rôle joué par la requérante dans la société.

Dans sa motivation, la Cour a observé que l'étude entreprise par l'ONG concernait le fonctionnement de la justice et le droit à un procès équitable, qui est un droit d'importance primordiale dans la CEDH. Étant donné que les informations demandées ne portaient pas sur des données se trouvant hors du domaine public, le droit au respect de la vie privée des personnes concernées (les avocats commis d'office) n'aurait pas été enfreint si la police avait donné à la requérante un accès aux informations. Les informations demandées par la requérante étaient de nature statistique et concernaient le nombre de fois où l'avocat commis d'office avait été désigné pour représenter des défendeurs dans des procédures pénales publiques.

Selon la Cour, étant donné que l'étude visait à contribuer à un important débat sur une question d'intérêt général, toute restriction à la démarche de l'ONG de publier l'étude en question aurait dû faire l'objet d'un contrôle minutieux. Les informations en question étaient d'intérêt public, celui-ci couvrant les « questions qui sont susceptibles de créer une forte controverse, qui portent sur un thème social important, ou qui ont trait à un problème dont le public aurait intérêt à être informé »[111]. Il couvrirait donc certainement une discussion sur la conduite de la justice et de procès équitables, qui était le sujet de l'étude de la requérante. Mettant en balance les différents droits en question et appliquant le principe de la proportionnalité, la CouEDH a conclu

111 *Ibid.*, para. 156.

à une violation injustifiée des droits de la requérante au titre de l'article 10 de la CEDH.

1.3.2. Secret professionnel

En droit national, certaines communications peuvent être soumises à une obligation de secret professionnel. Le secret professionnel peut s'entendre comme un devoir éthique spécial impliquant une obligation juridique inhérente à certaines professions et fonctions, fondée sur la confiance et la loyauté. Les personnes et les institutions qui remplissent ces fonctions sont tenues de ne pas révéler les informations confidentielles qu'elles reçoivent dans l'exercice de leur travail. Le secret professionnel s'applique surtout à la profession médicale et à la relation avocat-client, de nombreuses juridictions admettant également une obligation de secret professionnel dans le secteur financier. Tout en n'étant pas un droit fondamental, le secret professionnel est néanmoins protégé comme une forme du droit au respect de la vie privée. La CJUE a par exemple déclaré que, dans certains cas, « il peut en effet être nécessaire d'interdire la divulgation de certaines informations qualifiées de confidentielles, afin de préserver le droit fondamental d'une entreprise au respect de la vie privée, consacré à l'article 8 de la convention de sauvegarde des droits de l'homme et des libertés fondamentales [...] et à l'article 7 de la charte »[112]. La CouEDH a également été amenée à se prononcer sur la question de savoir si des restrictions imposées au secret professionnel constituent une violation de l'article 8 de la CEDH, comme en témoignent les exemples suivants.

Exemple : dans l'affaire *Pruteanu c. Roumanie*[113], le requérant était l'avocat d'une société commerciale interdite d'opérations bancaires à la suite d'accusations de fraude. Durant l'enquête, les juridictions roumaines autorisèrent le ministère public à intercepter et à enregistrer les conversations téléphoniques d'un associé de la société pendant un certain temps. Les enregistrements et les interceptions incluaient ses communications avec son avocat.

M. Pruteanu a dénoncé une ingérence dans son droit au respect de sa vie privée et de sa correspondance. Dans son arrêt, la CouEDH a souligné le rôle et l'importance de la relation entre un avocat et son client. L'interception des

112 CJUE, T-462/12 R, *Pilkington Group Ltd c. Commission européenne*, ordonnance du président du Tribunal, 11 mars 2013, point 44.

113 CouEDH, *Pruteanu c. Roumanie*, nº 30181/05, 3 février 2015.

conversations entre un avocat et son client a indéniablement violé le secret professionnel, qui est le fondement de la relation entre ces deux personnes. En pareil cas, l'avocat était également en droit de dénoncer une ingérence dans son droit au respect de la vie privée et de la correspondance. La Cour a considéré qu'il y avait eu violation de l'article 8 de la CEDH.

Exemple : dans l'affaire *Brito Ferrinho Bexiga Villa-Nova c. Portugal*[114], la requérante, une avocate, a refusé de présenter les relevés de son compte bancaire personnel à l'administration fiscale en invoquant les secrets professionnel et bancaire. Le parquet a ouvert une enquête pour fraude fiscale et a demandé la levée du secret professionnel. La juridiction nationale a ordonné la levée des secrets professionnel et bancaire, considérant que l'intérêt public devait primer sur les intérêts privés de la requérante.

Lorsque l'affaire fut portée devant la CouEDH, celle-ci a considéré que l'accès aux relevés bancaires de la requérante constituait une ingérence dans son droit au respect du secret professionnel, lequel est inclus dans la notion de vie privée. L'ingérence avait un fondement juridique, dans la mesure où il était basé sur le code de procédure pénale et poursuivait un but légitime. Cependant, lors de l'examen de la nécessité et de la proportionnalité de l'ingérence, la Cour a fait valoir que la procédure visant la levée du secret professionnel s'était déroulée sans que la requérante y participe ou en ait connaissance. La requérante n'a donc pas pu présenter ses arguments. En outre, bien que la législation nationale prévoie la consultation de l'ordre des avocats dans le cadre d'une telle procédure, celui-ci n'a pas été sollicité. Enfin, la requérante n'a pas eu la possibilité de contester effectivement la levée du secret professionnel ni d'utiliser une autre voie de recours pour contester la mesure. Eu égard à l'absence de garanties procédurales et d'un contrôle juridictionnel effectif de la mesure de levée du secret professionnel, la CouEDH a conclu à une violation de l'article 8 de la CEDH.

L'interaction entre le secret professionnel et la protection des données est souvent ambivalente. D'une part, les règles et garanties relatives à la protection des données inscrites dans la législation contribuent à assurer le secret professionnel. Ainsi en est-il des règles imposant aux responsables du traitement et aux sous-traitants de mettre en œuvre des mesures solides pour assurer la sécurité des données

114 CouEDH, *Brito Ferrinho Bexiga Villa-Nova c. Portugal*, nº 69436/10, 1er décembre 2015.

afin d'éviter, entre autres choses, la perte de confidentialité des données personnelles protégées par le secret professionnel. De plus, le Règlement général sur la protection des données permet le traitement des données relatives à la santé, qui constituent des catégories particulières de données à caractère personnel méritant une protection renforcée, mais le subordonne à la mise en place de mesures adéquates et spécifiques destinées à préserver les droits des personnes concernées, en particulier le secret professionnel[115].

D'autre part, les obligations de secret professionnel imposées aux responsables du traitement et aux sous-traitants pour certaines données à caractère personnel peuvent limiter les droits des personnes concernées, notamment celui de recevoir des informations. Bien que le RGPD contienne une longue liste des informations qui doivent, en principe, être fournies à la personne concernée lorsque les données à caractère personnel n'ont pas été collectées auprès d'elle, cette exigence de divulgation ne s'applique pas lorsque les données à caractère personnel doivent rester confidentielles en vertu d'une obligation de secret professionnel réglementée par le droit de l'Union ou le droit des États membres[116].

Le Règlement général sur la protection des données permet aux États membres d'adopter, par la voie législative, des règles spécifiques afin de protéger les obligations de secret professionnel ou d'autres obligations de secret équivalentes et de concilier le droit à la protection des données à caractère personnel et l'obligation de secret professionnel[117].

Le RGPD dispose que les États membres peuvent adopter des règles spécifiques sur les pouvoirs des autorités de contrôle à l'égard des responsables du traitement ou des sous-traitants qui sont soumis à une obligation de secret professionnel. Ces règles spécifiques concernent le pouvoir d'obtenir l'accès aux locaux du responsable du traitement ou d'un sous-traitant, à son matériel de traitement des données et aux données à caractère personnel qu'il détient, lorsque ces données ont été collectées dans le cadre d'une activité couverte par le secret professionnel. Par conséquent, les autorités de contrôle chargées de la protection des données doivent respecter les obligations de secret professionnel qui lient les responsables du traitement et les sous-traitants. De plus, les membres des autorités de contrôle sont eux-mêmes soumis au secret professionnel dans l'exercice de leur mandat et après la fin

115 RGPD, art. 9, para. 2, point h), et art. 9, para. 3.

116 *Ibid.*, art. 14, para. 5, point d).

117 *Ibid.*, considérant 164 et art. 90.

de celui-ci. Dans l'exercice de leurs missions, les membres et les agents des autorités de contrôle peuvent avoir connaissance d'informations confidentielles. L'article 54, paragraphe 2, du règlement prévoit clairement qu'ils sont soumis au secret professionnel concernant ces informations confidentielles.

Le RGPD exige que les États membres notifient à la Commission les règles qu'ils adoptent pour concilier la protection des données et les principes établis par le règlement en ce qui concerne le secret professionnel.

1.3.3. Liberté de religion et de conviction

La liberté de religion et de conviction est protégée par l'article 9 de la CEDH (liberté de pensée, de conscience et de religion) et par l'article 10 de la Charte des droits fondamentaux de l'UE. Les données à caractère personnel qui révèlent des convictions religieuses ou philosophiques sont considérées comme des « données sensibles » tant dans le droit de l'Union que dans le droit du CdE et leur traitement et utilisation font l'objet d'une protection renforcée.

Exemple : le requérant dans l'affaire *Sinan Işık c. Turquie*[118] était membre de la communauté religieuse alévie, dont la confession est influencée par le soufisme et d'autres croyances préislamiques et est considérée par certains penseurs comme une religion à part entière, alors que pour d'autres, elle fait partie de l'islam. Le requérant a introduit une plainte fondée sur le fait que, contre sa volonté, sa carte d'identité contient une rubrique consacrée à la religion où figure la mention « islam » plutôt qu'« alévi ». Les juridictions nationales ont rejeté sa demande de changer la mention sur sa carte d'identité en « alévi » au motif que ce terme désigne un sous-groupe de l'islam et non une religion distincte. Il a ensuite porté l'affaire devant la CouEDH, en dénonçant le fait qu'il avait été contraint de divulguer sa foi, sans son consentement, au motif qu'il est obligatoire d'indiquer sa religion sur la carte d'identité, en violation de son droit à la liberté de religion et de conscience, étant donné en particulier que la mention « islam » sur sa carte d'identité était inexacte.

La CouEDH a rappelé que la liberté de religion implique la liberté de manifester sa religion de manière collective, en public et dans le cercle de

118 CouEDH, *Sinan Işık c. Turquie*, nº 21924/05, 2 février 2010.

ceux dont on partage la foi, mais aussi individuellement et en privé. La législation nationale applicable au moment des faits obligeait les individus à porter une carte d'identité sur laquelle figurait leur religion, ce document devant être présenté à la demande d'une administration publique ou d'une entreprise privée. Pareille obligation ne reconnaissait pas que le droit de manifester sa religion conférait également le droit inverse, à savoir celui de ne pas être obligé de manifester ses convictions. Bien que le gouvernement ait fait valoir que la législation nationale avait été modifiée de telle sorte que les individus pouvaient demander que la rubrique consacrée à la religion soit laissée vierge sur leur carte d'identité, selon la Cour, le simple fait de devoir demander que la religion soit effacée pouvait constituer une divulgation d'informations relatives à leur attitude envers la religion. De plus, lorsque des cartes d'identité contiennent une rubrique consacrée à la religion, le fait de laisser celle-ci vide a une connotation spécifique, étant donné que les titulaires d'une carte d'identité sans information concernant la religion se distingueraient des personnes qui ont une carte d'identité sur laquelle figurent leurs convictions religieuses. La CouEDH a conclu que la législation nationale était contraire à l'article 9 de la CEDH.

Le fonctionnement des églises et des associations ou communautés religieuses peut toutefois nécessiter le traitement des informations personnelles des membres afin de permettre la communication et l'organisation d'activités au sein de la congrégation. Les églises et les associations religieuses appliquent donc souvent des règles relatives au traitement de données à caractère personnel. Conformément à l'article 91 du RGPD, lorsque ces règles forment un ensemble complet, elles peuvent continuer à s'appliquer à condition de les mettre en conformité avec les dispositions du règlement. Les églises et les associations qui ont de telles règles doivent être soumises au contrôle d'une autorité de contrôle indépendante qui peut être spécifique, pour autant qu'elle remplisse les conditions fixées par le RGPD pour ces autorités[119].

Les organisations religieuses peuvent traiter des données à caractère personnel pour plusieurs raisons, par exemple pour maintenir un contact avec leur congrégation ou communiquer des informations sur des festivités et événements religieux ou caritatifs. Dans certains États, les églises doivent tenir à jour des registres de leurs membres à des fins fiscales, étant donné que l'appartenance

119 RGPD, art. 91, para. 2.

à des institutions religieuses peut avoir une incidence sur les impôts des personnes physiques. En tout état de cause, selon le droit de l'Union, les données révélant les convictions religieuses sont des données sensibles et les églises doivent être responsables de la manipulation et du traitement de ces données, en particulier parce que les informations traitées par des organisations religieuses concernent souvent des enfants, des personnes âgées ou d'autres membres vulnérables de la société.

1.3.4. 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 des droits fondamentaux de l'UE. Ce droit découle principalement du droit à la liberté de pensée et d'expression et il s'exerce au titre de l'article 1er de la Charte (dignité humaine). La CouEDH considère que la liberté des arts est protégée par l'article 10 de la CEDH[120]. Le droit garanti par l'article 13 de la Charte peut aussi faire l'objet de limitations autorisées par l'article 52, paragraphe 1, de la Charte, qui peut aussi être interprété à la lumière de l'article 10, paragraphe 2, de la CEDH[121].

Exemple : dans l'affaire *Vereinigung bildender Künstler c. Autriche*[122], 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 et demandé l'interdiction d'exposer le tableau. La juridiction nationale 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

120 CouEDH, *Müller et autres c. Suisse*, nº 10737/84, 24 mai 1988.

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

122 CouEDH, *Vereinigung bildender Künstler c. Autriche*, nº 68345/01, 25 janvier 2007, paras. 26 et 34.

que l'on pouvait « difficilement considérer que le 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 qu'« 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 Cour a conclu à une violation de l'article 10 de la CEDH.

Le droit européen en matière de protection des données reconnaît également la valeur particulière des sciences pour la société. Le RGPD et la Convention 108 modernisée permettent de conserver des données pour des périodes plus longues dans la mesure où les données à caractère personnel sont traitées uniquement à des fins de recherche scientifique ou historique. Par ailleurs et indépendamment de la finalité initiale d'un traitement spécifique, l'utilisation ultérieure de données à caractère personnel à des fins de recherche scientifique n'est pas considérée comme une finalité incompatible[123]. Parallèlement, des garanties adéquates doivent être mises en œuvre pour ce traitement afin de protéger les droits et libertés des personnes concernées. Le droit de l'Union ou le droit des États membres peuvent prévoir des dérogations aux droits des personnes concernées, comme le droit d'accès, de rectification, de limitation du traitement et d'opposition, pour ce qui concerne le traitement des données à caractère personnel les concernant à des fins de recherche scientifique ou historique ou à des fins statistiques (voir aussi section 6.2 et section 9.4).

1.3.5. Protection de la propriété intellectuelle

Le droit à la protection de la propriété est consacré à l'article 1er du premier Protocole à la CEDH et à l'article 17, paragraphe 1, de la Charte des droits fondamentaux de l'UE. Un aspect important du droit à la propriété particulièrement pertinent pour la protection des données est la protection de la propriété intellectuelle, explicitement mentionnée à l'article 17, paragraphe 2, de la Charte. Il existe dans l'ordre juridique de l'UE plusieurs directives 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 le droit des brevets, le droit des marques et les droits connexes.

123 RGPD, art. 5, para. 1, point b) et Convention 108 modernisée, art. 5, para. 4, point b.

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[124]. Dans certaines affaires, des organisations 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 souvent à des internautes 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*[125] concernait le refus d'un fournisseur d'accès à 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 en demandant si de telles données à caractère personnel devaient être communiquées, en vertu du droit communautaire, dans le cadre 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 les 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.

124 CJUE, C-275/06, *Productores de Música de España (Promusicae) c. Telefónica de España SAU* [GC], 29 janvier 2008, points 62 à 68.

125 *Ibid.*, points 54 et 60.

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 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 »[126].

Exemple : l'affaire *Bonnier Audio AB et autres c. Perfect Communication Sweden AB*[127] concernait la mise en balance des droits de propriété intellectuelle et de la protection des données à caractère personnel. Les requérantes – cinq sociétés d'édition titulaires de droits d'auteur sur 27 livres audio – ont engagé une action devant une juridiction suédoise, alléguant qu'il aurait été porté atteinte à ces droits d'auteur au moyen d'un serveur FTP (un protocole de transfert de données qui permet le partage de fichiers et le transfert de données via internet). Les requérantes ont demandé au fournisseur de services internet (ISP) de divulguer le nom et l'adresse de la personne utilisant l'adresse IP d'où les fichiers étaient envoyés. L'ISP, ePhone, s'est opposé à cette demande en soutenant qu'elle était contraire à la Directive 2006/24 (Directive relative à la conservation des données, invalidée en 2014).

La juridiction suédoise a saisi la CJUE et lui a demandé si la Directive 2006/24 s'oppose à l'application d'une disposition de droit national instituée sur la base de l'article 8 de la Directive 2004/48 (Directive relative au respect des droits de propriété intellectuelle), qui permet d'enjoindre à un fournisseur d'accès à internet de communiquer au titulaire d'un droit d'auteur des informations sur les abonnés dont les adresses IP auraient servi à l'atteinte audit droit. La question reposait sur l'hypothèse que la requérante avait produit des preuves manifestes de l'atteinte à un droit d'auteur particulier et que la mesure était proportionnée.

126 *Ibid.*, points 65 et 68 ; voir aussi CJUE, C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) c. Netlog NV*, 16 février 2012.

127 CJUE, C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB et Storyside AB c. Perfect Communication Sweden AB*, 19 avril 2012.

La CJUE a souligné que la Directive 2006/24 concernait exclusivement le traitement et la conservation de données générées par les fournisseurs de services de communications électroniques aux fins de recherche, de détection et de poursuites d'infractions graves, ainsi que leur transmission aux autorités nationales compétentes. Dès lors, une disposition nationale transposant la Directive relative au respect des droits de propriété intellectuelle ne relève pas du champ d'application de la Directive 2006/24 et ne s'oppose donc pas à cette directive[128].

En ce qui concerne la communication du nom et de l'adresse en cause, demandée par les requérantes, la CJUE a fait valoir qu'elle constitue un traitement de données à caractère personnel et relève donc du champ d'application de la Directive 2002/58 (Directive « vie privée et communications électroniques »). Elle a également observé que la communication de ces données est requise dans le cadre d'une procédure civile, au bénéfice du titulaire d'un droit d'auteur, en vue d'assurer la protection effective dudit droit et relève donc, par son objet, du champ d'application de la Directive 2004/48[129].

La CJUE a conclu que les Directives 2002/58 et 2004/48 doivent être interprétées en ce sens qu'elles ne s'opposent pas à une législation nationale, telle que celle en cause au principal, dans la mesure où cette législation permet à la juridiction nationale saisie d'une demande d'injonction de communiquer des données à caractère personnel et de mettre en balance, en fonction des circonstances de chaque espèce et en tenant dûment compte des exigences résultant du principe de la proportionnalité, les intérêts opposés en présence.

1.3.6. Protection des données et intérêts économiques

À l'ère du numérique ou des « mégadonnées », les données ont été qualifiées de « nouveau pétrole » de l'économie pour stimuler l'innovation et la créativité[130]. De nombreuses entreprises ont développé des modèles commerciaux solides autour

128 *Ibid.*, points 40 et 41.

129 *Ibid.*, points 52 à 54. Voir aussi CJUE, C-275/06, *Productores de Música de España (Promusicae) c. Telefónica de España SAU* [GC], 29 janvier 2008, point 58.

130 Voir, par exemple, *Financial Times* (2016), « Data is the new oil... Who's going to own it? », 16 novembre 2016.

du traitement de données et ce traitement concerne souvent des données à caractère personnel. Certaines entreprises peuvent croire que des règles spécifiques à la protection des données à caractère personnel peuvent, en pratique, entraîner des obligations excessivement lourdes de nature à affecter leurs intérêts économiques. La question qui se pose alors est celle de savoir si les intérêts économiques des responsables du traitement et des sous-traitants ou du grand public pourraient justifier de limiter le droit à la protection des données.

Exemple : dans l'affaire *Google Spain*[131], la CJUE a conclu que, dans certaines conditions, les personnes ont le droit de demander aux moteurs de recherche de supprimer des résultats de leur index de recherche. Dans sa motivation, la Cour a souligné que l'utilisation de moteurs de recherche et la liste des résultats de recherche peuvent établir un profil détaillé de la personne concernée. Ces informations touchent potentiellement une multitude d'aspects de la vie privée de la personne concernée et n'auraient pas pu être aisément trouvées ou interconnectées sans un moteur de recherche. Cela constituait donc une ingérence potentiellement grave dans l'exercice des droits fondamentaux des personnes concernées au respect de la vie privée et à la protection des données à caractère personnel.

La CJUE a ensuite examiné la question de savoir si l'ingérence pouvait être justifiée. S'agissant de l'intérêt économique du traitement pour l'exploitant du moteur de recherche, la CJUE a déclaré que « force est de constater que [l'ingérence] ne saurait être justifiée par le seul intérêt économique de l'exploitant d'un tel moteur dans ce traitement » et qu'« en principe », les droits fondamentaux consacrés aux articles 7 et 8 de la Charte prévalent non seulement sur cet intérêt économique, mais également sur l'intérêt du public à trouver les informations lors d'une recherche portant sur le nom de la personne concernée[132].

L'un des objectifs essentiels du droit européen de la protection des données est de donner aux personnes concernées davantage de contrôle sur leurs données personnelles. À l'ère du numérique en particulier, il existe un déséquilibre entre le pouvoir des entités commerciales qui traitent et ont accès à des quantités considérables

131 CJUE, C-131/12, *Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 13 mai 2014.

132 *Ibid.*, points 81 et 97.

de données personnelles et celui des personnes concernées auxquelles ces données appartiennent de contrôler les informations les concernant. La CJUE suit une approche au cas par cas lors de la mise en balance de la protection des données et des intérêts économiques, comme les intérêts de tiers par rapport aux sociétés par actions et aux sociétés à responsabilité limitée, ainsi que l'illustre l'arrêt *Manni*.

Exemple : l'affaire *Manni*[133] portait sur l'inclusion des données à caractère personnel d'un individu dans un registre commercial public. M. Manni avait demandé à la chambre de commerce de Lecce d'effacer ses données personnelles de ce registre après avoir découvert que des clients potentiels pourraient consulter le registre et voir qu'il avait été l'administrateur d'une entreprise déclarée en faillite plus de dix ans auparavant. Ces informations créaient un préjugé dans l'esprit de ses clients potentiels et pouvaient avoir un effet négatif sur ses intérêts commerciaux.

La CJUE était invitée à déterminer si le droit de l'Union reconnaît un droit d'effacement dans ce cas. Pour se prononcer, la Cour a mis en balance les règles de l'UE relatives à la protection des données et l'intérêt commercial de M. Manni à effacer les informations relatives à la faillite de son ancienne société avec l'intérêt du public à avoir accès à ces informations. Elle a pris acte du fait que la publication dans le registre des sociétés était prévue par la loi et, en particulier, par une directive européenne visant à rendre les informations sur les sociétés plus aisément accessibles aux tiers. La publicité était importante pour protéger les intérêts des tiers souhaitant entrer en relation d'affaires avec une société donnée, dès lors que les seules garanties offertes aux tiers par les sociétés par actions et les sociétés à responsabilité limitée sont leur patrimoine social. À cette fin, « la publicité doit permettre aux tiers de connaître les actes essentiels de la société concernée et certaines indications la concernant, notamment l'identité des personnes qui ont le pouvoir de l'engager »[134].

Vu l'importance du but légitime poursuivi par le registre, la CJUE a conclu que M. Manni n'avait pas le droit d'obtenir l'effacement de ses données à caractère personnel, au motif que la nécessité de protéger les intérêts des tiers par rapport aux sociétés par actions et aux sociétés à responsabilité limitée et d'assurer la sécurité juridique, la loyauté des transactions

133 CJUE, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce c. Salvatore Manni*, 9 mars 2017.

134 *Ibid.*, point 49.

commerciales et, partant, le bon fonctionnement du marché intérieur, prévalait sur ses droits au titre de la législation relative à la protection des données. Ceci était particulièrement vrai compte tenu du fait que les personnes choisissant de participer aux échanges économiques par l'intermédiaire d'une société par actions ou d'une société à responsabilité limitée sont conscientes qu'elles sont tenues de rendre publiques les données tenant à leur identité et à leurs fonctions au sein de celle-ci.

Tout en concluant qu'il n'y avait pas de raisons justifiant l'effacement en l'espèce, la Cour a reconnu l'existence d'un droit d'opposition au traitement et a relevé qu'« il ne saurait [...] être exclu que puissent exister des situations particulières dans lesquelles des raisons prépondérantes et légitimes tenant au cas concret de la personne concernée justifient exceptionnellement que l'accès aux données à caractère personnel la concernant inscrites dans le registre soit limité, à l'expiration d'un délai suffisamment long [...], aux tiers justifiant d'un intérêt spécifique à leur consultation »[135].

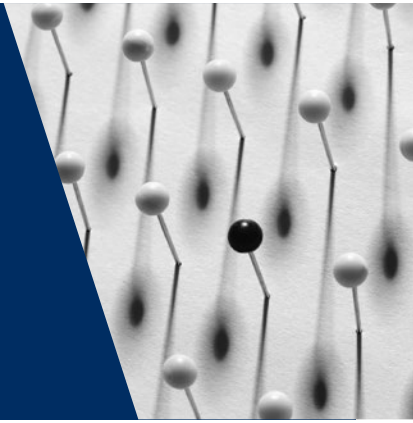
La CJUE a indiqué qu'il appartient aux juridictions nationales d'apprécier, au cas par cas et compte tenu de toutes les circonstances pertinentes tenant à la situation de la personne concernée, l'existence ou l'absence de raisons prépondérantes et légitimes qui pourraient exceptionnellement justifier que l'accès aux données à caractère personnel la concernant inscrites dans le registre des sociétés soit limité à certains tiers. Elle a toutefois précisé que, dans le cas de M. Manni, le simple fait que la publication de ses données à caractère personnel dans le registre aurait affecté sa clientèle ne pouvait pas être considéré comme une raison légitime et prépondérante. Les clients potentiels de M. Manni ont un intérêt légitime à disposer des informations concernant la dissolution de sa société précédente.

L'ingérence dans les droits fondamentaux de M. Manni et d'autres personnes inscrites dans le registre au respect de la vie privée et à la protection des données à caractère personnel, garantis par les articles 7 et 8 de la Charte, poursuivait un objectif d'intérêt général et était nécessaire et proportionnée.

Dans l'affaire *Manni*, la CJUE a dès lors conclu que les droits à la protection des données et au respect de la vie privée ne prévalaient pas sur l'intérêt des tiers à avoir accès aux informations contenues dans le registre des sociétés concernant les sociétés par actions et les sociétés à responsabilité limitée.

135 *Ibid.*, point 60.

2 Terminologie de la protection des données



UE	Questions traitées	CdE
Données à caractère personnel		
RGPD, art. 4, para. 1 RGPD, art. 4, para. 5, et art. 5, para. 1, point e) RGPD, art. 9 CJUE, affaires jointes C-92/09 et C-93/09, *Volker und Markus Schecke GbR et Hartmut Eifert c. Land Hessen* [GC], 2010 CJUE, C-275/06, *Productores de Música de España (Promusicae) c. Telefónica de España SAU* [GC], 2008 CJUE, C-70/10, *Scarlet Extended SA c. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 2011 CJUE, C-582/14, *Patrick Breyer c. Bundesrepublik Deutschland*, 2016 CJUE, affaires jointes C-141/12 et C-372/12, *YS c. Minister voor Immigratie, Integratie en Asiel* et *Minister voor Immigratie, Integratie en Asiel c. M et S*, 2014	**Définition juridique de la protection des données**	Convention 108 modernisée, art. 2, point a) CouEDH, *Bernh Larsen Holding AS et autres c. Norvège*, nº 24117/08, 2013 CouEDH, *Uzun c. Allemagne*, nº 35623/05, 2010 CouEDH, *Amann c. Suisse* [GC], nº 27798/95, 2000

UE	Questions traitées	CdE
CJUE, C-101/01, *Procédure pénale contre Bodil Lindqvist*, 2003	**Catégories particulières de données à caractère personnel (données sensibles)**	Convention 108 modernisée, art. 6, para. 1
CJUE, C-434/16, *Peter Nowak c. Data Protection Commissioner*, 2017	**Données personnelles anonymisées et pseudonymisées**	Convention 108 modernisée, art. 5, para. 4, point e) Rapport explicatif sur la Convention 108 modernisée, para. 50
Traitement des données		
RGPD, art. 4, para. 2 CJUE, C-212/13, *František Ryneš c. Úřad pro ochranu osobních údajů*, 2014 CJUE, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce c. Salvatore Manni*, 2017 CJUE, C-101/01, *Procédure pénale contre Bodil Lindqvist*, 2003 CJUE, C-131/12, *Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 2014	**Définitions**	Convention 108 modernisée, art. 2, points b) et c)
Utilisateurs de données		
RGPD, art. 4, para. 7 CJUE, C-212/13, *František Ryneš c. Úřad pro ochranu osobních údajů*, 2014 CJUE, C-131/12, *Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 2014	**Responsable du traitement**	Convention 108 modernisée, art. 2, point d) Recommandation sur le profilage, art. 1er, point g)*
RGPD, art. 4, para. 8	**Sous-traitant**	Convention 108 modernisée, art. 2, point f) Recommandation sur le profilage, art. 1er, point h)
RGPD, art. 4, para. 9	**Destinataire**	Convention 108 modernisée, art. 2, point e)
RGPD, art. 4, para. 10	**Tiers**	

UE	Questions traitées	CdE
Consentement		
RGPD, art. 4, para. 11, et art. 7 CJUE, C-543/09, *Deutsche Telekom AG c. Bundesrepublik Deutschland*, 2011 CJUE, C-536/15, *Tele2 (Netherlands) BV et autres c. Autoriteit Consument en Markt (AMC)*, 2017	**Définition et exigences applicables à un consentement valable**	Convention 108 modernisée, art. 5, para. 2 Recommandation relative à la protection des données médicales, art. 6, et diverses recommandations ultérieures CouEDH, *Elberte c. Lettonie*, nº 61243/08, 2015

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

2.1. Données à caractère personnel

Points clés

- Les données sont des données à caractère personnel lorsqu'elles portent sur une personne identifiée ou identifiable, la « personne concernée ».
- Pour déterminer si une personne physique est identifiable, le responsable du traitement ou toute autre personne doit prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés pour identifier la personne physique directement ou indirectement, comme le ciblage.
- Par authentification, on entend le fait de démontrer qu'une personne donnée 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 modernisée et dans la Directive de l'UE relative à la protection des données, qui requièrent une protection accrue et sont, par conséquent, soumises à un régime juridique spécial.
- Les données sont anonymisées lorsqu'elles ne sont plus liées à une personne identifiée ou identifiable.

- La pseudonymisation est un processus par lequel les données à caractère personnel ne peuvent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, qui sont conservées séparément. La « clé » qui permet de ré-identifier les personnes concernées doit être conservée séparément et sécurisée. Les données qui subissent un processus de pseudonymisation restent des données à caractère personnel. Il n'existe pas de concept de « données pseudonymisées » dans le droit de l'Union.
- Les principes et règles applicables à la protection des données ne s'appliquent pas aux données anonymisées. Elles s'appliquent toutefois aux données pseudonymisées.

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[136], 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. Pour déterminer si une personne physique est identifiable, le responsable du traitement ou toute autre personne doit prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés pour identifier la personne physique directement ou indirectement, tels que le ciblage, qui permet de traiter une personne différemment d'une autre[137].

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

La personne concernée

Dans le droit de l'UE, les personnes physiques sont les seules bénéficiaires des règles relatives à la protection des données[138] et seule une personne vivante est protégée par le droit européen en matière de protection des données[139]. Le RGPD définit les données à caractère personnel comme toute information se rapportant à une personne physique identifiée ou identifiable.

136 RGPD, art. 4, para. 1 ; Convention 108 modernisée, art. 2, point a).

137 RGPD, considérant 26.

138 *Ibid.*, art. 1er.

139 *Ibid.*, considérant 27. Voir également Groupe de travail « Article 29 », *Avis 4/2007 sur le concept de données à caractère personnel*, WP 136, 20 juin 2007, p. 22.

Le droit du CdE, notamment la Convention 108 modernisée, fait également référence à la protection des personnes à l'égard du traitement de leurs données personnelles. Là aussi, on entend par données à caractère personnel toute information relative à une personne identifiée ou identifiable. Cette personne physique ou cet individu, comme le nomment respectivement le RGPD et la Convention 108 modernisée, est connue comme la personne concernée dans le droit de la protection des données.

Les personnes morales jouissent également d'une certaine protection. Il existe une jurisprudence de la CouEDH statuant sur des recours formés par des personnes morales qui allèguent une violation de leur droit à la protection contre l'utilisation de leurs données au titre de l'article 8 de la CEDH. Cet article couvre à la fois le droit au respect de la vie privée et de la vie familiale et le droit au respect du domicile et de la correspondance. La Cour peut donc traiter des affaires sous l'angle de ce dernier plutôt que sous celui de la vie privée.

Exemple : l'affaire *Bernh Larsen Holding AS et autres c. Norvège*[140] 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 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 conclu qu'il n'y avait dès lors pas eu de violation de l'article 8.

140 CouEDH, *Bernh Larsen Holding AS et autres c. Norvège*, nº 24117/08, 14 mars 2013. Voir cependant aussi CouEDH, *Liberty et autres c. Royaume-Uni*, nº 58243/00, 1er juillet 2008.

Selon la Convention 108 modernisée, 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. Le rapport explicatif sur la Convention modernisée indique que le droit national peut protéger les intérêts légitimes des personnes morales en étendant la portée de la Convention à ces acteurs[141]. **Le droit de l'UE en matière de protection des données** ne couvre pas le traitement de données relatif à des personnes morales et, en particulier, il ne concerne pas les entreprises ayant un statut juridique, y compris le nom et la forme de la personne morale et ses coordonnées[142]. La Directive « vie privée et communications électroniques » protège toutefois la confidentialité des communications et les intérêts légitimes des personnes morales à l'égard de la capacité accrue de stockage et de traitement automatisés des données relatives aux abonnés et aux utilisateurs[143]. De même, le projet de Règlement relatif à la vie privée et aux communications électroniques étend la protection aux personnes morales.

Exemple : dans l'affaire *Volker and Markus Schecke et Hartmut Eifert c. Land Hessen*[144], 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 [...] »[145].

Pondérant l'intérêt de l'Union à garantir la transparence dans l'octroi des aides, d'une part, et les droits fondamentaux au respect de la vie privée et à la protection des données des personnes physiques bénéficiaires des aides, d'autre part, la CJUE a considéré que l'ingérence dans ces droits fondamentaux était disproportionnée. Elle a estimé que l'objectif de transparence aurait pu

141 Rapport explicatif sur la Convention 108 modernisée, para. 30.

142 RGPD, considérant 14.

143 Directive « vie privée et communications électroniques », considérant 7 et art. 1er, para. 2.

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

145 *Ibid.*, points 52 et 53.

être atteint de manière effective par des mesures moins intrusives pour les droits des personnes concernées. Toutefois, lorsqu'elle a procédé à l'examen de la proportionnalité de publier des informations sur des personnes morales bénéficiaires d'une aide, la CJUE est parvenue à une conclusion différente et a jugé que cette publication ne dépassait pas les limites du principe de proportionnalité. Elle a déclaré que « la gravité de l'atteinte au droit à la protection des données à caractère personnel se présente différemment pour les personnes morales et pour les personnes physiques »[146]. Les personnes morales sont soumises à des obligations plus lourdes de publication des données les concernant. La CJUE a considéré qu'obliger les autorités nationales compétentes à examiner avant la publication des données en cause, pour chaque personne morale bénéficiaire, si le nom de celle-ci identifie des personnes physiques, imposerait à ces autorités une charge administrative démesurée. Dès lors, la législation imposant la publication généralisée des données relatives aux personnes morales a instauré un juste équilibre entre les intérêts respectifs en présence.

Nature des données

Tout type d'informations peut constituer des données à caractère personnel à condition qu'elles concernent une personne identifiée ou identifiable.

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. Ceci est le cas même s'il est possible qu'elle ne reflète que tout ou partie de l'opinion personnelle du supérieur (par exemple : « le salarié ne manifeste pas de dévouement envers son travail ») et non des faits (par exemple : « le salarié a été absent de son travail pendant cinq semaines au cours des six derniers mois »).

Les données à caractère personnel recouvrent les informations relatives à la vie privée d'une personne, ce qui inclut les activités professionnelles, ainsi que des informations sur sa vie professionnelle et publique.

146 *Ibid.*, point 87.

Dans l'affaire *Amann*[147], la CouEDH a interprété l'expression « données à caractère personnel » comme n'étant pas limitée aux questions relevant de la sphère privée d'un individu. Cette acception de l'expression « données à caractère personnel » est aussi valable pour le RGPD.

Exemple : dans l'affaire *Volker und Markus Schecke et Hartmut Eifert c. Land Hessen*[148], la CJUE a déclaré que « 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" ».

Exemple : dans les affaires jointes *YS c. Minister voor Immigratie, Integratie en Asiel* et *Minister voor Immigratie, Integratie en Asiel c. M et S*[149], la CJUE a déclaré que l'analyse juridique figurant dans un projet de décision du service d'immigration et de naturalisation concernant les demandes de permis de séjour ne constitue pas en elle-même une donnée à caractère personnel, bien qu'elle puisse en contenir.

La jurisprudence de la CouEDH relative à l'article 8 de la CEDH confirme qu'il peut être malaisé de séparer totalement les questions relevant de la vie privée et celles de la vie professionnelle[150].

Exemple : dans l'affaire *Bărbulescu c. Roumanie*[151], le requérant avait été licencié pour avoir utilisé le réseau internet de son employeur pendant ses heures de travail en violation du règlement intérieur. Son employeur avait surveillé ses communications sur un compte et les enregistrements, qui contenaient des messages de nature strictement privée, ont été produits

147 Voir CouEDH, *Amann c. Suisse* [GC], nº 27798/95, 16 février 2000, para. 65.

148 CJUE, affaires jointes C-92/09 et C-93/09, *Volker und Markus Schecke GbR et Hartmut Eifert c. Land Hessen* [GC], 9 novembre 2010, point 59.

149 CJUE, affaires jointes C-141/12 et C-372/12, *YS c. Minister voor Immigratie, Integratie en Asiel* et *Minister voor Immigratie, Integratie en Asiel c. M et S*, 17 juillet 2014, point 39.

150 Voir, par exemple, CouEDH, *Rotaru c. Roumanie* [GC], nº 28341/95, 4 mai 2000, para. 43 ; CouEDH, *Niemietz c. Allemagne,* nº 13710/88, 16 décembre 1992, para. 29.

151 CouEDH, *Bărbulescu c. Roumanie* [GC], nº 61496/08, 5 septembre 2017, para. 121.

durant les procédures internes. Jugeant l'article 8 applicable, la CouEDH n'a pas répondu à la question de savoir si le règlement strict de l'employeur laissait au requérant une confiance raisonnable dans le respect de sa vie privée, mais a en tout état de cause conclu que les règles d'un employeur ne pouvaient pas réduire à néant la vie sociale privée sur le lieu de travail. Sur le fond, les États contractants devaient jouir d'une marge d'appréciation étendue pour déterminer la nécessité d'établir un cadre juridique régissant les conditions dans lesquelles un employeur peut réglementer les communications non professionnelles de ses salariés – sous forme électronique ou autre – sur le lieu de travail. Les juridictions internes devaient toutefois s'assurer que la mise en place par un employeur de mesures de surveillance de la correspondance et des autres communications, quelles qu'en soient l'étendue et la durée, s'accompagnait de garanties adéquates et suffisantes contre les abus. La proportionnalité et les garanties procédurales contre l'arbitraire sont des éléments essentiels et la CouEDH a circonscrit plusieurs facteurs pertinents dans le cas d'espèce. Ces facteurs incluaient, notamment, l'étendue de la surveillance des employés par l'employeur et le degré d'intrusion dans la vie privée de l'employé, les conséquences de cette surveillance pour l'employé et l'existence de garanties adéquates. De plus, les autorités internes devaient veiller à ce que les employés dont les communications avaient été surveillées puissent bénéficier d'une voie de recours devant un organe juridictionnel ayant compétence pour statuer, du moins sur le fond, sur le respect des critères énoncés ainsi que sur la licéité des mesures contestées. Dans cette affaire, la CouEDH a conclu à une violation de l'article 8 au motif que les autorités nationales n'avaient pas protégé de manière adéquate le droit du requérant au respect de sa vie privée et de sa correspondance et n'avaient dès lors pas ménagé un juste équilibre entre les intérêts en jeu.

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 ou identifiable dans cette information ; ou
- 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 de la protection des données. Le caractère directement ou indirectement identifiable d'une personne requiert une appréciation continue, « en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci »[152]. La CouEDH a déclaré à plusieurs reprises que la notion de « données à caractère personnel » au sens de la CEDH était la même que dans la Convention 108, en particulier à l'égard de l'exigence selon laquelle elles doivent concerner des personnes identifiées ou identifiables[153].

Le RGPD dispose qu'une personne physique est identifiable lorsqu'elle « peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale »[154]. L'identification requiert donc des éléments qui décrivent une personne de telle sorte qu'elle puisse être distinguée de toutes les autres et qu'elle soit reconnaissable en tant qu'individu. Le nom d'une personne est un excellent exemple de ces éléments descriptifs et peut identifier directement une personne. Dans certains cas exceptionnels, d'autres identifiants peuvent avoir un effet similaire à un nom, en rendant une personne indirectement identifiable. Le numéro de téléphone, le numéro de sécurité sociale ou le numéro d'immatriculation d'un véhicule sont autant d'exemples d'informations qui rendent un individu identifiable. On peut également utiliser des identifiants, comme des fichiers informatiques, des cookies et des outils de surveillance du trafic sur internet, pour cibler des individus en identifiant leur comportement et leurs habitudes. Comme l'expliquait le Groupe de travail « Article 29 » dans son avis, « [s]ans même s'enquérir du nom et de l'adresse de la personne, on peut la caractériser en fonction de critères socio-économiques, psychologiques, philosophiques ou autres et lui attribuer certaines décisions dans la mesure où le point de contact de la personne (l'ordinateur) ne nécessite plus nécessairement la révélation de son identité au sens étroit du terme »[155]. La définition des données à caractère personnel dans le droit de l'Union et dans celui du CdE est suffisamment large pour couvrir toutes les possibilités d'identification (et, partant, tous les degrés de caractère identifiable).

152 RGPD, considérant 26.

153 Voir CouEDH, *Amann c. Suisse* [GC], nº 27798/95, 16 février 2000, para. 65.

154 RGPD, art. 4, para. 1.

155 Groupe de travail « Article 29 », *Avis 4/2007 sur le concept de données à caractère personnel*, WP 136, 20 juin 2007, p. 15.

Exemple : dans l'affaire *Promusicae*[156], la CJUE a indiqué qu'« il n'est par ailleurs pas contesté que la communication, sollicitée par Promusicae, des noms et des adresses de certains utilisateurs [d'une certaine plateforme 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 [devenu article 4, paragraphe 1, du RGPD]. 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 »[157].

Exemple : l'affaire *Scarlet Extended SA c. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*[158] concernait le refus du fournisseur d'accès à internet Scarlet d'installer un système de filtrage des communications électroniques utilisant un logiciel de partage de fichiers afin d'éviter que le partage de fichiers ne porte atteinte aux droits d'auteur protégés par la SABAM, une société de gestion qui représente les auteurs, les compositeurs et les éditeurs d'œuvres musicales. La CJUE a conclu que les adresses IP des utilisateurs « sont des données protégées à caractère personnel, car elles permettent l'identification précise desdits utilisateurs ».

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 personne. Il faut parfois combiner des identifiants directs et indirects pour identifier la personne concernée par les données. 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. Les données fiscales transférées[159], les données concernant le demandeur d'un permis de séjour figurant dans un document administratif[160] et les documents concernant des relations bancaires et

156 CJUE, C-275/06, *Productores de Música de España (Promusicae) c. Telefónica de España SAU* [GC], 29 janvier 2008, point 45.

157 Ex-article 2, point b), de la directive 95/46, devenu article 4, para. 2, du RGPD.

158 CJUE, C-70/10, *Scarlet Extended SA c. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24 novembre 2011, point 51.

159 CJUE, C-201/14, *Smaranda Bara et autres c. Casa Națională de Asigurări de Sănătate et autres*, 1er octobre 2015.

160 CJUE, *YS c. Minister voor Immigratie, Integratie en Asiel* et *Minister voor Immigratie, Integratie en Asiel c. M et S*, 17 juillet 2014.

fiduciaires[161] peuvent être des données à caractère personnel. À l'ère du numérique, les données biométriques, telles que les empreintes digitales, les photos numériques ou les scans de l'iris, prennent de plus en plus d'importance dans l'identification des personnes.

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, en effet, 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[162]. Conformément au considérant 26 du RGPD, 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 infliger une amende aux personnes ne respectant pas les limitations de vitesse. Une personne concernée porte plainte, affirmant que l'autorité locale ne dispose d'aucune base juridique au titre de la législation relative à la protection des données pour collecter ces données. L'autorité locale soutient qu'elle ne collecte pas de données à caractère personnel. Les plaques d'immatriculation sont, selon elle, des données 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 du RGPD. 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 directement de moyens d'identification, elles transmettront les données à l'autorité compétente, la police, qui, elle, dispose de tels 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

161 CouEDH, *M.N. et autres c. Saint-Marin*, nº 28005/12, 7 juillet 2015.

162 RGPD, art. 4, para. 1.

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 en vertu de la législation relative à la protection des données.

« Pour établir si des moyens sont raisonnablement susceptibles d'être utilisés pour identifier une personne physique, il convient de prendre en considération l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci »[163].

Exemple : dans l'affaire *Breyer c. Bundesrepublik Deutschland*[164], la CJUE a examiné la notion de caractère identifiable indirect des personnes concernées. L'affaire concernait des adresses IP dynamiques, qui changent à chaque connexion à internet. Les sites web administrés par les services fédéraux allemands ont enregistré et stocké des adresses IP dynamiques afin de se prémunir contre des cyberattaques et de rendre possibles des poursuites pénales, si nécessaire. Seul le fournisseur d'accès à internet que M. Breyer utilisait disposait des informations supplémentaires nécessaires pour l'identifier.

La CJUE a considéré qu'une adresse IP dynamique, que le fournisseur de services de médias en ligne enregistre lorsqu'une personne consulte un site internet que le fournisseur a rendu accessible au public, ne constitue une donnée à caractère personnel que lorsqu'un tiers – le fournisseur d'accès à internet en l'espèce – détient les informations supplémentaires nécessaires pour identifier la personne[165]. Elle a déclaré qu'« il n'est pas requis que toutes les informations permettant d'identifier la personne concernée doivent se trouver entre les mains d'une seule personne » pour qu'une donnée puisse être qualifiée de donnée à caractère personnel. Les utilisateurs d'une adresse IP dynamique enregistrée par un fournisseur d'accès à internet peuvent être identifiés dans certains cas, par exemple dans le cadre de poursuites pénales en cas d'attaques cybernétiques, avec

163 *Ibid.*, considérant 26.

164 CJUE, C-582/14, *Patrick Breyer c. Bundesrepublik Deutschland*, 19 octobre 2016, para. 43.

165 Ancienne 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, art. 2, point a).

l'aide d'autres personnes[166]. Selon la Cour, lorsque le fournisseur dispose « de moyens légaux lui permettant de faire identifier la personne concernée grâce aux informations supplémentaires dont dispose le fournisseur d'accès à internet de cette personne », ceci constitue « un moyen susceptible d'être raisonnablement mis en œuvre afin d'identifier la personne concernée ». Ces données sont donc considérées comme des données à caractère personnel.

Dans le droit du CdE, le caractère identifiable est compris de façon similaire. Le rapport explicatif sur la Convention 108 modernisée comprend une description similaire : le terme « identifiable » ne fait pas seulement référence à l'identité civile ou juridique en tant que telle de la personne, mais également à tout élément susceptible « d'individualiser » ou de désigner une personne parmi d'autres et d'avoir comme conséquence potentielle qu'elle soit traitée différemment). Cette « individualisation » pourrait se faire, par exemple, par une référence à la personne, ou à un appareil ou une combinaison d'appareils (ordinateur, téléphone portable, appareil photographique, consoles de jeux, etc.) liée à un numéro d'identification, un pseudonyme, des données biométriques ou génétiques, des données de localisation, une adresse IP ou un autre identifiant[167]. Une personne physique n'est pas considérée comme « identifiable » si son identification nécessite des délais, des efforts ou des ressources déraisonnables. Tel est par exemple le cas lorsque l'identification de la personne concernée exige des opérations excessivement complexes, longues et coûteuses. Il convient d'examiner au cas par cas ce qui constitue des délais, des efforts ou des ressources déraisonnables, en tenant compte de facteurs tels que la finalité du traitement, le coût et les bénéfices de l'identification, le type de responsable du traitement et la technologie employée[168].

Il est important de souligner que 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[169],

166 CJUE, C-70/10, *Scarlet Extended SA c. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24 novembre 2011, points 47 et 48.

167 Rapport explicatif sur la Convention 108 modernisée, para. 18.

168 *Ibid.*, para. 17.

169 CouEDH, *Von Hannover c. Allemagne*, nº 59320/00, 24 juin 2004 ; CouEDH, *Sciacca c. Italie*, nº 50774/99, 11 janvier 2005 ; CJUE, C-212/13, *František Ryneš c. Úřad pro ochranu osobních údajů*, 11 décembre 2014.

y compris des séquences[170] ou des sons de télévision en circuit fermé (CCTV)[171]. Les informations enregistrées électroniquement ainsi que les informations sur support papier, peuvent être des données à caractère personnel. Même des échantillons de cellules de tissu humain – qui contiennent l'ADN d'une personne – peuvent être des sources dont on peut extraire des données[172], pour autant que les données concernent les caractéristiques génétiques innées ou acquises de l'individu, fournissent des informations uniques sur sa santé ou sa physiologie, et proviennent de l'analyse d'un échantillon biologique de cette personne[173].

Anonymisation

Conformément au principe de la conservation des données pendant une durée limitée, inscrit à la fois dans le RGPD et dans la Convention 108 modernisée (discuté 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 au regard des finalités pour lesquelles elles sont traitées »[174]. Par conséquent, il pourrait être nécessaire d'effacer ou d'anonymiser les données si un responsable du traitement souhaite les conserver alors qu'elles ne sont plus nécessaires et ne servent plus leur finalité initiale.

Le processus d'anonymisation de données signifie que tous les éléments identifiants ont été supprimés d'un ensemble de données à caractère personnel, de sorte que la personne concernée n'est plus identifiable[175]. Dans son avis 5/2014, le Groupe de travail « Article 29 » analyse l'efficacité et les limites de différentes techniques d'anonymisation[176]. Il reconnaît la valeur potentielle de ces techniques, mais souligne que certaines d'entre elles ne fonctionnent pas nécessairement dans tous les cas. Pour trouver la solution optimale dans une situation donnée, la technique appropriée

170 CouEDH, *Peck c. Royaume-Uni*, nº 44647/98, 28 janvier 2003 ; CouEDH, *Köpke c. Allemagne* (décision), nº 420/07, 5 octobre 2010 ; CEPD (2010), *Lignes directrices du CEPD sur la vidéosurveillance*, 17 mars 2010.

171 CouEDH, *P.G. et J.H. c. Royaume-Uni*, nº 44787/98, 25 septembre 2001, paras. 59 et 60 ; CouEDH, *Wisse c. France*, nº 71611/01, 20 décembre 2005.

172 Voir : Groupe de travail « Article 29 » (2007), *Avis 4/2007 sur le concept de données à caractère personnel*, WP 136, 20 juin 2007, p. 9 ; CdE, Recommandation Rec(2006)4 du Comité des Ministres aux États membres sur la recherche utilisant du matériel biologique d'origine humaine, 15 mars 2006.

173 RGPD, art. 4, para. 13.

174 *Ibid.*, art. 5, para. 1, point e) ; Convention 108 modernisée, art. 5, para. 4, point e).

175 RGPD, considérant 26.

176 Groupe de travail « Article 29 » (2014), *Avis 05/2014 sur les techniques d'anonymisation*, WP 216, 10 avril 2014.

devrait être choisie au cas par cas. Indépendamment de la technique utilisée, l'identification doit être empêchée de manière irréversible. En d'autres termes, pour que les données soient anonymisées, les données ne doivent plus contenir aucun élément raisonnablement susceptible d'être utilisé pour ré-identifier la personne ou les personnes concernées[177]. Le risque de ré-identification peut être évalué en tenant compte « des délais, efforts ou ressources nécessaires au regard de la nature des données, du contexte de leur utilisation, des techniques de ré-identification disponibles et des coûts correspondants »[178].

Lorsque des données ont été correctement anonymisées, elles ne sont plus des données à caractère personnel et la législation relative à la protection des données ne s'applique donc plus.

Le RGPD prévoit que la personne ou l'organisation responsable du traitement de données à caractère personnel ne peut être tenue de conserver, d'obtenir ou de traiter des informations supplémentaires pour identifier la personne concernée à la seule fin de respecter le règlement. Cette règle comporte toutefois une exception majeure : chaque fois que la personne concernée, dans le cadre de l'exercice de ses droits d'accès, de rectification, d'effacement, de limitation du traitement et de portabilité des données, fournit des informations supplémentaires au responsable du traitement qui permettent son identification, les données qui ont été anonymisées auparavant redeviennent des données à caractère personnel[179].

Pseudonymisation

Les informations personnelles contiennent des identifiants, tels que le nom, la date de naissance, le sexe, l'adresse ou d'autres éléments susceptibles de conduire à une identification. Lorsque des informations personnelles sont pseudonymisées, les identifiants sont remplacés par un pseudonyme.

Le droit de l'Union définit la « pseudonymisation » comme « le traitement de données à caractère personnel de telle façon qu'elles ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que celles-ci soient conservées séparément et soumises à des

177 RGPD, considérant 26.

178 CdE, Comité de la Convention 108 (2017), *Lignes directrices sur la protection des personnes à l'égard du traitement des données à caractère personnel à l'ère des mégadonnées*, 23 janvier 2017, para. 6.2.

179 RGPD, art. 11.

mesures techniques et organisationnelles afin de garantir cette non-attribution à une personne identifiée ou identifiable »[180]. Contrairement aux données anonymisées, les données pseudonymisées sont toujours des données à caractère personnel et sont donc soumises à la législation relative à la protection des données. Bien que la pseudonymisation puisse réduire les risques liés à la sécurité pour les personnes concernées, elle n'est pas exclue du champ d'application du RGPD.

Le RGPD reconnaît différentes utilisations de la pseudonymisation comme étant une mesure technique appropriée et celle-ci est spécifiquement mentionnée dans le cadre de la protection des données par défaut et de la sécurité de leur traitement[181]. Elle constitue également une garantie adéquate qui pourrait servir au traitement de données à caractère personnel à d'autres fins que celles pour lesquelles elles ont été initialement collectées[182].

La pseudonymisation n'est pas expressément mentionnée dans la définition légale de la Convention 108 modernisée du **CdE**. Toutefois, le rapport explicatif sur la Convention 108 modernisée précise que « [l]'utilisation d'un pseudonyme ou de tout identifiant/identité numérique n'entraîne pas l'anonymisation des données, la personne concernée pouvant encore être identifiable ou individualisée »[183]. Une technique de pseudonymisation est le cryptage des données. Une fois les données pseudonymisées, le lien avec l'identité réside dans la forme du pseudonyme associé à une clé de cryptage. Sans cette clé, il est difficile d'identifier des données pseudonymisées. Cependant, pour toute personne habilitée à utiliser la clé de décryptage, une ré-identification est possible aisément. Il convient de veiller particulièrement à éviter toute utilisation de clés de cryptage par des personnes non autorisées. Les « données pseudonymisées doivent donc être considérées comme des données à caractère personnel [...] » couvertes par les dispositions de la Convention 108 modernisée[184].

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

180 *Ibid.*, art. 4, para. 5.

181 *Ibid.*, art. 25, para. 1.

182 *Ibid.*, art. 6, para. 4.

183 Rapport explicatif sur la Convention 108 modernisée, para. 18.

184 *Ibid.*

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 figurant dans un passeport) avec les données de la personne qui se présente à un contrôle d'immigration[185], 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, les signatures électroniques, parfois associées à des codes PIN, sont un outil particulièrement utile pour identifier et authentifier une personne dans des communications électroniques.

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**.** Ces données sont soumises à un principe d'interdiction de traitement et celui-ci n'est licite que dans un nombre limité de cas.

La Convention 108 modernisée (article 6) et le RGPD (article 9) citent comme données sensibles les catégories de données suivantes :

- données à caractère personnel qui révèlent l'origine raciale ou ethnique ;
- données à caractère personnel qui révèlent les opinions politiques, les convictions religieuses ou d'autres convictions, y compris philosophiques ;
- données à caractère personnel qui révèlent l'appartenance syndicale ;
- données génétiques et biométriques traitées aux fins d'identifier une personne physique ;

185 *Ibid.*, paras. 56 et 57.

- données à caractère personnel concernant la santé, la vie sexuelle ou l'orientation sexuelle.

Exemple : l'affaire *Bodil Lindqvist*[186] concernait la référence, sur une page internet, à différentes personnes par leur nom ou par d'autres moyens, par exemple leur numéro de téléphone ou des informations relatives à leurs passe-temps. La CJUE a déclaré 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 »[187].

Données à caractère personnel relatives aux condamnations pénales et aux infractions

La Convention 108 modernisée inclut les données à caractère personnel relatives aux infractions, aux procédures pénales et aux condamnations pénales et les mesures de sûreté connexes dans la liste des catégories particulières de données à caractère personnel[188]. Dans le cadre du RGPD, les données à caractère personnel relatives aux condamnations pénales et aux infractions ou les mesures de sûreté connexes ne sont pas mentionnées en tant que telles dans la liste des catégories particulières de données, mais sont abordées dans un article distinct. L'article 10 du RGPD dispose que le traitement de ces données ne peut être effectué que « sous le contrôle de l'autorité publique ou si le traitement est autorisé par le droit de l'Union ou par le droit d'un État membre qui prévoit des garanties appropriées pour les droits et libertés des personnes concernées ». Par ailleurs, les registres complets contenant des informations sur les condamnations pénales ne peuvent être tenus que sous le contrôle d'autorités publiques spécifiques[189]. Dans l'UE, le traitement de données à caractère personnel à des fins répressives est régi par un instrument spécifique, la Directive 2016/680/UE[190]. La directive établit des règles particulières pour la protection des données, qui lient les autorités compétentes lorsqu'elles traitent

186 CJUE, C-101/01, *Procédure pénale contre Bodil Lindqvist*, 6 novembre 2003, point 51.

187 Ex-article 8, para. 1, de la Directive 95/46/CE, devenu article 9, para. 1, du RGPD.

188 Convention 108 modernisée, art. 6, para. 1.

189 RGPD, art. 10.

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

des données à caractère personnel spécifiquement à des fins de prévention, d'enquête, de détection et de poursuite d'infractions pénales (voir la section 8.2.1).

2.2. Traitement de données

Points clés

- Le « traitement de données » couvre toute opération effectuée sur des données à caractère personnel.
- Le terme « traitement » fait référence au traitement automatisé et manuel.
- 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.

2.2.1. La notion de traitement des données

La notion de traitement des données est un concept exhaustif **aussi bien dans le droit de l'Union que dans celui du CdE** : « [...] "traitement de données à caractère personnel" désigne toute opération [...], telle que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction »[191] appliquée à des données à caractère personnel. La Convention 108 modernisée ajoute la préservation des données à caractère personnel à la définition[192].

Exemple : dans l'affaire *František Ryneš*[193], M. Ryneš avait enregistré l'image de deux individus cassant des vitres de sa maison grâce au système de surveillance CCTV qu'il avait installé pour protéger sa propriété. La CJUE a considéré que la vidéosurveillance impliquant l'enregistrement et la sauvegarde de données à caractère personnel constituait un traitement

191 RGPD, art. 4, para. 2. Voir aussi la Convention 108 modernisée, art. 2, point b).

192 Convention 108 modernisée, art. 2, point b).

193 CJUE, C-212/13, *František Ryneš c. Úřad pro ochranu osobních údajů*, 11 décembre 2014, point 25.

automatique de données relevant du champ d'application de la législation de l'UE en matière de protection des données.

Exemple : dans l'affaire *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce c. Salvatore Manni*[194], M. Manni avait demandé l'effacement des données à caractère personnel le concernant du registre des sociétés, qui le reliaient à la liquidation d'une société immobilière, ce qui avait un effet négatif sur sa réputation. La CJUE a déclaré qu'« en transcrivant et en conservant lesdites informations dans le registre et en communiquant celles-ci, le cas échéant, sur demande à des tiers, l'autorité chargée de la tenue de ce registre effectue un "traitement de données à caractère personnel", pour lequel elle est le "responsable" ».

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 modernisée et du RGPD. 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 – et en l'absence de tout autre motif légitime du traitement –, le transfert de données constitue un traitement illicite.

2.2.2. Traitement automatisé de données

Selon la Convention 108 modernisée et le RGPD, la protection des données s'applique pleinement au traitement automatisé de données.

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

194 CJUE, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce c. Salvatore Manni*, 9 mars 2017, point 35.

partie à l'aide de procédés automatisés »[195]. La Convention 108 modernisée contient une définition similaire[196]. Dans la pratique, cela signifie que tout traitement automatisé de données à caractère personnel à l'aide, par exemple, d'un ordinateur, d'un appareil portable ou d'un routeur, est couvert à la fois par les règles de l'UE et du CdE en matière de protection des données.

Exemple : l'affaire *Bodil Lindqvist*[197] concernait la référence, sur une page internet, à différentes personnes par leur nom ou par d'autres moyens, par exemple leur numéro de téléphone ou des informations relatives à leurs passe-temps. La CJUE a déclaré que « l'opération consistant à faire référence, sur une page internet, à diverses personnes et à les identifier soit par leur nom, soit par d'autres moyens, par exemple leur numéro de téléphone ou des informations relatives à leurs conditions de travail et à leurs passe-temps, constitue un "traitement de données à caractère personnel, automatisé en tout ou en partie", au sens de l'article 3, paragraphe 1, de la directive 95/46 »[198].

Exemple : dans l'affaire *Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos (AEPD) et Mario Costeja González*[199], M. González a demandé la suppression ou la modification d'un lien entre son nom dans le moteur de recherche Google et deux pages d'un quotidien contenant une annonce pour une vente aux enchères immobilière liée à une saisie pratiquée en recouvrement de dettes envers la sécurité sociale. La CJUE a considéré qu'« en explorant de manière automatisée, constante et systématique Internet à la recherche des informations qui y sont publiées, l'exploitant d'un moteur de recherche "collecte" de telles données qu'il "extrait", "enregistre" et "organise" par la suite dans le cadre de ses programmes d'indexation, "conserve" sur ses serveurs et, le cas échéant, "communique à" et "met à disposition de" ses utilisateurs sous forme de listes des résultats de leurs recherches »[200]. La Cour a conclu que ces opérations constituent un

195 RGPD, art. 2, para. 1, et art. 4, para. 2.

196 Convention 108 modernisée, art. 2, points b) et c) ; Rapport explicatif sur la Convention 108 modernisée, para. 21.

197 CJUE, C-101/01, *Procédure pénale contre Bodil Lindqvist*, 6 novembre 2003, point 27.

198 RGPD, art. 2, para. 1.

199 CJUE, C-131/12, *Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 13 mai 2014.

200 *Ibid.*, point 28.

« traitement », « sans qu'il importe que l'exploitant du moteur de recherche applique les mêmes opérations également à d'autres types d'information et ne distingue pas entre celles-ci et les données à caractère personnel ».

2.2.3. Traitement manuel de données

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[201]. Un système d'archivage structuré est un système qui classe un ensemble de données à caractère personnel et les rend accessibles selon certains critères. Par exemple, si un employeur tient à jour un dossier papier intitulé « congé des salariés », qui contient tous les détails des congés que les membres du personnel ont pris au cours de l'année écoulée et qu'il est classé par ordre alphabétique, le dossier constituera un système d'archivage manuel régi par les règles de l'UE en matière de protection des données. 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 rapide et aisée ; 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[202].

Dans le **droit du CdE**, la définition du traitement automatisé des données reconnaît que certaines étapes de traitement manuel de données à caractère personnel peuvent être nécessaires entre des opérations automatisées[203]. Aux termes de l'article 2, point c), de la Convention 108 modernisée, « [l]orsque aucun procédé automatisé n'est utilisé, le traitement de données désigne une opération ou des opérations effectuée(s) sur des données à caractère personnel au sein d'un ensemble structuré de données qui sont accessibles ou peuvent être retrouvées selon des critères spécifiques ».

201 RGPD, art. 2, para. 1.

202 RGPD, considérant 15.

203 Convention 108 modernisée, art. 2, points b) et c).

2.3. Utilisateurs de données à caractère personnel

Points clés

- Quiconque décide des moyens et des finalités du traitement de données à caractère personnel de tiers 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 personne physique ou morale 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 décide lui-même des moyens et des finalités du traitement de données.
- Toute personne à laquelle des données à caractère personnel sont divulguées est un « destinataire ».
- Un « tiers » est une personne physique ou morale autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui sont habilitées à traiter des données à caractère personnel sous l'autorité directe du responsable du traitement ou du sous-traitant.
- Le consentement comme base juridique du traitement de données à caractère personnel doit être libre, informé et spécifique. Il doit être une indication non équivoque des souhaits qui se traduit par un acte positif clair signifiant que la personne concernée accepte le traitement.
- Le traitement de catégories particulières de données sur la base d'un consentement requiert un consentement explicite.

2.3.1. Responsables du traitement et sous-traitants

Assumer la fonction de responsable du traitement ou de sous-traitant a pour conséquence la plus importante l'obligation légale de respecter les obligations respectives prévues par le droit en matière de protection des données. Dans le secteur privé, il s'agit habituellement d'une personne physique ou morale, tandis que dans le secteur public, il s'agit généralement d'une autorité. Il existe une différence fondamentale entre un responsable du traitement et un sous-traitant : le premier est la personne physique ou morale qui détermine les finalités et les modalités du traitement, alors que le second est la personne physique ou morale qui traite des données pour le compte du responsable du traitement, en suivant strictement ses

instructions. En principe, c'est le responsable du traitement qui doit contrôler le traitement et qui en est responsable, y compris sur le plan juridique. Cependant, à la suite de la réforme des règles relatives à la protection des données, les sous-traitants sont désormais tenus de se conformer à un grand nombre d'exigences applicables aux responsables du traitement. Ainsi, selon le RGPD, les sous-traitants doivent tenir un registre de toutes les catégories d'activités de traitement afin de prouver qu'ils se conforment à leurs obligations au titre du règlement[204]. Les sous-traitants sont également tenus de mettre en œuvre les mesures techniques et organisationnelles appropriées[205], de désigner un délégué à la protection des données dans certains cas[206] et de notifier au responsable du traitement toute violation de données[207].

Les éléments factuels ou les circonstances de chaque cas détermineront si une personne est habilitée à décider et à déterminer la finalité et les modalités du traitement. Selon la définition que donne le RGPD d'un responsable du traitement, une personne physique, une personne morale ou un autre organisme peut être un responsable du traitement. Toutefois, le Groupe de travail « Article 29 » a souligné qu'afin que les personnes concernées puissent s'adresser à une entité plus stable lorsqu'elles exercent leurs droits, « il serait préférable de considérer comme responsable du traitement la société ou l'organisme en tant que tel, plutôt qu'une personne en son sein »[208]. À titre d'exemple, une entreprise qui vend des produits de soins de santé à des praticiens est le responsable du traitement qui consiste à compiler et à tenir à jour la liste de distribution de tous les praticiens dans une zone donnée et non le responsable des ventes qui utilise et tient effectivement la liste à jour.

> 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.

204 RGPD, art. 30, para. 2.

205 *Ibid.*, art. 32.

206 *Ibid.*, art. 37.

207 *Ibid.*, art. 33, para. 2.

208 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.

Des personnes physiques peuvent être responsables du traitement tant dans le droit de l'Union que dans le droit du CdE. Cependant, les personnes privées qui traitent des données relatives à des tiers dans le cadre d'une activité strictement personnelle ou domestique ne relèvent pas des règles du RGPD ou de la Convention 108 modernisée et ne sont pas considérées comme des responsables du traitement[209]. Un individu qui conserve sa correspondance ou qui tient un journal intime décrivant des incidents avec des amis et des collègues et des dossiers de santé de membres de la famille peut être exempté des règles relatives à la protection des données, car ces activités pourraient être strictement personnelles ou domestiques. Le RGPD précise par ailleurs que les activités personnelles ou domestiques peuvent également englober l'utilisation de réseaux sociaux et les activités en ligne qui ont lieu dans le cadre de ces activités[210]. En revanche, les règles relatives à la protection des données s'appliquent pleinement aux responsables du traitement et aux sous-traitants qui fournissent les moyens de traiter des données à caractère personnel pour de telles activités personnelles ou domestiques (comme les plateformes de réseaux sociaux).[211]

L'accès des citoyens à internet et la possibilité d'utiliser des plateformes de commerce en ligne, des réseaux sociaux et des blogs pour partager des informations personnelles sur eux-mêmes et sur des tiers ont pour conséquence qu'il est de plus en plus difficile de séparer un traitement personnel d'un traitement qui ne l'est pas[212]. Le fait que des activités soient strictement personnelles ou domestiques dépend des circonstances[213]. Les activités qui comportent un aspect professionnel ou commercial ne peuvent pas relever de l'exemption domestique[214]. Par conséquent, lorsque l'ampleur et la fréquence du traitement des données suggèrent une activité professionnelle ou à temps plein, un particulier pourrait être considéré comme responsable du traitement. Outre le caractère professionnel ou commercial de l'activité de traitement, un autre facteur doit être pris en considération, à savoir le fait que les données à caractère personnel soient ou non rendues accessibles à un grand nombre de personnes manifestement étrangères à la sphère privée de la personne concernée. La jurisprudence se rapportant à la Directive relative à la protection des

209 RGPD, considérant 18 et art. 2, para. 2, point c) ; Convention 108 modernisée, art. 3, para. 2.

210 RGPD, considérant 18.

211 *Ibid.*, considérant 18 ; Rapport explicatif sur la Convention 108 modernisée, para. 29.

212 Voir la déclaration du Groupe de travail « Article 29 » sur les discussions concernant la réforme complète de la protection des données (2013), *Annexe 2 : Propositions et modifications concernant l'exemption pour activités personnelles ou domestiques*, 27 février 2013.

213 Rapport explicatif sur la Convention 108 modernisée, para. 28.

214 Voir RGPD, considérant 18, et Rapport explicatif sur la Convention 108 modernisée, para. 27.

données a retenu que le droit en matière de protection des données doit s'appliquer lorsqu'une personne privée publie des données sur des tiers sur un site web public dans le cadre de l'utilisation d'internet. La CJUE ne s'est pas encore prononcée sur des faits similaires dans le cadre du RGPD, qui fournit davantage d'orientations sur des sujets qui pourraient être considérés comme ne relevant pas du champ d'application de la législation sur la protection des données en vertu de l'« exemption domestique », comme l'utilisation des réseaux sociaux à des fins personnelles.

Exemple : l'affaire *Bodil Lindqvist*[215] concernait la référence, sur une page internet, à différentes personnes par leur nom ou par d'autres moyens, par exemple leur numéro de téléphone ou des informations relatives à leurs passe-temps. 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 [relative à la protection des données] »[216].

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 »[217].

Selon la CJUE, dans certains cas, les enregistrements vidéo d'une caméra de sécurité installée par un particulier peuvent également être couverts par la législation de l'UE en matière de protection des données.

Exemple : dans l'affaire *František Ryneš*[218], M. Ryneš avait enregistré l'image de deux individus cassant des vitres de sa maison grâce au système de surveillance CCTV qu'il avait installé pour protéger sa propriété.

215 CJUE, C-101/01, *Procédure pénale contre Bodil Lindqvist*, 6 novembre 2003.

216 *Ibid.*, point 27 ; ex-article 3, para. 1, de la Directive 95/46/CE, devenu article 2, para. 1, du RGPD.

217 CJUE, C-101/01, *Procédure pénale contre Bodil Lindqvist*, 6 novembre 2003, point 47.

218 CJUE, C-212/13, *František Ryneš c. Úřad pro ochranu osobních údajů*, 11 décembre 2014, point 33.

L'enregistrement a été remis à la police et a été invoqué au cours de la procédure pénale.

La CJUE a déclaré que « [d]ans la mesure où une vidéosurveillance [...] s'étend, même partiellement, à l'espace public et, de ce fait, est dirigée vers l'extérieur de la sphère privée de celui qui procède au traitement des données par ce moyen, elle ne saurait être considérée comme une activité exclusivement "personnelle ou domestique" »[219].

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 »[220]. La décision d'un responsable du traitement explique pourquoi et comment des données doivent être traitées.

Dans le droit du CdE, la Convention 108 modernisée définit un responsable du traitement comme « la personne physique ou morale, l'autorité publique, le service, l'agence ou tout autre organisme qui, seul ou conjointement avec d'autres, dispose du pouvoir de décision à l'égard du traitement des données »[221]. Ce pouvoir de décision concerne les finalités et les moyens du traitement de données, ainsi que les catégories de données à traiter et l'accès à celles-ci[222]. Le fait que ce pouvoir découle d'une désignation officielle ou de circonstances factuelles doit être apprécié au cas par cas[223].

Exemple : l'affaire *Google Spain*[224] a été engagée par un ressortissant espagnol qui souhaitait qu'un vieil article de journal relatif à sa situation financière passée soit retiré de Google.

219 Ex-article 3, para. 2, deuxième tiret, de la Directive 95/46/CE, devenu article 2, para. 2, point c), du RGPD.

220 RGPD, art. 4, para. 7.

221 Convention 108 modernisée, art. 2, point d).

222 Rapport explicatif sur la Convention 108 modernisée, para. 22.

223 *Ibid.*

224 CJUE, C-131/12, *Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 13 mai 2014.

La CJUE a demandé si Google, en tant qu'exploitant d'un moteur de recherche, était le « responsable du traitement » des données au sens de l'article 2, point d), de la Directive relative à la protection des données[225]. La CJUE a tenu compte d'une définition large de la notion de « responsable du traitement » pour assurer une « protection effective et complète des personnes concernées »[226]. La Cour a conclu que l'exploitant du moteur de recherche a déterminé les finalités et les moyens de l'activité et qu'il a rendu des données chargées sur des pages web par des éditeurs de sites internet accessibles à tout internaute effectuant une recherche à partir du nom de la personne concernée[227]. La Cour a donc conclu que Google peut être considéré comme le « responsable du traitement »[228].

Lorsqu'un responsable du traitement ou un sous-traitant est établi en dehors de l'UE, la société doit désigner par écrit un représentant dans l'Union[229]. Le RGPD précise que le représentant doit être établi dans « un des États membres dans lesquels se trouvent les personnes physiques dont les données à caractère personnel font l'objet d'un traitement lié à l'offre de biens ou de services, ou dont le comportement fait l'objet d'un suivi »[230]. Si aucun représentant n'est désigné, une action en justice peut être intentée contre le responsable du traitement ou le sous-traitant lui-même[231].

Responsabilité conjointe

Le RGPD prévoit que lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont considérés comme les responsables conjoints du traitement. En d'autres termes, ils décident ensemble de traiter des données pour une finalité commune[232]. Le rapport explicatif sur la

225 RGPD, art. 4, para. 7 ; CJUE, C-131/12, *Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 13 mai 2014, point 21.

226 CJUE, C-131/12, *Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 13 mai 2014, point 34.

227 *Ibid.*, points 35 à 40.

228 *Ibid.*, point 41.

229 RGPD, art. 27, para. 1.

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

231 *Ibid.*, art. 27, para. 5.

232 *Ibid.*, art. 4, para. 7, et art. 26.

Convention 108 modernisée précise qu'il est également possible d'avoir plusieurs responsables ou coresponsables du traitement **dans le cadre du CdE**[233].

Le Groupe de travail « Article 29 » souligne qu'une responsabilité conjointe peut revêtir différentes formes et que la participation des différents responsables du traitement aux activités de contrôle peut être inégale[234]. Cette flexibilité permet de faire face à la complexité croissante de la réalité du traitement de données[235]. Les responsables conjoints du traitement doivent donc définir leurs responsabilités respectives pour se conformer aux obligations imposées par le règlement dans le cadre d'un accord spécifique[236].

La responsabilité conjointe conduit à une coresponsabilité dans la réalisation d'une activité de traitement[237]. Dans le cadre du droit de l'Union, cela signifie que chaque responsable du traitement ou sous-traitant peut être tenu responsable du dommage dans sa totalité causé par le traitement en vertu d'une responsabilité conjointe, afin de garantir à la personne concernée une réparation effective[238].

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.

Les dispositions légales ne précisent 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 seulement. Il n'existe toutefois encore aucune jurisprudence au niveau européen. Dans son avis de 2010 sur les responsables du traitement et les sous-traitants, le Groupe de travail « Article 29 » indique que les coresponsables du traitement peuvent soit partager toutes les

233 Convention 108 modernisée, art. 2, point d) ; Rapport explicatif sur la Convention 108 modernisée, para. 22.

234 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.

235 *Ibid.*

236 RGPD, considérant 79.

237 *Ibid.*, para. 21.

238 *Ibid.*, art. 82, para. 4.

finalités et tous les moyens du traitement, soit ne partager que certaines finalités ou moyens ou une partie de ceux-ci[239]. Alors que la première option impliquerait une relation très proche entre les différents acteurs, la seconde indiquerait une relation plus distante.

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[240]. 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, au départ, employé SWIFT comme sous-traitant pour procéder à des transferts de données dans le cadre de transactions bancaires. SWIFT avait divulgué ces données bancaires, 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[241].

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[242]. 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.

239 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.

240 *Ibid*.

241 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.

242 RGPD, art. 4, para. 8.

Dans le droit du CdE, la notion de sous-traitant a la même signification que dans le droit de l'UE[243].

Les sous-traitants, en plus de traiter des données pour des tiers, sont 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.

> Exemple : 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. 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 les finalités et les moyens du traitement. Le RGPD indique également clairement que le sous-traitant ne peut traiter des données à caractère personnel que sur instruction du responsable du traitement, à moins d'y être obligé par le droit de l'Union ou le droit d'un État membre[244]. Le contrat qui lie le responsable du traitement et le sous-traitant est un élément essentiel de leur relation et est une exigence légale[245].

> Exemple : le directeur de la société Sunshine décide que la société Cloudy, spécialisée dans le stockage de données sur le Cloud, doit gérer les données clients de Sunshine. La société Sunshine reste le responsable du traitement et la société Cloudy n'est qu'un sous-traitant puisque, aux termes du contrat, Cloudy 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 de manière appropriée sur les décisions du sous-traitant concernant les modalités du traitement.

243 Convention 108 modernisée, art. 2, point f).

244 RGPD, art. 29.

245 *Ibid.*, art. 28, para. 3.

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.

En outre, si un sous-traitant ne respectait pas les conditions d'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 illicitement. À son tour, le responsable initial du traitement serait tenu d'expliquer comment le sous-traitant a pu ne pas honorer son mandat[246]. 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[247].

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[248].

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[249]. Celui-ci doit notamment préciser l'objet, la nature, la finalité et la durée du traitement, le type de données à caractère personnel et les catégories de personnes concernées. Il devrait également stipuler les obligations et les droits du responsable du traitement et du sous-traitant, telles que les exigences en termes de confidentialité et de sécurité. 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. Lorsqu'un dommage est causé

246 *Ibid*., art. 82, para. 2.

247 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. 25 ; 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.

248 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. 26.

249 RGPD, art. 28, paras. 3 et 9.

parce que le sous-traitant n'a pas respecté les instructions légales du responsable du traitement, ce dernier n'est pas le seul qui peut être tenu responsable ; le sous-traitant peut l'être aussi[250]. Le sous-traitant doit tenir un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement[251]. Ces registres doivent être mis à la disposition de l'autorité de contrôle à sa demande, étant donné que le responsable du traitement et le sous-traitant doivent coopérer avec cette autorité dans l'exécution de ses missions[252]. Les responsables du traitement et les sous-traitants ont la possibilité d'adhérer à un code de conduite ou à un mécanisme de certification approuvé pour démontrer leur conformité avec les exigences énoncées dans le RGPD[253].

Certains sous-traitants pourraient vouloir déléguer certaines tâches à d'autres sous-traitants. La loi le permet, pour autant que des clauses contractuelles appropriées soient convenues entre le responsable du traitement et le sous-traitant, y compris en ce qui concerne la question de savoir si l'autorisation du responsable du traitement est nécessaire dans chaque cas, ou si une simple information suffit. Le RGPD dispose que lorsqu'un sous-traitant ne remplit pas ses obligations en matière de protection des données, le sous-traitant initial demeure pleinement responsable devant le responsable du traitement de ses obligations[254].

Dans le droit du CdE, l'interprétation des notions de responsable du traitement et de sous-traitant, expliquées ci-dessus, est pleinement applicable[255].

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.

250 *Ibid.*, art. 82, para. 2.

251 *Ibid.*, art. 30, para. 2.

252 *Ibid.*, art. 30, para. 4, et art. 31.

253 *Ibid.*, art. 28, para. 5, et art. 42, para. 4.

254 *Ibid.*, art. 28, para. 4.

255 Voir, par exemple, Convention 108 modernisée, article 2, points b) et f) ; Recommandation sur le profilage, article premier.

Un « tiers » est une personne légalement distincte du responsable du traitement et du sous-traitant. Conformément à l'article 4, paragraphe 10, du RGPD, un tiers est « une personne physique ou morale, une autorité publique, un service ou un organisme autre que 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 autorisées à traiter les données à caractère personnel ». Cela signifie que les personnes qui travaillent pour une organisation qui est juridiquement 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 du siège ne seraient pas des « tiers »[256].

Le terme « destinataire » est plus large que celui de « tiers ». Selon l'article 4, paragraphe 9, du RGPD, on entend par destinataire « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, 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 pour des motifs juridiques spécifiques dans un cas particulier.

Exemple : un salarié du responsable du traitement, 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 responsable du traitement. Ainsi, si un employeur divulgue des données à caractère personnel sur ses salariés à son département des ressources humaines pour les prochaines évaluations de performance, l'équipe des ressources humaines sera le

256 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. 31.

destinataire des données à caractère personnel, puisque les données lui ont été transmises dans le cadre du traitement pour le responsable du traitement.

En revanche, si l'organisation fournit des données sur ses salariés à une société de formation qui les utilisera pour adapter son programme de formation aux salariés, cette société de formation est un tiers. En effet, la société de formation n'a pas de légitimité ou d'autorisation particulière (laquelle, dans le cas des « ressources humaines », découle de la relation d'emploi avec le responsable du traitement) pour traiter ces données à caractère personnel. En d'autres termes, elle n'a pas reçu les informations dans le cadre de son emploi chez le responsable du traitement.

2.4. Consentement

Points clés

- Le consentement comme base juridique du traitement de données à caractère personnel doit être une manifestation de volonté libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte le traitement de ses données par un acte positif clair.
- Le traitement de catégories particulières de données requiert un consentement explicite.

Comme cela sera approfondi dans le chapitre 4, le consentement est l'un des six motifs légitimes du traitement de données à caractère personnel. On entend par consentement « toute manifestation de volonté, libre, spécifique, éclairée et univoque » de la personne concernée[257].

Le droit de l'UE définit plusieurs éléments de la validité du consentement, l'objectif étant de garantir que les personnes concernées souhaitent véritablement accepter une utilisation particulière de leurs données[258].

- Le consentement doit être donné par un acte positif clair représentant une manifestation libre, spécifique, éclairée et univoque que la personne concernée

257 RGPD, art. 4, para. 11. Voir aussi la Convention 108 modernisée, art. 5, para. 2.

258 RGPD, art. 7.

accepte le traitement de ses données. Cet acte peut être une action ou une déclaration.

- La personne concernée doit avoir le droit de retirer son consentement à tout moment.

- Dans le cadre d'une déclaration écrite qui concerne également d'autres questions, comme des « conditions de service », la demande de consentement doit être présentée en des termes clairs et simples et sous une forme compréhensible et aisément accessible, qui distingue clairement le consentement de ces autres questions ; si une partie de cette déclaration est contraire au RGPD, elle ne sera pas contraignante.

Le consentement ne sera valable dans le contexte de la législation en matière de protection des données que si toutes ces conditions sont remplies. Il appartient au responsable du traitement de démontrer que la personne concernée a donné son consentement au traitement de ses données[259]. Les éléments d'un consentement valable seront discutés à la section 4.1.1 sur la licéité du traitement de données à caractère personnel.

La Convention 108 ne contient pas de définition du consentement ; cette question est laissée à l'appréciation du législateur national. Toutefois, **dans le droit du CdE**, les éléments d'un consentement valable correspondent à ceux exposés plus haut[260].

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 de conditions juridiques préalables essentielles. Le consentement nul de personnes dépourvues de capacité juridique entraîne l'absence de base juridique pour le traitement de données concernant ces personnes. S'agissant de la capacité juridique des mineurs à conclure un contrat, le RGPD prévoit que ses règles relatives à l'âge minimum pour obtenir un consentement valable ne portent pas atteinte au droit général des contrats des États membres[261].

259 *Ibid.*, art. 7, para. 1.

260 Convention 108 modernisée, art. 5, para. 2 ; Rapport explicatif sur la Convention 108 modernisée, paras. 42 à 45.

261 RGPD, art. 8, para. 3.

Le consentement doit être donné de façon claire de manière à ne laisser aucun doute quant à l'intention de la personne concernée[262]. Il doit être explicite lorsqu'il concerne le traitement de données sensibles et peut se faire au moyen d'une déclaration orale ou écrite[263]. Cet acte peut être effectué par voie électronique[264]. **Dans le droit de l'UE** et **dans celui du CdE**, le consentement au traitement des données à caractère personnel doit être donné par la personne concernée soit par le biais d'une déclaration, soit par une action affirmative claire[265]. Le silence, l'inaction, des cases à cocher prévalidées ou des formulaires précomplétés ne peuvent donc pas constituer un consentement[266].

262 *Ibid.*, art. 6, para. 1, point a), et art. 9, para. 2, point a).

263 *Ibid.*, considérant 32.

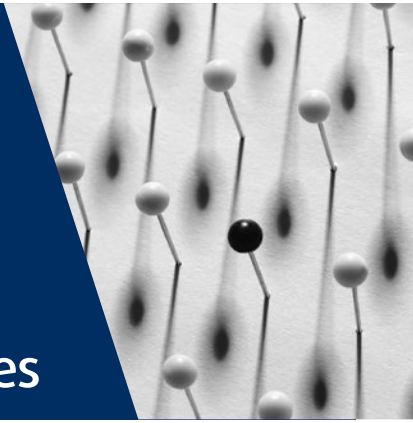
264 *Ibid.*

265 *Ibid.*, art. 4, para. 11 ; Rapport explicatif sur la Convention 108 modernisée, para. 42.

266 RGPD, considérant 32 ; Rapport explicatif sur la Convention 108 modernisée, para. 42.

3

Principes clés du droit européen en matière de protection des données



UE	Questions traitées	CdE
RGPD, art. 5, para. 1, point a)	Le principe du traitement licite	Convention 108 modernisée, art. 5, para. 3
RGPD, art. 5, para. 1, point a)	Le principe du traitement loyal	Convention 108 modernisée, art. 5, para. 4, point a) CouEDH, *K.H. et autres c. Slovaquie*, nº 32881/04, 2009
RGPD, art. 5, para. 1, point a) CJUE, C-201/14, *Smaranda Bara et autres c. Casa Națională de Asigurări de Sănătate et autres*, 2015	Le principe de la transparence	Convention 108 modernisée, art. 5, para. 4, point a), et art. 8 CouEDH, *Haralambie c. Roumanie*, nº 21737/03, 2009
RGPD, art. 5, para. 1, point b)	Le principe de la limitation de la finalité	Convention 108 modernisée, art. 5, para. 4, point b)
RGPD, art. 5, para. 1, point c) CJUE, affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland* et Kärntner Landesregierung *et autres* [GC], 2014	Le principe de la minimisation des données	Convention 108 modernisée, art. 5, para. 4, point c)
RGPD, art. 5, para. 1, point d) CJUE, C-553/07, *College van burgemeester en wethouders van Rotterdam c. M. E. E. Rijkeboer*, 2009	Le principe de l'exactitude des données	Convention 108 modernisée, art. 5, para. 4, point d)
RGPD, art. 5, para. 1, point e) CJUE, affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland* et Kärntner Landesregierung *et autres* [GC], 2014	Le principe de la limitation de la durée de conservation	Convention 108 modernisée, art. 5, para. 4, point e) CouEDH, *S. et Marper c. Royaume-Uni* [GC], nº 30562/04 et nº 30566/04, 2008

UE	Questions traitées	CdE
RGPD, art. 5, para. 1, point f), et art. 32	Le principe de la sécurité (intégrité et confidentialité) des données	Convention 108 modernisée, art. 7
RGPD, art. 5, para. 2	Le principe de la responsabilité	Convention 108 modernisée, art. 10

L'article 5 du Règlement général sur la protection des données énonce les principes qui régissent le traitement de données à caractère personnel. Ces principes couvrent :

- la licéité, la loyauté et la transparence ;
- la limitation de la finalité ;
- la minimisation des données ;
- l'exactitude des données ;
- la limitation de la durée de conservation ;
- l'intégrité et la confidentialité.

Ces principes servent de point de départ aux dispositions plus détaillées des articles suivants du règlement. Ils sont également mentionnés aux articles 5, 7, 8 et 10 de la Convention 108 modernisée. Toute la législation postérieure relative à la protection des données au niveau du CdE ou de l'UE doit se conformer à ces principes, qui doivent être gardés à l'esprit dans l'interprétation de cette législation. Dans le droit de l'Union, les restrictions aux principes applicables au traitement ne sont autorisées que dans la mesure où elles correspondent aux droits et obligations prévus aux articles 12 à 22 et elles doivent respecter le contenu essentiel des droits et libertés fondamentaux. Toute exception ou restriction afférente à ces principes clés peut être prévue au niveau national ou de l'UE[267] ; elle doit être prévue par la loi, poursuivre un objectif légitime et être nécessaire et proportionnée dans une société démocratique[268]. Ces trois conditions sont cumulatives.

267 Convention 108 modernisée, art. 9, para. 1 ; RGPD, art. 23, para. 1.

268 RGPD, art. 23, para. 1.

3.1. Les principes de licéité, de loyauté et de transparence du traitement

Points clés

- Les principes de licéité, de loyauté et de transparence s'appliquent à tout traitement de données à caractère personnel.
- Conformément au RGPD, la licéité requiert :
  - le consentement de la personne concernée,
  - la nécessité de conclure un contrat,
  - une obligation légale,
  - la nécessité de protéger les intérêts vitaux de la personne concernée ou d'une autre personne physique,
  - la nécessité d'exécuter une tâche dans l'intérêt public,
  - la nécessité de protéger les intérêts légitimes du responsable du traitement ou d'un tiers, lorsque les intérêts et les droits de la personne concernée ne priment pas sur ceux-ci.
- Les données à caractère personnel doivent être traitées de manière loyale.
  - La personne concernée doit être informée du risque afin de s'assurer que le traitement n'a pas d'effets négatifs imprévisibles.
- Les données à caractère personnel doivent être traitées de manière transparente.
  - Les responsables du traitement doivent informer les personnes concernées du traitement de leurs données, notamment de la finalité du traitement ainsi que de l'identité et de l'adresse du responsable du traitement.
  - Les informations relatives au traitement doivent être communiquées en termes clairs et simples afin de permettre aux personnes concernées de comprendre aisément les règles, les risques, les garanties et les droits concernés.
  - Les personnes concernées ont le droit d'accéder à leurs données chaque fois qu'elles sont traitées.

3.1.1. Licéité du traitement

Le droit de l'UE et celui du CdE en matière de protection des données imposent tous deux que le traitement de données à caractère personnel soit licite[269]. Pour être licite, le traitement doit être fondé sur le consentement de la personne concernée ou reposer sur tout autre fondement légitime prévu par la législation relative à la protection des données[270]. L'article 6, paragraphe 1, du RGPD énumère cinq fondements légitimes d'un traitement, outre le consentement, à savoir que le traitement de données à caractère personnel est nécessaire à l'exécution d'un contrat ou à l'exécution d'une mission relevant de l'exercice de l'autorité publique, au respect d'une obligation légale, aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers ou est nécessaire pour protéger les intérêts fondamentaux de la personne concernée. Ce point sera discuté plus en détail à la section 4.1.

3.1.2. Loyauté du traitement

Outre la licéité du traitement, le droit de l'UE et celui du CdE en matière de protection des données imposent que le traitement de données à caractère personnel soit loyal[271]. Le principe de loyauté du traitement régit essentiellement la relation entre le responsable du traitement et la personne concernée.

Les responsables du traitement devaient informer les personnes concernées et le grand public qu'ils vont traiter des données de manière licite et transparente et ils doivent être en mesure de démontrer que les traitements sont conformes au RGPD. Les traitements ne doivent pas être réalisés en secret et les personnes concernées doivent être conscientes des risques potentiels. En outre, les responsables du traitement doivent, dans la mesure du possible, agir de façon à se conformer rapidement aux souhaits de la personne concernée, en particulier quand son consentement constitue la base juridique du traitement des données.

Exemple : dans l'affaire *K.H. et autres c. Slovaquie*[272], les requérantes étaient des femmes d'origine rom, qui avaient été suivies dans deux hôpitaux de l'est de la Slovaquie pendant leur grossesse et leur accouchement. Par la suite,

269 Convention 108 modernisée, art. 5, para. 3 ; RGPD, art. 5, para. 1, point a).

270 Charte des droits fondamentaux de l'Union européenne, art. 8, para. 2 ; RGPD, considérant 40 et art. 6 à 9 ; Convention 108 modernisée, art. 5, para. 2 ; Rapport explicatif sur la Convention 108 modernisée, para. 41.

271 RGPD, art. 5, para. 1, point a) ; Convention 108 modernisée, art. 5, para. 4, point a).

272 CouEDH, *K.H. et autres c. Slovaquie*, nº 32881/04, 28 avril 2009.

aucune d'elles n'a plus pu concevoir d'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 prétendu 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 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. En tout état de cause, le principe de loyauté va au-delà des obligations de transparence et pourrait également être lié au traitement de données à caractère personnel de manière éthique.

Exemple : le département de recherche d'une université conduit une expérience visant à analyser les changements d'humeur de 50 personnes. Celles-ci sont invitées à noter toutes les heures leurs pensées dans un fichier électronique, à heure fixe. Les cinquante personnes ont donné leur consentement pour ce projet particulier et à cette utilisation spécifique des données par l'université. Le département de recherche découvre rapidement que l'enregistrement électronique de pensées serait extrêmement utile pour un autre projet axé sur la santé mentale et coordonné par une autre équipe. Même si l'université, en tant que responsable du traitement, aurait pu utiliser les mêmes données pour les travaux d'une autre équipe sans autres mesures

destinées à garantir la licéité du traitement de ces données, étant donné que les finalités sont compatibles, l'université a informé les personnes concernées et a demandé leur consentement, conformément à son code de déontologie de recherche et au principe de loyauté du traitement.

3.1.3. Transparence du traitement

Tant le droit de l'UE que le droit du CdE en matière de protection des données imposent que le traitement des données à caractère personnel soit effectué « de manière transparente au regard de la personne concernée »[273].

Ce principe impose au responsable du traitement l'obligation de prendre toute mesure appropriée pour fournir aux personnes concernées – qui peuvent être des utilisateurs ou des clients – des informations sur la manière dont leurs données sont utilisées[274]. La transparence peut faire référence aux informations fournies à la personne avant le début du traitement[275], aux informations qui devraient être aisément accessibles aux personnes concernées durant le traitement[276], mais aussi aux informations fournies aux personnes concernées à la suite d'une demande d'accès aux données les concernant[277].

Exemple : dans l'affaire *Haralambie c. Roumanie*[278], le requérant n'a obtenu l'accès au dossier que les services secrets avaient constitué à son sujet que cinq ans après sa demande. La CouEDH a rappelé que les personnes faisant l'objet de fichiers personnels détenus par les pouvoirs publics ont un intérêt vital 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 dossier

273 RGPD, art. 5, para. 1, point a) ; Convention 108 modernisée, art. 5, para. 4, point a), et art. 8.

274 RGPD, art. 12.

275 *Ibid.*, art. 13 et 14.

276 Groupe de travail « Article 29 », *Avis 2/2017 sur le traitement des données au travail*, p. 23.

277 RGPD, art. 15.

278 CouEDH, *Haralambie c. Roumanie*, nº 21737/03, 27 octobre 2009.

personnel dans un délai raisonnable. La CouEDH a donc conclu à une violation de l'article 8 de la CEDH.

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. Cela signifie que la personne concernée doit connaître la finalité spécifique du traitement de données à caractère personnel lors de la collecte des données la concernant[279]. La transparence du traitement exige que des termes clairs et simples soient utilisés[280]. Les personnes concernées doivent être clairement informées des risques, règles, garanties et droits liés au traitement de leurs données à caractère personnel[281].

Le droit du CdE précise également que le responsable du traitement doit fournir de façon proactive certaines informations essentielles aux personnes concernées. Les informations sur le nom et l'adresse du responsable du traitement (ou des coresponsables), la base légale et les finalités du traitement effectué, les catégories de données traitées et leurs destinataires ainsi que les moyens d'exercer les droits, peuvent être fournies sous tout format approprié (par le biais d'un site web, d'outils technologiques sur des dispositifs personnels, etc.) dès lors qu'elles sont présentées de manière effective et loyale à la personne concernée. Ces informations doivent être facilement accessibles, lisibles, compréhensibles et adaptées aux personnes concernées (dans un langage adapté aux enfants, par exemple). Tout autre renseignement nécessaire pour garantir un traitement loyal des données ou qui serait utile en ce sens, comme la durée de conservation des données, la connaissance du raisonnement qui sous-tend le traitement des données ou des informations sur les transferts de données vers une Partie à la Convention ou un État qui n'y est pas Partie (notamment sur la question de savoir si cette non-Partie offre ou non un niveau de protection approprié ou sur les mesures prises par le responsable du traitement pour garantir un tel niveau de protection) devra également être fourni.[282]

En vertu du droit d'accès[283], à sa demande, la personne concernée a le droit d'obtenir du responsable du traitement la confirmation que ses données sont traitées et,

279 RGPD, considérant 39.

280 *Ibid.*

281 *Ibid.*

282 Rapport explicatif sur la Convention 108 modernisée, para. 68.

283 RGPD, art. 15.

lorsqu'elles le sont, quelles données font l'objet du traitement[284]. De plus, au titre du droit à l'information[285], les responsables du traitement ou les sous-traitants doivent informer de manière proactive les personnes dont les données sont traitées des finalités du traitement, de sa durée et des moyens utilisés, entre autres choses, en principe avant le début du traitement.

> Exemple : l'affaire *Smaranda Bara et autres c. Președintele Casei Naționale de Asigurări de Sănătate, Casa Națională de Administrare Fiscală (ANAF)*[286] concernait la transmission de données fiscales relatives aux revenus de travailleurs indépendants par l'administration fiscale nationale au fonds national roumain d'assurance maladie. Sur base de ces données, le paiement d'arriérés de contributions au régime d'assurance maladie a été exigé. La CJUE était invitée à déterminer si la personne concernée aurait dû être informée au préalable de l'identité du responsable du traitement et de la finalité de la transmission des données avant que celles-ci ne soient traitées par le fonds national d'assurance maladie. La CJUE a conclu que lorsqu'une administration publique d'un État membre transmet des données à caractère personnel à une autre administration publique qui traite ultérieurement ces données, les personnes concernées doivent être informées de la transmission ou du traitement.

Dans certains cas, des dérogations à l'obligation d'informer les personnes concernées du traitement de leurs données sont autorisées ; celles-ci seront discutées plus en détail à la section 6.1.

3.2. Principe de la limitation de la finalité

Points clés

- La finalité du traitement des données doit être définie avant le début du traitement.

284 Convention 108 modernisée, art. 8 et art. 9, para. 1, point b).

285 RGPD, art. 13 et 14.

286 CJUE, C-201/14, *Smaranda Bara et autres c. Casa Națională de Asigurări de Sănătate et autres*, 1er octobre 2015, points 28 à 46.

- Il ne peut y avoir de traitement ultérieur des données incompatible avec la finalité initiale, bien que le Règlement général sur la protection des données prévoie des exceptions à cette règle à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique et à des fins statistiques.
- Fondamentalement, le principe de la limitation de la finalité signifie que tout traitement de données à caractère personnel doit être réalisé pour une finalité particulière bien définie et uniquement pour des finalités supplémentaires spécifiques compatibles avec la finalité initiale.

Le principe de la limitation de la finalité est l'un des principes fondamentaux du droit européen de la protection des données. Il est étroitement lié à la transparence, à la prévisibilité et au contrôle par l'utilisateur : en effet, si la finalité du traitement est suffisamment précise et claire, les personnes savent à quoi s'attendre et la transparence et la sécurité juridique s'en trouvent renforcées. Parallèlement, une délimitation claire de la finalité est importante pour permettre aux personnes concernées d'exercer effectivement leurs droits, comme celui de s'opposer au traitement[287].

Ce principe impose que tout traitement de données à caractère personnel soit effectué pour une finalité particulière bien définie et uniquement pour des finalités supplémentaires compatibles avec la finalité initiale[288]. Le traitement de données à caractère personnel à des fins indéfinies et/ou illimitées est donc illicite. En l'absence d'une finalité spécifique, le traitement de données à caractère personnel reposant simplement sur l'idée que les données pourraient être utiles à un moment donné dans le futur, n'est pas licite non plus. La légitimité du traitement de données à caractère personnel dépendra de sa finalité, qui doit être déterminée, explicite et légitime.

Chaque nouvelle finalité du traitement de données qui n'est pas compatible avec la finalité initiale doit avoir sa propre base juridique et ne peut se fonder sur le fait que les données ont été collectées ou traitées initialement pour une autre finalité légitime. À son tour, un traitement légitime est limité à la finalité définie initialement et toute nouvelle finalité requerra une nouvelle base juridique distincte. À titre d'exemple, la communication de données à caractère personnel à des tiers pour une finalité nouvelle devra être envisagée avec prudence, car la divulgation nécessitera une nouvelle base juridique, distincte de celle de la collecte des données.

287 Groupe de travail « Article 29 » (2013), *Avis 3/2013 sur la limitation de la finalité*, WP 203, 2 avril 2013.

288 RGPD, art. 5, para. 1, point b).

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 tels que celui d'un fauteuil roulant, et les exigences alimentaires particulières, telles qu'une nourriture casher ou halal. S'il est demandé à des compagnies aériennes de communiquer 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 la collecte des données. Le transfert de ces données à un service de l'immigration nécessitera par conséquent une nouvelle base juridique distincte.

Pour apprécier l'étendue et les limites d'une finalité particulière, la Convention 108 modernisée et le Règlement général sur la protection des données s'en remettent au concept de la compatibilité : l'utilisation de données à des fins compatibles est permise sur le fondement de la base juridique initiale. Les données ne doivent pas faire l'objet d'un traitement ultérieur que la personne concernée pourrait considérer comme inattendu, inapproprié ou contestable[289]. Afin d'établir si la finalité d'un traitement ultérieur est compatible, le responsable du traitement devrait tenir compte, entre autres :

- « de tout lien entre ces finalités et les finalités du traitement ultérieur prévu ;
- du contexte dans lequel les données à caractère personnel ont été collectées, en particulier les attentes raisonnables des personnes concernées, en fonction de leur relation avec le responsable du traitement, quant à l'utilisation ultérieure desdites données ;
- la nature des données à caractère personnel ;
- les conséquences pour les personnes concernées du traitement ultérieur prévu ; et

289 Rapport explicatif sur la Convention 108 modernisée, para. 49.

- l'existence de garanties appropriées à la fois dans le cadre du traitement initial et du traitement ultérieur prévu »[290]. Ceci pourrait, par exemple, se faire par cryptage ou par pseudonymisation.

Exemple : la société Sunshine acquiert des données clients dans le cadre de la gestion de la relation client (GRC). Elle transmet ensuite ces données à une société de prospection, Moonlight, qui souhaite utiliser ces données pour contribuer aux campagnes marketing d'autres entreprises. La transmission par Sunshine de ces données à des fins de marketing par d'autres entreprises constitue une utilisation ultérieure des données pour une nouvelle finalité, incompatible avec la gestion de la relation client, qui est la finalité initiale de la société Sunshine justifiant la collecte des données clients. La transmission des données à Moonlight requiert donc une base juridique propre.

En revanche, l'utilisation par la société Sunshine des données GRC à ses propres fins de marketing, c'est-à-dire pour l'envoi de messages commerciaux à ses propres clients pour ses propres produits, est généralement reconnue comme une finalité compatible.

Le RGPD et la Convention 108 modernisée disposent que le « traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques » est, *a priori* jugé compatible avec la finalité initiale[291]. Toutefois, des garanties appropriées, telles que l'anonymisation, le cryptage ou la pseudonymisation des données et la restriction d'accès aux données, doivent être appliquées lors du traitement ultérieur de données à caractère personnel[292]. Le RGPD ajoute que « [l]orsque la personne concernée a donné son consentement ou que le traitement est fondé sur le droit de l'Union ou le droit d'un État membre qui constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir, en particulier, d'importants objectifs d'intérêt public général, le responsable du traitement devrait être autorisé à effectuer un traitement ultérieur des données à caractère personnel indépendamment de la compatibilité des

290 RGPD, considérant 50 et art. 6, para. 4 ; Rapport explicatif sur la Convention 108 modernisée, para. 49.

291 RGPD, art. 5, para. 1, point b) ; Convention 108 modernisée, art. 5, para. 4, point b). La loi autrichienne relative à la protection des données (*Datenschutzgesetz*), Journal officiel fédéral I nº 165/1999, para. 46, en est un exemple.

292 RGPD, art. 6, para. 4 ; Convention 108 modernisée, art. 5, para. 4, point b) ; Rapport explicatif sur la Convention 108 modernisée, para. 50.

finalités »[293]. Lors du traitement ultérieur, l'information de la personne concernée au sujet de ces autres finalités et de ses droits, y compris le droit de s'opposer au traitement, devrait être assurée[294].

Exemple : 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 juridique nouvelle, telle que le consentement des personnes concernées, n'est nécessaire. Toutefois, pour le traitement ultérieur des données à caractère personnel à des fins statistiques, la société Sunshine doit mettre en place des garanties appropriées afin de protéger les droits et libertés de la personne concernée. Les mesures techniques et organisationnelles que Sunshine doit appliquer peuvent inclure la pseudonymisation.

3.3. Le principe de la minimisation des données

Points clés

- Le traitement des données doit être limité à ce qui est nécessaire au regard d'une finalité légitime.
- Le traitement de données à caractère personnel ne devrait avoir lieu que lorsque la finalité du traitement ne peut raisonnablement pas être atteinte par d'autres moyens.
- Le traitement des données ne peut interférer de manière disproportionnée avec les intérêts, les droits et les libertés en cause.

Ne sont traitées que les données qui sont « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont collectées et/ou traitées ultérieurement »[295]. Les catégories de données choisies pour le traitement

293 RGPD, considérant 50.

294 *Ibid.*

295 Convention 108 modernisée, art. 5, para. 4, point c) ; RGPD, art. 5, para. 1, point c).

doivent être nécessaires pour atteindre l'objectif général déclaré des traitements et un responsable du traitement doit limiter au strict minimum la collecte de données aux informations directement pertinentes pour la finalité spécifique poursuivie par le traitement.

Exemple : dans l'affaire *Digital Rights Ireland*[296], la CJUE a examiné la validité de la Directive relative à la conservation des données, qui visait à harmoniser les dispositions nationales applicables à la conservation des données à caractère personnel générées ou traitées par des services ou des réseaux de communications électroniques accessibles au public en vue de leur transmission éventuelle aux autorités chargées de la lutte contre les infractions graves, comme le crime organisé et le terrorisme. Nonobstant le fait que la Cour a considéré que cela constituait une finalité répondant à un objectif d'intérêt général, le fait que la directive couvre de manière généralisée « toute personne et tous les moyens de communication électronique ainsi que l'ensemble des données relatives au trafic sans qu'aucune différenciation, limitation ni exception ne soient opérées en fonction de l'objectif de lutte contre les infractions graves » a été jugé problématique[297].

Par ailleurs, grâce à l'utilisation de technologies spéciales renforçant la protection de la vie privée, il est parfois possible d'éviter complètement l'utilisation de données à caractère personnel ou d'appliquer des mesures permettant de réduire la capacité de réattribuer des données à une personne concernée (par exemple, par la pseudonymisation), ce qui aboutit à une solution respectueuse de la vie privée. Ceci est particulièrement approprié dans le cadre de systèmes de traitement plus vastes.

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, par exemple les bus et les trams. Les données lues par l'appareil font l'objet

296 CJUE, affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources et autres* et *Kärntner Landesregierung et autres* [GC], 8 avril 2014.

297 *Ibid.*, points 44 et 57.

d'une vérification électronique dans la base de données contenant les noms des personnes ayant acheté la carte.

Ce système n'est pas totalement conforme au principe de la minimisation des données : vérifier qu'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-barres, 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 minimisation, puisque ce principe entraîne l'obligation de minimiser la collecte de données.

L'article 5, paragraphe 1, de la Convention 108 modernisée impose une obligation de proportionnalité du traitement des données à caractère personnel au regard de la finalité légitime poursuivie. Un juste milieu doit être trouvé entre tous les intérêts en jeu à toutes les étapes du traitement. En d'autres termes, « des données qui seraient adéquates et pertinentes mais entraîneraient une ingérence disproportionnée dans les droits et libertés fondamentaux en jeu doivent être considérées comme excessives et ne pas être traitées »[298].

3.4. Le principe de l'exactitude des données

Points clés

- Le responsable du traitement doit appliquer le principe de l'exactitude des données à tous les traitements.
- Les données inexactes doivent être effacées ou corrigées sans délai.
- Il peut être nécessaire de vérifier et de mettre à jour régulièrement les données afin de garantir leur exactitude.

298 Rapport explicatif sur la Convention 108 modernisée, para. 52 ; RGPD, art. 5, para. 1, point c).

Un responsable du traitement qui détient des informations personnelles ne peut utiliser celles-ci sans prendre de mesures pour s'assurer, avec une certitude raisonnable, que les données sont exactes et à jour[299].

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

Exemple : dans l'affaire *Rijkeboer*[300], la CJUE a examiné la demande d'un ressortissant néerlandais de recevoir des informations de l'administration communale d'Amsterdam sur l'identité des personnes auxquelles des données le concernant provenant de l'administration communale avaient été transmises au cours des deux années précédentes ainsi que sur le contenu des données communiquées. La CJUE a déclaré que le « droit au respect de la vie privée implique que la personne concernée puisse s'assurer que ses données à caractère personnel sont traitées de manière exacte et licite, c'est-à-dire, en particulier, que les données de base la concernant sont exactes et qu'elles sont adressées à des destinataires autorisés ». La Cour a ensuite fait référence à l'exposé des motifs de la Directive relative à la protection des données, qui dispose que toute personne concernée doit pouvoir bénéficier du droit d'accès aux données la concernant afin de s'assurer de leur exactitude[301].

Dans certains cas, la mise à jour des données sauvegardées est interdite par la loi parce que la finalité du stockage est essentiellement de documenter des événements à la manière d'un « instantané » historique.

Exemple : le protocole d'une intervention médicale ne doit pas être modifié, c'est-à-dire « mis à jour », même s'il apparaît plus tard que les conclusions figurant dans le protocole étaient 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.

299 RGPD, art. 5, para. 1, point d) ; Convention 108 modernisée, art. 5, para. 4, point d).

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

301 Ex-considérant 41 de l'exposé des motifs de la Directive 95/46/CE.

Ceci étant, il existe des situations dans lesquelles une mise à jour des données, et un contrôle régulier de leur exactitude sont d'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 de crédit 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 des données incorrectes ou qui ne sont plus d'actualité sur une personne, cette dernière peut rencontrer des problèmes graves. Les responsables de telles bases de données doivent donc déployer des efforts particuliers pour respecter le principe de l'exactitude.

3.5. Le principe de la limitation de la durée de conservation

Points clés

- Le principe de la limitation de la durée de conservation implique que les données à caractère personnel doivent être supprimées ou anonymisées dès qu'elles ne sont plus nécessaires pour les finalités pour lesquelles elles ont été collectées.

L'article 5, paragraphe 1, point e), du RGPD et l'article 5, paragraphe 4, point e), de la Convention 108 modernisée imposent que les 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 traitées ». Les données doivent donc être effacées ou anonymisées lorsque ces finalités ont été atteintes. Afin de garantir que les données ne sont pas conservées plus longtemps que nécessaire, « des délais devraient être fixés par le responsable du traitement pour leur effacement ou pour un examen périodique »[302].

302 RGPD, considérant 39.

Dans l'affaire *S. et Marper*, la CouEDH a conclu que les principes fondamentaux des instruments pertinents du Conseil de l'Europe, de même que le droit et la pratique des autres Parties contractantes, exigent que la conservation de données soit proportionnée à l'objet de la collecte et limitée dans le temps, en particulier dans le secteur de la police[303].

> Exemple : dans l'affaire *S. et Marper*[304], la CouEDH a conclu que la conservation illimitée des empreintes digitales, des échantillons cellulaires et des profils ADN des deux requérants était disproportionnée et inutile dans une société démocratique, étant donné que la procédure pénale contre eux s'était conclue par un acquittement et une décision de classement sans suite, respectivement.

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.

Les données archivées dans l'intérêt du public, à des fins scientifiques ou historiques ou à des fins statistiques peuvent être conservées pour des durées plus longues pour autant qu'elles soient traitées exclusivement à ces fins[305]. Des mesures techniques et organisationnelles appropriées doivent être mises en œuvre pour le maintien de la conservation et l'utilisation de données à caractère personnel afin de garantir les droits et libertés de la personne concernée.

La Convention 108 modernisée admet également des exceptions au principe de la limitation de la durée de conservation à la condition qu'elles soient prévues par la loi, respectent le contenu essentiel des droits et libertés fondamentaux et constituent une mesure nécessaire et proportionnée pour poursuivre un nombre restreint de buts légitimes[306]. Ces exceptions incluent, notamment, la protection de la sécurité nationale, l'enquête et la poursuite d'infractions pénales, l'exécution de sanctions

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

304 CouEDH, *S. et Marper c. Royaume-Uni* [GC], n° 30562/04 et n° 30566/04, 4 décembre 2008.

305 RGPD, art. 5, para. 1, point e) ; Convention 108 modernisée, art. 5, para. 4, point b), et art. 11, para. 2.

306 Convention 108 modernisée, art. 9, para. 1 ; Rapport explicatif sur la Convention 108 modernisée, paras. 91 à 98.

pénales, la protection de la personne concernée et la sauvegarde des droits et libertés fondamentaux d'autrui.

Exemple : dans l'affaire *Digital Rights Ireland*[307], la CJUE a examiné la validité de la Directive relative à la conservation des données, qui visait à harmoniser les dispositions nationales applicables à la conservation des données à caractère personnel générées ou traitées par des services ou des réseaux de communications électroniques accessibles au public afin de lutter contre les infractions graves, comme le crime organisé et le terrorisme. La Directive relative à la conservation des données imposait la conservation de celles-ci pendant une période « d'au moins six mois sans que soit opérée une quelconque distinction entre les catégories de données prévues à l'article 5 de cette directive en fonction de leur utilité éventuelle aux fins de l'objectif poursuivi ou selon les personnes concernées »[308]. La CJUE a également observé que la directive ne mentionnait pas de critères objectifs sur la base desquels la durée exacte de conservation des données – qui pouvait varier entre six mois au minimum et vingt-quatre mois au maximum – devait être déterminée afin de garantir que celle-ci soit limitée au strict nécessaire[309].

3.6. Le principe de la sécurité des données

Points clés

- La sécurité et la confidentialité des données à caractère personnel sont essentielles pour prévenir tout effet négatif pour la personne concernée.
- Les mesures de sécurité peuvent être d'ordre technique et/ou organisationnel.
- La pseudonymisation est un processus permettant de protéger des données à caractère personnel.
- Le caractère approprié des mesures de sécurité doit être déterminé au cas par cas et réexaminé régulièrement.

307 CJUE, affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources et autres* et *Kärntner Landesregierung et autres* [GC], 8 avril 2014.

308 *Ibid.*, point 63.

309 *Ibid.*, point 64.

Le principe de la sécurité des données impose que des mesures techniques ou organisationnelles appropriées soient mises en œuvre lors du traitement de données à caractère personnel afin de les protéger contre un accès, une utilisation, une modification, une divulgation, une perte, une destruction ou un dommage accidentel, non autorisé ou illicite.[310] Le RGPD précise que le responsable du traitement et le sous-traitant devraient tenir compte « de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques » lorsqu'ils mettent en œuvre ces mesures[311]. Selon les circonstances spécifiques de chaque cas, les mesures techniques et organisationnelles appropriées pourraient, par exemple, inclure la pseudonymisation et le chiffrement des données à caractère personnel et/ou une procédure visant à tester et à évaluer régulièrement l'efficacité des mesures pour assurer la sécurité du traitement[312].

Comme expliqué à la section 2.1.1, la pseudonymisation des données implique de remplacer les identifiants des données à caractère personnel – qui permettent d'identifier la personne concernée – par un pseudonyme et de conserver ces identifiants séparément, dans le cadre de mesures techniques et organisationnelles. Le processus de pseudonymisation ne doit pas être confondu avec l'anonymisation, par laquelle tous les liens permettant d'identifier la personne sont rompus.

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

« YESz3201 est le père d'une famille de quatre enfants, deux garçons et deux filles ».

310 RGPD, considérant 39 et art. 5, para. 1, point f) ; Convention 108 modernisée, art. 7.

311 RGPD, art. 32, para. 1.

312 *Ibid.*

Les utilisateurs accédant à ces données pseudonymisées ne pourront généralement pas identifier « Charles Spencer, né le 3 avril 1967 » à partir de « 324 » ou de « YESz3201 ». Ces données sont donc probablement mieux protégées contre les abus.

Le premier exemple est toutefois 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, celui-ci pourra être facilement reconnu. La méthode de pseudonymisation utilisée peut donc affecter l'efficacité de la protection des données.

Des données à caractère personnel contenant des identifiants cryptés ou conservés séparément sont utilisées dans de nombreux contextes pour garder secrète l'identité des personnes. C'est particulièrement utile lorsque les responsables du traitement doivent s'assurer qu'ils traitent les mêmes personnes concernées mais n'ont pas besoin, ou ne devraient pas avoir besoin, de connaître les véritables identités de ces personnes. C'est le cas, par exemple, quand un chercheur étudie l'évolution d'une maladie chez des patients dont l'identité n'est connue que de l'hôpital où ils sont traités et auprès duquel le chercheur obtient les dossiers pseudonymisés. La pseudonymisation est donc un maillon fort dans l'arsenal des technologies renforçant la protection de la vie privée. Elle peut représenter un élément important dans la mise en œuvre du respect de la vie privée dès la conception (« *privacy by design* »), ce qui requiert que la protection des données soit intégrée dans le maillage des systèmes de traitement des données.

L'article 25 du RGPD, qui traite de la protection des données dès la conception, cite expressément la pseudonymisation parmi les exemples de mesures techniques et organisationnelles appropriées que les responsables du traitement devraient mettre en œuvre afin de tenir compte des principes de la protection des données et d'intégrer les garanties nécessaires. De la sorte, les responsables du traitement répondront aux exigences du règlement et protégeront les droits de la personne concernée lors du traitement des données la concernant.

L'adhésion à un code de conduite approuvé ou à un mécanisme de certification approuvé peut servir d'élément pour démontrer le respect de l'exigence de sécurité du traitement[313]. Dans son avis sur les implications en matière de protection des données du traitement des dossiers passagers, le Conseil de l'Europe

313 *Ibid.*, art. 32, para. 3.

présente d'autres exemples de mesures de sécurité appropriées pour la protection des données dans les systèmes de dossiers passagers. Parmi eux, on compte la conservation des données dans un environnement physique sûr, la limitation de l'accès basé sur une identification à niveaux multiples et la protection de la communication des données par un solide dispositif de cryptographie[314].

Exemple : les réseaux sociaux et les fournisseurs de services de courrier électronique permettent aux utilisateurs d'ajouter une couche supplémentaire de sécurité aux services qu'ils proposent en introduisant une authentification à deux niveaux. Outre la saisie d'un mot de passe personnel, les utilisateurs doivent procéder à une deuxième identification pour accéder à leur compte personnel. Il peut, par exemple, s'agir de la saisie d'un code de sécurité envoyé au numéro de portable relié au compte personnel. Une vérification en deux temps offre ainsi une meilleure protection des informations personnelles contre tout accès non autorisé à des comptes personnels par hameçonnage.

Le rapport explicatif sur la Convention 108 modernisée présente d'autres exemples de garanties adéquates, comme la mise en place d'une obligation de secret professionnel ou l'adoption de mesures de sécurité technique particulières, comme le chiffrement des données[315]. Lorsqu'il met en place des mesures de sécurité spécifiques, le responsable du traitement – ou, le cas échéant, le sous-traitant – devrait tenir compte de plusieurs éléments, tels que la nature et le volume des données à caractère personnel traitées, les conséquences négatives potentielles pour les personnes concernées et la nécessité d'un accès restreint aux données[316]. L'état de l'art actuel en matière de méthodes et de techniques de sécurisation pour le traitement des données doit être pris en compte lors de la mise en œuvre de mesures de sécurité appropriées. Leur coût doit être proportionné à la gravité et à la probabilité des risques potentiels. Elles devraient être revues régulièrement afin de pouvoir les actualiser si nécessaire[317].

314 CdE, Comité de la Convention 108, *Avis sur les implications en matière de protection des données du traitement des dossiers passagers*, T-PD(2016)18rev, 19 août 2016, p. 9.

315 Rapport explicatif sur la Convention modernisée, para. 56.

316 *Ibid.*, para. 62.

317 *Ibid.*, para. 63.

En cas de violation de données à caractère personnel, tant la Convention 108 modernisée que le RGPD imposent au responsable du traitement de notifier la violation à l'autorité de contrôle compétente ainsi que les risques pour les droits et libertés des personnes physiques dans les meilleurs délais[318]. Une obligation similaire de communication à la personne concernée existe lorsque la violation des données à caractère personnel est susceptible d'engendrer un risque élevé pour ses droits et libertés[319]. La communication de ces violations aux personnes concernées doit être faite en des termes clairs et simples[320]. Lorsque le sous-traitant a connaissance d'une violation de données à caractère personnel, le responsable du traitement doit en être immédiatement informé[321]. Dans certains cas, il peut exister des exceptions à l'obligation de notification. Par exemple, le responsable du traitement n'est pas tenu de notifier l'autorité de contrôle lorsque « le risque élevé pour les droits et libertés des personnes concernées [...] n'est plus susceptible de se matérialiser »[322]. Il n'est pas non plus nécessaire d'informer la personne concernée lorsque les mesures de sécurité appliquées rendent les données incompréhensibles pour toute personne non autorisée ou lorsque des mesures ultérieures garantissent que le risque élevé n'est plus susceptible de se matérialiser[323]. Lorsque la communication d'une violation de données à caractère personnel aux personnes concernées exigerait des efforts disproportionnés de la part du responsable du traitement, une communication publique ou une mesure similaire peut permettre « aux personnes concernées d'être informées de manière tout aussi efficace »[324].

3.7. Le principe de la responsabilité

Points clés

- La responsabilité requiert la mise en œuvre active et continue de mesures par les responsables du traitement et les sous-traitants pour promouvoir et garantir la protection des données dans le cadre de leurs activités de traitement.

318 Convention 108 modernisée, art. 7, para. 2 ; RGPD, art. 33, para. 1.

319 Convention 108 modernisée, art. 7, para. 2 ; RGPD, art. 34, para. 1.

320 RGPD, art. 34, para. 2.

321 *Ibid.*, art. 33, para. 1.

322 *Ibid.*, art. 32, para. 1.

323 *Ibid.*, art. 34, para. 3, points a) et b).

324 *Ibid.*, art. 34, para. 3, point c).

- Les responsables du traitement et les sous-traitants répondent de la conformité de leurs traitements avec le droit en matière de protection des données et leurs obligations respectives.
- 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. Les sous-traitants doivent également se conformer à certaines obligations strictement liées à la responsabilité (comme la tenue d'un registre des traitements et la désignation d'un délégué à la protection des données).

Le RGPD et la Convention 108 modernisée disposent que le responsable du traitement est responsable du respect des principes applicables au traitement de données à caractère personnel décrits dans le présent chapitre et est en mesure de le démontrer[325]. À cet effet, le responsable du traitement doit mettre en œuvre des mesures techniques et organisationnelles appropriées[326]. Bien que le principe de la responsabilité visé à l'article 5, paragraphe 2, du RGPD ne s'adresse qu'aux responsables du traitement, les sous-traitants sont également considérés comme tels, étant donné qu'ils doivent se conformer à plusieurs obligations et qu'ils ont un rapport direct avec la responsabilité.

Le droit de l'UE et du CdE en matière de protection des données établit que le responsable du traitement répond du respect des principes applicables à la protection des données discutés aux sections 3.1 à 3.6 et doit être en mesure de le démontrer[327]. Le Groupe de travail « Article 29 » souligne que « le type de procédures et de mécanismes varierait selon les risques que posent le traitement et la nature des données »[328].

Le responsable du traitement peut se conformer à cette exigence de différentes manières, notamment :

- en tenant un registre des activités de traitement et en le mettant à la disposition de l'autorité de contrôle à sa demande[329] ;

325 *Ibid.*, art. 5, para. 2 ; Convention modernisée 108, art. 10, para. 1.

326 RGPD, art. 24.

327 *Ibid.*, art. 5, para. 2 ; Convention 108 modernisée, art. 10, para. 1.

328 Groupe de travail « Article 29 », *Avis 3/2010 sur le principe de la responsabilité*, WP 173, Bruxelles, 13 juillet 2010, para. 12.

329 RGPD, art. 30.

- dans certains cas, en désignant un délégué à la protection des données, qui est associé à toutes les questions relatives à la protection des données à caractère personnel[330] ;

- en réalisant une analyse d'impact relative à la protection des données pour les types de traitement susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques[331] ;

- en intégrant la protection des données dès la conception et par défaut[332] ;

- en mettant en œuvre des modalités et des procédures pour l'exercice des droits des personnes concernées[333] ;

- en adhérant à un code de conduite ou à un mécanisme de certification approuvé[334].

Si le principe de la responsabilité visé à l'article 5, paragraphe 2, du RGPD n'est pas spécifiquement destiné aux sous-traitants, certaines dispositions relatives à la responsabilité leur imposent également des obligations, comme la tenue d'un registre des activités de traitement et la désignation d'un délégué à la protection des données pour toute activité de traitement qui en exige un[335]. Les sous-traitants doivent également veiller à ce que toutes les mesures nécessaires pour assurer la sécurité des données aient été mises en place[336]. Le contrat juridiquement contraignant liant le responsable du traitement et le sous-traitant doit préciser que le sous-traitant aide le responsable du traitement à répondre à certaines exigences de conformité, comme la réalisation d'une analyse d'impact relative à la protection des données ou en notifiant au responsable le traitement de toute violation de données à caractère personnel dès qu'il en a connaissance[337].

330 *Ibid.*, art. 37 à 39.

331 *Ibid.*, art. 35 ; Convention 108 modernisée, art. 10, para. 2.

332 RGPD, art. 25, Convention 108 modernisée, art. 10, paras. 2 et 3.

333 *Ibid.*, art. 12 et 24.

334 *Ibid.*, art. 40 et 42.

335 *Ibid.*, art. 5, para. 2, et art. 30 et 37.

336 *Ibid.*, art. 28, para. 3, point c).

337 *Ibid.*, art. 28, para. 3, point d).

En 2013, l'Organisation de coopération et de développement économiques (OCDE) a adopté des lignes directrices sur la vie privée, qui soulignent le fait que les responsables du traitement jouent un rôle important dans le fonctionnement pratique de la protection des données. Ces 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 »[338].

Exemple : l'amendement de 2009[339] 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 qui sont relatives à la sécurité, le législateur a donc 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 »[340], 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.

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

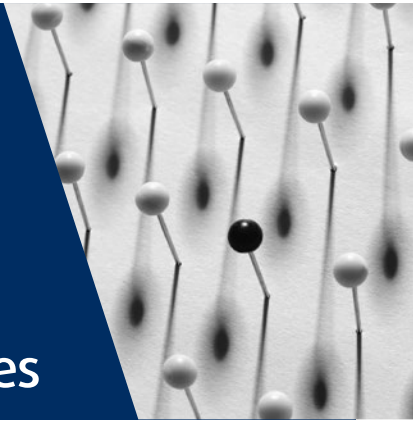
339 Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) nº 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.

340 Groupe de travail « Article 29 », *Avis 3/2010 sur le principe de la responsabilité*, WP 173, Bruxelles, 13 juillet 2010.

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.

4

Les règles du droit européen en matière de protection des données



UE	Questions traitées	CdE
Règles relatives à la licéité du traitement des données		
RGPD, art. 6, para. 1, point a) CJUE, C-543/09, *Deutsche Telekom AG c. Bundesrepublik Deutschland*, 2011 CJUE, C-536/15, *Tele2 (Netherlands) BV et autres c. Autoriteit Consument en Markt (AMC)*, 2017	**Consentement**	Recommandation sur le profilage, art. 3, para. 4, point b), et art. 3, para. 6 Convention 108 modernisée, art. 5, para. 2
RGPD, art. 6, para. 1, point b)	**Relations (pré) contractuelles**	Recommandation sur le profilage, art. 3, para. 4, point b)
RGPD, art. 6, para. 1, point c)	**Obligations légales du responsable du traitement**	Recommandation sur le profilage, art. 3, para. 4, point a)
RGPD, art. 6, para. 1, point d)	**Intérêt vital de la personne concernée**	Recommandation sur le profilage, art. 3, para. 4, point b)
RGPD, art. 6, para. 1, point e) CJUE, C-524/06, *Huber c. Bundesrepublik Deutschland* [GC], 2008	**Intérêt public et exercice de l'autorité publique**	Recommandation sur le profilage, art. 3, para. 4, point b)

UE	Questions traitées	CdE
RGPD, art. 6, para. 1, point f) CJUE, C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde c. Rīgas pašvaldības SIA 'Rīgas satiksme'*, 2017 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*, 2011	Intérêts légitimes de tiers	Recommandation sur le profilage, art. 3, para. 4, point b) CouEDH, *Y c. Turquie*, nº 648/10, 2015
RGPD, art. 6, para. 4	Exception à la limitation de la finalité : traitement ultérieur à d'autres fins	Convention 108 modernisée, art. 5, para. 4, point b)
Règles relatives au traitement licite de données sensibles		
RGPD, art. 9, para. 1	Interdiction générale de traitement	Convention 108 modernisée, art. 6
RGPD, art. 9, para. 2	Exceptions à l'interdiction générale	Convention 108 modernisée, art. 6
Règles relatives à la sécurité du traitement		
RGPD, art. 32	Obligation de veiller à la sécurité du traitement	Convention 108 modernisée, art. 7, para. 1 CouEDH, *I c. Finlande*, nº 20511/03, 2008
RGPD, art. 28 et art. 32, para. 1, point b)	Obligation de confidentialité	Convention 108 modernisée, art. 7, para. 1
RGPD, art. 34 Directive « vie privée et communications électroniques », art. 4, para. 2	Notifications de violation de données	Convention 108 modernisée, art. 7, para. 2
Règles relatives à la responsabilité et à la promotion de la conformité		
RGPD, art. 12, 13 et 14	Transparence en général	Convention 108 modernisée, art. 8
RGPD, art. 37, 38 et 39	Délégués à la protection des données	Convention 108 modernisée, art. 10, para. 1
RGPD, art. 30	Registres des activités de traitement	

UE	Questions traitées	CdE
RGPD, art. 35 et 36	Analyse d'impact et consultation préalable	Convention 108 modernisée, art. 10, para. 2
RGPD, art. 33 et 34	Notifications de violation de données	Convention 108 modernisée, art. 7, para. 2
RGPD, art. 40 et 41	Codes de conduite	
RGPD, art. 42 et 43	Certification	
Protection des données dès la conception et par défaut		
RGPD, art. 25, para. 1, point a)	Protection des données dès la conception	Convention 108 modernisée, art. 10, para. 2
RGPD, art. 25, para. 1, point b)	Protection des données par défaut	Convention 108 modernisée, art. 10, para. 3

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 modernisée. 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 de l'Union afin d'harmoniser le niveau de protection des données des législations nationales des États membres. Le RGPD établit une série de règles détaillées, régies par les principes énoncés en son article 5, qui sont directement applicables dans l'ordre juridique national. Les observations ci-après sur les règles détaillées en matière de protection des données au niveau européen concernent donc principalement le 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 elles satisfont à l'un des critères suivants :
  - le traitement repose sur le consentement de la personne concernée ;
  - une relation contractuelle implique le traitement de données à caractère personnel ;

- le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;
- l'intérêt vital de la personne concernée ou d'un tiers impose le traitement de ses données ;
- le traitement est nécessaire à l'exécution d'une mission d'intérêt public ;
- les intérêts légitimes de responsables du traitement ou de tiers sont la raison du traitement, mais uniquement pour autant qu'ils ne s'effacent pas devant les intérêts ou les droits fondamentaux des personnes concernées.

- Le traitement licite de données personnelles sensibles est soumis à un régime spécial plus strict.

4.1.1. Fondements licites du traitement de données

Le chapitre II du Règlement général sur la protection des données, intitulé « Principes », dispose que tout traitement de données à caractère personnel doit d'abord être conforme aux principes relatifs à la qualité des données, énoncés en son article 5. L'un de ces principes est que les données à caractère personnel doivent être « traitées de manière licite, loyale et transparente ». Ensuite, pour que les données soient traitées de manière licite, le traitement doit être conforme à l'un des fondements juridiques qui rendent le traitement des données légitime et sont énoncés à l'article 6[341] pour les données personnelles non sensibles et à l'article 9 pour les catégories particulières de données (ou « données sensibles »). De la même façon, le chapitre II de la Convention 108 modernisée, qui énonce les « Principes de base pour la protection des données à caractère personnel », dispose que pour être licite, le traitement de données doit être « proportionné à la finalité légitime poursuivie ».

Indépendamment du fondement licite du traitement invoqué par un responsable du traitement pour débuter un traitement de données à caractère personnel, ce dernier devra également appliquer les garanties prévues dans le régime juridique général de la protection des données.

341 CJUE, affaires jointes C-465/00, C-138/01 et C-139/01, *Rechnungshof c. Österreichischer Rundfunk et autres* et *Christa Neukomm et Joseph Lauermann c. Österreichischer Rundfunk*, 20 mai 2003, point 65 ; CJUE, C-524/06, *Heinz Huber c. Bundesrepublik Deutschland* [GC], 16 décembre 2008, point 48 ; 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, point 26.

Consentement

Dans le droit du CdE, le consentement est mentionné à l'article 5, paragraphe 2, de la Convention 108 modernisée. Il est également mentionné dans la jurisprudence de la CouEDH et dans plusieurs recommandations du CdE[342]. **Dans le droit de l'UE**, le consentement en tant que base du traitement licite de données est solidement établi à l'article 6 du RGPD et est également expressément mentionné à l'article 8 de la Charte. Les caractéristiques d'un consentement valable sont expliquées dans la définition du consentement à l'article 4, tandis que les conditions d'obtention d'un consentement valable sont décrites à l'article 7 et les règles particulières applicables au consentement d'un enfant à l'égard de services de la société de l'information sont énoncées à l'article 8 du RGPD.

Comme expliqué à la section 2.4, le consentement doit être libre, spécifique, éclairé et univoque. Le consentement doit être une déclaration ou une action affirmative qui indique clairement l'acceptation du traitement et la personne a le droit de retirer son consentement à tout moment. Les responsables du traitement ont l'obligation de tenir un registre vérifiable du consentement.

Consentement libre

Dans le cadre de la Convention 108 modernisée du **CdE**, le consentement de la personne concernée doit « représenter la libre expression d'un choix intentionnel »[343]. Le consentement libre ne peut être 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 »[344]. À cet égard, **le droit de l'UE** précise que le consentement n'est pas considéré comme ayant été donné librement « si la personne concernée ne dispose pas d'une véritable liberté de choix ou n'est pas en mesure de refuser ou de retirer son consentement sans subir de préjudice »[345]. Le RGPD souligne qu'« [a]u moment de déterminer si le consentement est donné librement, il y a lieu de tenir

342 Voir, par exemple, CdE, Comité des Ministres (2010), Recommandation CM/Rec(2010)13 du Comité des Ministres aux États membres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage, 23 novembre 2010, art. 3, para. 4, point b).

343 Rapport explicatif sur la Convention 108 modernisée, para. 42.

344 Voir également Groupe de travail « Article 29 », *Avis 15/2011 sur la définition du consentement*, WP 187, 13 juillet 2011, p. 12.

345 RGPD, considérant 42.

le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat »[346]. Le rapport explicatif sur la Convention 108 modernisée observe qu'« [a]ucune influence ou pression indues (de nature économique ou autre), directe ou indirecte, ne peut être exercée sur la personne concernée et le consentement ne doit pas être considéré comme libre si elle n'a pas de véritable choix ou de liberté de choix ou ne peut refuser ou retirer son consentement sans subir de préjudice »[347].

Exemple : plusieurs municipalités de l'État A ont décidé d'instituer des cartes de séjour avec une puce intégrée. Les résidents ne sont pas tenus d'acquérir ces cartes électroniques. Toutefois, les résidents qui n'en possèdent pas n'ont pas accès à une série de services administratifs importants, comme la possibilité de payer les taxes municipales en ligne, d'introduire une plainte par voie électronique en bénéficiant d'un délai de trois jours dans lequel l'autorité doit répondre et même de passer outre les files d'attente, d'acheter des billets à tarif réduit pour la salle de concert municipale et d'utiliser les scanners à l'entrée.

Dans cet exemple, le traitement de données à caractère personnel par les municipalités ne peut pas reposer sur un consentement. Étant donné qu'il existe à tout le moins une pression indirecte exercée sur les résidents pour qu'ils se procurent la carte électronique et acceptent le traitement, le consentement n'est pas donné librement. La mise en place par les municipalités d'un système de cartes électroniques devrait donc reposer sur un autre fondement légitime justifiant le traitement. Elles pourraient, par exemple, faire valoir que le traitement est nécessaire à l'exécution d'une mission d'intérêt public, ce qui constitue une base licite pour le traitement, conformément à l'article 6, paragraphe 1, point e), du RGPD[348].

La liberté du consentement pourrait également être mise en doute dans des situations de subordination, dans lesquelles il existe un important

346 *Ibid.*, art. 7, para. 4.

347 Rapport explicatif sur la Convention 108 modernisée, para. 42.

348 Groupe de travail « Article 29 » (2011), *Avis 15/2011 sur la définition du consentement*, WP 187, Bruxelles, 13 juillet 2011, p. 16. D'autres exemples de cas où le traitement de données ne saurait être basé sur le consentement, mais nécessite une autre base juridique pour justifier le traitement, sont présentés aux pages 14 et 17 de l'avis.

déséquilibre économique ou autre entre le responsable du traitement qui obtient le consentement et la personne concernée qui le donne[349]. Un exemple typique de ces déséquilibres et de subordination est le traitement de données à caractère personnel par un employeur dans le cadre d'une relation d'emploi. Selon le Groupe de travail « Article 29 », « [l]es employés sont très rarement en mesure de donner, de refuser ou de révoquer librement leur consentement, étant donné la dépendance qui découle de la relation employeur/employé. Compte tenu du déséquilibre de pouvoir, les employés ne peuvent donner leur libre consentement que dans des circonstances exceptionnelles, dans lesquelles l'acceptation ou le rejet d'une proposition n'a aucune conséquence »[350].

Exemple : une grande entreprise envisage de créer un répertoire contenant le nom de tous ses employés, leur fonction dans la société et leur adresse professionnelle, dans le seul but d'améliorer les communications internes. Le chef du personnel propose d'ajouter une photo de chaque employé au répertoire afin de permettre aux collègues de se reconnaître plus facilement lors des réunions. Les représentants des employés exigent que la photo ne soit ajoutée que si l'employé y consent.

Dans un tel cas, le consentement de l'employé devrait être reconnu comme base juridique du traitement des photos dans le répertoire, parce que l'on peut penser que l'employé ne subira aucune conséquence s'il décide d'accepter ou de refuser que sa photo soit publiée dans le répertoire.

Exemple : la société A organise une réunion entre trois de ses employés et les directeurs de la société B afin de discuter d'une coopération future potentielle sur un projet. La réunion se déroulera dans les locaux de la société B, qui demande à la société A de lui envoyer par courrier électronique le nom, le CV et la photo des participants à la réunion. La société B fait valoir qu'elle a besoin du nom et de la photo des participants afin qu'à l'entrée du bâtiment, le personnel de sécurité vérifie qu'il s'agit des personnes

349 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 ; Groupe de travail « Article 29 » (2005), Document de travail sur une interprétation commune de l'article 26, para. 1, de la directive 95/46/CE du 24 octobre 1995, WP 114, Bruxelles, 25 novembre 2005 ; Groupe de travail « Article 29 » (2017), *Avis 2/2017 sur le traitement des données au travail*, WP 249, Bruxelles, 8 juin 2017.

350 Groupe de travail « Article 29 », *Avis 2/2017 sur le traitement des données au travail*, WP 249, Bruxelles, 8 juin 2017.

désignées, tandis que les CV permettront aux directeurs de mieux se préparer pour la réunion. Dans ce cas, la communication par la société A de données à caractère personnel de ses employés ne peut être fondée sur un consentement. Le consentement ne pourrait pas être considéré comme « donné librement », étant donné qu'il est possible que les employés doivent faire face à des conséquences dommageables s'ils refusent l'offre (par exemple, ils pourraient être remplacés par un autre collègue non seulement lors de la réunion, mais également pour les contacts avec la société B et la contribution au projet en général). Le traitement doit donc reposer sur un autre fondement légitime justifiant le traitement.

Ceci ne signifie toutefois pas qu'un consentement ne puisse jamais être valable lorsque l'absence de consentement aurait des conséquences négatives. Par exemple, si le refus d'une carte de client d'un supermarché a pour seul résultat de ne pas bénéficier d'une petite réduction sur le prix de certains produits, le consentement pourrait être une base juridique valable pour le traitement des données à caractère personnel des clients qui ont donné leur accord à l'obtention d'une telle carte. Il n'y a pas de lien de subordination entre l'entreprise et le client et les conséquences du refus ne sont pas suffisamment graves pour empêcher la personne concernée de choisir librement (pour autant que la réduction de prix soit suffisamment modeste pour ne pas influencer son libre choix).

En revanche, lorsque des produits ou des services ne peuvent être obtenus que si certaines données à caractère personnel sont communiquées au responsable du traitement ou par la suite à des tiers, le consentement de la personne concernée à la divulgation de ses données, qui ne sont pas nécessaires au contrat, ne peut être considéré comme une décision libre et n'est donc pas valable en vertu du droit de protection des données[351]. Le RGPD interdit assez strictement de lier le consentement à la fourniture de biens et de services[352].

Exemple : l'accord donné par des passagers à une compagnie aérienne l'autorisant à transférer des « dossiers passagers » (c'est-à-dire des données sur leur identité, leurs habitudes alimentaires ou leurs problèmes de santé) aux services de l'immigration d'un pays étranger donné ne peut être considéré comme un consentement valable en vertu du droit de

351 RGPD, art. 7, para. 4.

352 *Ibid.*

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 juridique autre que le consentement est requise et il s'agira très probablement d'une loi spécifique.

Consentement éclairé

La personne concernée doit disposer d'informations suffisantes avant de prendre sa décision. De façon générale, le consentement éclairé comprendra une description précise et facilement compréhensible de l'affaire nécessitant un consentement. Comme l'explique le Groupe de travail « Article 29 », le consentement doit être fondé sur l'appréciation et la compréhension des faits et des conséquences du consentement de la personne concernée au traitement. Dès lors, « [l]a personne concernée doit recevoir, de façon claire et compréhensible, des informations exactes et complètes sur tous les éléments pertinents, [...] tels que la nature des données traitées, les finalités du traitement, les destinataires d'éventuels transferts et ses droits »[353]. Cela suppose également que la personne doit être consciente des conséquences du refus de consentir au traitement.

Compte tenu de l'importance d'un consentement éclairé, le RGPD et le rapport explicatif sur la Convention 108 modernisée ont visé à clarifier cette notion. Il est expliqué dans l'exposé des motifs du RGPD que pour que le consentement soit éclairé, « la personne concernée devrait connaître au moins l'identité du responsable du traitement et les finalités du traitement auquel sont destinées les données à caractère personnel »[354].

Dans le cas exceptionnel d'un consentement utilisé comme une dérogation pour servir de fondement légitime à un transfert de données international, le responsable du traitement doit informer la personne concernée des risques que ce transfert pourrait comporter pour elle, en raison de l'absence de décision d'adéquation et de garanties appropriées, pour que ce consentement soit considéré comme valable[355].

353 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.

354 RGPD, considérant 42.

355 *Ibid*., art. 49, para. 1, point a).

Le rapport explicatif sur la Convention 108 modernisée précise que des informations doivent être fournies sur les implications de la décision de la personne concernée de donner son consentement, à savoir « ce que signifie le fait de donner son consentement et l'étendue de ce dernier »[356].

La qualité des informations est importante. Par qualité des informations, on entend que la manière dont les informations sont formulées doit être adaptée aux destinataires prévisibles. Les informations doivent être communiquées sans jargon, en termes clairs et simples, qu'un utilisateur moyen devrait être en mesure de comprendre[357]. Les informations doivent aussi être aisément accessibles pour la personne concernée et peuvent être fournies oralement ou par écrit. L'accessibilité et la visibilité des informations sont également des éléments importants : les informations doivent être clairement visibles et mises en évidence. Dans un environnement électronique, des informations hiérarchisées peuvent être une bonne solution, dans la mesure où elles permettent aux personnes concernées de choisir d'accéder à des versions courtes ou plus élaborées des informations.

Consentement spécifique

Pour être valable, le consentement doit aussi être spécifique à la finalité du traitement, laquelle doit être décrite clairement et en termes non équivoques. 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 moyenne seront pertinentes. Il convient de solliciter à nouveau le consentement de la personne concernée lorsque 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, et entraînent donc un changement de finalité. Lorsque le traitement poursuit plusieurs finalités, le consentement doit être donné pour chacune d'elles[358].

Exemples : dans l'affaire *Deutsche Telekom AG*[359], la CJUE a statué sur la question de savoir si un fournisseur de services de télécommunications ayant

356 Rapport explicatif sur la Convention 108 modernisée, para. 42.

357 Groupe de travail « Article 29 » (2011), *Avis 15/2011 sur la définition du consentement*, WP 187, Bruxelles, 13 juillet 2011, p. 19.

358 RGPD, considérant 32.

359 CJUE, C-543/09, *Deutsche Telekom AG c. Bundesrepublik Deutschland*, 5 mai 2011. Voir, en particulier, points 53 et 54.

transféré des données à caractère personnel sur des abonnés en vue de leur publication dans des annuaires, devait obtenir un nouveau consentement des personnes concernées[360], dans la mesure où les destinataires n'étaient pas nommément connus lorsque le consentement avait été donné.

La CJUE a retenu que, conformément à l'article 12 de la Directive « vie privée et communications électroniques », un nouveau consentement avant la transmission des données n'était pas nécessaire. Étant donné que les personnes concernées 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.

Comme l'a souligné la Cour, « 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 »[361]. De plus, « 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 »[362], plutôt que l'identité de l'éditeur.

L'affaire *Tele2 (Netherlands) BV, Ziggo BV et Vodafone Libertel BV c. Autoriteit Consument en Markt (AMC)*[363] concernait une entreprise belge offrant des services de renseignements téléphoniques et d'annuaires, qui avait demandé aux entreprises qui attribuent des numéros de téléphone aux Pays-Bas de lui donner accès aux données relatives à leurs abonnés. L'entreprise belge se fondait sur une obligation découlant de la Directive « services universels »[364]. Celle-ci impose aux entreprises qui attribuent des numéros de téléphone de

360 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 »).

361 CJUE, C-543/09, *Deutsche Telekom AG c. Bundesrepublik Deutschland*, 5 mai 2011, point 61.

362 *Ibid.*, point 62.

363 CJUE, C-536/15, *Tele2 (Netherlands) BV et autres c. Autoriteit Consument en Markt (AMC)*, 15 mars 2017.

364 Directive 2002/22/CE du Parlement européen et du Conseil du 7 mars 2002 concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques (Directive « service universel »), JO 2002 L 108, p. 51, telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 (Directive « services universels »), JO 209 L 337, p. 11.

mettre leurs annuaires à la disposition de ceux qui les demandent à condition que les abonnés aient consenti à ce que leur numéro de téléphone soit publié. Les entreprises néerlandaises ont refusé de le faire en alléguant qu'elles n'étaient pas tenues de fournir les données en cause à une entreprise établie dans un autre État membre. Elles ont soutenu que les utilisateurs avaient donné leur consentement à la publication de leur numéro en pensant qu'il serait publié dans un annuaire néerlandais. La CJUE a retenu que la Directive « services universels » couvre toutes les demandes émanant d'entreprises fournissant des services de renseignements téléphoniques, quel que soit l'État membre où elles sont établies. Elle a également conclu que la transmission de ces mêmes données à une autre entreprise visant à publier un annuaire public sans qu'un nouveau consentement ait été donné par les abonnés ne saurait porter atteinte à la substance même du droit à la protection des données à caractère personnel[365]. Par conséquent, il n'y a pas lieu pour l'entreprise qui attribue des numéros de téléphone à ses abonnés de formuler la demande de consentement adressée à l'abonné de sorte que celui-ci exprime ce consentement de manière distincte selon l'État membre vers lequel les données le concernant peuvent être transmises[366].

Consentement univoque

Tout consentement doit être donné de manière univoque[367]. En d'autres termes, il ne doit pas exister de doute raisonnable quant au fait que la personne concernée souhaitait donner son accord au traitement de ses données. Ainsi, l'inaction d'une personne concernée ne constitue pas un consentement univoque.

Tel serait le cas d'un responsable du traitement qui obtient un consentement en utilisant dans sa politique de confidentialité des déclarations telles qu'« en utilisant notre service, vous consentez au traitement de vos données à caractère personnel ». Dans ce cas, le responsable du traitement pourrait avoir l'obligation de s'assurer que les utilisateurs consentent manuellement et individuellement à cette politique.

Si un consentement est signifié par écrit dans le cadre d'un contrat, le consentement au traitement de données à caractère personnel doit être individualisé et, en tout

365 CJUE, C-536/15, *Tele2 (Netherlands) BV et autres c. Autoriteit Consument en Markt (AMC)*, 15 mars 2017, point 36.

366 *Ibid.*, points 40 et 41.

367 RGPD, art. 4, para. 11.

état de cause, « des garanties devraient exister afin de garantir que la personne concernée est consciente du consentement donné et de sa portée »[368].

Exigences applicables au consentement des enfants

Le RGPD prévoit une protection spécifique pour les enfants en ce qui concerne la fourniture de services de la société de l'information, « parce qu'ils peuvent être moins conscients des risques, des conséquences et des garanties concernées et de leurs droits liés au traitement des données à caractère personnel »[369]. Par conséquent, dans le **droit de l'UE**, lorsque des fournisseurs de services de la société de l'information traitent des données à caractère personnel d'enfants de moins de 16 ans sur la base d'un consentement, ce traitement n'est licite que « si, et dans la mesure où, le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant »[370]. Les États membres peuvent prévoir un âge inférieur dans leur droit national, pour autant que celui-ci ne soit pas inférieur à 13 ans[371]. Le consentement du titulaire de la responsabilité parentale n'est pas nécessaire « dans le cadre de services de prévention ou de conseil proposés directement à un enfant »[372]. Toute information et communication, lorsque le traitement concerne un enfant, devraient être rédigées en des termes clairs et simples que l'enfant peut aisément comprendre[373].

Droit de retirer le consentement à tout moment

Le RGPD prévoit un droit général de retirer le consentement à tout moment[374]. La personne concernée doit être informée de ce droit avant de donner son consentement et elle peut l'exercer à sa discrétion. Il ne devrait exister ni obligation de motiver le retrait du consentement ni risque de conséquences dommageables outre la cessation des avantages qui pouvaient découler de l'utilisation des données à laquelle il avait été consenti. Il devrait être aussi simple de retirer que de donner son consentement[375]. Le consentement ne peut pas être considéré comme ayant été

368 *Ibid.*, considérant 42.

369 *Ibid.*, considérant 38.

370 *Ibid.*, art. 8, para. 1, premier alinéa. La notion de services de la société de l'information est définie à l'article 4, para. 25, du RGPD.

371 RGPD, art. 8, para. 1, second alinéa.

372 *Ibid.*, considérant 38.

373 *Ibid.*, considérant 58. Voir aussi la Convention 108 modernisée, art. 15, para. 2, point e). Rapport explicatif sur la Convention 108 modernisée, paras. 68 et 125.

374 RGPD, art. 7, para. 3. Rapport explicatif sur la Convention 108 modernisée, para. 45.

375 RGPD, art. 7, para. 3.

donné librement si la personne concernée n'est pas en mesure de le retirer sans subir de préjudice ou si le retirer n'est pas aussi simple que de le donner[376].

> 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. Le retrait est toutefois exercé pour l'avenir et ne produit pas d'effet rétroactif. La période durant laquelle les données à caractère personnel du client ont été traitées de manière licite, du fait de son consentement, était légitime. Le retrait interdit tout traitement ultérieur de ces données, à moins que ce traitement ne soit conforme au droit à l'effacement[377].

Nécessaire à l'exécution d'un contrat

Dans le droit de l'UE, l'article 6, paragraphe 1, point b), du RGPD prévoit une autre base de traitement légitime, à savoir que le traitement soit « nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ». Cette disposition est également applicable aux relations précontractuelles. Par exemple, lorsqu'une partie a l'intention de conclure un contrat, mais ne l'a pas encore fait, peut-être parce que certaines vérifications restent à faire. Si une partie a besoin de traiter des données à cette fin, ce traitement est légitime pour autant qu'il soit « nécessaire à l'exécution de mesures précontractuelles prises à la demande de la personne concernée »[378].

La notion de traitement de données comme « fondement légitime prévu par la loi » visée à l'article 5, paragraphe 2, de la Convention 108 modernisée englobe également « le traitement de données nécessaire à l'exécution d'un contrat (ou de mesures précontractuelles, à la demande de la personne concernée) auquel la personne concernée est partie »[379].

376 RGPD, considérant 42 ; Rapport explicatif sur la Convention 108 modernisée, para. 42.

377 RGPD, art. 17, para. 1, point b).

378 *Ibid.*, art. 6, para. 1, point b).

379 Rapport explicatif sur la Convention 108 modernisée, para. 46 ; CdE, Comité des Ministres (2010), Recommandation CM/Rec(2010)13 du Comité des Ministres aux États membres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage, 23 novembre 2010, art. 3, para. 4, point b).

Obligations légales du responsable du traitement

Le droit de l'UE mentionne explicitement un autre critère de légitimation du traitement des données, à savoir qu'« il est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis » (article 6, paragraphe 1, point c), du RGPD). Cette disposition fait référence à des responsables du traitement des secteurs public et privé ; les obligations légales des responsables du traitement du secteur public peuvent également relever de l'article 6, paragraphe 1, point e), du RGPD. Il existe de nombreux exemples de situations dans lesquelles la loi oblige des responsables du traitement du secteur privé à traiter des données sur des personnes concernées spécifiques. Ainsi, les employeurs doivent traiter des données sur leurs employés à des fins fiscales et de sécurité sociale et les entreprises doivent traiter des données sur leurs clients à des fins fiscales.

L'obligation légale peut trouver sa source dans le droit de l'Union ou dans le droit d'un État membre, lequel peut servir de base à une ou plusieurs opérations de traitement. Il reviendrait à la loi de déterminer la finalité du traitement, d'établir les critères pour l'identification du responsable du traitement, le type de données à caractère personnel faisant l'objet du traitement, les personnes concernées, les entités auxquelles les données à caractère personnel peuvent être divulguées, les limitations de la finalité, la durée de conservation et d'autres mesures visant à garantir un traitement licite et loyal[380]. Ce droit, qui sert de fondement au traitement de données à caractère personnel, doit être conforme aux articles 7 et 8 de la Charte ainsi qu'à l'article 8 de la CEDH.

Les obligations légales du responsable du traitement servent également de base au traitement légitime de données **dans le droit du CdE**[381]. Comme indiqué précédemment, les obligations légales d'un responsable du traitement du secteur privé ne sont qu'un exemple spécifique d'intérêts légitimes d'autrui visés à l'article 8, paragraphe 2, de la CEDH. L'exemple du traitement par les employeurs de données sur leurs employés est donc également pertinent pour le droit du CdE.

380 RGPD, considérant 45.

381 CdE, Comité des Ministres (2010), Recommandation CM/Rec(2010)13 du Comité des Ministres aux États membres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage, 23 novembre 2010, art. 3, para. 4, point a).

Intérêt vital de la personne concernée ou d'une autre personne physique

Dans le droit de l'UE, l'article 6, paragraphe 1, point d), du RGPD 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 ou d'une autre personne physique ». Ce fondement légitime ne peut être invoqué pour le traitement de données à caractère personnel fondé sur l'intérêt vital d'une autre personne physique que lorsqu'il « ne peut manifestement pas être fondé sur une autre base juridique »[382]. Certains types de traitement peuvent être justifiés à la fois par des motifs d'intérêt public et par les intérêts vitaux de la personne concernée ou d'une autre personne. C'est le cas, par exemple, pour le suivi des épidémies et de leur propagation ou dans les cas d'urgence humanitaire.

Dans le droit du CdE, l'intérêt vital de la personne concernée n'est pas mentionné à l'article 8 de la CEDH. Toutefois, l'intérêt vital de la personne concernée est considéré comme implicite dans la notion de « fondement légitime » mentionnée à l'article 5, paragraphe 2, de la Convention 108 modernisée, qui traite de la légitimité du traitement de données à caractère personnel[383].

Intérêt public et exercice de l'autorité publique

Compte tenu des nombreuses possibilités d'organisation des affaires publiques, l'article 6, paragraphe 1, point e), du RGPD prévoit que des données à caractère personnel peuvent faire l'objet d'un traitement licite lorsque « le traitement 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 »[384].

Exemple : dans l'affaire *Huber c. Bundesrepublik Deutschland*[385] 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 résidant en Allemagne depuis plus de trois mois, est utilisé à des

382 RGPD, considérant 46.

383 Rapport explicatif sur la Convention 108 modernisée, para. 46.

384 Voir RGPD, considérant 45.

385 CJUE, C-524/06, *Heinz Huber c. Bundesrepublik Deutschland* [GC], 16 décembre 2008.

fins statistiques et par les autorités répressives et judiciaires dans le cadre d'activités d'enquêtes 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 retenu que, conformément à l'article 7, point e), de la Directive 95/46[386], des données à caractère personnel peuvent faire légalement l'objet d'un traitement 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 qu'elle résulte de l'article 7, point e), de la directive 95/46[387] [...] ne saurait avoir un contenu variable en fonction des États membres. Dès lors, 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 celle-ci »[388].

La Cour a relevé que le droit de libre circulation 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. Dès lors, 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 n'était 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.

386 Ex-article 7, point e), de la Directive relative à la protection des données, devenu article 6, para. 1, point e), du RGPD.

387 *Ibid.*

388 CJUE, C-524/06, *Heinz Huber c. Bundesrepublik Deutschland* [GC], 16 décembre 2008, point 52.

Il appartenait à la juridiction nationale de vérifier si ces conditions étaient satisfaites en l'espèce. Dans la 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)[389], de la Directive 95/46/CE[390].

Enfin, s'agissant de la question de l'utilisation des données contenues dans le registre aux fins de la 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 »[391].

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** et est censée être couverte, le cas échéant, par l'article 5, paragraphe 2 de la Convention 108 modernisée[392].

Intérêts légitimes poursuivis par le responsable du traitement ou par un tiers

Dans le **droit de l'UE**, la personne concernée n'est pas la seule à avoir un intérêt légitime. L'article 6, paragraphe 1, point f), du RGPD dispose que des données à caractère personnel peuvent faire l'objet d'un traitement licite s'il « est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par le tiers ou des parties [à l'exception des autorités publiques dans l'exécution de leurs

389 Ex-article 7, point e), de la Directive relative à la protection des données, devenu article 6, para. 1, point e), du RGPD.

390 CJUE, C-524/06, *Heinz Huber c. Bundesrepublik Deutschland* [GC], 16 décembre 2008, points 54, 58, 59 et 66 à 68.

391 *Ibid.*, points 78 et 81.

392 Rapport explicatif sur la Convention 108 modernisée, paras. 46 et 47.

missions], à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel [...] »[393].

L'existence d'un intérêt légitime devrait faire l'objet d'une évaluation attentive au cas par cas[394]. Si les intérêts légitimes du responsable du traitement sont identifiés, une mise en balance entre ceux-ci et les intérêts ou les libertés et droits fondamentaux de la personne concernée doit être réalisée[395]. Les attentes raisonnables de la personne concernée doivent être prises en compte dans cette évaluation afin de déterminer si les intérêts du responsable du traitement prévalent sur les intérêts ou les droits fondamentaux de la personne concernée[396]. Si les droits de la personne concernée l'emportent sur les intérêts légitimes du responsable du traitement, ce dernier peut prendre des mesures et mettre en œuvre des garanties afin de s'assurer que l'impact sur les droits de la personne concernée est limité au minimum (par exemple, en pseudonymisant les données) et inverser l'« équilibre » avant de pouvoir invoquer légalement ce fondement légitime pour justifier le traitement. Dans son avis sur la notion d'intérêt légitime du responsable du traitement, le Groupe de travail « Article 29 » a souligné le rôle crucial de la responsabilité et de la transparence ainsi que des droits de la personne concernée à s'opposer au traitement de ses données ou à l'accès, à la modification, à l'effacement ou au transfert de celles-ci, lors de la mise en balance des intérêts légitimes du responsable du traitement et des intérêts des droits fondamentaux de la personne concernée[397].

Dans l'exposé des motifs du RGPD, le législateur présente plusieurs exemples de ce qui constitue un intérêt légitime du responsable du traitement. Par exemple, le traitement de données à caractère personnel est autorisé sans le consentement de la personne concernée lorsqu'il poursuit des fins de prospection ou lorsque ce traitement est « strictement nécessaire à des fins de prévention de la fraude »[398].

Dans sa jurisprudence, la CJUE a développé le critère permettant de déterminer ce qui constitue un intérêt légitime.

393 Par rapport à la Directive 95/46, le RGPD présente plus d'exemples de cas considérés constitutifs d'un intérêt légitime.

394 RGPD, exposé des motifs, considérant 47.

395 Groupe de travail « Article 29 », *Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE*, 4 avril 2014.

396 *Ibid*.

397 *Ibid*.

398 RGPD, exposé des motifs, considérant 47.

Exemple : l'affaire *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde*[399] concernait des dommages causés à un trolleybus de l'entreprise de transport Rīgas par le passager d'un taxi ayant ouvert soudainement la portière du véhicule. Rīgas satiksme voulait poursuivre le passager pour les dommages causés. Cependant, la police n'a communiqué que le nom du passager et a refusé de communiquer le numéro d'identification et l'adresse de celui-ci au motif que cette divulgation serait illicite en vertu de la législation nationale en matière de protection des données.

La juridiction de renvoi lettonne a demandé à la CJUE de rendre une décision préjudicielle sur la question de savoir si la législation de l'UE en matière de protection des données impose l'obligation de divulguer toutes les données à caractère personnel nécessaires à l'introduction d'un recours au civil contre la personne présumée responsable d'une infraction administrative[400].

La Cour a précisé que le droit de l'UE en matière de protection des données exprime une faculté et non une obligation de communiquer à un tiers les données nécessaires à la réalisation d'un intérêt légitime poursuivi par celui-ci[401]. La CJUE a énoncé trois conditions cumulatives pour qu'un traitement de données à caractère personnel soit licite sur le fondement des « intérêts légitimes »[402]. Premièrement, le tiers auquel les données sont communiquées doit poursuivre un intérêt légitime. En l'espèce, cela signifie que demander des informations personnelles pour poursuivre une personne ayant causé une atteinte à la propriété constitue un intérêt légitime d'un tiers. Deuxièmement, le traitement de données à caractère personnel doit être nécessaire pour la réalisation de l'intérêt légitime poursuivi. En l'espèce, l'obtention d'informations personnelles comme l'adresse et/ou le numéro d'identification est strictement nécessaire à l'identification de cette personne. Troisièmement, les libertés et droits fondamentaux de la personne concernée ne doivent pas prévaloir sur l'intérêt légitime du responsable du traitement ou de tiers. La pondération des intérêts doit se faire au cas par cas en tenant compte d'éléments tels que la gravité de l'atteinte aux droits de la personne concernée, voire, dans certaines circonstances, l'âge de la personne concernée. Toutefois, dans cette affaire, la CJUE n'a pas jugé que

399 CJUE, C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde c. Rīgas pašvaldības SIA « Rīgas satiksme »*, 4 mai 2017.

400 *Ibid.*, point 23.

401 *Ibid.*, point 26.

402 *Ibid.*, points 28 à 34.

le refus de communication des données était justifié par le simple fait que la personne concernée était mineure.

Dans l'affaire *ASNEF et FECEMD*[403], la CJUE s'est expressément prononcée sur le traitement de données basé sur le fondement légitime « intérêt légitime », qui, à l'époque, était prévu à l'article 7, point f), de la Directive relative à la protection des données.

Exemple : dans l'affaire *ASNEF et FECEMD*[404], 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 des données[405]. Celle-ci concernait une disposition du droit espagnol en matière de protection des données selon laquelle d'autres parties privées ne pouvaient 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[406] 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 non plus conduire à affaiblir la protection qu'elles assurent. Elle doit au contraire, avoir pour objectif de garantir un niveau élevé de protection dans l'UE[407]. 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[408] prévoit

403 Ex-article 7, point f), de la Directive relative à la protection des données, devenu article 6, para. 1, point f), du RGPD.

404 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.

405 Ex-article 7, point f), de la Directive relative à la protection des données, devenu article 6, para. 1, point f), du RGPD.

406 Ancienne directive relative à la protection des données, devenue Règlement général sur la protection des données (RGPD).

407 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, point 28. Voir Directive relative à la protection des données, considérants 8 et 10.

408 Ex-article 7 de la Directive relative à la protection des données, devenu article 6, para. 1, point f), du RGPD.

une liste exhaustive et limitative des 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[409], ni prévoir des exigences supplémentaires qui viendraient modifier la portée de l'un des six principes prévus à cet article »[410]. La Cour a reconnu que, s'agissant de la pondération nécessaire en vertu de l'article 7, point 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 selon que les données en cause figurent déjà, ou non, dans des sources accessibles au public.

Toutefois, « l'article 7, point f), de cette directive s'oppose à ce qu'un État membre exclut 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, point f), de la directive 95/46[411] 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, excluant de façon catégorique et généralisée tout traitement de données ne figurant pas dans de telles sources »[412].

Chaque fois que des données à caractère personnel sont traitées sur la base d'un « intérêt légitime », la personne a le droit de s'opposer à tout moment au traitement, pour des motifs tenant à sa situation particulière, conformément à l'article 21,

409 Ex-article 7 de la Directive relative à la protection des données, devenu article 6 du RGPD.

410 *Ibid*.

411 Ex-article 7, point f), de la Directive relative à la protection des données, devenu article 6, para. 1, point f), du RGPD.

412 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, paras. 40, 44, 48 et 49.

paragraphe 1, du RGPD. Le responsable du traitement doit mettre un terme au traitement, à moins qu'il ne démontre l'existence de motifs légitimes impérieux pour le poursuivre.

En ce qui concerne le **droit du CdE**, la Convention 108 modernisée[413] et les recommandations du CdE contiennent des formulations similaires. La Recommandation sur le profilage reconnaît le traitement des données à caractère personnel aux fins du 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 »[414]. De plus, « la protection des droits et libertés d'autrui » est mentionnée à l'article 8, paragraphe 2, de la CEDH comme l'un des fondements légitimes de la limitation du droit à la protection des données.

> Exemple : dans l'affaire *Y c. Turquie*[415], le requérant était séropositif. Étant donné qu'il était inconscient lors de son arrivée à l'hôpital, les ambulanciers ont informé le personnel de l'hôpital de sa séropositivité. Le requérant a fait valoir devant la CouEDH que la communication de cette information avait violé son droit au respect de la vie privée. Toutefois, compte tenu de la nécessité de protéger la sécurité du personnel hospitalier, la transmission de l'information n'a pas été considérée comme une violation de ses droits.

4.1.2. Traitement de catégories particulières de données (données sensibles)

Le droit du CdE laisse au droit national la tâche d'énoncer les mesures de protection appropriées pour l'utilisation de données sensibles, pour autant que les conditions visées à l'article 6 de la Convention 108 modernisée soient satisfaites, à savoir que des garanties appropriées qui complètent les autres dispositions de la Convention sont inscrites dans le droit. S'agissant du **droit de l'UE**, l'article 9 du RGPD prévoit un système détaillé pour le traitement de catégories particulières de données (également appelées « données sensibles »). Ces données révèlent l'origine raciale ou

413 Rapport explicatif sur la Convention 108 modernisée, para. 46.

414 CdE, Comité des Ministres (2010), Recommandation CM/Rec(2010)13 du Comité des Ministres aux États membres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage, 23 novembre 2010, art. 3, para. 4, point b) (Recommandation sur le profilage).

415 CouEDH, *Y c. Turquie*, nº 648/10, 17 février 2015.

ethnique, les opinions politiques, les convictions religieuses ou philosophiques et l'appartenance syndicale, ainsi que pour le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique. Le traitement de données sensibles est en principe interdit[416].

Il existe toutefois une liste exhaustive d'exceptions à cette interdiction, qui sont énumérées à l'article 9, paragraphe 2, du règlement et constituent des fondements légitimes pour le traitement de données sensibles. Ces exceptions incluent les cas où :

- la personne concernée donne explicitement son consentement au traitement des données ;
- le traitement est réalisé par un organisme à but non lucratif poursuivant une finalité politique, philosophique, religieuse ou syndicale dans le cadre de ses activités légitimes et se rapporte exclusivement à ses membres ou anciens membres ou aux personnes entretenant des contacts réguliers avec celui-ci en liaison avec ses finalités ;
- le traitement porte sur des données manifestement rendues publiques par la personne concernée ;
- le traitement est nécessaire :
    - aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail, de sécurité sociale et de protection sociale ;
    - à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique (dans le cas où la personne concernée se trouve dans l'incapacité de donner son consentement) ;
    - à la constatation, à l'exercice ou à la défense d'un droit en justice ou chaque fois que des juridictions agissent dans le cadre de leur fonction juridictionnelle ;

416 Ex-article 7, point f), de la Directive relative à la protection des données, devenu article 9, para. 1, du RGPD.

- aux fins de la médecine préventive ou de la médecine du travail : « aux fins de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale sur la base du droit de l'Union, du droit d'un État membre ou en vertu d'un contrat conclu avec un professionnel de la santé » ;

- à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques ;

- pour des motifs d'intérêt public dans le domaine de la santé publique ; ou

- pour des motifs d'intérêt public important.

Aux fins du traitement de catégories particulières de données, une relation contractuelle avec la personne concernée n'est donc pas considérée comme une base juridique pour le traitement légitime de données sensibles, hormis dans le cas d'un contrat conclu avec un professionnel de la santé et soumis à l'obligation de secret professionnel[417].

Consentement explicite de la personne concernée

Dans le **droit de l'UE**, le premier motif possible de traitement légitime, qu'il s'agisse ou non de données sensibles, est le consentement de la personne concernée. Dans le cas de données sensibles, le consentement doit être explicite. Le droit de l'Union ou le droit d'un État membre peut, toutefois, prévoir que l'interdiction de traitement portant sur des catégories particulières de données ne peut pas être levée par la personne concernée[418]. Tel pourrait, par exemple, être le cas lorsque le traitement implique des risques inhabituels pour la personne concernée.

Droit du travail, droit de la sécurité sociale et droit de la protection sociale

Dans le **droit de l'UE**, l'interdiction visée à l'article 9, paragraphe 1, peut être levée si le traitement est nécessaire aux fins de l'exécution des obligations ou de l'exercice des droits propres au responsable du traitement ou à la personne concernée en

417 RGPD, art. 9, para. 2, points h) et i).

418 *Ibid.*, art. 9, para. 2, point a).

matière d'emploi ou de sécurité sociale. Cependant, le traitement doit être autorisé par le droit de l'UE, par le droit d'un État membre ou par une convention collective conclue en vertu du droit d'un État membre qui prévoit des garanties appropriées pour le droit de l'Union et les intérêts de la personne concernée[419]. Les registres d'emploi tenus par une organisation peuvent contenir des données à caractère personnel sensibles à certaines conditions précisées dans le RGPD et dans le droit national applicable. L'appartenance syndicale ou des informations relatives à la santé sont des exemples de données sensibles.

Intérêts vitaux de la personne concernée ou d'une autre personne

Dans le **droit de l'UE**, comme dans le cas des données non sensibles, les données sensibles peuvent être traitées pour des raisons tenant aux intérêts vitaux de la personne concernée ou d'une autre personne physique[420]. Lorsque le traitement est fondé sur les intérêts vitaux d'une autre personne, ce fondement légitime ne peut être invoqué que si le traitement « ne peut manifestement pas être fondé sur une autre base juridique »[421]. Certains types de traitement de données à caractère personnel peuvent servir à la fois l'intérêt public et l'intérêt de la personne concernée, par exemple lorsque le traitement est nécessaire à des fins humanitaires[422].

Pour que le traitement de données sensibles soit légitime sur ce fondement, il doit avoir été impossible de demander le consentement à la personne concernée, par exemple parce qu'elle était inconsciente ou absente et ne pouvait être jointe. En d'autres termes, la personne était dans l'incapacité physique ou juridique de donner son consentement.

Associations caritatives ou organismes à but non lucratif

Le traitement de données à caractère personnel est également autorisé dans le cadre des activités légitimes de fondations, d'associations ou d'autres organismes à but non lucratif et poursuivant une finalité politique, philosophique, religieuse ou syndicale. Toutefois, le traitement doit se rapporter exclusivement aux membres ou aux anciens membres dudit organisme ou aux personnes entretenant des contacts

419 RGPD, art. 9, para. 2, point b).

420 *Ibid.*, art. 9, para. 2, point c).

421 *Ibid.*, considérant 46.

422 *Ibid.*

réguliers avec celui-ci[423]. Les données sensibles ne peuvent pas être communiquées en dehors de cet organisme sans le consentement de la personne concernée.

Données manifestement rendues publiques par la personne concernée

L'article 9, paragraphe 2, point e), du RGPD prévoit que le traitement n'est pas interdit lorsqu'il porte sur des données qui sont manifestement rendues publiques par la personne concernée. Bien que le règlement ne définisse pas le sens de l'expression « manifestement rendues publiques par la personne concernée », dans la mesure où elle constitue une exception à l'interdiction de traitement des données sensibles, elle doit être interprétée strictement comme imposant à la personne concernée de rendre délibérément publiques ses données personnelles. Par conséquent, lorsque la télévision diffuse une vidéo provenant d'une caméra de vidéosurveillance qui montre, notamment, un pompier blessé alors qu'il tente d'évacuer un bâtiment, on ne saurait considérer que le pompier a manifestement rendu les données publiques. Par contre, si le pompier décidait de décrire l'incident et publiait la vidéo et des photos sur une page web publique, il poserait un acte affirmatif délibéré pour rendre publiques des données à caractère personnel. Il importe d'observer que rendre ses données publiques ne constitue pas un consentement, mais est une autre façon d'autoriser le traitement de catégories particulières de données.

Le fait que la personne concernée ait rendu publiques les données à caractère personnel traitées ne libère pas les responsables du traitement de leurs obligations au titre du droit de la protection des données. Le principe de la limitation de la finalité, par exemple, continue de s'appliquer aux données à caractère personnel même si celles-ci ont été rendues publiques[424].

Actions en justice

Le traitement de catégories particulières de données qui est « nécessaire aux fins de la constatation, de l'exercice ou de la défense d'un droit en justice », que ce soit dans le cadre d'une procédure judiciaire, administrative ou extrajudiciaire[425], est éga-

423 *Ibid.*, art. 9, para. 2, point d).

424 Groupe de travail « Article 29 » (2013), *Avis 3/2013 sur la limitation de la finalité*, WP 203, 2 avril 2013, p. 14.

425 RGPD, exposé des motifs, considérant 52.

lement autorisé par le RGPD[426]. Dans ce cas, le traitement doit être pertinent pour un droit en justice spécifique à son exercice ou à sa défense, respectivement, et peut être demandé par l'une des parties au litige.

Dans l'exercice de leur fonction juridictionnelle, les juridictions peuvent traiter des catégories particulières de données dans le cadre de la résolution d'un litige[427]. Des exemples de ces catégories particulières de données traitées dans ce contexte pourraient être des données génétiques lors de l'établissement d'une filiation ou des données relatives à la santé lorsqu'une partie des preuves concerne les détails d'une blessure subie par la victime d'une infraction.

Motifs d'intérêt public important

Aux termes de l'article 9, paragraphe 2, point g), du RGPD, les États membres peuvent prévoir d'autres circonstances dans lesquelles des données sensibles peuvent être traitées, pour autant que :

- le traitement des données soit nécessaire pour des motifs d'intérêt public important :
- le traitement soit prévu par le droit de l'UE ou le droit d'un État membre ;
- le droit de l'UE ou le droit national soit proportionné, respecte le droit à la protection des données et prévoie des mesures appropriées et spécifiques pour la sauvegarde des droits et des intérêts de la personne concernée[428].

Un exemple majeur est celui des dossiers médicaux électroniques. Ces systèmes 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 ce patient à une grande échelle, généralement au niveau du pays.

Le Groupe de travail « Article 29 » a conclu que la mise en place de ces systèmes n'était pas possible dans le cadre de la réglementation existante en matière de

426 *Ibid.*, art. 9, para. 2, point f).

427 *Ibid.*

428 *Ibid.*, art. 9, para. 2, point g).

traitement de données sur les patients[429]. Il est toutefois possible de mettre en place des dossiers médicaux électroniques lorsqu'ils sont basés sur des « motifs d'intérêt public important »[430]. Cela nécessiterait une base juridique explicite, qui prévoirait également les mesures nécessaires pour s'assurer que le système est géré de manière sûre[431].

Autres motifs de traitement des données sensibles

Le RGPD dispose que les données sensibles peuvent être traitées lorsque le traitement est nécessaire[432] :

- aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale sur la base du droit de l'Union, du droit d'un État membre ou en vertu d'un contrat conclu avec un professionnel de la santé ;

- pour des motifs d'intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontalières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux, sur la base du droit de l'Union ou du droit de l'État membre qui prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée ;

- à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques sur la base du droit de l'Union ou du droit d'un État membre. Le droit doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée.

429 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. Voir également RGPD, art. 9, para. 3.

430 RGPD, art. 9, para. 2, point g).

431 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.

432 RGPD, art. 9, para. 2, points h), i) et j).

Conditions supplémentaires dans le droit national

Le RGPD autorise également les États membres à introduire ou à maintenir des conditions supplémentaires, notamment des limitations concernant le traitement des données génétiques, biométriques et relatives à la santé[433].

4.2. Règles relatives à la sécurité du traitement

Points clés

- Les règles relatives à la sécurité du traitement obligent le responsable du traitement et le sous-traitant à 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 ;
  - les risques du traitement des données pour les droits et libertés fondamentaux des personnes concernées.
- Assurer la confidentialité des données à caractère personnel fait partie d'un principe général reconnu par le Règlement général sur la protection des données.

Tant dans le **droit de l'UE que dans le droit du CdE**, les responsables du traitement ont l'obligation générale de faire preuve de transparence et de responsabilité dans le traitement des données à caractère personnel et, en particulier, sur les violations des données et le moment où ces violations surviennent. En cas de violation de données à caractère personnel, les responsables du traitement sont tenus de notifier l'autorité de contrôle, à moins que la violation ne soit pas susceptible de générer un risque pour les droits et libertés des personnes physiques. Les personnes concernées devraient également être informées de la violation de leurs données à caractère personnel lorsque celle-ci est susceptible d'engendrer un risque élevé pour les droits et libertés de personnes physiques.

433 *Ibid.*, art. 9, para. 2, point h), et art. 9, para. 4.

4.2.1. Éléments de la sécurité des données

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

> *« Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque [...] »*[434].

Ces mesures incluent notamment :

- la pseudonymisation et le chiffrement des données à caractère personnel[435] ;
- des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement[436] ;
- des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique[437] ;
- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures pour assurer la sécurité du traitement[438].

Une disposition similaire existe dans le **droit du CdE** :

> *« Chaque Partie prévoit que le responsable du traitement ainsi que, le cas échéant, le sous-traitant prend des mesures de sécurité appropriées contre les risques tels que l'accès accidentel ou non autorisé aux données à caractère personnel, leur destruction, perte, utilisation, modification ou divulgation »*[439].

434 *Ibid.*, art. 32, para. 1.
435 *Ibid.*, art. 32, para. 1, point a).
436 *Ibid.*, art. 32, para. 1, point b).
437 *Ibid.*, art. 32, para. 1, point c).
438 *Ibid.*, art. 32, para. 1, point d).
439 Convention 108 modernisée, art. 7, para. 1.

Dans le **droit de l'UE** et dans le **droit du CdE**, une violation des données susceptible d'avoir un impact sur les droits et libertés des personnes oblige le responsable du traitement à en notifier l'autorité de contrôle (voir section 4.2.3).

Des normes sectorielles, nationales et internationales ont souvent été élaborées pour assurer la sécurité du traitement des 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 étudie les possibilités de certification de produits, en particulier des logiciels, afin de faciliter la conformité avec le 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, de ses États membres et des entreprises à prévenir, traiter et répondre aux problèmes de sécurité des réseaux et de l'information[440]. L'ENISA publie régulièrement des analyses des menaces de sécurité ainsi que des conseils sur la façon d'y répondre[441].

La sécurité des données ne s'obtient pas simplement par la mise en place du bon équipement (matériel et logiciel). Elle requiert également des règles d'organisation interne appropriées, qui devraient idéalement 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 pour 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 ;
- protection de l'accès aux sites, au matériel et aux logiciels du responsable du traitement ou du sous-traitant, y compris le contrôle des autorisations d'accès ;

440 Règlement (UE) nº 526/2013 du Parlement européen et du Conseil du 21 mai 2013 concernant l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) et abrogeant le règlement (CE) nº 460/2004, JO L 2013 L 165.

441 Par exemple, ENISA, (2016), Cyber Security and Resilience of smart cars. Good practices and recommendations; ENISA (2016), Security of Mobile Payments and Digital Wallets.

- garantie 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 contrôles réguliers de ces protocoles par le bureau de contrôle interne (ce qui requiert que toutes les activités de traitement de données soient enregistrées) ;

- documentation consciencieuse pour les formes de diffusion autres 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 de sécurité. Des procédures de vérification doivent également être en place pour garantir que non seulement des mesures appropriées existent sur le papier, mais qu'elles sont appliquées et fonctionnent dans la pratique (comme des audits internes ou externes).

Les mesures visant à améliorer le niveau de sécurité d'un responsable du traitement ou d'un sous-traitant 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*[442], la requérante n'avait pas été en mesure de prouver que son dossier médical avait fait l'objet d'un accès illicite par des employés 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 dossiers au sein de l'hôpital avec les exigences légales du

442 CouEDH, *I c. Finlande*, nº 20511/03, 17 juillet 2008.

droit national était un élément déterminant auquel les juridictions nationales n'avaient pas accordé suffisamment de poids

L'UE a adopté la Directive concernant la sécurité des réseaux et des systèmes d'information (Directive RSI)[443], qui est le premier instrument légal relatif à la cybersécurité couvrant toute l'UE. La directive vise à améliorer la cybersécurité au niveau national, d'une part, et à renforcer la coopération au sein de l'UE, d'autre part. Elle impose également des obligations aux opérateurs de services essentiels (y compris les opérateurs actifs dans les secteurs de l'énergie, de la santé, de la banque, du transport, de l'infrastructure numérique, etc.) et aux fournisseurs de services numériques afin de gérer les risques, d'assurer la sécurité de leurs réseaux et systèmes d'information et de signaler les incidents de sécurité.

Perspectives

En septembre 2017, la Commission européenne a proposé un projet de règlement visant à modifier le mandat de l'ENISA afin de tenir compte des nouvelles compétences et responsabilités que lui confère la Directive RSI. La proposition de règlement a pour but de développer les missions de l'ENISA et de renforcer son rôle comme « point de référence dans l'écosystème de cybersécurité de l'UE »[444]. La proposition ne devrait pas porter atteinte aux principes du RGPD et, en clarifiant les éléments nécessaires qui composent les systèmes européens de certification en matière de cybersécurité, elle devrait également renforcer la sécurité des données à caractère personnel. Parallèlement, la Commission européenne a présenté en septembre 2017 un projet de règlement d'exécution précisant les éléments que les fournisseurs de services numériques doivent prendre en compte pour faire en sorte que leurs réseaux et systèmes d'information soient sûrs, comme l'impose l'article 16, paragraphe 8, de la Directive RSI. Au moment de rédiger ce manuel, les discussions sur ces deux propositions se poursuivaient.

443 Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, JO 2016 L 194.

444 Proposition de règlement du Parlement européen et du Conseil relatif à l'ENISA, Agence de l'Union européenne pour la cybersécurité, et abrogeant le règlement (UE) nº 526/2013, et relatif à la certification des technologies de l'information et des communications en matière de cybersécurité (Règlement sur la cybersécurité), COM/2017/477, 13 septembre 2017, p. 6.

4.2.2. Confidentialité

Dans le droit de l'UE, le RGPD reconnaît la confidentialité des données à caractère personnel en tant que principe général[445]. Les fournisseurs de services de communications électroniques accessibles au public doivent garantir la confidentialité. Ils sont également soumis à l'obligation de préserver la sécurité de leurs services[446].

> Exemple : un salarié d'une compagnie d'assurances 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.

Conformément à l'article 5, paragraphe 1, point f), les données à caractère personnel doivent être traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles (« intégrité et confidentialité »).

Selon l'article 32, le responsable du traitement et le sous-traitant doivent mettre en œuvre des mesures techniques et organisationnelles afin de garantir un niveau de sécurité élevé. Ces mesures incluent, entre autres, la pseudonymisation et le chiffrement des données à caractère personnel, des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes du traitement, une procédure visant à tester et à évaluer l'efficacité des mesures et des moyens permettant de rétablir le traitement en cas d'incident physique ou technique. De plus, l'adhésion à un code de conduite approuvé ou à un mécanisme de certification approuvé peut servir à démontrer le respect du principe d'intégrité et de confidentialité. Par ailleurs, conformément à l'article 28 du RGPD, le contrat liant le responsable du traitement au sous-traitant doit stipuler que le sous-traitant veille à ce que les personnes autorisées à traiter des données à caractère personnel se

445 RGPD, art. 5, para. 1, point f).

446 Directive « vie privée et communications électroniques », art. 5, para. 1.

soient engagées à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité.

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, les articles 32 et 28 du RGPD ne s'appliquent pas, puisque l'utilisation de données à caractère personnel par des particuliers n'entre absolument pas dans le champ d'application du règlement, dès lors que cette utilisation relève des limites de l'exemption domestique[447]. 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 »[448]. Depuis la décision de la CJUE dans l'affaire *Bodil Lindqvist*[449], cette exemption doit toutefois être interprétée de façon restreinte, en particulier à l'égard de la divulgation 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 ou au traitement des données ayant un caractère professionnel ou commercial (pour plus d'informations sur l'affaire, voir sections 2.1.2, 2.2.2 et 2.3.1).

La « confidentialité des communications » est un autre aspect de la confidentialité, qui fait l'objet d'une *lex specialis*. Les règles particulières concernant la confidentialité des communications électroniques énoncées par la Directive « vie privée et communications électroniques » imposent aux États membres d'interdire à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker ou de soumettre à tout autre moyen d'interception ou de surveillance les communications et les métadonnées y afférentes sans le consentement des utilisateurs concernés[450]. La législation nationale peut autoriser des exceptions à ce principe uniquement pour des raisons de sécurité nationale, de défense, de prévention ou de détection d'infractions pénales et uniquement si ces mesures sont nécessaires et proportionnées aux objectifs poursuivis[451]. Les mêmes règles s'appliqueront au futur Règlement relatif aux communications électroniques et à la vie privée, mais le champ d'application de l'instrument juridique en la matière sera étendu aux services de communications électroniques accessibles au public afin de couvrir également les

447 RGPD, art. 2, para. 2, point c).

448 *Ibid.*

449 CJUE, C-101/01, *Procédure pénale contre Bodil Lindqvist*, 6 novembre 2003.

450 Directive « vie privée et communications électroniques », art. 5, para. 1.

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

communications passant par des services d'accès direct (« over-the-top »), comme des applications mobiles.

Dans le droit du CdE, l'obligation de confidentialité est sous-entendue dans la notion de sécurité des données figurant à l'article 7, paragraphe 1, de la Convention 108, consacré à la sécurité des données**.**

Pour les sous-traitants, la confidentialité signifie qu'ils ne peuvent pas divulguer les données à des tiers ou à d'autres destinataires sans autorisation. 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 un responsable de traitement et ses sous-traitants. En outre, les responsables de 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 Parties contractantes à la Convention 108.

4.2.3. Notifications de violation de données à caractère personnel

On entend par violation de données à caractère personnel une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel traitées ou l'accès non autorisé à de telles données[452]. Bien que les nouvelles technologies, comme le chiffrement, offrent désormais davantage de possibilités pour assurer la sécurité du traitement, les violations de données restent un phénomène courant. Les causes peuvent aller d'erreurs accidentelles commises par des personnes travaillant au sein d'une organisation à des menaces extérieures, comme des hackeurs ou des organisations actives dans la cybercriminalité.

452 RGPD, art. 4, para. 12 ; voir également Groupe de travail « Article 29 » (2017), *Guidelines on Personal data breach notification under Regulation 2016/679*, WP 250, 3 octobre 2017, p. 8.

Les violations de données peuvent causer un préjudice considérable aux droits au respect de la vie privée et à la protection des données des particuliers qui, du fait de la violation, perdent le contrôle de leurs données à caractère personnel. Les violations peuvent entraîner une usurpation d'identité ou une fraude, une perte financière ou des dommages matériels, la perte de la confidentialité de données personnelles protégées par le secret professionnel et une atteinte à la réputation de la personne concernée. Dans ses lignes directrices sur la notification des violations de données à caractère personnel au titre du Règlement 2016/679, le Groupe de travail « Article 29 » explique qu'une violation de données à caractère personnel peut entraîner trois types d'effet sur ces données : la divulgation, la perte et/ou l'altération[453]. Outre l'obligation de prendre des mesures pour assurer la sécurité du traitement, comme expliqué à la section 4.2, il est tout aussi important de veiller à ce que les responsables du traitement traitent les violations de données de manière appropriée et en temps utile lorsqu'elles surviennent.

Les autorités de contrôle et les personnes physiques ignorent souvent qu'une violation de données s'est produite, ce qui empêche les personnes de prendre des mesures pour se protéger contre ses conséquences négatives. Pour affirmer les droits des particuliers et limiter les conséquences des violations de données, **l'UE et le CdE** imposent une obligation de notification aux responsables du traitement dans certaines circonstances.

En vertu de la Convention 108 modernisée du **CdE**, les Parties contractantes doivent, à tout le moins, imposer aux responsables du traitement de notifier à l'autorité de contrôle compétente les violations de données susceptibles de porter gravement atteinte aux droits des personnes concernées. Cette notification doit avoir lieu « sans délai »[454].

Le droit de l'UE établit un système détaillé qui réglemente le moment et le contenu des notifications[455]. Les responsables du traitement doivent ainsi notifier certaines violations de données aux autorités de contrôle dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance. Lorsque la notification n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard. Les responsables du traitement ne sont exemptés de l'obligation de notification que s'ils

453 Groupe de travail « Article 29 » (2017), *Guidelines on Personal data breach notification under Regulation 2016/679*, WP 250, 3 octobre 2017, p. 6.

454 Convention 108 modernisée, art. 7, para. 2 ; Rapport explicatif sur la Convention 108 modernisée, paras. 64-66.

455 RGPD, art. 33 et 34.

sont en mesure de prouver que la violation de données n'est pas susceptible de générer un risque pour les droits et libertés des personnes concernées.

Le règlement énumère les informations que doit au minimum contenir la notification afin de permettre à l'autorité de contrôle de prendre les mesures nécessaires[456]. La notification doit, à tout le moins, décrire la nature de la violation de données et les catégories et le nombre approximatif de personnes concernées touchées, ainsi que les conséquences probables de la violation de données et les mesures prises par le responsable du traitement pour en atténuer les conséquences. En outre, le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact doivent être communiqués afin de permettre à l'autorité de contrôle compétente d'obtenir des informations supplémentaires, si nécessaire.

Lorsqu'une violation de données est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement doit communiquer la violation à celle-ci (la personne concernée) dans les meilleurs délais[457]. La communication à la personne concernée, y compris la description de la violation de données, doit être rédigée en des termes clairs et simples et contenir les mêmes informations que celles exigées pour les notifications aux autorités de contrôle. Dans certains cas, les responsables du traitement peuvent être exemptés de l'obligation de notifier ces violations aux personnes concernées. Ces exemptions s'appliquent lorsque le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées et que ces mesures ont été appliquées aux données à caractère personnel affectées par ladite violation, en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le chiffrement. Les mesures prises par le responsable du traitement après la violation afin de garantir que le risque pour les droits des personnes concernées n'est plus susceptible de se matérialiser peuvent également exempter le responsable du traitement de l'obligation de notification aux personnes concernées. Enfin, si la notification implique des efforts disproportionnés pour le responsable du traitement, les personnes concernées peuvent être informées de l'atteinte par d'autres moyens, comme une communication publique ou des mesures similaires[458].

456 *Ibid.*, art. 33, para. 3.

457 *Ibid.*, art. 34.

458 *Ibid.*, art. 34, para. 3, point c).

L'obligation de notifier les violations de données aux autorités de contrôle et aux personnes concernées est imposée aux responsables du traitement. Cependant, des violations de données peuvent survenir indépendamment du fait que le traitement est réalisé par un responsable du traitement ou par un sous-traitant. C'est pourquoi il est essentiel de s'assurer que les sous-traitants sont également tenus de signaler les violations de données. Dans un tel cas, les sous-traitants doivent notifier les violations de données au responsable du traitement dans les meilleurs délais[459]. Le responsable du traitement est alors tenu de notifier la violation aux autorités de contrôle et aux personnes concernées touchées, dans le respect des règles et délais susvisés.

4.3. Règles relatives à la responsabilité et à la promotion de la conformité

Points clés

- Afin de garantir la responsabilité du traitement de données à caractère personnel, les responsables du traitement et les sous-traitants doivent tenir à jour des registres des activités de traitement effectuées sous leur responsabilité et les communiquer aux autorités de contrôle sur demande.
- Le Règlement général sur la protection des données établit plusieurs instruments destinés à promouvoir la conformité :
  - la désignation de délégués à la protection des données dans certains cas ;
  - la réalisation d'une analyse d'impact avant le début des activités de traitement susceptibles de représenter un risque élevé pour les droits et libertés des personnes ;
  - la consultation préalable de l'autorité de contrôle compétente lorsque l'analyse d'impact indique que le traitement présente des risques qui ne peuvent pas être atténués ;
  - des codes de conduite pour les responsables du traitement et les sous-traitants précisant l'application du règlement dans divers secteurs ;
  - des mécanismes de certification, des labels et des marques.
- Le droit du CdE propose des instruments similaires pour la promotion de la conformité dans la Convention 108 modernisée.

459 *Ibid.*, art. 33, para. 2.

Le principe de la responsabilité est particulièrement important pour garantir l'application des règles relatives à la protection des données en Europe. Le responsable du traitement est chargé de la conformité avec les règles relatives à la protection des données et doit être en mesure de la démontrer. La responsabilité ne doit pas devenir un enjeu uniquement après une violation de données. Les responsables du traitement sont plutôt soumis à une obligation proactive de suivre des politiques appropriées en matière de gestion des données à toutes les étapes du traitement des données. La législation européenne en matière de protection des données impose aux responsables du traitement de mettre en œuvre des mesures techniques et organisationnelles afin de veiller à ce que le traitement soit effectué conformément à la loi et d'être en mesure de le démontrer. Parmi ces mesures figurent la désignation de délégués à la protection des données, la tenue de registres et d'une documentation relative au traitement et la réalisation d'analyses d'impact sur la vie privée.

4.3.1. Délégués à la protection des données

Les délégués à la protection des données (DPD) sont des personnes qui donnent des conseils sur la conformité avec les règles relatives à la protection des données au sein d'organisations qui effectuent des traitements de données. Ils sont la « pierre angulaire de la responsabilité », car ils favorisent la conformité tout en servant d'intermédiaires entre les autorités de contrôle, les personnes concernées et l'organisation par laquelle ils ont été désignés.

Dans le droit du CdE, l'article 10, paragraphe 1, de la Convention 108 modernisée impose une responsabilité générale aux responsables du traitement et aux sous-traitants. Cette disposition oblige les responsables du traitement et les sous-traitants à prendre toutes les mesures appropriées afin de se conformer aux règles de protection des données énoncées dans la Convention et d'être en mesure de démontrer que le traitement dont ils sont responsables est en conformité avec les dispositions de la Convention. Bien que la Convention ne précise pas les mesures concrètes que les responsables du traitement et les sous-traitants devraient adopter, le rapport explicatif sur la Convention 108 modernisée indique que la désignation d'un DPD est une des mesures possibles pour faciliter la démonstration de la conformité. Les DPD devraient disposer de tous les moyens nécessaires à l'accomplissement de leur mandat[460].

Contrairement au droit du CdE, **dans celui de l'UE**, la désignation d'un DPD n'est pas toujours laissée à la discrétion des responsables du traitement et des sous-traitants,

460 Rapport explicatif sur la Convention 108 modernisée, para. 87.

mais elle est obligatoire dans certains cas. Le RGPD attribue au DPD un rôle clé dans le nouveau système de gouvernance et contient des dispositions détaillées sur la désignation du DPD, sa fonction, ses obligations et ses tâches[461].

Le RGPD impose la désignation d'un DPD dans trois cas particuliers : lorsque le traitement est effectué par une autorité publique ou un organisme public, lorsque les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui exigent un suivi régulier et systématique à grande échelle des personnes concernées ou lorsque les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données ou de données à caractère personnel relatives à des condamnations pénales et à des infractions[462]. Bien que des expressions telles que « suivi systématique à grande échelle » et « activités de base » ne soient pas définies dans le règlement, le Groupe de travail « Article 29 » a publié des lignes directrices sur leur interprétation[463].

Exemple : des sociétés de réseaux sociaux et des moteurs de recherche sont susceptibles d'être considérés comme des responsables de traitement dont les opérations de traitement exigent le suivi régulier et systématique à grande échelle des personnes concernées. Le modèle commercial de ces entreprises repose sur le traitement d'importantes quantités de données à caractère personnel et elles génèrent des revenus considérables en proposant des services de publicité ciblée et en autorisant des entreprises à publier des annonces sur leurs sites. La publicité ciblée est une manière de publier des annonces en se fondant sur la démographie et sur l'historique d'achats ou le comportement passé des consommateurs. Elle requiert donc le suivi systématique des habitudes et des comportements en ligne des personnes concernées.

Exemple : un hôpital et une compagnie d'assurance maladie sont des exemples typiques de responsables du traitement dont les activités consistent en un traitement à grande échelle de catégories particulières de données à caractère personnel. Les données qui révèlent des informations sur la santé d'une personne constituent des catégories particulières de

461 RGPD, art. 37 à 39.

462 *Ibid.*, art. 37, para. 1.

463 Groupe de travail « Article 29 » (2017), *Lignes directrices concernant les délégués à la protection des données (DPD)*, WP 243 rev.01, version révisée et adoptée le 5 avril 2017.

données à caractère personnel tant dans le droit du CdE que de l'UE et nécessitent donc une protection accrue. Le droit de l'UE reconnaît par ailleurs les données biométriques et les données génétiques comme des catégories particulières de données. Dans la mesure où des établissements hospitaliers et des compagnies d'assurances traitent de telles données à grande échelle, le RGPD leur impose de désigner un délégué à la protection des données.

En outre, l'article 37, paragraphe 4, du RGPD prévoit que dans les cas autres que les trois cas obligatoires visés au paragraphe 1 de cette disposition, le responsable du traitement, le sous-traitant ou des associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants peuvent ou, si le droit de l'Union ou le droit d'un État membre l'exige, sont tenus de désigner un délégué à la protection des données.

Les autres organismes ne sont pas légalement tenus de désigner un DPD. Le RGPD prévoit toutefois que les responsables du traitement et les sous-traitants peuvent choisir de leur plein gré de désigner un DPD, tout en laissant également aux États membres la possibilité de rendre cette désignation obligatoire pour d'autres types d'organismes que ceux prévus dans le règlement[464].

Dès qu'un responsable du traitement désigne un DPD, il doit veiller à ce qu'il « soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel » au sein de l'organisme[465]. À titre d'exemple, le DPD devrait intervenir en donnant des conseils sur l'exécution des analyses d'impact relatives à la protection des données et en créant et tenant à jour des registres des activités de traitement de l'organisation. Afin de permettre aux DPD d'accomplir efficacement leur mission, les responsables du traitement et les sous-traitants doivent les doter des ressources nécessaires, notamment financières, ainsi que de l'infrastructure et de l'équipement dont ils ont besoin. Entre autres obligations, il y a lieu de donner aux DPD suffisamment de temps pour remplir leurs fonctions ainsi qu'une formation continue afin de leur permettre de développer leurs compétences et de se tenir au courant de tous les développements de la législation relative à la protection des données[466].

464 RGPD, art. 37, paras. 3 et 4.

465 *Ibid.*, art. 38, para. 1.

466 Groupe de travail « Article 29 » (2017), *Lignes directrices concernant les délégués à la protection des données (DPD)*, WP 243 rev.01, version révisée et adoptée le 5 avril 2017, para. 3.1.

Le RGPD prévoit certaines garanties essentielles afin que les DPD puissent agir en toute indépendance. Les responsables du traitement et les sous-traitants doivent veiller à ce que les DPD ne reçoivent aucune instruction de l'entreprise, y compris du niveau le plus élevé de la direction, dans l'exercice de leurs missions relatives à la protection des données. De plus, ils ne doivent pas être renvoyés ou en aucune manière pénalisés pour avoir accompli leurs tâches[467]. Prenons l'exemple d'un DPD qui conseille à un responsable du traitement ou à un sous-traitant de mener une analyse d'impact sur la protection des données parce qu'il considère que le traitement est susceptible d'engendrer un risque élevé pour les personnes concernées. L'entreprise ne partage pas l'avis du DPD, ne le juge pas fondé et décide donc de ne pas réaliser l'analyse d'impact. L'entreprise peut ignorer l'avis, mais elle ne peut ni renvoyer ni pénaliser le DPD pour l'avoir donné.

Enfin, les missions et obligations des DPD sont détaillées à l'article 39 du RGPD. Elles comprennent les missions d'informer et de conseiller les entreprises et les employés qui procèdent au traitement sur les obligations qui leur incombent en vertu de la législation et de contrôler le respect du droit de l'Union ou du droit des États membres en matière de protection des données, en réalisant des audits et en formant le personnel participant aux opérations de traitement. Les DPD doivent aussi coopérer avec l'autorité de contrôle et faire office de point de contact pour celle-ci sur les questions relatives au traitement, telles que, par exemple, une violation de données.

S'agissant des données à caractère personnel traitées par des institutions et organes de l'UE, le Règlement 45/2001 dispose que chaque institution ou organe de l'UE doit désigner un DPD. Le DPD est chargé de veiller à l'application appropriée des dispositions du règlement au sein des institutions et organes de l'UE et de veiller à ce que les personnes concernées et les responsables du traitement soient informés de leurs droits et obligations[468]. Il lui incombe également de répondre aux demandes du CEPD et de coopérer avec lui le cas échéant. Tout comme le RGPD, le Règlement 45/2001 contient des dispositions sur l'indépendance des DPD dans l'accomplissement de leurs missions et sur la nécessité de leur fournir le personnel et les ressources nécessaires[469]. Avant qu'une institution ou un organe de l'UE (ou des services de ces

467 RGPD, art. 38, paras. 2 et 3.

468 Pour la liste complète des tâches du DPD, voir Règlement (CE) nº 45/2001, art. 24, para. 1.

469 Règlement (CE) nº 45/2001, art. 24, paras. 6 et 7.

organismes) entreprenne un traitement, le DPD doit en être informé et doit tenir un registre de toutes les opérations de traitement qui lui sont notifiées[470].

4.3.2. Registres des activités de traitement

Pour pouvoir prouver la conformité et assumer leurs responsabilités, les entreprises sont souvent légalement tenues de documenter et de tenir un registre de leurs activités. Un exemple important est la législation fiscale et l'audit, qui imposent à toutes les entreprises de conserver de nombreux documents et de tenir des registres. L'imposition d'exigences similaires dans d'autres domaines juridiques, notamment en droit de la protection des données, est également importante, étant donné que la tenue de registres est un moyen majeur de favoriser la conformité avec les règles en matière de protection des données. Le **droit de l'UE** prévoit donc que les responsables du traitement ou leur représentant tiennent un registre des activités de traitement effectuées sous leur responsabilité[471]. Cette obligation a pour but de faire en sorte que les autorités de contrôle disposent, le cas échéant, des documents nécessaires pour leur permettre de confirmer la licéité d'un traitement.

Le registre contient les informations suivantes :

- le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du DPD ;
- les finalités du traitement ;
- une description des catégories de personnes concernées et des catégories de données à caractère personnel ;
- des informations sur les catégories de destinataires dont les données à caractère personnel ont été ou seront communiquées ;
- des informations sur la question de savoir si des transferts de données à caractère personnel vers un pays tiers ou une organisation internationale ont été ou seront réalisés ;

470 *Ibid.*, art. 25 et 26.

471 RGPD, art. 30.

- dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données à caractère personnel, ainsi qu'une description générale des mesures techniques adoptées pour garantir la sécurité du traitement[472].

L'obligation de tenir un registre des activités de traitement énoncée dans le RGPD s'applique aussi bien aux responsables du traitement qu'aux sous-traitants. Il s'agit d'une évolution majeure, étant donné qu'avant l'adoption du règlement, le contrat conclu entre le responsable du traitement et le sous-traitant couvrait essentiellement les obligations du sous-traitant. L'obligation qui leur est faite de tenir un registre est désormais directement prévue par la loi.

Le RGPD prévoit une exception à cette obligation. Les obligations de tenir un registre ne s'appliquent pas à une entreprise ou à une organisation (responsable du traitement ou sous-traitant) qui compte moins de de 250 employés. L'exception est toutefois soumise à l'exigence que l'organisation concernée n'entreprenne pas un traitement susceptible de comporter un risque pour les droits et libertés des personnes concernées, que le traitement soit uniquement occasionnel et qu'il ne porte pas sur les catégories particulières de données visées à l'article 9, paragraphe 1, ou sur des données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10.

La tenue d'un registre des activités de traitement devrait permettre aux responsables du traitement et aux sous-traitants d'apporter la preuve de la conformité avec le règlement. Elle devrait également permettre aux autorités de contrôle de vérifier la licéité du traitement. Lorsqu'une autorité de contrôle demande l'accès à ces registres, les responsables du traitement et les sous-traitants sont tenus de coopérer avec elle et de mettre ces registres à sa disposition.

4.3.3. Analyse d'impact relative à la protection des données et consultation préalable

Les opérations de traitement présentent des risques intrinsèques pour les droits des particuliers. Les données à caractère personnel peuvent être perdues, divulguées à des tiers non autorisés ou traitées de manière illicite. Les risques varient évidemment selon la nature et la portée du traitement. Les opérations à grande échelle qui impliquent le traitement de données sensibles, par exemple, présentent un risque

472 *Ibid.*, art. 30, para. 1.

nettement plus élevé pour les personnes concernées que les risques potentiels que représente une petite entreprise qui traite les adresses et les numéros de téléphone personnel de ses employés.

À mesure que de nouvelles technologies apparaissent et que le traitement devient plus complexe, les responsables du traitement doivent traiter ces risques en analysant l'impact probable du traitement prévu avant le début de celui-ci. Cela permet aux organisations d'identifier, de traiter et d'atténuer adéquatement les risques à l'avance, en limitant de façon significative le risque de conséquences négatives du traitement sur les particuliers.

Tant le droit du CdE que celui de l'UE prévoient des analyses d'impact relatives à la protection des données. Dans le cadre juridique du CdE, l'article 10 paragraphe 2 de la Convention 108 modernisée impose aux Parties contractantes de veiller à ce que les responsables du traitement et les sous-traitants procèdent « préalablement au commencement de tout traitement, à l'examen de l'impact potentiel du traitement de données envisagé sur les droits et libertés fondamentales des personnes concernées » et, à la suite de l'analyse, conçoivent le traitement de données de manière à prévenir ou à minimiser les risques liés au traitement.

Le droit de l'UE impose une obligation similaire, mais plus détaillée, aux responsables du traitement qui relèvent du champ d'application du RGPD. L'article 35 prévoit qu'une analyse d'impact doit être effectuée lorsque le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques. Le règlement ne définit pas la manière dont la probabilité du risque doit être évaluée, mais indique plutôt quels pourraient être ces risques[473]. Il dresse une liste des opérations de traitement considérées comme présentant un risque élevé et pour lesquelles une analyse d'impact préalable est particulièrement nécessaire, à savoir lorsque :

- des données à caractère personnel sont traitées afin de prendre des décisions concernant des personnes physiques à la suite d'une évaluation systématique et approfondie d'aspects personnels concernant ces personnes (profilage) ;

- des données sensibles ou des données à caractère personnel relatives à des condamnations pénales et à des infractions sont traitées à grande échelle ;

473 RGPD, exposé des motifs, considérant 75.

- le traitement implique la surveillance systématique à grande échelle de zones accessibles au public.

Les autorités de contrôle doivent établir et publier une liste des types d'opérations de traitement pour lesquelles une analyse d'impact est requise. Elles peuvent également dresser une liste des opérations de traitement exemptées de cette obligation[474].

Lorsqu'une analyse d'impact est requise, le responsable du traitement doit évaluer la nécessité et la proportionnalité du traitement et les risques potentiels pour les droits des personnes physiques. L'analyse d'impact doit également contenir les mesures de sécurité prévues pour faire face aux risques identifiés. Pour établir les listes, les autorités de contrôle des États membres sont tenues de coopérer entre elles et avec le Comité européen de la protection des données. Cette coopération assurera une approche cohérente au sein de l'Union à l'égard des opérations requérant une analyse d'impact et les responsables du traitement seront soumis à des exigences similaires, quel que soit l'endroit où ils se trouvent.

S'il ressort d'une analyse d'impact que le traitement engendrera un risque élevé pour les droits des personnes concernées et qu'aucune mesure n'a été prise pour atténuer ce risque, le responsable du traitement doit consulter l'autorité de contrôle compétente avant de commencer le traitement[475].

Le Groupe de travail « Article 29 » a publié des lignes directrices concernant les analyses d'impact relatives à la protection des données et la manière de déterminer si un traitement est ou non susceptible de générer un risque élevé[476]. Il a élaboré neuf critères afin de déterminer plus aisément si une analyse d'impact relative à la protection des données est requise dans une situation donnée[477] : (1) évaluation ou notation ; (2) prise de décisions automatisée produisant un effet juridique ou similaire significatif ; (3) surveillance systématique ; (4) données sensibles ; (5) données traitées à grande échelle ; (6) ensembles de données correspondantes

474 *Ibid.*, art. 35, paras. 4 et 5.

475 *Ibid.*, art. 36, para. 1 ; Groupe de travail « Article 29 » (2017), *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in high risk" for the purposes of Regulation 2016/679*, WP 248 rev.01, Bruxelles, 4 octobre 2017.

476 Groupe de travail « Article 29 » (2017), *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in high risk" for the purposes of Regulation 2016/679*, WP 248 rev.01, Bruxelles, 4 octobre 2017.

477 *Ibid.*, p. 9 à 11.

ou combinées ; (7) données relatives à des personnes concernées vulnérables ; (8) utilisation innovante ou application de solutions technologiques ou organisationnelles ; (9) lorsque le traitement proprement dit « empêche les personnes concernées d'exercer un droit ou d'utiliser un service ou un contrat ». Le Groupe de travail « Article 29 » a introduit la règle selon laquelle les opérations de traitement qui satisfont à moins de deux critères représentent un risque moindre et ne requièrent pas une analyse d'impact relative à la protection des données, tandis que celles qui remplissent deux critères ou plus nécessiteront une telle analyse. Lorsque la nécessité d'une analyse d'impact relative à la protection des données n'est pas claire, le Groupe de travail « Article 29 » recommande de procéder à l'analyse parce qu'elle « sera un outil utile pour aider les responsables du traitement à se conformer à la législation en matière de protection des données »[478]. Lorsqu'une nouvelle technique de traitement de données est utilisée, il est important qu'une analyse d'impact relative à la protection des données soit réalisée[479].

4.3.4. Codes de conduite

Les codes de conduite sont destinés à être utilisés dans différents secteurs de l'industrie afin d'encadrer et de préciser l'application du RGPD dans les secteurs spécifiques. Pour les responsables du traitement et les sous-traitants, l'élaboration de ces codes peut grandement améliorer la conformité et la mise en œuvre des règles de l'UE en matière de protection des données. L'expertise des membres du secteur privilégiera la recherche de solutions pratiques et, partant, susceptibles d'être appliquées. Reconnaissant l'importance de ces codes pour l'application effective de la législation relative à la protection des données, le RGPD invite les États membres, les autorités de contrôle, la Commission et le Comité européen de la protection des données à encourager l'élaboration de codes de conduites destinés à contribuer à la bonne application du règlement dans l'Union[480]. Ces codes pourraient préciser l'application du règlement dans des secteurs spécifiques, y compris des questions telles que la collecte de données à caractère personnel, les informations à fournir aux personnes concernées et au public et l'exercice des droits des personnes concernées.

Pour garantir que les codes de conduite soient conformes aux règles établies par le RGPD, ils doivent être soumis à l'autorité de contrôle compétente avant leur adoption. L'autorité de contrôle rend alors un avis sur la question de savoir si le projet de

478 *Ibid.*, p. 9.

479 *Ibid.*

480 RGPD, art. 40, para. 1.

code respecte le règlement et elle l'approuve si elle estime qu'il offre des garanties appropriées[481]. Les autorités de contrôle doivent publier les codes de conduite approuvés ainsi que les critères sur lesquels elles ont fondé leur approbation. Lorsqu'un projet de code de conduite concerne des activités de traitement menées dans plusieurs États membres, l'autorité de contrôle compétente soumet le projet de code, la modification ou la prorogation avant approbation au Comité européen de la protection des données, qui rend un avis sur la conformité du code avec le RGPD. La Commission peut décider, par voie d'actes d'exécution, que le code de conduite approuvé qui lui a été soumis est d'application générale au sein de l'Union.

L'adhésion à un code de conduite présente des avantages majeurs tant pour les personnes concernées que pour les responsables du traitement et les sous-traitants. Ces codes fournissent des orientations détaillées qui adaptent les exigences légales aux secteurs concernés et renforcent la transparence des activités de traitement. Les responsables du traitement et les sous-traitants peuvent également utiliser l'adhésion aux codes comme une preuve tangible de leur respect du droit de l'UE et comme un moyen d'améliorer leur image publique d'organisations qui font de la protection des données une priorité et s'engagent à la respecter dans leurs activités. Des codes de conduite approuvés, assortis d'engagements contraignants et opposables, peuvent servir de garanties appropriées pour le transfert de données vers des pays tiers. Pour garantir que les organisations qui adhèrent aux codes de conduite s'y conforment effectivement, un organisme spécial (agréé par l'autorité de contrôle compétente) peut être désigné pour contrôler et assurer la conformité. Afin de remplir sa mission, cet organisme doit être indépendant, posséder une expertise avérée dans les questions réglementées par le code de conduite et disposer de procédures et de structures transparentes lui permettant de traiter les réclamations relatives aux violations du code[482].

Dans le droit du CdE, la Convention 108 modernisée prévoit que le niveau de protection des données garanti par la législation nationale peut être utilement complété par des mesures de réglementation volontaire, par exemple des codes de bonnes pratiques ou des règles de conduite professionnelle. Il ne s'agit toutefois que de mesures volontaires au titre de la Convention 108 modernisée : on ne saurait en déduire aucune obligation légale d'adopter de telles mesures, bien que ce soit

481 *Ibid.*, art. 40, para. 5.

482 *Ibid.*, art. 41, paras. 1 et 2.

souhaitable et que de telles mesures ne suffisent pas à elles seules à assurer le respect plein et entier de la Convention[483].

4.3.5. Certification

Outre les codes de conduite, des mécanismes de certification et des labels et marques de protection des données sont un autre moyen permettant aux responsables du traitement et aux sous-traitants de démontrer qu'ils respectent le RGPD. À cet effet, le règlement prévoit un système de certification volontaire par lequel certains organismes ou autorités de contrôle peuvent délivrer des certifications. Les responsables du traitement et les sous-traitants qui choisissent d'adhérer à un mécanisme de certification peuvent gagner en visibilité et en crédibilité, étant donné que les certifications, labels et marques permettent aux personnes concernées d'évaluer rapidement le niveau de protection des traitements de données d'une organisation. Il y a lieu de souligner que le fait qu'un responsable du traitement ou un sous-traitant dispose d'une telle certification ne réduit en rien ses obligations et responsabilités à l'égard du respect de toutes les exigences imposées par le règlement.

4.4. Protection des données dès la conception et par défaut

Protection des données dès la conception

Le droit de l'UE exige que les responsables de traitement instaurent des mesures destinées à mettre en œuvre de manière effective les principes relatifs à la protection des données et à intégrer les garanties nécessaires afin de répondre aux exigences du règlement et de protéger les droits des personnes concernées[484]. Ces mesures doivent être mises en œuvre tant au moment du traitement qu'au moment de la détermination des moyens du traitement. Pour mettre en œuvre ces mesures, le responsable du traitement doit tenir compte de l'état des connaissances, des coûts de mise en œuvre, de la nature, de la portée et des finalités du traitement de

483 Rapport explicatif sur la Convention modernisée, para. 33.

484 RGPD, art. 25, para. 1.

données à caractère personnel ainsi que des risques et de leur gravité pour les droits et libertés de la personne concernée[485].

Le droit du CdE requiert que les responsables du traitement et les sous-traitants procèdent, préalablement au commencement de tout traitement, à l'examen de l'impact potentiel du traitement de données à caractère personnel sur les droits et libertés fondamentales des personnes concernées. En outre, les responsables du traitement et les sous-traitants doivent concevoir le traitement de données de manière à prévenir ou à minimiser les risques d'atteinte à ces droits et libertés, et mettre en œuvre des mesures techniques et organisationnelles tenant compte des implications du droit à la protection des données à caractère personnel, à tous les stades du traitement des données[486].

Protection des données par défaut

Le droit de l'UE impose que le responsable du traitement mette en œuvre les mesures appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard des finalités sont traitées. Cette obligation s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité[487]. Une telle mesure vise, par exemple, à garantir que tous les employés du responsable du traitement n'ont pas accès aux données à caractère personnel de la personne concernée. Le CEPD a élaboré d'autres orientations dans son *Guide pour l'évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel*[488].

Le droit du CdE prévoit que les responsables du traitement et les sous-traitants prennent des mesures techniques et organisationnelles tenant compte des implications du droit à la protection des données, et qu'ils mettent en œuvre les mesures techniques et organisationnelles prenant en compte les implications du droit à la

485 Groupe de travail « Article 29 » (2017), *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, WP 248 rev.01, Bruxelles, 4 octobre 2017. Voir aussi ENISA (2015), Privacy and Data Protection by Design - from policy to engineering, 12 janvier 2015.

486 Convention 108 modernisée, art. 10, paras. 2 et 3 ; Rapport explicatif sur la Convention 108 modernisée, para. 89

487 RGPD, art. 25, para. 2.

488 Contrôleur européen de la protection des données (CEPD), (2017), *Guide pour l'évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel*, Bruxelles, 11 avril 2017.

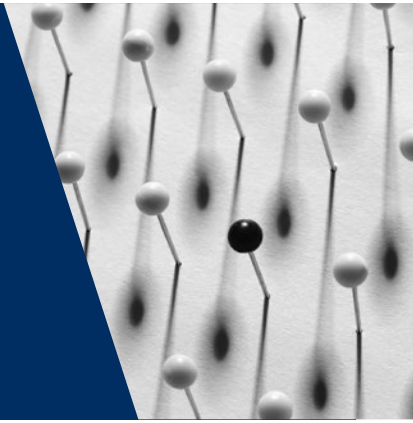
protection des données à caractère personnel à tous les stades du traitement des données[489].

En 2016, l'ENISA a publié un rapport sur les outils et services disponibles en matière de protection de la vie privée[490]. Entre autres considérations, cette évaluation contient une liste de critères et de paramètres servant d'indicateurs de bonnes ou de mauvaises pratiques en matière de respect de la vie privée. Alors que certains critères se rapportent directement aux dispositions du RGPD, comme le recours à la pseudonymisation et à des mécanismes de certification approuvés, d'autres prévoient des initiatives innovantes pour assurer le respect de la vie privée dès la conception et par défaut. Ainsi, le critère d'accessibilité, quoiqu'il ne se rapporte pas directement à la vie privée, peut la renforcer, étant donné qu'il peut permettre l'adoption à plus grande échelle d'un outil ou d'un service de protection de la vie privée. En effet, les outils de protection de la vie privée qui sont difficiles à mettre en œuvre dans la pratique peuvent être très peu adoptés par le public, même s'ils offrent des garanties très solides en termes de respect de la vie privée. En outre, le critère de maturité et de stabilité de l'outil de protection de la vie privée, c'est-à-dire la manière dont un outil évolue dans le temps et répond aux défis existants ou nouveaux en matière de vie privée, revêt une importance capitale. D'autres technologies renforçant la vie privée, par exemple dans le cadre des communications sécurisées, comprennent le chiffrement de bout en bout (communication dans laquelle les seules personnes qui peuvent lire les messages sont les personnes qui communiquent), le chiffrement client-serveur (cryptage du canal de communication entre un client et un serveur), l'authentification (vérification de l'identité des parties qui communiquent) et la communication anonyme (aucun tiers ne peut identifier les parties qui communiquent).

489 Convention 108 modernisée, art. 10, para. 3 ; Rapport explicatif sur la Convention 108 modernisée, para. 89.

490 ENISA, PETs controls matrix: A systematic approach for assessing online and mobile privacy tools, 20 décembre 2016.

5 Contrôle indépendant



UE	Questions traitées	CdE
Charte des droits fondamentaux, art. 8, para. 3 Traité sur le fonctionnement de l'Union européenne, art. 16, para. 2 RGPD, art. 51 à 59 CJUE, C-518/07, *Commission européenne c. République fédérale d'Allemagne* [GC], 2010 CJUE, C-614/10, *Commission européenne c. République d'Autriche* [GC], 2012 CJUE, C-288/12, *Commission européenne c. Hongrie* [GC], 2014 CJUE, C-362/14, *Maximillian Schrems c. Data Protection Commissioner* [GC], 2015	**Autorités de contrôle**	Convention 108 modernisée, art. 15
RGPD, art. 60 à 67	**Coopération entre autorités de contrôle**	Convention 108 modernisée, art. 16 à 21
RGPD, art. 68 à 76	**Comité européen de la protection des données**	

Points clés

- Un contrôle indépendant est un élément essentiel du droit européen de la protection des données et est consacré par l'article 8, paragraphe 3, de la Charte.
- Pour garantir la protection effective des données, il appartient au droit national d'établir des autorités de contrôle indépendantes.
- Les autorités de contrôle doivent agir en toute indépendance, laquelle doit être garantie par le droit fondateur et reflétée dans la structure organisationnelle de l'autorité de contrôle.
- Les autorités de contrôle ont des missions et des pouvoirs spécifiques, parmi lesquels :
  - 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 ;
  - entendre les réclamations et aider les personnes concernées en cas de violations alléguées du droit à la protection des données ;
  - contrôler les responsables du traitement et les sous-traitants.
- Les autorités de contrôle ont également le pouvoir d'intervenir si nécessaire en :
  - avertissant, admonestant, voire en verbalisant les responsables du traitement et les sous-traitants ;
  - ordonnant la correction, le verrouillage ou l'effacement des données ;
  - imposant une interdiction de traitement ou une amende administrative ;
  - soumettant l'affaire aux tribunaux.
- Le traitement de données à caractère personnel faisant souvent intervenir des responsables du traitement, des sous-traitants et des personnes concernées établies dans différents États, les autorités de contrôle sont tenues de coopérer entre elles sur des questions transfrontalières afin d'assurer la protection effective des personnes en Europe.
- Dans l'UE, le Règlement général sur la protection des données instaure un mécanisme à guichet unique pour les affaires de traitement transfrontalier. Certaines entreprises réalisent des activités de traitement transfrontalières parce qu'elles traitent des données à caractère personnel dans le cadre des activités d'établissements situés dans plus d'un État membre ou d'un établissement unique dans l'Union, mais qui affectent de manière significative des personnes concernées de plus d'un État membre. Dans le cadre de ce mécanisme, ces entreprises n'auront affaire qu'à une seule autorité nationale de contrôle de la protection des données.

- Un mécanisme de coopération et de compatibilité permettra de mettre en place une approche coordonnée entre toutes les autorités de contrôle intervenant dans un cas particulier. L'autorité de contrôle chef de file – ou de l'établissement principal ou unique – consultera les autres autorités de contrôle concernées et leur soumettra son projet de décision.
- À l'instar de l'actuel Groupe de travail « Article 29 », l'autorité de contrôle de chaque État membre et le Contrôleur européen de la protection des données (CEPD) seront membres du Comité européen de la protection des données.
- Le Comité européen de la protection des données aura, notamment, pour missions de surveiller la bonne application du règlement, de conseiller la Commission sur des questions pertinentes et de publier des avis, des lignes directrices ou des bonnes pratiques sur différents sujets.
- La différence majeure réside dans le fait que le Comité européen de la protection des données n'émettra pas uniquement des avis, comme c'était le cas sous la Directive 95/46/CE. Il rendra également des décisions contraignantes dans des cas où une autorité de contrôle a soulevé une objection pertinente et motivée concernant des guichets uniques, où les avis divergent sur la question de savoir quelle autorité de contrôle est chef de file et, enfin, où l'autorité de contrôle compétente ne demande pas ou ne suit pas l'avis du Comité. L'objectif est de veiller à l'application uniforme du règlement dans tous les États membres.

Un contrôle indépendant est un élément essentiel du droit européen de la protection des données. Tant le droit de l'UE que celui du CdE considèrent l'existence d'autorités de contrôle indépendantes comme indispensable à la protection effective des droits et libertés des personnes à l'égard du traitement de leurs données à caractère personnel. Le traitement des données étant omniprésent et de plus en plus difficile à comprendre pour les particuliers, ces autorités sont les gardiens de l'ère du numérique. Dans l'UE, l'existence d'autorités de contrôle indépendantes est considérée comme l'un des éléments fondamentaux du droit à la protection des données à caractère personnel, consacré par le droit primaire de l'UE. L'article 8, paragraphe 3, de la Charte des droits fondamentaux de l'Union européenne et l'article 16, paragraphe 2, du TFUE reconnaissent la protection des données à caractère personnel comme un droit fondamental et affirment qu'une autorité indépendante doit contrôler le respect des règles relatives à la protection des données.

L'importance d'un contrôle indépendant de la législation relative à la protection des données a également été reconnue dans la jurisprudence.

Exemple : dans l'affaire *Schrems*[491], la CJUE s'inquiétait de savoir si le transfert de données à caractère personnel vers les États-Unis (US) en vertu du premier accord UE-États-Unis relatif à la sphère de sécurité était conforme au droit de l'UE en matière de protection des données, compte tenu des révélations d'Edward Snowden sur la surveillance de masse mise en place par la National Security Agency (NSA) américaine. Le transfert de données à caractère personnel vers les États-Unis reposait sur une décision de la Commission européenne adoptée en 2000, qui permettait ledit transfert de l'UE vers des organismes américains autocertifiés en vertu du mécanisme de la sphère de sécurité, étant donné que ce mécanisme garantit un niveau adéquat de protection des données à caractère personnel. Sollicitée pour enquêter sur la plainte du requérant concernant la légalité des transferts de données après les révélations de M. Snowden, l'autorité de contrôle irlandaise a rejeté la plainte au motif que l'existence de la décision de la Commission sur l'adéquation du régime américain de protection des données reflétée dans les principes de la sphère de sécurité (la « Décision relative à la sphère de sécurité ») l'empêchait de poursuivre ses investigations.

La CJUE a toutefois conclu que l'existence d'une décision de la Commission autorisant les transferts de données vers des pays tiers qui garantissent un niveau de protection adéquat n'ôte ni ne réduit les pouvoirs des autorités nationales de contrôle. La CJUE a fait valoir que les pouvoirs dont disposent ces autorités pour contrôler et garantir le respect des règles de l'UE en matière de protection des données résultent du droit primaire de l'UE, notamment de l'article 8, paragraphe 3, de la Charte et de l'article 16, paragraphe 2, du TFUE. « L'institution [...] d'autorités de contrôle indépendantes constitue donc [...] un élément essentiel du respect de la protection des personnes à l'égard du traitement des données à caractère personnel »[492].

La CJUE a donc conclu que même lorsque le transfert de données à caractère personnel est soumis à une décision d'adéquation de la Commission, lorsqu'une personne saisit une autorité de contrôle nationale d'une réclamation, celle-ci doit examiner la réclamation avec diligence. L'autorité de contrôle peut rejeter la réclamation si elle la juge non fondée. Dans cette hypothèse, la Cour a souligné que le droit à un recours effectif exige que les personnes soient en mesure de contester cette décision devant

491 CJUE, C-362/14, *Maximillian Schrems c. Data Protection Commissioner* [GC], 6 octobre 2015.

492 *Ibid.*, point 41.

les juridictions nationales, qui peuvent saisir la CJUE d'une procédure de renvoi préjudiciel en appréciation de validité de la décision de la Commission. Lorsque les autorités de contrôle estiment la réclamation fondée, elles doivent pouvoir ester en justice et saisir les juridictions nationales. Celles-ci peuvent saisir la CJUE de l'affaire, étant donné qu'elle est la seule instance compétente pour se prononcer sur la validité de la décision de la Commission relative au niveau de protection adéquat[493].

La Cour a ensuite examiné la validité de la Décision relative à la sphère de sécurité afin de déterminer si le système des transferts était ou non conforme aux règles de l'UE en matière de protection des données. Elle a retenu que l'article 3 de la Décision relative à la sphère de sécurité restreignait les pouvoirs des autorités de contrôle nationales (résultant de la Directive relative à la protection des données) de prendre des mesures pour empêcher les transferts de données en cas de niveau inadéquat de protection des données à caractère personnel aux États-Unis. Eu égard à l'importance d'autorités de contrôle indépendantes pour assurer le respect de la législation relative à la protection des données, la CJUE a conclu qu'en vertu de la Directive relative à la protection des données, lue conjointement avec la Charte, la Commission n'était pas compétente pour restreindre de la sorte les pouvoirs d'autorités de contrôle indépendantes. La limitation des pouvoirs des autorités de contrôle était l'un des motifs ayant conduit la Cour à déclarer nulle la Décision relative à la sphère de sécurité.

Le droit européen fait donc du contrôle indépendant un mécanisme important pour garantir la protection effective des données. Les autorités de contrôle indépendantes sont le premier point de contact des personnes concernées en cas d'atteintes à la vie privée[494]. Des autorités de contrôle doivent être instituées tant en vertu du droit de l'UE que de celui du CdE. Les deux cadres juridiques décrivent les missions et les compétences de ces autorités de manière similaire à ce qui est prévu par le RGPD. En principe, les autorités de contrôle devraient donc fonctionner de la même façon en vertu du droit de l'UE et de celui du CdE[495].

493 *Ibid.*, points 53 à 66.

494 RGPD, art. 13, para. 2, point d).

495 *Ibid.*, art. 51 ; Convention 108 modernisée, art. 15.

5.1. Indépendance

Le droit de l'UE et **celui du CdE** exigent que chaque autorité de contrôle exerce en toute indépendance les missions et les pouvoirs dont elle est investie[496]. L'indépendance de l'autorité de contrôle et de ses membres, ainsi que de son personnel, par rapport aux influences extérieures, qu'elles soient directes ou indirectes, est fondamentale pour garantir son objectivité pleine et entière lorsqu'elle se prononce sur des questions relatives à la protection des données. Non seulement la loi portant création d'un organe de contrôle doit contenir des dispositions qui garantissent son indépendance, mais la structure organisationnelle de l'autorité doit également refléter son indépendance. En 2010, la CJUE a, pour la première fois, examiné le degré d'indépendance requis des autorités de contrôle en matière de protection des données[497]. Les exemples ci-après illustrent la manière dont la CJUE définit l'expression « en toute indépendance ».

Exemple : dans l'affaire *Commission européenne c. République fédérale d'Allemagne*[498], 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, avait manqué à ses obligations découlant de l'article 28, paragraphe 1, de la Directive relative à la protection des données. Selon la Commission, le fait que l'Allemagne avait placé les autorités de contrôle compétentes en matière de traitement des données à caractère personnel sous la tutelle de l'État dans les différents Länder pour assurer la conformité avec la législation relative à la protection des données était contraire à l'exigence d'indépendance.

La Cour a souligné que l'expression « en toute indépendance » devait être interprétée en se fondant sur le libellé même de cette disposition ainsi que sur les objectifs et l'économie de la législation de l'UE relative à la protection des données[499]. La Cour a souligné que les autorités de contrôle étaient « les gardiennes » des droits liés au traitement de données à caractère personnel.

496 RGPD, art. 52, para. 1 ; Convention 108 modernisée, art. 15, para. 5.

497 FRA (2010), *Droits fondamentaux : défis et réalisations en 2010*, Rapport annuel 2010, p. 59 ; FRA (2010), *La protection des données à caractère personnel dans l'Union européenne : le rôle des autorités nationales chargées de la protection des données*, mai 2010.

498 CJUE, C-518/07, *Commission européenne c. République fédérale d'Allemagne* [GC], 9 mars 2010, point 27.

499 *Ibid.*, points 17 et 29.

Par conséquent, leur institution dans les États membres est considérée comme « un élément essentiel de la protection des personnes à l'égard du traitement des données à caractère personnel »[500]. 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 »[501].

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 de l'UE. Dans ce règlement, la notion d'indépendance impose que le CEPD ne sollicite ni n'accepte d'instructions de quiconque.

Par conséquent, la CJUE a considéré que les autorités de contrôle allemandes n'étaient pas totalement indépendantes au sens de la législation de l'UE en matière de protection des données en raison de la tutelle des autorités de l'État.

Exemple : dans l'affaire *Commission européenne c. République d'Autriche*[502], la CJUE a mis en évidence des problèmes similaires concernant l'indépendance de certains membres et du personnel de l'autorité autrichienne de protection des données (commission de protection des données, « DSK »). La Cour a conclu que le fait que le personnel de l'autorité de contrôle était fourni par la Chancellerie fédérale mettait à mal l'exigence d'indépendance énoncée dans la législation de l'UE relative à la protection des données. La CJUE a conclu que l'obligation d'informer à tout moment la Chancellerie de son travail empêchait l'autorité de contrôle d'exercer ses fonctions en toute indépendance.

Exemple : dans l'affaire *Commission européenne c. Hongrie*[503], des pratiques nationales similaires touchant l'indépendance du personnel ont été interdites. La CJUE a souligné que « l'exigence [...] selon laquelle il convient de garantir

500 *Ibid.*, point 23.

501 *Ibid.*, point 25.

502 CJUE, C-614/10, *Commission européenne c. République d'Autriche* [GC], 16 octobre 2012, points 59 et 63.

503 CJUE, C-288/12, *Commission européenne c. Hongrie* [GC], 8 avril 2014, points 50 et 67.

> 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 ». La Cour a également considéré qu'« 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 [...] ».

La notion et les critères couverts par l'expression « en toute indépendance » sont désormais clairement définis dans le RGPD, qui intègre les principes établis par les arrêts précités de la CJUE. Conformément au règlement, l'exercice des missions et des pouvoirs en toute indépendance implique que[504] :

- les membres de chaque autorité de contrôle doivent être libres de toute influence extérieure, qu'elle soit directe ou indirecte, et ne doivent pas accepter d'instructions de quiconque ;
- les membres de chaque autorité de contrôle doivent s'abstenir de tout acte incompatible avec leurs obligations afin d'éviter tout conflit d'intérêts ;
- les États membres doivent fournir à chaque autorité de contrôle les ressources humaines, techniques et financières ainsi que l'infrastructure nécessaires à l'exercice effectif de ses missions ;
- les États membres doivent veiller à ce que chaque autorité de contrôle choisisse ses propres agents ;
- le contrôle financier auquel est soumise chaque autorité de contrôle conformément au droit national ne doit pas menacer son indépendance. Les autorités de contrôle doivent disposer d'un budget annuel public propre, leur permettant de fonctionner correctement.

L'indépendance des autorités de contrôle est également considérée comme une exigence essentielle par le droit du CdE. La Convention 108 modernisée exige des autorités de contrôle qu'elles « agissent avec indépendance et impartialité dans l'accomplissement de leurs fonctions et l'exercice de leurs pouvoirs », sans solliciter

504 RGPD, art. 69.

ni accepter d'instructions[505]. Ce faisant, la Convention reconnaît que ces autorités ne peuvent protéger efficacement les droits et libertés individuels à l'égard du traitement des données que si elles exercent leurs fonctions en toute indépendance. Le rapport explicatif sur la Convention 108 modernisée énumère une série d'éléments qui contribuent à assurer cette indépendance. Il s'agit notamment de la possibilité donnée aux autorités de contrôle de recruter leurs propres agents et d'adopter des décisions sans être soumis à une influence extérieure ainsi que de facteurs liés à la durée d'exercice et aux conditions de cessation de leurs fonctions[506].

5.2. Compétence et pouvoirs

Dans le droit de l'UE, le RGPD décrit les compétences et la structure organisationnelle des autorités de contrôle et exige qu'elles soient compétentes et disposent du pouvoir d'exercer les missions dont elles sont investies conformément au règlement.

L'autorité de contrôle est le principal organe du droit national qui veille au respect de la législation de l'UE en matière de protection des données. Outre la surveillance, les autorités de contrôle sont investies d'un large éventail de missions et de pouvoirs, incluant des activités de contrôle proactives et préventives. Outre ces missions, les autorités de contrôle doivent disposer des pouvoirs d'enquête, d'adoption de mesures correctrices et des pouvoirs consultatifs appropriés énumérés à l'article 48 du RGPD, afin de[507] :

- conseiller les responsables du traitement et les personnes concernées sur toutes les questions relatives à la protection des données ;
- autoriser les clauses contractuelles types, les règles d'entreprise contraignantes ou les arrangements administratifs ;
- mener des enquêtes sur des traitements et intervenir en conséquence ;
- demander la présentation de toute information pertinente pour le contrôle des activités du responsable du traitement ;

505 Convention 108 modernisée, art. 15, para. 5.

506 Rapport explicatif sur la Convention 108 modernisée.

507 RGPD, art. 58. Voir également Convention 108, Protocole additionnel, article premier.

- avertir ou rappeler à l'ordre les responsables du traitement et leur ordonner de communiquer à la personne concernée une violation de données à caractère personnel ;
- ordonner la rectification, le verrouillage, l'effacement ou la destruction de données ;
- interdire temporairement ou définitivement un traitement ou imposer une amende administrative ;
- ester en justice.

Pour exercer ses fonctions, l'autorité de contrôle doit avoir accès à toutes les données et informations personnelles nécessaires à son enquête ainsi qu'aux locaux dans lesquels le responsable du traitement conserve les informations pertinentes. Selon la CJUE, les pouvoirs de l'autorité de contrôle doivent être interprétés largement afin de donner plein effet à la protection des données des personnes concernées dans l'UE.

> Exemple : dans l'affaire *Schrems*, la CJUE s'inquiétait de savoir si le transfert de données à caractère personnel vers les États-Unis en vertu du premier accord UE-États-Unis relatif à la sphère de sécurité était conforme au droit de l'UE en matière de protection des données, compte tenu des révélations d'Edward Snowden. Dans son raisonnement, la Cour a retenu que les autorités de contrôle nationales, agissant en leur qualité de contrôleurs indépendants des traitements de données effectués par les ressortissants, peuvent empêcher le transfert de données à caractère personnel vers un pays tiers en dépit de l'existence d'une décision d'adéquation s'il existe une preuve raisonnable que le niveau adéquat de protection n'est plus garanti dans le pays tiers[508].

Chaque autorité de contrôle est compétente pour exercer des pouvoirs d'enquête et d'intervention sur son territoire. Cependant, étant donné que les activités des responsables du traitement et des sous-traitants sont souvent transfrontalières et que le traitement de données touche des personnes concernées établies dans de

508 CJUE, C-362/14, *Maximillian Schrems c. Data Protection Commissioner* [GC], 6 octobre 2015, points 26 à 36, 40 et 41.

nombreux États membres, la question de la répartition des compétences entre les différentes autorités de contrôle se pose. La CJUE a eu l'occasion de se pencher sur cette question dans l'affaire *Weltimmo*.

Exemple : dans l'affaire *Weltimmo*[509], la CJUE s'est interrogée sur la compétence des autorités nationales de contrôle concernant des questions relatives à des entreprises établies en dehors de leur juridiction. Weltimmo était une société enregistrée en Slovaquie, qui exploitait un site internet d'annonces immobilières concernant des biens situés en Hongrie. Les annonceurs ont déposé une plainte auprès de l'autorité de contrôle hongroise chargée de la protection des données pour une infraction à la législation hongroise en la matière et cette autorité a infligé une amende à Weltimmo. La société a contesté l'amende devant les juridictions nationales et la CJUE a été saisie de la question de savoir si la Directive de l'UE relative à la protection des données autorisait les autorités de contrôle d'un État membre à appliquer son droit national en matière de protection des données à une société enregistrée dans un autre État membre.

La CJUE a interprété l'article 4, paragraphe 1, point a), de la Directive relative à la protection des données en ce sens qu'il permet l'application de la législation relative à la protection des données à caractère personnel d'un État membre autre que celui dans lequel le responsable du traitement de ces données est enregistré, « pour autant que celui-ci exerce, au moyen d'une installation stable sur le territoire de cet État membre, une activité effective et réelle, même minime, dans le cadre de laquelle ce traitement est effectué ». La Cour a observé que, sur la base des informations dont elle disposait, Weltimmo menait une activité effective et réelle en Hongrie, puisqu'elle avait un représentant en Hongrie figurant dans le registre slovaque des sociétés avec une adresse en Hongrie, ainsi qu'un compte bancaire et une boîte aux lettres en Hongrie et qu'elle exerçait également des activités en langue hongroise dans ce pays. Ces informations indiquaient l'existence d'un établissement et soumettaient l'activité de Weltimmo à la législation hongroise en matière de protection des données et à la compétence de l'autorité de contrôle hongroise. La Cour a toutefois laissé à la juridiction nationale le soin de vérifier les informations et de décider si Weltimmo avait effectivement un établissement en Hongrie.

509 CJUE, C-230/14, *Weltimmo s. r. o. c. Nemzeti Adatvédelmi és Információszabadság Hatóság*, 1er octobre 2015.

Dans l'hypothèse où la juridiction de renvoi considérait que Weltimmo disposait d'un établissement en Hongrie, l'autorité de contrôle hongroise serait compétente pour infliger une amende. Néanmoins, si la juridiction nationale considérait le contraire, à savoir que Weltimmo ne disposait pas d'un établissement en Hongrie, le droit applicable serait alors celui de l'État membre ou des États membres dans lequel la société était enregistrée. Dans ce cas, les pouvoirs des autorités de contrôle devant être exercés dans le respect de la souveraineté territoriale des autres États membres, l'autorité hongroise ne serait pas en mesure d'infliger une amende. Étant donné que la Directive relative à la protection des données incluait une obligation de coopération entre les autorités de contrôle, l'autorité hongroise pourrait toutefois demander à son homologue slovaque d'examiner la question, de constater l'existence d'une infraction au droit slovaque et d'imposer les sanctions prévues par la législation slovaque.

Grâce à l'adoption du RGPD, des règles détaillées sont désormais établies concernant la compétence des autorités de contrôle dans les affaires transfrontalières. Le règlement instaure un « mécanisme de guichet unique » et contient des dispositions qui imposent aux autorités de contrôle de coopérer entre elles. Afin de garantir une coopération efficace dans les affaires transfrontalières, le RGPD impose que soit établie une autorité de contrôle chef de file en tant qu'autorité de contrôle de l'établissement principal ou de l'établissement unique du responsable du traitement ou du sous-traitant[510]. L'autorité de contrôle chef de file est chargée des affaires transfrontalières, est le seul interlocuteur du responsable du traitement ou du sous-traitant et coordonne la coopération avec les autres autorités de contrôle afin de parvenir à un consensus. La coopération couvre l'échange d'informations, l'assistance mutuelle en matière de contrôle et d'enquête et l'adoption de décisions contraignantes[511].

Dans le droit du CdE, les compétences et les pouvoirs des autorités de contrôle sont énoncés à l'article 15 de la Convention 108 modernisée. Ces pouvoirs correspondent à ceux dont sont investies les autorités de contrôle dans le droit de l'UE, notamment les pouvoirs d'enquête et d'intervention, les pouvoirs de rendre des décisions et d'infliger des sanctions administratives en cas de violations des dispositions de la Convention et le pouvoir d'ester en justice. Les autorités de contrôle indépendantes sont également compétentes pour traiter les demandes et les plaintes dont elles sont saisies par les personnes concernées, sensibiliser le public à la législation en

510 RGPD, art. 56, para. 1.

511 *Ibid.*, art. 60.

matière de protection des données et conseiller les responsables nationaux sur toute proposition législative ou administrative impliquant des traitements de données à caractère personnel.

5.3. Coopération

Le RGPD établit un cadre général de coopération entre les autorités de contrôle et prévoit des règles plus spécifiques en matière de coopération des autorités de contrôle dans le cas de traitements transfrontaliers de données.

En application du RGPD, les autorités de contrôle se prêtent mutuellement assistance et partagent les informations pertinentes en vue de mettre en œuvre et d'appliquer le règlement de façon cohérente[512]. Ceci inclut l'autorité de contrôle à laquelle il est demandé de mener des consultations, des inspections et des enquêtes. Les autorités de contrôle peuvent mener des opérations conjointes, y compris en effectuant des enquêtes conjointes et en prenant des mesures répressives conjointes, auxquelles participent des agents de toutes les autorités de contrôle[513].

Dans l'UE, les responsables du traitement et les sous-traitants opèrent de plus en plus à une échelle transnationale. Cette situation requiert une coopération étroite entre les autorités de contrôle compétentes des États membres afin de garantir que le traitement des données à caractère personnel est conforme aux exigences du RGPD. En vertu du mécanisme de « guichet unique » instauré par le règlement, si un responsable du traitement ou un sous-traitant dispose d'établissements dans plusieurs États membres ou s'il possède un établissement unique mais que les traitements affectent grandement les personnes concernées de plus d'un État membre, l'autorité de contrôle de l'établissement principal (ou unique) est l'autorité chef de file des activités transfrontalières du responsable du traitement ou du sous-traitant. L'autorité chef de file est compétente pour prendre des mesures répressives à l'encontre du responsable du traitement ou du sous-traitant. Le mécanisme du guichet unique vise à renforcer l'harmonisation et à améliorer l'application uniforme de la législation de l'UE en matière de protection des données dans les différents États membres. Il est également bénéfique pour les entreprises, étant donné qu'elles ne doivent traiter qu'avec l'autorité chef de file et non avec plusieurs autorités de contrôle. Ce mécanisme accroît la sécurité juridique pour les entreprises et, dans la pratique, il devrait également permettre de prendre des décisions plus rapidement

512 *Ibid.*, art. 61, paras. 1 à 3, et art. 62, para. 1.

513 *Ibid.*, art. 62, para. 1.

et d'éviter que les entreprises ne soient confrontées à différentes autorités de contrôle leur imposant des obligations contradictoires.

L'identification de l'autorité chef de file implique la localisation de l'établissement principal d'une entreprise dans l'UE. Le RGPD définit l'expression « établissement principal ». En outre, le Groupe de travail « Article 29 » a publié des lignes directrices concernant la désignation de l'autorité de contrôle chef de file d'un responsable du traitement ou sous-traitant, qui contiennent les critères à appliquer pour identifier l'établissement principal.[514]

Afin de garantir un niveau élevé de protection des données dans l'UE, l'autorité de contrôle chef de file n'agit pas seule. Elle doit coopérer avec les autres autorités de contrôle concernées pour adopter des décisions sur des traitements de données à caractère personnel effectués par des responsables du traitement et des sous-traitants en s'efforçant de parvenir à un consensus et d'assurer la cohérence. La coopération entre les autorités de contrôle concernées inclut l'échange d'informations, l'assistance mutuelle, la réalisation d'enquêtes conjointes et des activités de contrôle[515]. Lorsqu'elles se prêtent mutuellement assistance, les autorités de contrôle doivent traiter adéquatement les demandes d'informations émanant des autres autorités de contrôle et prendre des mesures de contrôle, telles que les demandes d'autorisation et de consultation préalables du responsable du traitement sur ses activités de traitement, les inspections ou les enquêtes. Une assistance mutuelle aux autorités de contrôle d'autres États membres doit être apportée sur demande, dans les meilleurs délais et au plus tard un mois après réception de la demande[516].

Lorsque le responsable du traitement possède des établissements dans plusieurs États membres, les autorités de contrôle peuvent mener des opérations conjointes, y compris en effectuant des enquêtes et en prenant des mesures répressives, auxquelles participent des membres du personnel des autorités de contrôle d'autres États membres[517].

La coopération entre les autorités de contrôle est une exigence importante dans le droit du CdE également. La Convention 108 modernisée dispose que les autorités de

514 Groupe de travail « Article 29 » (2016), *Lignes directrices concernant la désignation d'une autorité de contrôle chef de file d'un responsable du traitement ou d'un sous-traitant*, WP 244, Bruxelles, 13 décembre 2016, version révisée et adoptée le 5 avril 2017.

515 RGPD, art. 60, paras. 1 à 3.

516 *Ibid.*, art. 61, paras. 1 et 2.

517 *Ibid.*, art. 62, para. 1.

contrôle doivent coopérer entre elles dans la mesure nécessaire à l'accomplissement de leurs fonctions[518]. Cette coopération peut, par exemple, prendre la forme d'un échange de toute information utile et pertinente, en coordonnant leurs investigations ou en menant des actions conjointes[519].

5.4. Le Comité européen de la protection des données

L'importance des autorités de contrôle indépendantes et les principales compétences dont elles sont investies par le droit européen de la protection des données ont été décrites précédemment dans ce chapitre. Le Comité européen de la protection des données est un autre acteur important chargé de veiller à l'application effective et cohérente des règles relatives à la protection des données dans l'UE.

Le RGPD a institué le Comité européen de la protection des données en tant qu'organe de l'UE doté de la personnalité juridique[520]. Il succède au Groupe de travail « Article 29 »[521], institué par la Directive relative à la protection des données pour conseiller la Commission sur toute mesure de l'UE menaçant les droits des personnes physiques à l'égard du traitement des données à caractère personnel et le respect de la vie privée, de promouvoir l'application uniforme de la directive et de donner un avis d'expert à la Commission sur des questions liées à la protection des données. Le Groupe de travail « Article 29 » était composé de représentants des autorités de contrôle des États membres de l'UE, ainsi que de la Commission et du CEPD.

Tout comme le Groupe de travail, le Comité européen de la protection des données se compose des chefs des autorités de contrôle de chaque État membre et du CEPD, ou de leurs représentants respectifs[522]. Le CEPD jouit de droits de vote égaux, à l'exception des cas relatifs au règlement d'un litige, où il ne peut voter qu'à l'égard

518 Convention 108 modernisée, art. 16 et 17.

519 *Ibid.*, art. 12 bis, para. 7.

520 RGPD, art. 68.

521 Aux termes de la Directive 95/46/CE, le Groupe de travail « Article 29 » avait pour mission de conseiller la Commission sur toute mesure de l'UE menaçant les droits des personnes physiques à l'égard du traitement des données à caractère personnel et le respect de la vie privée, de promouvoir l'application uniforme de la directive et de donner un avis d'expert à la Commission sur des questions liées à la protection des données. Le Groupe de travail « Article 29 » était composé de représentants des autorités de contrôle des États membres de l'UE, ainsi que de la Commission et du CEPD.

522 RGPD, art. 68, para. 3.

des décisions concernant des principes et règles applicables aux institutions de l'UE qui correspondent, en substance, à ceux énoncés dans le RGPD. La Commission a le droit de participer aux activités et réunions du Comité, mais sans droit de vote[523]. Le Comité élit son président (qui le représente) et deux vice-présidents en son sein à la majorité simple, pour un mandat de cinq ans. Par ailleurs, le Comité dispose également d'un secrétariat, qui est assuré par le CEPD, de sorte que le Comité bénéficie d'un soutien analytique, administratif et logistique[524].

Les missions du Comité européen de la protection des données sont décrites aux articles 64, 65 et 70 du RGPD et comprennent des obligations exhaustives qui peuvent être réparties en trois activités principales :

- **Cohérence :** le Comité peut adopter des décisions contraignantes dans trois cas : lorsqu'une autorité de contrôle a soulevé une objection pertinente et motivée concernant des guichets uniques, lorsqu'il existe des avis divergents quant à l'autorité de contrôle qui est chef de file et, enfin, lorsque l'autorité de contrôle compétente ne demande pas ou ne suit pas l'avis du Comité[525]. La responsabilité première du Comité est de veiller à ce que le RGPD soit appliqué de façon cohérente dans l'UE et il joue un rôle essentiel dans le mécanisme de cohérence, tel qu'il est décrit à la section 5.5.

- **Consultation :** les missions du Comité incluent de conseiller la Commission sur toute question relative à la protection des données à caractère personnel dans l'Union, telle que des modifications du RGPD, des révisions de la législation de l'UE impliquant des traitements de données et susceptibles d'être contraires aux règles de l'UE en matière de protection des données ou l'adoption de décisions d'adéquation de la Commission qui autorisent le transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale.

- **Lignes directrices :** le Comité publie également des lignes directrices, recommandations et bonnes pratiques afin d'encourager l'application cohérente du règlement et de promouvoir la coopération et les échanges d'information entre autorités de contrôle. Il doit en outre encourager les associations de responsables du traitement ou de sous-traitants à rédiger des codes de conduite et

523 *Ibid.*, art. 68, paras. 4 et 5.

524 *Ibid.*, art. 73 et 75.

525 *Ibid.*, art. 65.

à mettre en place des labels et des mécanismes de certification de la protection des données.

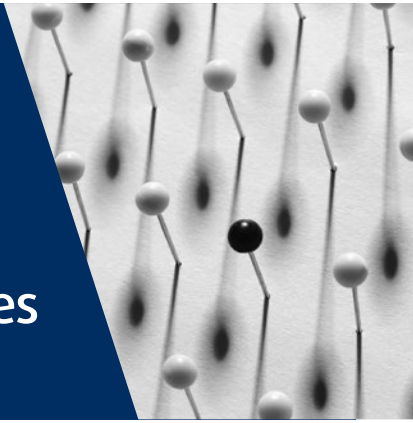
Les décisions du Comité européen de la protection des données peuvent être contestées devant la CJUE.

5.5. Le mécanisme de cohérence établi par le RGPD

Le RGPD instaure un mécanisme de cohérence, par lequel les autorités de contrôle coopèrent entre elles et, le cas échéant, avec la Commission, pour faire en sorte que le règlement soit appliqué de façon cohérente dans tous les États membres. Ce mécanisme de cohérence est utilisé dans deux cas de figure. Le premier concerne les avis rendus par le Comité lorsqu'une autorité de contrôle compétente entend adopter des mesures, comme une liste de traitements requérant une analyse d'impact relative à la protection des données (AIPD), ou établir des clauses contractuelles types. Le second concerne des décisions contraignantes du Comité destinées aux autorités de contrôle dans le cas d'affaires liées au guichet unique et lorsqu'une autorité de contrôle ne suit pas ou ne sollicite pas un avis du Comité.

6

Les droits des personnes concernées et leur application



UE	Questions traitées	CdE
Droit d'être informé		
RGPD, art. 12 CJUE, C-473/12, *Institut professionnel des agents immobiliers (IPI) c. Englebert*, 2013 CJUE, C-201/14, *Smaranda Bara et autres c. Casa Națională de Asigurări de Sănătate et autres*, 2015	**Transparence des informations**	Convention 108 modernisée, art. 8
RGPD, art. 13, paras. 1 et 2, et art. 14, paras. 1 et 2	**Contenu des informations**	Convention 108 modernisée, art. 8, para. 1
RGPD, art. 13, para. 1, et art. 14, para. 3	**Moment de la communication des informations**	Convention 108 modernisée, art. 9, para. 1, point b)
RGPD, art. 12, paras. 1, 5 et 7	**Moyens de communication des informations**	Convention 108 modernisée, art. 9, para. 1, point b)
RGPD, art. 13, para. 2, point d), et art. 14, para. 2, point e), articles 77, 78 et 79	**Droit d'introduire une réclamation**	Convention 108 modernisée, art. 9, para. 1, point f)
Droit d'accès		
RGPD, art. 15, para. 1 CJUE, C-553/07, *College van burgemeester en wethouders van Rotterdam c. M. E. E. Rijkeboer*, 2009	**Droit d'accès à ses propres données**	Convention 108 modernisée, art. 9, para. 1, point b) CouEDH, *Leander c. Suède*, nº 9248/81, 1987

UE	Questions traitées	CdE
CJUE, affaires jointes C-141/12 et C-372/12, *YS c. Minister voor Immigratie, Integratie en Asiel* et *Minister voor Immigratie, Integratie en Asiel c. M et S*, 2014 CJUE, C-434/16, *Peter Nowak c. Data Protection Commissioner*, 2017		
Droit de rectification		
RGPD, art. 16	Rectification des données à caractère personnel inexactes	Convention 108 modernisée, art. 9, para. 1, point e) CouEDH, *Cemalettin Canlı c. Turquie*, nº 22427/04, 2008 CouEDH, *Ciubotaru c. Moldova*, nº 27138/04, 2010
Droit d'effacement		
RGPD, art. 17, para. 1	Effacement de données à caractère personnel	Convention 108 modernisée, art. 9, para. 1, point e) CouEDH, *Segerstedt-Wiberg et autres c. Suède*, nº 62332/00, 2006
CJUE, C-131/12, *Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 2014 CJUE, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce c. Salvatore Manni*, 2017	Droit à l'oubli	
Droit à la limitation du traitement		
RGPD, art. 18, para. 1	Droit de limiter l'utilisation de données à caractère personnel	
RGPD, art. 19	Obligation de notification	
Droit à la portabilité des données		
RGPD, art. 20	Droit à la portabilité des données	

UE	Questions traitées	CdE
Droit d'opposition		
RGPD, art. 21, para. 1 CJUE, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce c. Salvatore Manni*, 2017	**Droit d'opposition pour des motifs tenant à la situation particulière de la personne concernée**	Recommandation sur le profilage, art. 5, para. 3 Convention 108 modernisée, art. 9, para. 1, point d)
RGPD, art. 21, para. 2	**Droit d'opposition à l'utilisation de données à des fins de prospection**	Recommandation sur le marketing direct, art. 4, para. 1
RGPD, art. 21, para. 5	**Droit d'opposition à l'aide de procédés automatisés**	
Droits relatifs à la prise de décisions automatisées et au profilage		
RGPD, art. 22	**Droits relatifs à la prise de décisions automatisée et au profilage**	Convention 108 modernisée, art. 9, para. 1, point a)
RGPD, art. 21	**Droits d'opposition à des décisions automatisées**	
RGPD, art. 13, para. 2, point f)	**Droits à une explication utile**	Convention 108 modernisée, art. 9, para. 1, point c)
Voies de recours, responsabilité, sanctions et réparation		
Charte des droits fondamentaux, art. 47 CJUE, C-362/14, *Maximillian Schrems c. Data Protection Commissioner* [GC], 2015 RGPD, articles 77 à 84	**Pour les infractions au droit national en matière de protection des données**	CEDH, art. 13 (uniquement pour les États membres du CdE) Convention 108 modernisée, art. 9, para. 1, point f), articles 12, 15, 16 à 21 CouEDH, *K.U. c. Finlande*, nº 2872/02, 2008 CouEDH, *Biriuk c. Lituanie*, nº 23373/03, 2008
Règlement relatif à la protection des données des institutions de l'UE, articles 34 et 49 CJUE, C-28/08 P, *Commission européenne c. The Bavarian Lager Co. Ltd* [GC], 2010	**Pour les infractions au droit de l'UE par des institutions et organes de l'UE**	

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. À l'ère du numérique, le traitement des données est devenu omniprésent et les particuliers ont de plus en plus de mal à le comprendre. Afin de réduire les déséquilibres de pouvoir entre les personnes concernées et les responsables du traitement, les particuliers disposent de certains droits pour exercer un plus grand contrôle sur le traitement des informations personnelles les concernant. Le droit d'accès à ses propres données et le droit de les faire rectifier sont consacrés par l'article 8, paragraphe 2, de la Charte des droits fondamentaux de l'Union européenne, un document qui relève du droit primaire de l'UE et occupe une place fondamentale dans l'ordre juridique de celle-ci. Le droit dérivé de l'UE, en particulier le Règlement général sur la protection des données, établit un cadre juridique cohérent qui renforce la position des personnes concernées en leur conférant des droits vis-à-vis des responsables de traitement. Outre les droits d'accès et de rectification, le RGPD reconnaît une série d'autres droits comme le droit à l'effacement (« droit à l'oubli »), le droit d'opposition ou de limitation du traitement des données et des droits liés à la prise de décisions automatisée et au profilage. Des garanties similaires permettant aux personnes concernées d'exercer un contrôle effectif sur leurs données sont également mentionnées dans la Convention 108 modernisée. Son article 9 énumère les droits que les personnes devraient pouvoir exercer à l'égard du traitement de leurs données personnelles. Les Parties contractantes doivent veiller à ce que chaque personne concernée relevant de leur juridiction dispose de ces droits et à ce qu'ils soient assortis de moyens légaux et pratiques effectifs permettant aux personnes concernées de les exercer.

En plus de doter les personnes concernées de droits, il est tout aussi important de mettre en place des mécanismes leur permettant de contester les atteintes à leurs droits, d'en faire porter la responsabilité aux responsables du traitement et de réclamer une compensation. Le droit à un recours effectif, tel qu'il est garanti par la CEDH et la Charte, impose que des recours juridictionnels soient ouverts à chacun.

6.1. Les droits des personnes concernées

Points clés

- Toute personne concernée a le droit d'obtenir du responsable du traitement des informations sur le traitement de ses données à caractère personnel, à quelques exceptions près.

- Les personnes concernées ont le droit :
  - d'avoir accès à leurs propres données et d'obtenir certaines informations sur le traitement ;
  - de faire rectifier leurs données par le responsable du traitement si elles sont inexactes ;
  - de faire effacer leurs données, le cas échéant, par le responsable du traitement si celui-ci les traite de manière illicite ;
  - de limiter temporairement le traitement ;
  - de faire transférer leurs données à un autre responsable du traitement sous certaines conditions.
- En outre, les personnes concernées ont le droit de s'opposer :
  - au traitement en raison de leur situation particulière ;
  - à l'utilisation de leurs données à des fins de prospection.
- Les personnes concernées ont le droit de ne pas faire l'objet de décisions basées uniquement sur un traitement automatisé, y compris un profilage, qui produisent des effets juridiques ou qui les affectent de manière significative. Les personnes concernées ont également le droit :
  - d'obtenir une intervention humaine du responsable du traitement ;
  - d'exprimer leur point de vue et de contester une décision prise sur la base d'un traitement automatisé.

6.1.1. Droit d'être informé

Selon le **droit du CdE** et **le droit de l'UE**, les responsables du traitement sont tenus d'informer la personne concernée, lors de la collecte de ses données à caractère personnel, sur le traitement envisagé. Cette obligation n'est pas subordonnée à une demande de la personne concernée, mais le responsable du traitement doit, de façon proactive, se conformer à cette obligation, que la personne concernée manifeste ou non un intérêt pour ces informations.

Dans le droit du CdE, l'article 8 de la Convention 108 modernisée dispose que les parties contractantes doivent prévoir que les responsables du traitement informent les personnes concernées de leur identité et de leur résidence habituelle, de la base juridique et des finalités du traitement, des catégories des données à caractère personnel traitées, des destinataires des données à caractère personnel, le cas échéant,

et des moyens d'exercer les droits énoncés à l'article 9, qui incluent les droits d'accès et de rectification et le recours judiciaire. Il convient également de communiquer aux personnes concernées toute autre information supplémentaire jugée nécessaire pour garantir un traitement loyal et transparent des données à caractère personnel. Le rapport explicatif sur la Convention 108 modernisée précise que les informations fournies aux personnes concernées « doivent être facilement accessibles, lisibles, compréhensibles et adaptées aux personnes concernées »[526].

Dans le droit de l'UE, le principe de transparence exige que tout traitement de données à caractère personnel soit transparent à l'égard des personnes physiques concernées. Celles-ci ont le droit de savoir quelles données à caractère personnel sont collectées, utilisées ou traitées d'une autre manière et comment elles le sont et elles doivent être informées des risques, garanties et droits liés au traitement[527]. L'article 12 du RGPD impose donc aux responsables du traitement une vaste obligation complète de fournir des informations transparentes et/ou d'indiquer comment les personnes concernées peuvent exercer leurs droits[528]. Les informations doivent être concises, transparentes, compréhensibles et aisément accessibles et rédigées en des termes clairs et simples. Elles doivent être fournies par écrit, y compris, lorsque c'est approprié, par voie électronique, et elles peuvent même être fournies oralement lorsque la personne concernée en fait la demande, à condition que son identité soit démontrée sans doute possible. Les informations sont communiquées sans délai ou frais excessifs[529].

Les articles 13 et 14 du RGPD traitent du droit des personnes concernées à être informées soit lorsque des données à caractère personnel ont été collectées directement auprès d'elles, soit lorsque les données n'ont pas été collectées auprès d'elles, respectivement.

La portée du droit à l'information et ses limitations dans le droit de l'UE ont été précisées dans la jurisprudence de la CJUE.

526 Rapport explicatif sur la Convention 108 modernisée, para. 68.

527 RGPD, considérant 39.

528 *Ibid.*, art. 13 et 14 ; Convention 108 modernisée, art. 8, para. 1, point b).

529 RGPD, art. 12, para. 5 ; Convention 108 modernisée, art. 9, para. 1, point b).

Exemple : dans l'affaire *Institut professionnel des agents immobiliers (IPI) c. Englebert*[530], la CJUE a été amenée à interpréter l'article 13, paragraphe 1, de la Directive 95/46. Cet article permettait aux États membres de choisir d'adopter ou non des mesures législatives visant à limiter la portée du droit de la personne concernée à être informée lorsqu'une telle limitation constituait une mesure nécessaire à la sauvegarde, notamment, des droits et libertés d'autrui et à la prévention et à la détection d'infractions pénales ou de manquements à la déontologie dans le cas des professions réglementées. L'IPI est un organe professionnel regroupant des agents immobiliers en Belgique et il est chargé de veiller au respect des bonnes pratiques dans la profession. L'IPI a demandé à une juridiction nationale de constater que les défendeurs avaient enfreint des règles professionnelles et d'ordonner qu'ils cessent diverses activités immobilières. Il a fondé son action sur des éléments probants recueillis par des détectives privés auxquels il a eu recours.

La juridiction nationale s'interrogeait sur la valeur à attribuer aux preuves fournies par les détectives, compte tenu de la possibilité qu'elles aient été obtenues sans respecter les exigences en matière de protection des données de la législation belge, en particulier l'obligation d'informer préalablement la personne concernée du traitement de ses données avant la collecte des informations. La CJUE a relevé que l'article 13, paragraphe 1, indiquait que les États membres « peuvent », mais ne sont pas tenus, de prévoir dans leur droit national des exceptions à l'obligation d'informer les personnes concernées du traitement de leurs données. Dès lors que l'article 13, paragraphe 1, couvrait la prévention, la recherche, la détection et la poursuite d'infractions pénales ou de manquements à la déontologie comme motifs susceptibles de fonder une limitation des droits des personnes, l'activité d'un organe comme l'IPI et les détectives privés agissant en son nom pouvaient se prévaloir de cette disposition. Toutefois, si un État membre n'a pas prévu une telle exception, la personne concernée doit être informée du traitement.

Exemple : dans l'affaire *Smaranda Bara et autres c. Casa Națională de Asigurări de Sănătate et autres*[531], la CJUE a précisé que le droit de l'UE interdit à une administration publique nationale de transmettre des données

530 CJUE, C-473/12, *Institut professionnel des agents immobiliers (IPI) c. Geoffrey Englebert et autres*, 7 novembre 2013.

531 CJUE, C-201/14, *Smaranda Bara et autres c. Casa Națională de Asigurări de Sănătate et autres*, 1er octobre 2015.

à caractère personnel à une autre administration publique en vue d'un traitement ultérieur sans que les personnes concernées soient informées de cette transmission et du traitement. Dans cette affaire, l'administration nationale n'avait pas informé les requérantes que leurs données avaient été transmises à la caisse nationale d'assurance maladie avant leur transfert.

La CJUE a estimé que l'exigence qu'impose le droit de l'Union d'informer les personnes concernées du traitement de leurs données personnelles est « d'autant plus importante qu'elle est une condition nécessaire à l'exercice par ces personnes de leur droit d'accès et de rectification des données traitées [...] et de leur droit d'opposition au traitement desdites données ». L'exigence de traitement loyal oblige une administration publique à informer les personnes concernées de la transmission de ces données à une autre administration publique en vue de leur traitement ultérieur par cette dernière. Aux termes de l'article 13, paragraphe 1, de la Directive 95/46, les États membres peuvent limiter le droit d'être informé lorsqu'une telle limitation est jugée nécessaire pour sauvegarder un intérêt économique important de l'État, y compris dans le domaine fiscal. Ces limitations doivent toutefois être imposées par des mesures législatives. Étant donné que ni la définition des données à transférer ni les modalités détaillées de leur transfert n'ont été établies par une mesure législative, mais uniquement dans un protocole entre les deux autorités publiques, les conditions de dérogation prévues par le droit de l'UE n'étaient pas satisfaites. Les requérants auraient dû être informés au préalable de la transmission de leurs données à la caisse nationale d'assurance maladie et du traitement ultérieur de celles-ci par cette dernière.

Contenu des informations

En vertu de l'article 8, paragraphe 1, de la Convention 108 modernisée, le responsable du traitement est tenu de fournir à la personne concernée toute information nécessaire pour garantir un traitement loyal et transparent des données à caractère personnel, y compris :

- l'identité et la résidence ou lieu d'établissement habituel(le) du responsable du traitement ;
- la base juridique et les finalités du traitement envisagé ;

- les catégories de données à caractère personnel traitées ;
- les destinataires ou les catégories de destinataires des données personnelles, le cas échéant ;
- des moyens dont disposent les personnes concernées pour exercer les droits.

Conformément au RGPD, lorsque des données à caractère personnel sont collectées auprès de la personne concernée, le responsable du traitement est tenu de lui fournir les informations suivantes au moment où les données en question sont obtenues[532] :

- l'identité et les coordonnées du responsable du traitement, y compris celles du DPD, le cas échéant ;
- la finalité et la base juridique du traitement, c'est-à-dire une obligation contractuelle ou juridique ;
- l'intérêt légitime du responsable du traitement si celui-ci sert de base au traitement ;
- les destinataires ou les catégories de destinataires des données à caractère personnel ;
- lorsque les données sont transférées vers un pays tiers ou à une organisation internationale et si ce transfert repose sur une décision d'adéquation ou sur des garanties appropriées ;
- la durée de conservation des données à caractère personnel ou, lorsqu'il n'est pas possible de la déterminer, les critères utilisés pour déterminer cette durée ;
- les droits des personnes concernées à l'égard du traitement, tels que le droit d'accès, de rectification, d'effacement, de limitation ou d'opposition au traitement ;

532 RGPD, art. 13, para. 1.

- lorsque la fourniture de données à caractère personnel est prévue par la loi ou par un contrat, si la personne concernée est tenue de les fournir ainsi que les conséquences de la non-fourniture de ces données ;
- l'existence d'une prise de décision automatisée, y compris un profilage ;
- le droit d'introduire une réclamation auprès d'une autorité de contrôle ;
- l'existence du droit de retirer son consentement.

Dans les cas de prise de décision automatisée, y compris un profilage, les personnes concernées doivent recevoir des informations utiles concernant la logique sous-jacente ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.

Lorsque les données à caractère personnel ne sont pas obtenues directement auprès de la personne concernée, le responsable du traitement doit informer la personne de l'origine de ces données. En tout état de cause, le responsable du traitement doit, notamment, informer les personnes concernées de l'existence d'une prise de décision automatisée, y compris un profilage[533]. Enfin, si un responsable de traitement a l'intention d'effectuer un traitement des données à caractère personnel pour une finalité autre que celle initialement déclarée à la personne concernée, les principes de limitation de la finalité et de transparence lui imposent de fournir à la personne concernée des informations au sujet de cette nouvelle finalité. Les responsables du traitement doivent fournir les informations avant tout traitement ultérieur. En d'autres termes, lorsque la personne concernée a donné son consentement au traitement de données la concernant, le responsable du traitement doit recevoir un nouveau consentement de cette personne si la finalité du traitement est modifiée ou si d'autres finalités sont ajoutées.

Moment de la communication des informations

Le RGPD opère une distinction entre deux scénarios et deux moments auxquels le responsable du traitement doit fournir des informations à la personne concernée.

- Lorsque les données à caractère personnel sont collectées directement auprès de la personne concernée, le responsable du traitement doit fournir à cette

533 RGPD, art. 13, para. 2, et art. 14, para. 2, point f).

dernière toutes les informations et droits afférents auxdites données prévues par le RGPD au moment où les données sont obtenues[534].
Lorsqu'il a l'intention d'effectuer un traitement ultérieur des données à caractère personnel pour une autre finalité, le responsable du traitement fournit toutes les informations pertinentes avant que ce traitement ait lieu.

- Lorsque les données à caractère personnel n'ont pas été directement collectées auprès de la personne concernée, le responsable du traitement est tenu de lui fournir des informations sur le traitement « dans un délai raisonnable après avoir obtenu les données à caractère personnel, mais ne dépassant pas un mois » ou avant que les données ne soient communiquées à un tiers[535].

Le rapport explicatif sur la Convention 108 modernisée précise que s'il est impossible d'informer les personnes concernées au début du traitement des données, cela peut être fait à un stade ultérieur, par exemple lorsque le responsable du traitement est mis en contact avec la personne concernée pour une raison quelconque[536].

Différentes manières de fournir des informations

Conformément au droit du CdE et de l'UE, les informations que le responsable du traitement doit fournir à la personne concernée doivent être concises, transparentes, compréhensibles et aisément accessibles. Elles doivent être communiquées par écrit ou par d'autres moyens, y compris par voie électronique, en utilisant des termes clairs, simples et aisément compréhensibles. Lorsqu'il fournit les informations, le responsable du traitement peut utiliser des icônes normalisées afin de présenter les informations d'une manière aisément visible et compréhensible[537]. Une icône représentant un verrou pourrait, par exemple, être utilisée pour signaler que les données sont collectées et/ou chiffrées de manière sûre. Les personnes concernées peuvent demander que les informations leur soient communiquées oralement. Les informations doivent être gratuites, à moins que les demandes de la personne concernée ne soient manifestement infondées ou excessives (par exemple, à caractère

534 *Ibid.*, art. 13, paras. 1 et 2, libellé introductif où le RGPD fait référence aux informations sur l'obligation à respecter « au moment où les données en question sont obtenues ».

535 *Ibid.*, art. 13, para. 3, et art. 14, para. 3 ; voir également la référence aux intervalles raisonnables et sans délai excessif à l'article 8, para. 1, point b), de la Convention 108 modernisée.

536 Rapport explicatif sur la Convention 108 modernisée, para. 70.

537 La Commission européenne adoptera des actes délégués pour déterminer plus précisément les informations à présenter sous la forme d'icônes ainsi que les procédures régissant la fourniture d'icônes normalisées ; voir RGPD, art. 12, para. 8.

répétitif)[538]. Il est essentiel que l'accès aux informations fournies soit aisé afin de permettre à la personne concernée d'exercer les droits que lui confère le droit de l'UE en matière de protection des données.

Le principe de la loyauté du traitement exige que les informations soient aisément compréhensibles par les personnes concernées. Le langage utilisé doit être adapté aux destinataires. Le niveau et le type de langage utilisés devraient varier selon que le public visé est un adulte ou un enfant, le grand public ou un expert académique. La question de savoir comment équilibrer cet aspect des informations compréhensibles est examinée dans l'avis du Groupe de travail « Article 29 » sur des « dispositions davantage harmonisées en matière d'informations ». Le Groupe de travail est favorable à l'idée de déclarations présentées dans un format multistrates[539], permettant à la personne concernée de décider du niveau de détail qu'elle préfère. Ce mode de présentation des informations n'exonère toutefois pas le responsable du traitement de son obligation au titre des articles 13 et 14 du RGPD. Il reste tenu de fournir toutes les informations à la personne concernée.

L'une des façons les plus efficaces de fournir des informations consiste à insérer des notices d'information appropriées sur la page d'accueil du responsable du traitement, par exemple une déclaration de confidentialité sur un site web. Néanmoins, une part significative de la population n'utilise pas internet et la politique d'information des entreprises ou des autorités publiques devrait en tenir compte.

Une déclaration de confidentialité sur le traitement de données à caractère personnel présentée sur une page internet pourrait ressembler à ceci :

Qui sommes-nous ?

Le « responsable du traitement » est Bed and Breakfast C&U, établi à [adresse : xxx], tél. : xxx ; fax : xxx ; courriel : info@c&u.com ; coordonnées du délégué à la protection des données : [xxx].

La notice d'information sur les données à caractère personnel fait partie des conditions générales régissant nos services hôteliers.

538 RGPD, art. 12, paras. 1, 5 et 7 ; Convention 108 modernisée, art. 9, para. 1, point b).

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

Quelles données collectons-nous sur vous ?

Nous collectons les données à caractère personnel suivantes à votre sujet : nom, adresse postale, numéro de téléphone, adresse électronique, informations de séjour, numéro de carte de débit et de crédit et adresses IP ou noms de domaine des ordinateurs que vous avez utilisés pour vous connecter à notre site internet.

Pourquoi collectons-nous vos données ?

Nous traitons vos données avec votre consentement et aux fins de prendre des réservations, de conclure et de respecter les contrats de services que nous vous offrons et de nous conformer aux obligations que la législation nous impose, comme la loi sur les taxes de séjour, qui nous oblige à collecter des données à caractère personnel pour pouvoir payer la taxe municipale sur le logement.

Comment traitons-nous vos données ?

Vos données personnelles seront conservées pendant trois mois. Elles ne feront pas l'objet de décisions automatisées.

Notre Bed & Breakfast C&U respecte des procédures de sécurité strictes afin que vos données personnelles ne soient pas endommagées, détruites ou divulguées à des tiers sans votre autorisation et afin de prévenir tout accès non autorisé. Les ordinateurs dans lesquels vos données sont conservées se trouvent dans un environnement sécurisé auquel l'accès physique est limité. Nous utilisons des pare-feu sécurisés et d'autres mesures pour limiter l'accès par voie électronique. Si les données doivent être transmises à un tiers, nous lui demandons de disposer de mesures similaires pour protéger vos données à caractère personnel.

Toutes les informations que nous collectons ou enregistrons sont limitées à nos bureaux. Seules les personnes ayant besoin des informations pour accomplir leurs tâches au titre de ce contrat ont accès aux données à caractère personnel. Nous vous demanderons expressément votre consentement lorsque nous aurons besoin d'informations pour vous identifier. Nous pouvons vous demander de coopérer à nos contrôles de sécurité avant de divulguer des informations vous concernant. Vous pouvez

mettre à jour les informations personnelles que vous nous donnez à tout moment en nous contactant directement.

Quels sont vos droits ?

Vous avez le droit d'accéder à vos données, d'en obtenir une copie, de demander leur effacement ou leur rectification ou de demander qu'elles soient transférées à un autre responsable du traitement.

Vous pouvez adresser vos demandes à info@c&u.com. Nous disposons d'un mois pour répondre à votre demande, mais si celle-ci est trop complexe ou si nous recevons trop d'autres demandes, nous vous informerons que ce délai peut être prolongé de deux mois supplémentaires.

Accès à vos données personnelles

Vous avez le droit d'accéder à vos données, d'obtenir, sur demande, connaissance du raisonnement qui sous-tend le traitement des données, de demander leur effacement ou leur rectification et vous avez le droit de ne pas être soumis à une décision prise uniquement sur le fondement d'un traitement automatisé sans que votre avis soit pris en compte. Vous pouvez adresser vos demandes à info@c&u.com. Vous avez également le droit de vous opposer au traitement, de retirer votre consentement et d'introduire une réclamation après de l'autorité nationale de contrôle si vous considérez que ce traitement est contraire à la législation, ainsi que de réclamer une indemnisation pour le préjudice subi du fait du traitement illicite.

Droit d'introduire une réclamation

Le RGPD impose au responsable du traitement d'informer les personnes concernées des mécanismes de sanction prévus par le droit national et le droit de l'UE en cas de violations de données à caractère personnel. Le responsable du traitement doit informer les personnes concernées de leur droit d'introduire une réclamation auprès d'une autorité de contrôle et, si nécessaire, d'une juridiction nationale en cas de violation de données à caractère personnel[540]. Le droit du CdE prescrit également le droit des personnes concernées d'être informées des moyens d'exercer leurs droits,

540 RGPD, art. 13, para. 2, point d), et art. 14, para. 2, point e) ; Convention 108 modernisée, art. 8, para. 1, point f).

notamment celui de disposer d'un recours tel que reconnu par l'Article 9, paragraphe 1, point f).

Exemptions de l'obligation d'informer

Le RGPD prévoit une exception à l'obligation d'informer. Conformément à l'article 13, paragraphe 4, et à l'article 14, paragraphe 5, du RGPD, l'obligation d'informer les personnes concernées ne s'applique pas lorsque la personne concernée dispose déjà de toutes les informations pertinentes[541]. De plus, lorsque les données à caractère personnel n'ont pas été obtenues auprès de la personne concernée, l'obligation d'informer ne s'applique pas lorsque la fourniture des informations se révèle impossible ou exige des efforts disproportionnés, en particulier lorsque les données à caractère personnel sont traitées à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques[542].

Par ailleurs, le RGPD accorde aux États membres un pouvoir d'appréciation pour limiter les obligations et les droits conférés par le règlement aux personnes physiques lorsque cela constitue une mesure nécessaire et proportionnée dans une société démocratique, par exemple pour protéger la sécurité nationale, la sûreté publique, la défense, des enquêtes et des procédures judiciaires ou des intérêts économiques et financiers, ainsi que des intérêts privés plus importants que la protection des données[543].

Toute exemption ou limitation doit être nécessaire dans une société démocratique et proportionnée à l'objectif poursuivi. Dans des cas très exceptionnels, par exemple en raison d'indications médicales, la protection de la personne concernée peut nécessiter une limitation de la transparence ; ceci concerne en particulier la limitation du droit d'accès de chaque personne concernée[544]. À titre de protection minimale, le droit national doit toutefois respecter l'essence des libertés et droits fondamentaux protégés par le droit de l'UE[545]. Ceci implique que le droit national contienne des dispositions spécifiques précisant la finalité du traitement, les catégories de données à caractère personnel visées, les garanties et d'autres exigences procédurales[546].

541 *Ibid.*, art. 13, para. 4, et art. 14, para. 5, point a).

542 *Ibid.*, art. 14, para. 5, points b) à e).

543 RGPD, art. 23, para. 1.

544 RGPD, art. 15.

545 RGPD, art. 23, para. 1.

546 *Ibid.*, art. 23, para. 2.

Lorsque les données sont collectées à des fins de recherche scientifique ou historique, à des fins statistiques ou à des fins archivistiques dans l'intérêt public, le droit des États membres ou le droit de l'Union peut prévoir des dérogations à l'obligation d'informer si elle risque de rendre impossible ou d'entraver sérieusement la réalisation des finalités spécifiques[547].

Des limitations similaires existent dans le droit du CdE, lorsque les droits des personnes concernées inscrits à l'article 9 de la Convention 108 modernisée peuvent être soumis à des restrictions conformément à l'article 11 de la Convention 108, selon des conditions strictes. De plus, selon l'article 8, paragraphe 2 de la Convention 108 modernisée, l'obligation de transparence du traitement imposé aux contrôleurs n'est pas applicable lorsque la personne concernée détient déjà l'information.

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 9 de la Convention 108 modernisée. Celui-ci prévoit que chaque personne a le droit d'obtenir, à sa demande, des informations sur le traitement de données à caractère personnel la concernant sous une forme intelligible. Le droit d'accès a été reconnu non seulement dans les dispositions de la Convention 108 modernisée, mais aussi dans la jurisprudence de la CouEDH. Celle-ci a maintes fois rappelé qu'il existe un droit d'accès aux informations concernant ses propres données et que ce droit découle de la nécessité de respecter la vie privée[548]. Le droit d'accès aux données à caractère personnel conservées par des organismes publics ou privés peut toutefois être limité dans certaines circonstances[549].

Dans le droit de l'UE, le droit d'accès à ses propres données est explicitement reconnu par l'article 15 du RGPD et il est également consacré, en tant que droit fondamental à la protection des données à l'article 8, paragraphe 2, de la Charte des droits fondamentaux de l'UE[550]. Le droit d'une personne à accéder à ses propres

547 *Ibid.*, art. 89, paras. 2 et 3.

548 CouEDH, *Gaskin c. Royaume-Uni*, nº 10454/83, 7 juillet 1989 ; CouEDH, *Odièvre c. France* [GC], nº 42326/98, 13 février 2003 ; CouEDH, *K.H. et autres c. Slovaquie*, nº 32881/04, 28 avril 2009 ; CouEDH, *Godelli c. Italie*, nº 33783/09, 25 septembre 2012.

549 CouEDH, *Leander c. Suède*, nº 9248/81, 26 mars 1987.

550 Voir également CJUE, affaires jointes C-141/12 et C-372/12, *YS c. Minister voor Immigratie, Integratie en Asiel* et *Minister voor Immigratie, Integratie en Asiel c. M et S*, 17 juillet 2014; CJUE, C-615/13 P, *ClientEarth, Pesticide Action Network Europe (PAN Europe) c. Autorité européenne de sécurité des aliments (EFSA), Commission européenne*, 16 juillet 2015.

données est un élément essentiel du droit européen en matière de protection des données[551].

Le RGPD dispose que chaque personne concernée a le droit d'accéder à ses propres données et à certaines informations sur le traitement, que les responsables du traitement doivent fournir[552]. En particulier, chaque personne concernée a le droit d'obtenir (du responsable du traitement) la confirmation que des données la concernant sont traitées et à tout le moins les informations suivantes :

- les finalités du traitement ;
- les catégories de données concernées ;
- les destinataires ou catégories de destinataires auxquels les données sont communiquées ;
- la durée de conservation des données envisagée ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ;
- l'existence du droit de demander la rectification ou l'effacement de données à caractère personnel ou une limitation du traitement des données à caractère personnel ;
- le droit d'introduire une réclamation auprès d'une autorité de contrôle ;
- toute information disponible quant à la source des données lorsque les données ne sont pas collectées auprès de la personne concernée ;
- dans le cas de décisions automatisées, la logique sous-jacente au traitement automatisé des données.

Le responsable du traitement doit fournir à la personne concernée une copie des données à caractère personnel faisant l'objet d'un traitement. La communication de ces informations à la personne concernée doit se faire sous une forme compréhensible, ce qui signifie que le responsable du traitement doit s'assurer que la

551 CJUE, affaires jointes C-141/12 et C-372/12, *YS c. Minister voor Immigratie, Integratie en Asiel* et *Minister voor Immigratie, Integratie en Asiel c. M et S*, 17 juillet 2014.

552 RGPD, art. 15, para. 1.

personne concernée peut comprendre les informations fournies. Par exemple, il ne suffit pas d'inclure des abréviations techniques, des termes codés ou des acronymes en réponse à une demande d'accès, à moins que la signification de ces termes soit expliquée. En cas de prise de décisions automatisée, y compris un profilage, la logique générale sous-tendant les décisions automatisées devra être expliquée, ainsi que les critères qui ont été pris en considération lors de l'évaluation de la personne concernée. Des exigences similaires existent dans le **droit du CdE**.[553]

Exemple : l'accès à ses propres données aidera une personne concernée à déterminer si elles sont exactes. Il est donc essentiel que la personne concernée soit informée, sous une forme compréhensible, non seulement des données à caractère personnel faisant effectivement l'objet d'un traitement, mais aussi des catégories de données traitées, telles que le nom, l'adresse IP, les coordonnées de géolocalisation, le numéro de carte de crédit, etc.

Lorsque les données ne sont pas collectées auprès de la personne concernée, des informations doivent être données sur la source de ces données en réponse à une demande d'accès, dans la mesure où ces informations sont disponibles. Cette disposition doit être comprise à la lumière des principes de loyauté, de transparence et de responsabilité. Un responsable du traitement ne peut pas détruire des informations sur la source des données pour se libérer de l'obligation de les communiquer, à moins que l'effacement n'ait eu lieu malgré la réception de la demande d'accès, et il doit toujours se conformer aux exigences générales de « responsabilité ».

Comme l'explique la jurisprudence de la CJUE, le droit d'accès aux données à caractère personnel ne peut pas être restreint indûment par des limites de temps. Les personnes concernées doivent également avoir une possibilité raisonnable d'obtenir des informations sur des traitements effectués dans le passé.

Exemple : dans l'affaire *Rijkeboer*[554], il a été demandé à la CJUE de déterminer si le droit d'un individu d'accéder à des informations sur les destinataires ou des catégories de destinataires de données à caractère personnel, et sur le contenu de ces données, pouvait être limité à un an avant sa demande d'accès.

553 Voir Convention 108 modernisée, art. 8, para. 1, point c).

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

Pour déterminer si la législation de l'UE 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 ou qu'il signale aux tiers auxquels les données ont été communiquées la rectification, l'effacement et le verrouillage. Un droit d'accès effectif est également nécessaire pour permettre à la personne concernée d'exercer son droit d'opposition au traitement de ses données à caractère personnel ou son droit d'introduire une réclamation et d'obtenir réparation[555].

Pour assurer l'effet utile des droits accordés aux personnes concernées, 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 incorrectes ainsi que d'introduire un recours juridictionnel et d'obtenir la réparation du préjudice subi ».

6.1.2. Droit de rectification

Le droit de l'UE et **celui du CdE** prévoient que les personnes concernées ont le droit de faire rectifier les données à caractère personnel les concernant. L'exactitude des données à caractère personnel est essentielle pour garantir un niveau élevé de protection des données aux personnes concernées[556].

Exemple : dans l'affaire *Ciubotaru c. Moldova*[557], le requérant n'avait pas été en mesure de faire remplacer son origine ethnique mentionnée dans les registres officiels en tant que « moldave » par « roumaine », au motif qu'il n'aurait pas étayé sa demande. La CouEDH a jugé acceptable que les États exigent des preuves objectives au moment de l'enregistrement de l'identité ethnique d'une personne. Lorsqu'une telle demande se fonde sur des raisons purement subjectives et dénuées de fondement, les autorités sont libres de la rejeter. Toutefois, la demande du requérant se fondait sur d'autres éléments que la perception subjective de sa propre origine ethnique ; il a été

555 RGPD, art. 15, para. 1, points c) et f), art. 16, art. 17, para. 2, art. 21 et chapitre VIII.

556 *Ibid.*, art. 16 et considérant 65 ; Convention 108 modernisée, art. 9, para. 1, point e).

557 CouEDH, *Ciubotaru c. Moldova*, nº 27138/04, 27 avril 2010, paras. 51 et 59.

en mesure de fournir des liens objectivement vérifiables avec le groupe ethnique roumain tels que la langue, le nom, l'empathie et d'autres éléments. Or, en droit interne, le requérant était tenu de produire des preuves du fait que ses parents avaient appartenu à l'ethnie roumaine. Eu égard à la réalité historique de la Moldova, pareille exigence a créé pour l'intéressé un obstacle insurmontable à l'enregistrement d'une identité ethnique autre que celle attribuée à ses parents par les autorités soviétiques. En l'empêchant de faire examiner son allégation d'appartenance à un certain groupe ethnique à la lumière de preuves objectivement vérifiables, l'État a failli à se conformer à son obligation positive de garantir au requérant le respect effectif de sa vie privée. La CouEDH a donc conclu à une violation de l'article 8 de la CEDH.

Dans certains cas, il suffira que la personne concernée demande simplement la rectification de l'orthographe d'un nom ou un changement d'adresse ou de numéro de téléphone, par exemple. **Selon le droit de l'UE** et **du CdE**, les données à caractère personnel inexactes doivent être rectifiées sans délai indu ou excessif[558]. Si, toutefois, de telles demandes sont liées à des questions juridiques d'importance significative, telles que l'identité légale de la personne concernée ou le lieu de résidence correct en vue d'obtenir la notification de documents juridiques, 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 imposer une charge de la preuve déraisonnable à la personne concernée et, par conséquent, l'empêcher d'obtenir la rectification de ses 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[559].

Exemple : dans l'affaire *Cemalettin Canlı c. Turquie*[560], la CouEDH a conclu à une violation de l'article 8 de la CEDH en raison des fichiers inexacts de la police présentés dans une procédure pénale.

Le requérant avait été poursuivi pénalement à deux reprises pour sa prétendue appartenance à des organisations illégales, mais il n'avait pas

558 RGPD, art. 16 ; Convention 108 modernisée, art. 9, para. 1.

559 CouEDH, *Rotaru c. Roumanie* [GC], nº 28341/95, 4 mai 2000

560 CouEDH, *Cemalettin Canlı c. Turquie*, nº 22427/04, 18 novembre 2008, paras. 33, 42 et 43 ; CouEDH, *Dalea c. France*, nº 964/07, 2 février 2010.

été condamné. Lors de son arrestation et de son inculpation pour une autre infraction pénale, la police a présenté devant la juridiction pénale un rapport intitulé « *formulaire d'information sur d'autres infractions* », où il était mentionné que le requérant était membre de deux organisations illégales. La demande du requérant de faire rectifier ledit rapport et les dossiers de police n'a pas abouti. La CouEDH a jugé que les informations contenues dans le rapport de police relevaient du champ d'application de l'article 8 de la CEDH, étant donné que les informations publiques systématiquement recueillies et conservées dans des fichiers tenus par les autorités pouvaient également relever de la « vie privée ». De plus, le rapport de police était inexact dans sa formulation et sa présentation à la juridiction pénale n'était pas conforme au droit interne. La CouEDH a donc conclu à une violation de l'article 8.

Lors d'un procès civil ou d'une procédure devant une autorité publique visant à déterminer si des données sont exactes, la personne concernée peut demander qu'une mention ou une note soit inscrite dans son dossier indiquant qu'elle en conteste l'exactitude et qu'une décision officielle est pendante[561]. Au cours de cette période, le responsable du traitement ne peut pas présenter les données comme étant exactes ou non soumises à une rectification, en particulier à des tiers.

6.1.3. Droit à l'effacement (« droit à l'oubli »)

Conférer aux personnes concernées un droit à l'effacement de leurs données revêt une importance particulière pour l'application effective des principes relatifs à la protection des données et, en particulier, le principe de la minimisation des données (les données à caractère personnel doivent être limitées à ce qui est nécessaire pour les finalités pour lesquelles ces données sont traitées). Un droit à l'effacement est donc prévu dans les instruments juridiques du CdE et de l'UE[562].

Exemple : dans l'affaire *Segerstedgt-Wiberg et autres c. Suède*[563], les requérants avaient été membres du parti libéral et du parti communiste. Ils soupçonnaient que des informations les concernant avaient été inscrites dans des fichiers de la Sûreté et en demandaient l'effacement. La CouEDH

561 RGPD, art. 18 et considérant 67.

562 *Ibid.*, art. 17.

563 CouEDH, *Segerstedt-Wiberg et autres c. Suède*, nº 62332/00, 6 juin 2006, paras. 89 et 90 ; voir aussi, par exemple, CouEDH, *M.K. c. France*, nº 19522/09, 18 avril 2013.

a estimé que la conservation des données en cause avait un fondement juridique et poursuivait un but légitime. Cependant, pour certains requérants, la CouEDH a conclu que la conservation prolongée des données constituait une ingérence disproportionnée dans leur vie privée. Par exemple, dans le cas d'un requérant, les autorités ont conservé des données selon lesquelles, en 1969, l'intéressé aurait préconisé une résistance violente aux contrôles de police durant des manifestations. La CouEDH a estimé que ces informations ne pouvaient répondre à des intérêts de sécurité nationale, compte tenu, en particulier, de leur ancienneté. La Cour a conclu à une violation de l'article 8 de la CEDH pour quatre des cinq requérants, étant donné que, vu le temps écoulé depuis les actes allégués des requérants, la conservation de leurs données n'était pas pertinente.

Exemple : dans l'affaire *Brunet c. France*[564], les requérants ont contesté la conservation de leurs données personnelles dans une base de données de la police contenant des informations sur des condamnés, des accusés et des victimes. Bien que la procédure pénale contre le requérant ait été classée sans suite, des informations le concernant figuraient dans la base de données. La Cour a conclu à une violation de l'article 8 de la CEDH. Dans sa conclusion, la Cour a considéré que, dans la pratique, il n'existait pas de possibilité permettant au requérant de faire effacer ses données à caractère personnel de la base de données. La CouEDH a également examiné la nature des informations contenues dans la base de données et a considéré qu'elles présentaient un caractère intrusif pour la vie privée du requérant en ce qu'elles faisaient apparaître des éléments détaillés de l'identité et de la personnalité de celui-ci. En outre, la Cour a constaté que la durée de conservation des fichiers personnels dans la base de données, qui est de vingt ans, était excessivement longue, compte tenu en particulier de l'absence de condamnation du requérant.

La Convention 108 modernisée reconnaît expressément que toute personne a le droit d'obtenir l'effacement de données inexactes, fausses ou traitées de façon illicite[565].

564 CouEDH, *Brunet c. France*, nº 21010/10, 18 septembre 2014.

565 Convention 108 modernisée, art. 9, para. 1, point e).

Dans le droit de l'UE, l'article 17 du RGPD donne effet aux demandes d'effacement ou de suppression des personnes concernées. Le droit d'obtenir l'effacement de ses propres données sans délai excessif s'applique lorsque :

- les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière ;
- la personne concernée retire le consentement sur lequel est fondé le traitement et il n'existe pas d'autre fondement juridique au traitement ;
- la personne concernée s'oppose au traitement et il n'existe pas de motif légitime impérieux pour le traitement ;
- les données à caractère personnel ont fait l'objet d'un traitement illicite ;
- les données à caractère personnel doivent être effacées pour respecter une obligation légale qui est prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis ;
- les données à caractère personnel ont été collectées dans le cadre de l'offre de services de la société de l'information à des enfants visée à l'article 8 du RGPD[566].

La charge de la preuve de la légitimité du traitement des données incombe au responsable du traitement, étant donné qu'il est responsable de la licéité du traitement[567]. Conformément au principe de la responsabilité, le responsable du traitement doit, à tout moment, être en mesure de démontrer qu'il existe une base juridique solide pour son traitement, à défaut de quoi celui-ci doit être arrêté[568]. Le RGPD énonce des exceptions au droit à l'oubli, notamment lorsque le traitement de données à caractère personnel est nécessaire :

- à l'exercice du droit à la liberté d'expression et d'information ;
- pour respecter une obligation légale requérant un traitement qui est prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable

566 RGPD, art. 17, para. 1.

567 *Ibid.*

568 *Ibid.*, art. 5, para. 2.

du traitement est assujetti, ou pour exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;

- pour des motifs d'intérêt public dans le domaine de la santé publique ;
- à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques ;
- à la constatation, à l'exercice ou à la défense de droits en justice[569].

La CJUE a affirmé l'importance du droit à l'effacement pour garantir un niveau élevé de protection des données.

Exemple : dans l'affaire *Google Spain*[570], la CJUE a examiné la question de savoir si Google était tenu de supprimer des informations obsolètes sur les difficultés financières du requérant de sa liste de résultats de recherche. Google a, notamment, contesté sa responsabilité, en alléguant qu'il se contente de fournir un lien hypertexte vers la page web de l'éditeur qui héberge les informations, en l'espèce un quotidien faisant état des problèmes d'insolvabilité du requérant[571]. Google a soutenu que la demande d'effacement d'informations obsolètes d'une page web devait être adressée à l'hébergeur de la page web et non à Google, qui fournit uniquement un lien vers la page originale. La CJUE a conclu que Google, lorsqu'il recherche des informations sur internet et sur des pages web et lorsqu'il indexe le contenu pour fournir des résultats de recherche, devient un responsable du traitement auquel s'appliquent les responsabilités et obligations prévues par le droit de l'UE.

569 *Ibid.*, art. 17, para. 3.

570 CJUE, C-131/12, *Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 13 mai 2014, points 55 à 58.

571 Google a également contesté l'application des règles de l'UE en matière de protection des données au motif que Google Inc. est établie aux États-Unis et que le traitement des données à caractère personnel en cause en l'espèce a également été effectué aux États-Unis. Un second argument à l'appui de l'inapplicabilité du droit de l'UE relatif à la protection des données reposait sur l'affirmation que des moteurs de recherche ne sauraient être considérés comme des « responsables du traitement » en ce qui concerne les données affichées dans leurs résultats, étant donné qu'ils n'ont pas connaissance des données et n'exercent pas de contrôle sur celles-ci. La CJUE a rejeté les deux arguments, a conclu que la Directive 95/46/CE s'appliquait au cas d'espèce et a poursuivi l'examen de la portée des droits qu'elle garantit, notamment le droit à l'effacement des données à caractère personnel.

La CJUE a précisé que les moteurs de recherche en ligne et les résultats de recherche fournissant des données à caractère personnel peuvent établir un profil détaillé d'une personne[572]. Les moteurs de recherche rendent universelles les informations contenues dans une telle liste de résultats. Au vu de sa gravité potentielle, cette ingérence ne saurait être justifiée par le seul intérêt économique de l'exploitant d'un tel moteur dans ce traitement. Il y a lieu de rechercher un juste équilibre entre l'intérêt légitime des internautes à accéder aux informations et les droits fondamentaux de la personne concernée au titre des articles 7 et 8 de la Charte des droits fondamentaux de l'UE. Compte tenu de la numérisation croissante de la société, l'exigence que les données à caractère personnel soient exactes et que leur publication n'aille pas au-delà de ce qui est nécessaire, c'est-à-dire informer le public, est essentielle pour garantir un niveau élevé de protection des données aux personnes concernées. Le « responsable du traitement doit assurer, dans le cadre de ses responsabilités, de ses compétences et de ses possibilités, que celui-ci satisfait aux exigences » du droit de l'UE, pour que les garanties prévues par celui-ci puissent développer leur plein effet[573]. Cela implique que le droit d'obtenir l'effacement de ses propres données lorsque le traitement est obsolète ou n'est plus nécessaire couvre également les responsables du traitement qui reproduisent les informations[574].

Sur la question de savoir si Google était tenu de supprimer les liens relatifs au requérant, la CJUE a conclu que, dans certaines conditions, les personnes concernées ont le droit d'obtenir l'effacement de leurs données à caractère personnel. Ce droit peut être invoqué lorsque les informations relatives à une personne sont inexactes, inadéquates, non pertinentes ou excessives aux fins du traitement des données. La CJUE a reconnu que ce droit n'est pas absolu et qu'il doit être mis en balance avec d'autres droits et intérêts, en particulier l'intérêt du public à avoir accès à certaines informations. Chaque demande d'effacement doit être appréciée au cas par cas afin de trouver un équilibre entre les droits fondamentaux à la protection des données à caractère personnel et au respect de la vie privée de la personne concernée, d'une

572 *Ibid.*, points 36, 38, 80, 81 et 97.

573 *Ibid.*, points 81 à 83.

574 CJUE, C-131/12, *Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 13 mai 2014, point 88. Voir également Groupe de travail « Article 29 » (2014), *Lignes directrices sur la mise en œuvre de l'arrêt de la CJUE sur « Google Spain and Inc. c. Agencia Española de Protección de Datos (AEPD) et Mario Costeja González » (C-131/12)*, WP 225, Bruxelles, 26 novembre 2014, et Recommandation CM/Rec 2012(3) du Comité des Ministres aux États membres sur la protection des droits de l'homme dans le contexte des moteurs de recherche, 4 avril 2012.

part, et les intérêts légitimes de tous les utilisateurs d'internet, y compris les éditeurs, d'autre part. La Cour a fourni des orientations sur les facteurs à prendre en considération dans cet exercice de mise en balance. La nature de l'information en cause est un facteur particulièrement important. Si l'information concerne la vie privée de la personne concernée et qu'il n'y a pas d'intérêt général à rendre cette information publique, la protection des données et le respect de la vie privée l'emporteront sur le droit du public à être informé. En revanche, s'il appert que la personne concernée est une personnalité publique ou que l'information est de nature à justifier l'octroi de l'accès du public à ces informations, l'intérêt prépondérant du public à avoir accès à ces informations peut justifier l'ingérence avec les droits fondamentaux à la protection des données et au respect de la vie privée.

À la suite de cet arrêt, le Groupe de travail « Article 29 » a adopté des lignes directrices sur la mise en œuvre de l'arrêt rendu par la Cour[575]. Ces lignes directrices contiennent une liste de critères communs que les autorités de contrôle peuvent utiliser pour traiter des réclamations se rapportant à des demandes d'effacement et expliquent ce qu'implique le droit à l'effacement, tout en guidant les autorités dans cet exercice de mise en balance des droits. Elles rappellent que les évaluations doivent se faire au cas par cas. Le droit à l'oubli n'étant pas absolu, l'issue d'une demande peut différer selon les cas. La jurisprudence de la CJUE après l'affaire *Google* l'illustre également.

Exemple : dans l'affaire *Camera di Commercio i Lecce c. Manni*[576], la CJUE a été amenée à déterminer si une personne avait le droit d'obtenir l'effacement de ses données personnelles publiées dans un registre public des sociétés, alors que sa société avait cessé d'exister. M. Manni avait demandé à la chambre de commerce de Lecce d'effacer ses données personnelles de ce registre après avoir découvert que des clients potentiels pouvaient consulter le registre et voir qu'il avait été l'administrateur d'une société déclarée en faillite plus de dix ans auparavant. Le requérant considérait que cette information dissuaderait des clients potentiels.

575 Groupe de travail « Article 29 » (2014), *Lignes directrices sur la mise en œuvre de l'arrêt de la CJUE sur « Google Spain and Inc. c. Agencia Española de Protección de Datos (AEPD) et Mario Costeja González » (C-131/12)*, WP 225, Bruxelles, 26 novembre 2014.

576 CJUE, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce c. Salvatore Manni*, 9 mars 2017.

En mettant en balance le droit de M. Manni à la protection de ses données à caractère personnel avec l'intérêt général du public d'avoir accès à ces informations, la CJUE s'est d'abord penchée sur la finalité du registre public. Elle a souligné que la publicité était prévue par la loi et, en particulier, par une directive européenne visant à rendre les informations sur les sociétés plus aisément accessibles aux tiers. Les tiers devaient donc avoir accès aux actes essentiels d'une société et à certaines indications la concernant et être en mesure de les examiner, « notamment l'identité des personnes qui ont le pouvoir de l'engager ». La publicité visait également à assurer la sécurité juridique dans la perspective d'une intensification des courants d'affaires entre les États membres en faisant en sorte que les tiers aient accès à toutes les données pertinentes sur les sociétés dans l'UE.

La CJUE a par ailleurs relevé que même après l'écoulement d'un certain délai, et même après la dissolution d'une société, des droits et des relations juridiques relatifs à celle-ci subsistent souvent. Les litiges se rapportant à une dissolution peuvent être longs et des questions concernant une société, ses responsables et ses liquidateurs peuvent surgir de nombreuses années après qu'une société a cessé d'exister. La CJUE a conclu que, vu la multitude des scénarios possibles et la disparité considérable dans les délais de prescription prévus par les différents droits nationaux, « il paraît, en l'état actuel, impossible d'identifier un délai unique, à compter de la dissolution d'une société, à l'expiration duquel l'inscription desdites données dans le registre et leur publicité ne serait plus nécessaire ». Compte tenu de l'objectif légitime de la publicité et de la difficulté à fixer un délai à l'expiration duquel les données à caractère personnel pourraient être supprimées du registre sans léser les intérêts de tiers, la CJUE a considéré que les règles de l'UE en matière de protection des données ne garantissent pas un droit à l'effacement des données à caractère personnel pour des personnes se trouvant dans la situation de M. Manni.

Lorsque le responsable du traitement a rendu publiques des données à caractère personnel et est tenu de les effacer, il doit prendre des mesures « raisonnables » pour informer d'autres responsables du traitement traitant les mêmes données de la demande d'effacement de la personne concernée. Les activités du responsable

du traitement doivent tenir compte des technologies disponibles et du coût de leur mise en œuvre[577].

6.1.4. Droit à la limitation du traitement

Conformément à l'article 18 du RGPD, la personne concernée a le droit d'obtenir du responsable du traitement la limitation du traitement de ses données à caractère personnel. La personne concernée peut demander au responsable du traitement de limiter le traitement lorsque :

- l'exactitude des données à caractère personnel est contestée ;
- le traitement est illicite et la personne concernée s'oppose à leur effacement et exige au lieu de l'effacement la limitation de leur utilisation ;
- les données doivent être conservées pour l'exercice ou la défense de droits en justice ;
- une décision portant sur le point de savoir si les motifs légitimes poursuivis par le responsable du traitement prévalent sur ceux de la personne concernée est pendante[578].

Les méthodes par lesquelles un responsable de traitement peut limiter le traitement de données à caractère personnel peuvent consister, par exemple, à déplacer temporairement les données sélectionnées vers un autre système de traitement, à rendre les données inaccessibles aux utilisateurs ou à retirer temporairement les données à caractère personnel[579]. Le responsable du traitement doit notifier la personne concernée avant que la limitation du traitement ne soit levée[580].

Obligation de notifier la rectification ou l'effacement de données à caractère personnel ou une limitation du traitement

Le responsable du traitement doit porter à la connaissance de chaque destinataire auquel il a communiqué les données à caractère personnel toute rectification ou

577 RGPD, art. 17, para. 2, et considérant 66.

578 *Ibid.*, art. 18, para. 1.

579 *Ibid.*, considérant 67.

580 *Ibid.*, art. 18, para. 3.

effacement de ces données ou toute limitation du traitement, à moins que cela ne se révèle impossible ou requière des efforts disproportionnés[581]. Si la personne concernée demande des informations sur les destinataires, le responsable du traitement doit les lui fournir[582].

6.1.5. Droit à la portabilité des données

Conformément au RGPD, les personnes concernées ont droit à la portabilité des données lorsque le traitement des données à caractère personnel qu'elles ont fournies à un responsable du traitement est effectué à l'aide de procédés automatisés et fondé sur le consentement ou lorsque le traitement des données à caractère personnel est nécessaire à l'exécution d'un contrat et est effectué à l'aide de procédés automatisés. Ceci signifie que le droit à la portabilité des données ne s'applique pas lorsque le traitement des données à caractère personnel repose sur un fondement juridique autre qu'un consentement ou un contrat[583].

Lorsque le droit à la portabilité des données s'applique, les personnes concernées ont le droit d'obtenir que leurs données à caractère personnel soient transmises directement d'un responsable du traitement à un autre, lorsque cela est techniquement possible[584]. Pour faciliter ce processus, le responsable du traitement devrait mettre au point des formats interopérables permettant la portabilité des données pour les personnes concernées[585]. Le RGPD précise que les formats doivent être structurés, couramment utilisés et lisibles par machine afin de faciliter l'interopérabilité[586]. L'interopérabilité peut être entendue, au sens large, comme la capacité des systèmes d'information à échanger des données et à permettre le partage d'informations[587]. Alors que le but des formats utilisés est d'atteindre l'interopérabilité, le RGPD n'impose pas de recommandations particulières sur le format spécifique à utiliser ; les formats peuvent donc varier selon les secteurs[588].

581 *Ibid.*, art 19.

582 *Ibid.*

583 *Ibid.*, considérant 68 et art. 20, para. 1.

584 *Ibid.*, art. 20, para. 2.

585 *Ibid.*, considérant 68 et art. 20, para. 1.

586 *Ibid.*, considérant 68.

587 Commission européenne, Communication « des systèmes d'information plus robustes et plus intelligents au service des frontières et de la sécurité », COM(2016) 205 final, 2 avril 2016.

588 Groupe de travail « Article 29 » (2016), *Lignes directrices relatives au droit à la portabilité des données*, WP 242, 13 décembre 2016, version révisée et adoptée le 5 avril 2017, p. 13.

Selon les lignes directrices du Groupe de travail « Article 29 », le droit à la portabilité des données « encourage le choix et le contrôle de l'utilisateur, ainsi que sa responsabilisation » afin de donner aux personnes concernées un contrôle sur leurs propres données[589]. Ces lignes directrices précisent les principaux éléments de la portabilité des données, à savoir :

- le droit des personnes concernées de recevoir les données à caractère personnel les concernant traitées par le responsable du traitement dans un format structuré, couramment utilisé, lisible par machine et permettant l'interopérabilité ;
- le droit de transmettre les données à caractère personnel d'un responsable du traitement à un autre sans que le premier y fasse obstacle, lorsque cela est techniquement possible ;
- le système de la responsabilité : les responsables du traitement qui répondent à des demandes de portabilité des données agissent sur instructions de la personne concernée, ce qui signifie qu'ils ne sont pas responsables du respect par le destinataire de la législation relative à la protection des données, étant donné que c'est la personne concernée qui choisit le destinataire ;
- l'exercice du droit à la portabilité des données est sans préjudice d'aucun autre droit, comme c'est le cas pour tout autre droit prévu par le RGPD.

6.1.6. Droit d'opposition

Les personnes concernées peuvent invoquer leur droit d'opposition au traitement de données les concernant pour des raisons tenant à leur situation particulière et au traitement de données à des fins de prospection. Le droit d'opposition peut être exercé à l'aide de moyens automatisés.

Droit d'opposition pour des motifs tenant à la situation particulière de la personne concernée

Les personnes concernées ne disposent pas d'un droit général de s'opposer au traitement de leurs données[590]. L'article 21, paragraphe 1, du RGPD donne à la personne

589 *Ibid.*

590 Voir également CouEDH, *M.S. c. Suède*, nº 20837/92, 27 août 1997 (des données médicales avaient été échangées sans consentement ni possibilité de s'y opposer) ; CouEDH, *Leander c. Suède*, nº 9248/81, 26 mars 1987 ; CouEDH, *Mosley c. Royaume-Uni*, nº 48009/08, 10 mai 2011.

concernée le droit de soulever des objections pour des raisons tenant à sa situation particulière lorsque la base juridique du traitement est l'exécution par le responsable du traitement d'une mission d'intérêt public ou lorsque le traitement est fondé sur des intérêts légitimes du responsable du traitement[591]. Le droit d'opposition s'applique aux activités de profilage. Un droit similaire a été reconnu par la Convention 108 modernisée[592].

Le droit d'opposition pour des motifs tenant à la situation particulière de la personne concernée vise à établir un juste équilibre entre les droits à la protection des données de la personne concernée et les droits légitimes de tiers au traitement des données. La CJUE a toutefois précisé que les droits de la personne concernée prévalent « en règle générale » sur les intérêts économiques d'un responsable du traitement en fonction de « la nature de l'information en question et de sa sensibilité pour la vie privée de la personne concernée ainsi que de l'intérêt du public à disposer de cette information »[593]. Selon le RGPD, la charge de la preuve incombe aux responsables du traitement, qui doivent démontrer des motifs impérieux justifiant la poursuite du traitement[594]. De même, le rapport explicatif sur la Convention 108 modernisée explique que l'existence de motifs légitimes pour le traitement des données (qui peuvent prévaloir sur le droit d'opposition de la personne concernée) doit être démontrée au cas par cas[595].

Exemple : dans l'affaire *Manni*[596], la CJUE a retenu qu'en raison du motif légitime de la publication de données à caractère personnel dans le registre des sociétés, en particulier la nécessité de protéger les intérêts des tiers et d'assurer la sécurité juridique, en principe, M. Manni n'a pas le droit d'obtenir l'effacement de ses données du registre des sociétés. Elle a toutefois reconnu l'existence d'un droit d'opposition au traitement en déclarant qu'« il ne saurait [...] être exclu que puissent exister des situations particulières dans lesquelles

591 RGPD, considérant 69 ; art. 6, para. 1, points e) et f).

592 Convention 108 modernisée, art. 9, para. 1, point d) ; Recommandation sur le profilage, art. 5, para. 3.

593 CJUE, C-131/12, *Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 13 mai 2014, point 81.

594 Voir également Convention 108 modernisée, art. 98, para. 1, point d), qui dispose que la personne concernée peut s'opposer à tout moment au traitement de ses données « à moins que le responsable du traitement ne démontre des motifs légitimes justifiant le traitement qui prévalent sur les intérêts, ou les droits et libertés fondamentales de la personne concernée ».

595 Rapport explicatif sur la Convention 108 modernisée, para. 78.

596 CJUE, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce c. Salvatore Manni*, 9 mars 2017, points 47 et 60.

des raisons prépondérantes et légitimes tenant au cas concret de la personne concernée justifient exceptionnellement que l'accès aux données à caractère personnel la concernant inscrites dans le registre soit limité, à l'expiration d'un délai suffisamment long [...], aux tiers justifiant d'un intérêt spécifique à leur consultation ».

La CJUE a considéré qu'il appartenait aux juridictions nationales d'apprécier chaque cas au regard de l'ensemble des circonstances pertinentes de la personne et en tenant compte de l'existence de raisons prépondérantes et légitimes qui seraient de nature à justifier exceptionnellement de limiter l'accès des tiers aux données à caractère personnel contenues dans le registre des sociétés. Elle a toutefois précisé que, dans le cas de M. Manni, le simple fait que la publication de ses données à caractère personnel dans le registre aurait eu des conséquences concernant sa clientèle ne saurait être considéré comme une raison légitime et prépondérante. Les clients potentiels de M. Manni ont un intérêt légitime à disposer des informations concernant la faillite de son ancienne société.

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

Droit d'opposition à l'utilisation de données à des fins de prospection

L'article 21, paragraphe 2, du RGPD prévoit un droit spécifique d'opposition à l'utilisation de données à caractère personnel à des fins de prospection, précisant ainsi davantage l'article 13 de la Directive « vie privée et communications électroniques ». Ce droit est également consacré par la Convention 108 modernisée et la Recommandation du CdE sur le marketing direct[597]. Le rapport explicatif sur la Convention 108 modernisée précise que l'opposition au traitement des données à des fins de marketing direct devrait entraîner l'effacement ou la suppression, sans autre condition, des données à caractère personnel faisant l'objet de l'opposition[598].

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

598 Rapport explicatif sur la Convention 108 modernisée, para. 79.

La personne concernée a le droit de s'opposer gratuitement et à tout moment à l'utilisation de ses données personnelles à des fins de prospection. Les personnes concernées doivent être clairement informées de ce droit, indépendamment de toute autre information.

Droit d'opposition à l'aide de procédés automatisés

Lorsque des informations personnelles sont utilisées et traitées pour des services de la société de l'information, la personne concernée peut exercer son droit à s'opposer au traitement des données à caractère personnel la concernant par des procédés automatisés.

On entend par « services de la société de l'information » tout service fourni normalement contre rémunération, à distance par voie électronique et à la demande individuelle d'un destinataire de services[599].

Les responsables du traitement qui proposent des services de la société de l'information doivent mettre en place des procédures et des modalités techniques appropriées afin de garantir que le droit d'opposition à l'aide de procédés automatisés puisse être exercé de manière effective[600]. Ceci peut, par exemple, nécessiter de bloquer les cookies sur des pages web ou de désactiver le suivi de la navigation sur internet.

Droit d'opposition à des fins de recherche scientifique ou historique ou à des fins statistiques

En vertu du droit de l'UE, la recherche scientifique doit être interprétée au sens large et couvrir, par exemple, le développement et la démonstration de technologies, la recherche fondamentale, la recherche appliquée et la recherche financée par le secteur privé[601]. La recherche historique comprend également les recherches à des fins généalogiques, étant entendu que le règlement ne devrait pas s'appliquer aux personnes décédées[602]. Par « fins statistiques », on entend toute opération de collecte et de traitement de données à caractère personnel nécessaires pour des enquêtes

599 Directive 98/34/CE telle que modifiée par la directive 98/48/CE prévoyant une procédure d'information dans le domaine des normes et réglementations techniques, art. 1er, para. 2.

600 RGPD, art. 21, para. 5.

601 *Ibid.*, considérant 159.

602 *Ibid.*, considérant 160.

statistiques ou la production de résultats statistiques[603]. Une fois encore, la situation particulière d'une personne concernée est la base juridique du droit d'opposition au traitement de données à caractère personnel à des fins de recherche[604]. La seule exception est la nécessité du traitement pour l'exécution d'une mission d'intérêt public. Toutefois, le droit à l'effacement ne s'applique pas lorsque le traitement est nécessaire (pour des raisons d'intérêt public ou non) à des fins de recherche scientifique ou historique ou à des fins statistiques[605].

Le RGPD met en balance les exigences de la recherche scientifique, statistique ou historique et les droits des personnes concernées en prévoyant des garanties et des dérogations spécifiques dans son article 89. La législation de l'Union ou des États membres peut donc prévoir des dérogations au droit d'opposition dans la mesure où ce droit est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs de la recherche et si ces dérogations sont nécessaires à la réalisation de ceux-ci.

Dans le **droit du CdE**, l'article 9, paragraphe 2, de la Convention 108 modernisée prévoit que des restrictions à l'exercice des droits des personnes concernées, notamment le droit d'opposition, peuvent être prévues par la loi pour le traitement des données utilisées à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, lorsqu'il n'existe pas de risque identifiable d'atteinte aux droits et libertés fondamentales des personnes concernées.

Toutefois, le rapport explicatif (paragraphe 41) reconnaît également que les personnes concernées devraient se voir offrir l'opportunité de donner leur consentement uniquement pour certains domaines de la recherche ou de certaines parties de projets de recherche, dans la mesure où la finalité visée le permet, et s'y opposer lorsqu'elles jugent que le traitement empiète excessivement sur leurs droits et libertés sans fondement légitime.

En d'autres termes, un tel traitement serait donc considéré, a priori, comme compatible pour autant que d'autres garanties existent et que les opérations excluent, en principe, toute utilisation des informations obtenues pour la prise de décisions ou de mesures à l'égard d'une personne précise.

603 *Ibid.*, considérant 162.

604 *Ibid.*, art. 21, para. 6.

605 *Ibid.*, art. 17, para. 3, point d).

6.1.7. Décision individuelle automatisée, y compris le profilage

Par « décisions automatisées », on entend l'utilisation de données à caractère personnel traitées exclusivement à l'aide de procédés automatisés, sans intervention humaine. **Dans le droit de l'UE**, les personnes concernées ne doivent pas faire l'objet de décisions automatisées produisant des effets juridiques ou les affectant dans une mesure significative de façon similaire. Lorsque de telles décisions sont susceptibles d'affecter la vie d'une personne de manière significative parce qu'elles concernent, par exemple, la solvabilité, le recrutement en ligne, le rendement au travail, l'analyse du comportement ou la fiabilité, une protection spéciale est nécessaire pour éviter les effets négatifs. Une décision automatisée inclut le profilage, qui consiste en toute forme d'évaluation automatique des « aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des aspects concernant le rendement au travail de la personne concernée, sa situation économique, sa santé, ses préférences ou centres d'intérêt personnels, sa fiabilité ou son comportement, ou sa localisation et ses déplacements »[606].

Exemple : pour évaluer rapidement la solvabilité d'un futur client, des agences de notation de crédit (ANC) recueillent certaines données, telles que la manière dont le client a honoré ses crédits et géré ses comptes auprès de fournisseurs de services/fournisseurs de services aux collectivités, les adresses précédentes du client et des informations obtenues auprès de sources publiques, comme les listes électorales, les registres publics (y compris les décisions judiciaires) ou les données concernant une faillite ou une insolvabilité. Ces données à caractère personnel sont ensuite saisies dans un algorithme de notation, qui calcule une valeur globale représentant la solvabilité du client potentiel.

Selon le Groupe de travail « Article 29 », le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé susceptible de produire des effets juridiques pour la personne concernée ou qui l'affecte de manière significative équivaut à une interdiction générale et n'exige pas que la personne concernée s'oppose activement à une telle décision[607].

606 *Ibid.*, considérant 71, art. 4, para. 4, et art. 22.

607 Groupe de travail « Article 29 », *Guidelines on Automated Individual Decision-Making and profiling for the purposes of Regulation 2016/679*, WP 251, 3 octobre 2017, p. 15.

Néanmoins, selon le RGPD, une décision automatisée produisant des effets juridiques ou affectant les personnes de manière significative peut être acceptable lorsqu'elle est nécessaire à la conclusion ou à l'exécution d'un contrat entre le responsable du traitement et la personne concernée ou lorsque la personne concernée a donné son consentement explicite. De même, une décision automatisée est acceptable lorsqu'elle est autorisée par la loi et lorsque les droits et libertés et les intérêts légitimes de la personne concernée sont dûment sauvegardés[608].

Le RGPD prévoit également que, parmi les obligations du responsable du traitement concernant les informations à fournir lorsque des données à caractère personnel sont collectées, figure celle d'informer les personnes concernées de l'existence de décisions automatisées, y compris le profilage[609]. Le droit d'accès aux données à caractère personnel traitées par le responsable du traitement n'en est pas affecté[610]. Non seulement les informations devraient mentionner le fait qu'un profilage aura lieu, mais elles devraient également contenir des informations utiles sur la logique sous-jacente du profilage et sur les conséquences prévues de ce traitement pour les personnes concernées[611]. Par exemple, une compagnie d'assurance maladie appliquant des décisions automatisées aux demandes devrait fournir aux personnes concernées des informations générales sur la manière dont fonctionne l'algorithme et sur les facteurs qu'il utilise pour calculer leur prime d'assurance. De la même façon, en exerçant leur « droit d'accès », les personnes concernées peuvent demander des informations au responsable du traitement sur l'existence de décisions automatisées, ainsi que des informations utiles sur la logique qui les sous-tend[612].

Les informations fournies aux personnes concernées ont pour but d'accroître la transparence et de permettre à ces dernières de donner un consentement éclairé, le cas échéant, ou d'obtenir une intervention humaine. Le responsable du traitement est tenu de mettre en œuvre des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée. Ceci inclut, au moins, le droit d'obtenir une intervention humaine de la part du responsable du traitement et la possibilité pour la personne concernée d'exprimer son point de vue et de contester une décision fondée sur le traitement automatisé de ses données personnelles[613].

608 RGPD, art. 22, para. 2.

609 *Ibid.* art. 12.

610 *Ibid.* art. 15.

611 *Ibid.* art. 13, para. 2, point f).

612 *Ibid.* art. 15, para. 1, point h).

613 *Ibid.* art. 22, para. 3.

Le Groupe de travail « Article 29 » a élaboré d'autres orientations sur l'utilisation de décisions automatisées dans le contexte du RGPD[614].

Dans le droit du CdE, les personnes ont le droit de ne pas être soumises à une décision les affectant de manière significative, qui serait prise uniquement sur le fondement d'un traitement automatisé de données, sans que leur point de vue soit pris en compte[615]. L'obligation de prise en compte du point de vue de la personne concernée lorsqu'une décision est prise exclusivement sur le fondement d'un traitement automatisé implique que cette personne a le droit de contester la décision et devrait être en mesure de contester toute inexactitude dans les données à caractère personnel que le responsable du traitement utilise et l'inadéquation du profil qui lui est appliqué[616]. La personne concernée ne pourra néanmoins pas exercer ce droit si la décision automatisée est prévue par la loi à laquelle le responsable du traitement est soumis et qui prévoit des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée. De plus, les personnes concernées ont le droit de se voir communiquer, à leur demande, le raisonnement qui sous-tend le traitement de données effectué[617]. Le rapport explicatif sur la Convention 108 modernisée donne l'exemple de la notation de crédit. Les personnes concernées devraient avoir le droit de connaître non seulement la décision de notation positive ou négative, mais également la *logique* qui sous-tend le traitement de leurs données personnelles et qui aboutit à la décision d'octroi ou de refus du crédit. « La compréhension de ces éléments contribue à l'exercice effectif d'autres garanties essentielles comme le droit d'opposition et le droit de recours auprès de l'autorité compétente »[618].

La Recommandation sur le profilage, bien qu'elle ne soit pas contraignante, énonce les conditions applicables à la collecte et au traitement de données à caractère personnel dans le cadre du profilage[619]. Elle inclut des dispositions sur la nécessité de veiller à ce que le traitement effectué dans le cadre du profilage soit loyal, licite, proportionné et qu'il poursuive des finalités spécifiques et légitimes. Elle contient

614 Groupe de travail « Article 29 », *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, WP 251, 3 octobre 2017, p. 15.

615 Convention 108 modernisée, art. 9, para. 1, point a).

616 Rapport explicatif sur la Convention 108 modernisée, para. 75.

617 Convention 108 modernisée, art. 9, para. 1, point c).

618 Rapport explicatif sur la Convention 108 modernisée, para. 77.

619 CdE, Recommandation CM/Rec(2010)13 du Comité des Ministres aux États membres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage, 23 novembre 2010, art. 5, para. 5.

également des dispositions sur les informations que le responsable du traitement doit fournir aux personnes concernées. Le principe de la qualité des données, qui impose aux responsables du traitement de prendre des mesures pour corriger les facteurs d'inexactitude des données, limiter les risques d'erreur qu'un profilage peut entraîner et évaluer régulièrement la qualité des données et les algorithmes utilisés, est également mentionné dans la recommandation.

6.2. Voies de recours, responsabilité, sanctions et réparation

Points clés

- Conformément à la Convention 108 modernisée, la législation nationale des Parties contractantes doit prévoir des voies de recours et des sanctions appropriées contre des violations du droit à la protection des données.
- Dans l'UE, le RGPD prévoit des voies de recours pour les personnes concernées en cas de violation de leurs droits ainsi que des sanctions contre les responsables du traitement et les sous-traitants qui enfreignent les dispositions dudit règlement. Il instaure également un droit à réparation et une responsabilité.
  - Les personnes concernées ont le droit d'introduire une réclamation auprès d'une autorité de contrôle pour violation présumée du règlement et ont droit à un recours juridictionnel effectif et à obtenir réparation.
  - Dans l'exercice de leur droit à un recours effectif, les personnes concernées peuvent être représentées par des organisations à but non lucratif actives dans le domaine de la protection des données.
  - Le responsable du traitement ou le sous-traitant est responsable de tout dommage matériel ou moral du fait d'une violation du règlement.
  - Les autorités de contrôle sont compétentes pour imposer des amendes administratives pouvant s'élever jusqu'à 20 000 000 EUR pour des violations des dispositions du règlement ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total, le montant le plus élevé étant retenu.
- Les personnes concernées peuvent, en dernier ressort et sous certaines conditions, saisir la CouEDH de violations de la législation relative à la protection des données.
- Toute personne physique ou morale a le droit porter plainte contre une décision du Comité européen de la protection des données devant la CJUE dans les conditions prévues par les traités.

L'adoption d'instruments légaux ne suffit pas à assurer la protection des données à caractère personnel en Europe. Pour que les règles européennes en matière de protection des données soient efficaces, il convient d'établir des mécanismes permettant aux personnes de dénoncer les violations de leurs droits et de demander réparation pour le dommage subi. Il importe également que les autorités de contrôle aient le pouvoir d'imposer des sanctions effectives, dissuasives et proportionnées en réponse à l'infraction en cause.

Les droits consacrés par la législation relative à la protection des données peuvent être exercés par la personne dont les droits sont menacés ; il s'agira de la personne concernée. Toutefois, d'autres personnes – qui remplissent les conditions nécessaires en vertu du droit national – peuvent également représenter les personnes concernées dans l'exercice de leurs droits. Selon plusieurs législations nationales, les enfants et les personnes intellectuellement déficientes doivent être représentés par leur tuteur[620]. En vertu du droit de l'UE en matière de protection des données, une association, dont l'objet légitime est de promouvoir les droits liés à la protection des données, peut représenter les personnes concernées devant une autorité de contrôle ou une juridiction[621].

6.2.1. Droit d'introduire une réclamation auprès d'une autorité de contrôle

Dans le **droit de l'UE** comme dans celui **du CdE**, les personnes concernées ont le droit d'introduire des demandes et des réclamations auprès de l'autorité de contrôle compétente si elles considèrent que le traitement de données à caractère personnel les concernant n'a pas été effectué conformément à la loi.

La Convention 108 modernisée reconnaît le droit de toute personne concernée de bénéficier de l'assistance d'une autorité de contrôle dans l'exercice de ses droits au titre de la Convention, quelle que soit sa nationalité ou sa résidence[622]. Une demande d'assistance ne peut être rejetée que dans des circonstances exceptionnelles et les personnes concernées ne doivent pas supporter les frais et droits afférents à l'assistance[623].

620 FRA (2015), Manuel de droit européen en matière des droits de l'enfant, Luxembourg, Office des publications ; FRA (2013), La capacité juridique des personnes souffrant de troubles mentaux et des personnes handicapées intellectuelles, Luxembourg, Office des publications.

621 RGPD, art. 80.

622 Convention 108 modernisée, art. 18.

623 *Ibid*., art. 16 et 17.

Des dispositions similaires existent dans le système juridique de l'UE. Le RGPD impose aux autorités de contrôle d'adopter des mesures en vue de faciliter l'introduction de réclamations, telles que la création d'un formulaire de réclamation électronique[624]. La personne concernée peut introduire une réclamation auprès de l'autorité de contrôle dans l'État membre dans lequel se trouve sa résidence habituelle, son lieu de travail ou le lieu où la violation aurait été commise[625]. Les réclamations doivent faire l'objet d'une enquête et l'autorité de contrôle doit informer la personne concernée de l'issue de la procédure[626].

Les violations potentielles par des institutions ou organes de l'UE peuvent être portées à l'attention du Contrôleur européen de la protection des données[627]. En l'absence de réponse du CEPD dans les six mois, la réclamation est réputée avoir été rejetée. Un recours contre une décision du CEPD peut être formé devant la CJUE au titre du Règlement (CE) nº 45/2001, qui impose aux institutions et organes de l'UE l'obligation de se conformer aux règles relatives à la protection des données.

Il doit exister une possibilité de recours juridictionnel contre les décisions d'une autorité nationale de contrôle. Ceci s'applique tant aux personnes concernées qu'aux responsables du traitement et aux sous-traitants qui ont été parties à une procédure devant une autorité de contrôle.

Exemple : en septembre 2017, l'autorité espagnole de protection des données a infligé une amende à Facebook pour violation de plusieurs règlements relatifs à la protection des données. L'autorité de contrôle a condamné le réseau social pour avoir collecté, stocké et traité des données à caractère personnel, y compris des catégories particulières de données à caractère personnel, à des fins publicitaires et sans obtenir le consentement des personnes concernées. La décision était fondée sur une enquête menée à l'initiative de l'autorité de contrôle.

624 RGPD, art. 57, para. 2.

625 *Ibid.*, art. 77, para. 1.

626 *Ibid.*, art. 77, para. 2.

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

6.2.2. Droit à un recours juridictionnel effectif

Outre le droit d'introduire une réclamation devant l'autorité de contrôle, toute personne doit avoir droit à un recours juridictionnel effectif et à porter l'affaire devant un tribunal. Le droit à un recours juridictionnel est bien ancré dans la tradition juridique européenne et est reconnu comme un droit fondamental à la fois par l'article 47 de la Charte des droits fondamentaux de l'UE et par l'article 13 de la CEDH[628].

Dans le droit de l'UE, l'importance de mettre à la disposition des personnes concernées des voies de recours juridictionnel effectif en cas de violation de leurs droits ressort clairement à la fois des dispositions du RGPD – qui établit un droit à un recours juridictionnel effectif contre les autorités de contrôle, les responsables du traitement et les sous-traitants – et de la jurisprudence de la CJUE.

Exemple : dans l'affaire *Schrems*[629], la CJUE a déclaré nulle la décision d'adéquation relative à la sphère de sécurité. Cette décision avait autorisé les transferts internationaux de données de l'UE vers des organisations établies aux États-Unis et ayant autocertifié leur adhésion au système de la sphère de sécurité. La CJUE a considéré que ce système présentait plusieurs lacunes, qui compromettaient les droits fondamentaux des citoyens de l'UE à la protection de la vie privée, à la protection des données à caractère personnel et au droit à un recours juridictionnel effectif.

Sur la violation des droits au respect de la vie privée et à la protection des données, la CJUE a souligné que la législation américaine autorisait certaines autorités publiques à accéder aux données à caractère personnel transférées des États membres vers les États-Unis et à les traiter d'une manière incompatible avec les finalités initiales du transfert et au-delà de ce qui était strictement nécessaire et proportionné pour la protection de la sécurité nationale. Sur le droit à un recours effectif, elle a relevé que les personnes concernées ne disposaient d'aucune voie de recours administratif ou judiciaire leur permettant d'accéder aux données les concernant ou à les faire rectifier ou effacer, selon le cas. La CJUE a conclu qu'une réglementation ne prévoyant aucune possibilité pour le justiciable d'exercer des voies de droit afin d'avoir accès à des données à caractère personnel le concernant,

628 Voir, par exemple, CouEDH, *Karabeyoğlu c. Turquie*, nº 30083/10, 7 juin 2016 ; CouEDH, *Mustafa Sezgin Tanrıkulu c. Turquie*, nº 27473/06, 18 juillet 2017.

629 CJUE, C-362/14, *Maximillian Schrems c. Data Protection Commissioner* [GC], 6 octobre 2015.

ou d'obtenir la rectification ou la suppression de celles-ci, « ne respecte pas le contenu essentiel du droit fondamental à une protection juridictionnelle effective, tel que consacré à l'article 47 de la Charte ». Elle a souligné que l'existence d'un recours juridictionnel garantissant le respect de la réglementation est inhérente à l'État de droit.

Les personnes physiques, les responsables du traitement ou les sous-traitants qui souhaitent contester une décision juridiquement contraignante d'une autorité de contrôle peuvent intenter une action devant un tribunal[630]. Le terme « décision » doit être interprété au sens large et couvrir l'exercice par les autorités de contrôle de leurs pouvoirs d'investigation, de sanction et d'autorisation ainsi que les décisions de rejet d'une réclamation. Toutefois, des mesures juridiquement non contraignantes, telles que des avis rendus par l'autorité de contrôle, ne sauraient faire l'objet d'une action devant un tribunal[631]. L'action doit être intentée devant les juridictions de l'État membre sur le territoire duquel l'autorité de contrôle compétente est établie[632].

Lorsqu'un responsable du traitement ou un sous-traitant viole les droits d'une personne concernée, les personnes concernées ont le droit d'intenter une action devant un tribunal[633]. S'agissant des actions intentées contre un responsable du traitement ou un sous-traitant, il est particulièrement important que les personnes concernées puissent choisir où elles engagent l'action. Elles peuvent choisir de le faire dans l'État membre dans lequel le responsable du traitement ou le sous-traitant dispose d'un établissement ou dans l'État membre dans lequel elles ont leur résidence habituelle[634]. Cette seconde possibilité permet aux personnes concernées d'exercer plus facilement leurs droits, étant donné qu'elles peuvent ainsi intenter une action dans l'État où elles résident et devant une juridiction qu'elles connaissent. Limiter l'endroit où une action peut être engagée contre un responsable du traitement ou un sous-traitant à l'État membre dans lequel il dispose d'un établissement pourrait dissuader les personnes concernées résidant dans un autre État membre d'intenter une action en justice, car cela impliquerait des déplacements et des frais supplémentaires et la procédure pourrait se dérouler dans une langue étrangère et devant une juridiction étrangère. La seule exception concerne les cas où le responsable du traitement ou le sous-traitant sont des autorités publiques et où le traitement est effectué dans

630 RGPD, art. 78.

631 *Ibid.*, considérant 143.

632 *Ibid.*, art. 78, para. 3.

633 *Ibid.*, art. 79.

634 *Ibid.*, art. 79, para. 2.

l'exercice de leurs prérogatives de puissance publique. Dans ce cas, seules sont compétentes les juridictions de l'État de l'autorité publique concernée[635].

Si, dans la plupart des cas, les affaires relatives aux règles en matière de protection des données sont tranchées devant les juridictions nationales, elles peuvent parfois être portées devant la CJUE. Dans le premier scénario, une personne concernée, un responsable du traitement, un sous-traitant ou une autorité de contrôle engage un recours en annulation contre une décision du Comité européen de la protection des données. Ce recours est toutefois soumis aux conditions prévues à l'article 263 du TFUE, ce qui implique que pour qu'il soit recevable, ces personnes et entités doivent démontrer que la décision du Comité les affecte directement et individuellement.

Le second scénario concerne les cas où des institutions ou organes de l'UE traitent des données à caractère personnel de manière illicite. Lorsque des institutions de l'UE violent la législation relative à la protection des données, les personnes concernées peuvent saisir directement le Tribunal de l'Union européenne (cette instance fait partie de la CJUE). En première instance, le Tribunal est compétent pour connaître des réclamations concernant des violations du droit de l'Union par des institutions de l'UE. Les réclamations dirigées contre le CEPD en tant qu'institution de l'UE peuvent donc également être portées devant le Tribunal[636].

Exemple : dans l'affaire *Bavarian Lager*[637], la société 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 en invoquant des intérêts prépondérants prévalant sur la protection des données[638]. Bavarian Lager a formé un recours contre cette décision devant le Tribunal de première instance (prédécesseur du Tribunal de l'Union européenne), en application de l'article 32 du Règlement relatif à la protection des données des institutions de l'UE. Dans sa décision (T-194/04, *Bavarian Lager Co. Ltd c. Commission des Communautés européennes*), le Tribunal de première instance a annulé la décision de la Commission rejetant

635 *Ibid*.

636 Règlement (CE) nº 45/2001, art. 32, para. 3.

637 CJUE, C-28/08 P, *Commission européenne c. The Bavarian Lager Co. Ltd* [GC], 2010.

638 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.

la demande d'accès. La Commission européenne a formé un recours contre cette décision devant la CJUE.

La Cour de justice (grande chambre) a annulé l'arrêt du Tribunal de première instance et a confirmé le rejet par la Commission européenne de la demande d'accès au procès-verbal complet de la réunion afin de protéger les données à caractère personnel des personnes présentes à la réunion. La CJUE a considéré que la Commission était fondée à refuser de divulguer ces informations, étant donné que les participants n'avaient pas consenti à la divulgation de leurs données à caractère personnel. En outre, Bavarian Lager n'avait pas démontré la nécessité d'accéder à ces informations.

Enfin, les personnes concernées, les autorités de contrôle, les responsables du traitement ou les sous-traitants peuvent, dans une procédure nationale, demander à la juridiction nationale de saisir la CJUE afin de clarifier l'interprétation et la validité des actes des institutions, organes, organismes ou agences de l'UE. Ces clarifications sont connues sous le nom de « décisions préjudicielles ». Il ne s'agit pas d'une voie de recours directe pour le plaignant, mais elle permet aux juridictions nationales de s'assurer qu'elles interprètent correctement le droit de l'UE. C'est par le biais de demandes de décisions préjudicielles que des affaires comme *Digital Rights Ireland* et *Kärntner Landesregierung et autres*[639] ou *Schrems*[640], qui font autorité et ont fortement influencé l'évolution du droit de l'UE en matière de protection des données, ont atteint la CJUE.

Exemple : *Digital Rights Ireland* et *Kärntner Landesregierung et autres*[641] étaient des affaires jointes présentées par la Haute Cour irlandaise et la Cour constitutionnelle autrichienne concernant la conformité de la Directive 2006/24/CE (Directive relative à la conservation des données) avec le droit de l'UE en matière de protection des données. 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 au regard des articles 7, 9 et 11 de la Charte des droits fondamentaux de l'UE. Parmi ces questions figurait celle de savoir si certaines dispositions de la loi fédérale autrichienne sur les

639 CJUE, affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources et autres* et *Kärntner Landesregierung et autres* [GC], 8 avril 2014.

640 CJUE, C-362/14, *Maximillian Schrems c. Data Protection Commissioner* [GC], 6 octobre 2015.

641 CJUE, affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources et autres et Kärntner Landesregierung et autres* [GC], 8 avril 2014.

télécommunications transposant la Directive relative à la conservation des données étaient incompatibles avec certains aspects de l'ancienne Directive relative à la protection des données et au Règlement relatif à la protection des données des institutions de l'UE.

Dans l'affaire *Kärtner Landesregierung et autres*, M. Seitlinger, l'un des requérants dans la procédure devant la Cour constitutionnelle, a indiqué utiliser le téléphone, internet, ainsi que le courriel pour un usage à la fois professionnel et privé. Par conséquent, les informations qu'il envoyait et recevait passaient sur les réseaux de télécommunications publics. La loi autrichienne sur les télécommunications de 2003 imposait à son fournisseur de services de télécommunication de collecter et d'enregistrer des données sur son utilisation du réseau. M. Seitlinger considérait que cette collecte et cette sauvegarde de ses données à caractère personnel n'étaient pas techniquement nécessaires aux fins de transmettre et recevoir des informations à travers le réseau. En outre, la collecte et le stockage de ces données n'étaient pas non plus nécessaires à des fins de facturation. M. Seitlinger a déclaré ne pas avoir consenti à cette utilisation de ses données à caractère personnel, qui n'étaient collectées et stockées qu'en application de 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 des droits fondamentaux de l'UE. Étant donné que la législation autrichienne transposait la législation de l'UE (la Directive relative à la conservation des données de l'époque), la Cour constitutionnelle autrichienne a saisi la CJUE et lui a demandé de se prononcer sur la compatibilité de la directive avec les droits à la vie privée et à la protection des données consacrés par la Charte des droits fondamentaux de l'UE.

La grande chambre de la CJUE s'est prononcée sur l'affaire en annulant la Directive européenne relative à la conservation des données. La CJUE a jugé que la directive constituait une ingérence particulièrement grave dans les droits fondamentaux au respect de la vie privée et à la protection des données, qui n'était pas limitée au strict nécessaire. La directive poursuivait un objectif légitime en permettant aux autorités nationales de disposer de possibilités supplémentaires d'enquête et de poursuite des infractions

graves et constituait donc un instrument utile pour les enquêtes pénales. La CJUE a toutefois observé que les limitations des droits fondamentaux ne devaient s'appliquer que si elles étaient strictement nécessaires et devaient être assorties de règles claires et précises concernant leur portée, ainsi que de garanties pour les individus.

De l'avis de la Cour, la directive ne répondait pas à ce critère de nécessité. Pour commencer, elle n'a pas établi de règles claires et précises limitant la portée de l'ingérence. Plutôt que d'exiger un lien entre les données conservées et des infractions graves, la directive s'appliquait à toutes les données relatives au trafic de tous les utilisateurs de tous les moyens de communication électronique. Elle comportait donc une ingérence dans les droits au respect de la vie privée et à la protection des données de la quasi-totalité de la population de l'UE. Elle ne prévoyait aucun critère permettant de limiter le nombre de personnes disposant d'une autorisation d'accès aux données à caractère personnel et cet accès n'était pas soumis à des conditions procédurales, telles qu'un contrôle préalable effectué par une juridiction ou une autorité administrative. Enfin, la directive ne prévoyait pas de garanties claires pour la protection des données conservées. Elle n'assurait donc pas une protection effective des données contre les risques d'abus ni contre tout accès et toute utilisation illicites de ces données[642].

En principe, la CJUE doit répondre aux questions qui lui sont posées et ne peut 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[643]. La CJUE ne rend une décision que sur les éléments constitutifs de la demande de décision préjudicielle et la juridiction nationale reste compétente pour statuer sur l'affaire initiale[644].

Dans le droit du CdE, les Parties contractantes doivent établir des recours juridictionnels et non juridictionnels visant les violations des dispositions de la Convention 108

642 CJUE, affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources et autres* et *Kärntner Landesregierung et autres* [GC], 8 avril 2014, point 69.

643 CJUE, C-244/80, *Pasquale Foglia c. Mariella Novello (n° 2)*, 16 décembre 1981 ; CJUE, C-467/04, *Procédure pénale c. Gasparini et autres*, 28 septembre 2006.

644 CJUE, C-438/05, *International Transport Workers' Federation, Finnish Seamen's Union c. Viking Line ABP, Ou Viking Line Eesti* [GC], 11 décembre 2007, point 85.

modernisée[645]. Les violations des droits à la protection des données, prétendument intervenues dans un État contractant à la CEDH et constituant 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. L'invocation d'une violation de l'article 8 de la CEDH devant la CouEDH doit également satisfaire à d'autres critères de recevabilité (articles 34 et 35 de la CEDH)[646].

Bien que les requêtes introduites devant la CouEDH puissent être directement dirigées contre des Parties contractantes, elles peuvent aussi porter indirectement sur des actions ou des omissions de particuliers, pour autant qu'une Partie contractante n'ait pas honoré ses obligations positives en vertu de la CEDH et n'ait pas apporté de protection suffisante contre des violations des droits de la protection des données dans le droit national.

Exemple : dans l'affaire *K.U. c. Finlande*[647], le requérant était un enfant qui se plaignait qu'une publicité à caractère sexuel le concernant avait été publiée sur un site de rencontres en ligne. Le fournisseur de services n'a pas divulgué l'identité de la personne qui avait publié les informations, en raison de l'obligation de confidentialité imposée par la législation finlandaise. Le requérant affirmait que le droit finlandais ne prévoyait pas de protection suffisante contre de telles actions d'un particulier plaçant des informations compromettantes concernant 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, la protection pratique et effective de ce dernier nécessitait l'adoption de mesures efficaces pour identifier et poursuivre l'auteur. Or, l'État n'avait pas offert une telle protection et la CouEDH a conclu qu'il y avait eu une violation de l'article 8 de la CEDH.

Exemple : dans l'affaire *Köpke c. Allemagne*[648], la requérante était soupçonnée de vol sur son lieu de travail et avait donc fait l'objet d'une surveillance vidéo discrète. La CouEDH a conclu que « rien n'indiquait que

645 Convention 108 modernisée, art. 12.

646 CEDH, articles 34 à 37.

647 CouEDH, *K.U. c. Finlande*, nº 2872/02, 2 décembre 2008.

648 CouEDH, *Köpke c. Allemagne* (déc.), nº 420/07, 5 octobre 2010.

les autorités nationales eussent échoué à 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 de ses droits de 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 constate qu'une Partie contractante a violé l'un des droits protégés par la CEDH, cette Partie est tenue d'exécuter la décision de la CouEDH (article 46 de la CEDH). 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 juste satisfaction au requérant aux dépens de la Partie contractante.

Droit de mandater un organisme, une organisation ou une association à but non lucratif

Le RGPD autorise toute personne introduisant une réclamation auprès d'une autorité de contrôle ou intentant une action devant un tribunal à mandater un organisme, une organisation ou une association à but non lucratif pour la représenter[649]. Ces entités à but non lucratif doivent avoir des objectifs statutaires d'intérêt public et être actives dans le domaine de la protection des données. Elles peuvent introduire la réclamation ou exercer le droit à un recours juridictionnel au nom de la personne concernée. Le règlement permet aux États membres de décider, conformément à leur droit national, si un organisme peut introduire une réclamation au nom de personnes concernées sans être mandaté par celles-ci.

Ce droit de représentation permet aux particuliers de bénéficier de l'expertise et de la capacité organisationnelle et financière de ces entités à but non lucratif, ce qui facilite grandement l'exercice de leurs droits. Le RGPD autorise ces entités à intenter des actions collectives au nom de multiples personnes concernées. Cette approche

649 RGPD, art. 80.

est également bénéfique pour le fonctionnement et l'efficacité du système judiciaire, dans la mesure où des réclamations similaires sont jointes et examinées ensemble.

6.2.3. Responsabilité et droit à réparation

Le droit à un recours effectif doit permettre aux particuliers de demander réparation pour tout dommage subi du fait du traitement de leurs données à caractère personnel d'une manière contraire à la législation en vigueur. Le RGPD reconnaît explicitement la responsabilité du responsable du traitement et du sous-traitant dans le traitement illicite[650]. Il donne aux particuliers le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du dommage matériel ou moral subi, tandis que ses considérants précisent que « la notion de dommage devrait être interprétée au sens large, à la lumière de la jurisprudence de la Cour de justice, d'une manière qui tienne pleinement compte des objectifs du présent règlement »[651]. Les responsables du traitement sont tenus responsables et peuvent être visés par des demandes d'indemnisation s'ils ne se conforment pas aux obligations que leur impose le règlement. Un sous-traitant n'est tenu pour responsable du dommage causé par le traitement que s'il n'a pas respecté les obligations prévues par le règlement qui incombent spécifiquement aux sous-traitants ou s'il n'a pas respecté les instructions licites du responsable du traitement. Lorsqu'un responsable du traitement ou un sous-traitant a réparé totalement le dommage subi, le RGPD prévoit que le responsable du traitement ou le sous-traitant est en droit de réclamer auprès des autres responsables du traitement ou sous-traitants ayant participé au même traitement la part de la réparation correspondant à leur part de responsabilité dans le dommage[652]. Dans le même temps, les exonérations de responsabilité sont très strictes et il doit être démontré que le responsable du traitement ou le sous-traitant n'est nullement responsable de l'événement ayant provoqué le dommage.

La réparation doit être « complète et effective » par rapport au dommage subi. Lorsque le dommage est causé par le traitement de plusieurs responsables du traitement et sous-traitants, chacun doit être tenu responsable de l'ensemble du dommage. Cette règle tend à assurer une réparation effective aux personnes concernées et une approche coordonnée de la conformité par les responsables du traitement et les sous-traitants participant aux activités de traitement.

650 *Ibid.*, art. 82.

651 *Ibid.*, considérant 146.

652 *Ibid.*, art. 82, paras. 2 et 5.

Exemple : les personnes concernées ne sont pas tenues d'intenter une action et de demander réparation auprès de toutes les entités responsables du dommage car cela pourrait entraîner des procédures longues et coûteuses. Il suffit d'engager une action contre l'un des responsables conjoints du traitement, qui peut alors être tenu responsable de l'ensemble du dommage. Dans un tel cas, un responsable du traitement ou un sous-traitant qui paie le dommage est ensuite en droit de récupérer le montant payé auprès des autres entités ayant participé au traitement et responsables de la violation à hauteur de leur part de responsabilité pour le dommage causé. Ces procédures entre les différents responsables conjoints du traitement et sous-traitants ont lieu après que la personne concernée a été indemnisée et cette dernière n'y prend pas part.

Dans le système juridique du CdE, l'article 12 de la Convention 108 modernisée exige des Parties contractantes qu'elles établissent des recours appropriés visant les violations du droit national mettant en œuvre les dispositions de la Convention. Le rapport explicatif sur la Convention 108 modernisée précise que les recours doivent prévoir la possibilité de contester par voie juridictionnelle une décision ou une pratique et que des recours non juridictionnels doivent également être mis à la disposition des personnes concernées[653]. Les modalités et les différentes règles relatives à l'accès à ces recours ainsi que la procédure à suivre sont laissées à l'appréciation de chaque Partie contractante. Les Parties contractantes et les juridictions nationales devraient également envisager une indemnisation financière pour les dommages matériels et moraux provoqués par le traitement, ainsi que des recours collectifs[654].

6.2.4. Sanctions

Dans le droit du CdE, l'article 12 de la Convention 108 modernisée dispose que des sanctions et recours appropriés doivent être établis par chaque Partie contractante concernant les violations des dispositions du droit interne donnant effet aux principes de base pour la protection des données énoncés dans la Convention 108. La Convention n'établit ni n'impose un ensemble particulier de sanctions. Au contraire, elle indique clairement que chaque Partie contractante a tout pouvoir d'appréciation pour déterminer la nature des sanctions juridictionnelles et non juridictionnelles, qui peuvent être de nature pénale, administrative ou civile. Le rapport explicatif sur la Convention 108 modernisée précise que les sanctions doivent être

653 Rapport explicatif sur la Convention 108 modernisée, para. 100.

654 *Ibid.*

effectives, proportionnées et dissuasives[655]. Les Parties doivent respecter ce principe lorsqu'elles déterminent la nature et la sévérité des sanctions disponibles dans leur ordre juridique interne.

Dans le droit de l'UE, l'article 83 du RGPD confère aux autorités de contrôle des États membres le pouvoir d'imposer des amendes administratives pour des violations du règlement. Le niveau des amendes et les circonstances que les autorités nationales prennent en compte pour décider s'il y a lieu d'imposer une amende, ainsi que pour déterminer le montant maximal de celle-ci, sont également prévus à l'article 83. Le régime de sanctions est donc harmonisé dans l'ensemble de l'Union.

Le RGPD prévoit une approche progressive en matière d'amendes. Les autorités de contrôle peuvent imposer pour des violations du règlement des amendes administratives dont le montant peut s'élever jusqu'à 20 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 4 % de son chiffre d'affaires annuel mondial total, le montant le plus élevé étant retenu. Les violations susceptibles de justifier un tel niveau d'amende sont, notamment, des violations des principes de base d'un traitement et les conditions applicables au consentement, les violations des droits des personnes concernées et les violations des dispositions du règlement qui régissent le transfert de données à caractère personnel à un destinataire situé dans un pays tiers. Pour d'autres violations, les autorités de contrôle peuvent imposer des amendes pouvant s'élever jusqu'à 10 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 2 % de son chiffre d'affaires annuel mondial total, le montant le plus élevé étant retenu.

Lorsqu'elles déterminent le type et le montant de l'amende, les autorités de contrôle doivent tenir compte d'une série de facteurs[656]. Elles doivent ainsi dûment tenir compte de la nature, de la gravité et de la durée de la violation, des catégories de données à caractère personnel concernées et du fait que la violation a été commise délibérément ou par négligence. Lorsqu'un responsable du traitement ou un sous-traitant a pris des mesures pour atténuer le dommage subi par les personnes concernées, cet élément doit également être pris en compte. De même, le degré de coopération établi avec l'autorité de contrôle à la suite de la violation et la manière dont l'autorité de contrôle a eu connaissance de celle-ci (par exemple, si elle a été signalée par l'entité responsable du traitement ou par une personne concernée dont

655 *Ibid*.

656 RGPD, art. 83, para. 2.

les droits ont été violés) sont d'autres facteurs importants qui guident les autorités de contrôle dans leur décision[657].

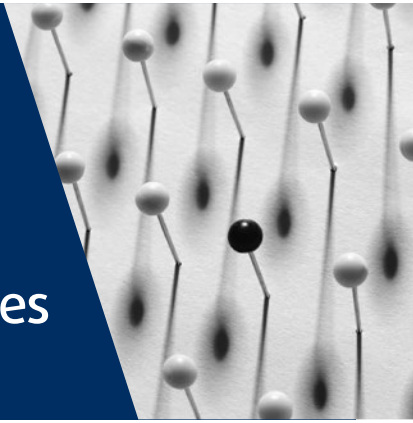
Outre la capacité d'imposer des amendes administratives, les autorités de contrôle disposent d'un large arsenal d'autres mesures correctrices. Les mesures « correctrices » que peuvent adopter les autorités de contrôle sont énumérées à l'article 58 du RGPD. Elles vont d'ordres, d'avertissements et de réprimandes aux responsables du traitement et aux sous-traitants à l'imposition d'interdictions temporaires, voire permanentes, des activités de traitement.

S'agissant des sanctions en cas de violations du droit de l'Union par des institutions ou des organismes de l'UE, étant donné la portée spécifique du Règlement relatif à la protection des données des institutions de l'UE, des sanctions peuvent prendre la forme de mesures disciplinaires. Conformément à l'article 49 de ce règlement, « tout manquement aux obligations auxquelles un 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 [...] ».

657 Groupe de travail « Article 29 », Lignes directrices sur l'application et la fixation des amendes administratives aux fins du règlement (UE) 2016/679, WP 253, 3 octobre 2017.

7

Transferts et flux transfrontières de données à caractère personnel



UE	Questions traitées	CdE
Transferts de données à caractère personnel		
RGPD, art. 44	Concept	Convention 108 modernisée, art. 14, paras. 1 et 2
Libre circulation de données à caractère personnel		
RGPD, art. 1er, para. 3, etconsidérant 170	Entre les États membres de l'UE	
	Entre les Parties contractantes à la Convention 108	Convention 108 modernisée, art. 14, para. 1
Transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales		
RGPD, art. 45 C-362/14, *Maximillian Schrems c. Data Protection Commissioner* [GC], 2015	Décision d'adéquation/pays tiers ou organisations internationales offrant un niveau de protection adéquat	Convention 108 modernisée, art. 14, para. 2
RGPD, art. 46, paras. 1 et 2	Garanties appropriées, y compris droits opposables et recours juridictionnels des personnes concernées, découlant de clauses contractuelles types, de règles d'entreprise contraignantes, de codes de conduite et de mécanismes de certification	Convention 108 modernisée, art. 14, paras. 2, 3, 5 et 6
RGPD, art. 46, para. 3	Sous réserve de l'autorisation de l'autorité de contrôle compétente : clauses contractuelles et dispositions contenues dans les arrangements administratifs entre autorités publiques	

UE	Questions traitées	CdE
RGPD, art. 46, para. 5	Autorisations existantes fondées sur la Directive 95/46/CE	
RGPD, art. 47	Règles d'entreprise contraignantes	
RGPD, art. 49	Dérogations pour situations particulières	Convention 108 modernisée, art. 14, para. 4
Exemples : Accord PNR UE-États-Unis Accord SWIFT UE-États-Unis	Accords internationaux	Convention 108 modernisée, art. 14, para. 3, point a)

Dans le droit de l'UE, le Règlement général sur la protection des données prévoit la libre circulation des données au sein de l'Union européenne. Il contient toutefois des exigences spécifiques concernant le transfert de données à caractère personnel vers des pays tiers en dehors de l'UE et à des organisations internationales. Le règlement reconnaît l'importance de ces transferts, notamment en raison de la coopération et du commerce internationaux, mais il reconnaît aussi le risque accru pour les données à caractère personnel. Il vise donc à offrir le même niveau de protection aux données à caractère personnel qui sont transférées vers des pays tiers que celui dont elles bénéficient dans l'UE[658]. Le droit du CdE reconnaît lui aussi l'importance de la mise en œuvre de règles pour les flux transfrontières de données entre les parties et prévoit des exigences spécifiques pour les transferts vers des États tiers.

7.1. Nature des transferts de données à caractère personnel

Points clés

- Le droit de l'UE et le droit du CdE contiennent des règles relatives aux transferts de données à caractère personnel vers des destinataires situés dans des pays tiers ou à des organisations internationales.
- La sauvegarde des droits des personnes concernées en cas de transfert de leurs données en dehors de l'UE permet à la protection conférée par le droit de l'UE de rester attachée aux données à caractère personnel en provenance de l'Union.

658 RGPD, considérants 101 et 116.

Dans **le droit du CdE**, les flux transfrontières de données sont définis comme le transfert de données à caractère personnel vers un destinataire qui est soumis à une juridiction étrangère[659]. Les flux transfrontières de données vers un destinataire qui ne relève pas de la juridiction d'une Partie contractante ne sont autorisés que s'ils offrent un niveau de protection approprié[660].

Le droit de l'UE régit le « transfert, vers un pays tiers ou à une organisation internationale, de données à caractère personnel qui font ou sont destinées à faire l'objet d'un traitement après ce transfert [...] »[661]. Ces flux de données ne sont autorisés que s'ils sont conformes aux règles énoncées au chapitre V du RGPD.

Les flux transfrontières de données à caractère personnel sont autorisés vers un destinataire qui relève de la juridiction d'une Partie contractante ou d'un État membre au titre du droit du CdE ou du droit de l'UE, respectivement. Les deux systèmes juridiques permettent le transfert de données vers un pays qui n'est pas une Partie contractante ou un État membre, sous certaines conditions.

7.2. Libre circulation/flux de données à caractère personnel entre États membres ou Parties contractantes

Points clés

- Les flux de données à caractère personnel à l'intérieur de l'UE tout comme les transferts de données à caractère personnel entre les Parties contractantes à la Convention 108 modernisée doivent être libres de toutes restrictions. Or, toutes les Parties contractantes à la Convention 108 modernisée n'étant pas des États membres de l'UE, les transferts d'un État membre de l'UE vers un pays tiers qui est, néanmoins, Partie à la Convention 108, ne sont possibles que s'ils satisfont aux conditions établies par le RGPD.

Dans le droit du CdE, les données à caractère personnel doivent circuler librement entre les Parties contractantes à la Convention 108 modernisée. Cependant, le transfert peut être interdit « lorsqu'il existe un risque réel et sérieux que le transfert à une

659 Rapport explicatif sur la Convention 108 modernisée, para. 102.

660 Convention 108 modernisée, art. 14, para. 2.

661 RGPD, art. 44.

autre Partie, ou de cette autre Partie à une non-Partie, conduise à contourner les dispositions de la Convention » ou si une Partie est « tenue de respecter des règles de protection harmonisées communes à des États appartenant à une organisation internationale régionale »[662].

Dans le droit de l'UE, la libre circulation des données à caractère personnel entre États membres de l'UE n'est ni limitée ni interdite pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel[663]. L'espace de libre circulation des données a été étendu par l'accord sur l'Espace économique européenne (EEE)[664], qui intègre l'Islande, le Liechtenstein et la Norvège dans le marché intérieur.

Exemple : si une filiale 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 limité ou interdit par le droit national slovène pour des motifs liés à la protection des données à caractère personnel.

Mais si la même filiale slovène souhaite transférer les mêmes données à caractère personnel vers la société mère en Malaisie, l'exportateur de données slovène doit prendre en considération les règles du chapitre V du RGPD. Ces dispositions visent à sauvegarder les données à caractère personnel des personnes concernées qui relèvent de la juridiction de l'UE.

Dans le droit de l'UE, les flux de données à caractère personnel vers des États membres de l'EEE à des fins de prévention, d'enquête, de détection ou de poursuites des infractions pénales ou d'exécution de sanctions pénales sont régis par la Directive 2016/680[665]. Cette directive garantit également que l'échange de données

662 Convention 108 modernisée, art. 14, para. 1.

663 RGPD, art. 1er, para. 3.

664 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.

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

à caractère personnel par les autorités compétentes au sein de l'Union ne soit ni limité ni interdit pour des motifs liés à la protection des données. Dans le droit du CdE, le traitement de toutes les données à caractère personnel (y compris leurs flux transfrontières vers d'autres Parties à la Convention 108) relève du champ d'application de ladite Convention, sans exceptions fondées sur des finalités ou des domaines d'activité, bien que les Parties contractantes puissent prévoir des dérogations. Tous les membres de l'EEE sont Parties à la Convention 108.

7.3. Transfert de données à caractère personnel vers des pays tiers/ non-parties ou à des organisations internationales

Points clés

- **Le droit du CdE et celui de l'UE** autorisent le transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales, sous réserve que certaines conditions relatives à la protection desdites données soient remplies.
  - **Dans le droit du CdE**, un niveau de protection approprié peut être prévu par la législation de l'État ou l'organisation internationale ou en mettant en place des normes appropriées.
  - **Dans le droit de l'UE**, des transferts peuvent avoir lieu lorsque le pays tiers assure un niveau de protection adéquat ou lorsque le responsable du traitement ou le sous-traitant prévoit des garanties appropriées, notamment des droits opposables et des voies de recours pour les personnes concernées, à l'aide de moyens tels que des clauses types de protection des données ou des règles d'entreprise contraignantes.
- **Tant le droit du CdE que le droit de l'UE** prévoient des clauses dérogatoires autorisant le transfert de données à caractère personnel dans des cas particuliers, même lorsqu'il n'existe ni un niveau de protection adéquat ni des garanties appropriées.

Si tant le système juridique du CdE que celui de l'UE autorisent les flux de données vers des pays tiers ou des organisations internationales, ils prévoient des conditions différentes. Chaque ensemble de conditions tient compte de la structure et des finalités différentes des organisations respectives.

Dans le droit de l'UE, il existe en principe deux façons d'autoriser le transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales. Les transferts de données à caractère personnel peuvent être effectués sur la base d'une décision d'adéquation adoptée par la Commission européenne[666] ou, en l'absence d'une telle décision, lorsque le responsable du traitement ou le sous-traitant offre des garanties appropriées, y compris des droits opposables et des voies de recours pour la personne concernée[667]. En l'absence d'une décision d'adéquation ou de garanties appropriées, plusieurs dérogations existent.

Dans le droit du CdE en revanche, la libre circulation de données vers des États non Parties à la Convention n'est autorisée que sur la base :

- de la législation de cet État ou de cette organisation internationale, y compris les traités ou accords internationaux applicables offrant des garanties appropriées ou

- des garanties *ad hoc* ou standardisées agréées, établies par des instruments juridiquement contraignants et opposables, conclus et mis en œuvre par les personnes agissant dans le transfert et le traitement ultérieur des données[668].

À l'instar du droit de l'UE, en l'absence d'un niveau de protection des données approprié, plusieurs dérogations existent.

7.3.1. Transferts fondés sur une décision d'adéquation

Dans le droit de l'UE, la libre circulation des données à caractère personnel vers des pays tiers offrant un niveau de protection des données adéquat est prévue à l'article 45 du RGPD. La CJUE a expliqué que l'expression « niveau de protection adéquat » implique que le pays tiers assure un niveau de protection des libertés et droits fondamentaux « substantiellement équivalent »[669] à celui garanti dans l'ordre juridique de l'UE. Dans le même temps, les moyens auxquels ce pays tiers a recours pour assurer un tel niveau de protection peuvent être différents de ceux

666 RGPD, art. 45.

667 *Ibid.*, art. 46.

668 Convention 108 modernisée, art. 14, para. 3, points a) et b).

669 CJUE, C-362/14, *Maximillian Schrems c. Data Protection Commissioner* [GC], 6 octobre 2015, point 96.

mis en œuvre au sein de l'UE, le critère d'adéquation n'exigeant pas une reproduction à l'identique des règles de l'UE[670].

La Commission européenne évalue le niveau de protection des données dans les pays étrangers en examinant leur législation nationale et les obligations internationales applicables. La participation d'un pays à des organisations multilatérales ou régionales, notamment en matière de protection des données à caractère personnel, doit également être prise en compte. Lorsque la Commission européenne considère que le pays tiers ou l'organisation internationale assure un niveau de protection adéquat, elle peut adopter une décision d'adéquation qui a un effet contraignant[671]. Néanmoins, la CJUE a affirmé que les autorités nationales de contrôle restent compétentes pour examiner la demande d'une personne relative à la protection de ses données à caractère personnel qui ont été transférées vers un pays tiers dont la Commission juge qu'il garantit un niveau de protection adéquat, lorsque cette personne fait valoir que le droit et les pratiques en vigueur dans ce pays n'offrent pas la garantie d'un niveau de protection adéquat[672].

La Commission européenne peut également évaluer l'adéquation d'un territoire à l'intérieur d'un pays tiers ou se limiter à des secteurs spécifiques, comme cela a été le cas pour le droit commercial privé du Canada, par exemple[673]. Des décisions d'adéquation portent aussi sur des transferts fondés sur des accords conclus entre l'UE et des pays tiers. Ces décisions concernent exclusivement un type unique de transfert de données, tel que la transmission des dossiers passagers (PNR) d'une compagnie aérienne à des autorités étrangères chargées du contrôle des frontières lorsque les appareils de la compagnie partent de l'UE vers certaines destinations étrangères (voir section 7.3.4).

Les décisions d'adéquation font l'objet d'un suivi permanent. La Commission européenne réexamine régulièrement ces décisions afin de surveiller les évolutions

670 *Ibid.*, point 74. Voir également Commission européenne (2017), Communication de la Commission au Parlement européen et au Conseil – Échange et protection de données à caractère personnel à l'ère de la mondialisation, COM(2017) 7 final du 10 janvier 2017, p. 6.

671 Pour une liste continuellement mise à jour des pays couvert par une décision constatant l'adéquation, voir la page d'accueil de la Commission européenne, Direction générale de la Justice.

672 CJUE, C-362/14, *Maximillian Schrems c. Data Protection Commissioner* [GC], 6 octobre 2015, points 63, 65 et 66.

673 Décision 2002/2/CE de la Commission 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.

qui pourraient porter atteinte aux décisions. Ainsi, lorsque la Commission européenne est d'avis que le pays tiers ou l'organisation internationale ne remplit plus les conditions justifiant la décision d'adéquation, elle peut la modifier, la suspendre ou l'abroger. La Commission peut également engager des négociations avec le pays tiers ou l'organisation internationale en cause en vue de remédier à la situation qui a motivé sa décision.

Les décisions d'adéquation adoptées par la Commission européenne au titre de la Directive 95/46/CE restent en vigueur jusqu'à leur modification, leur remplacement ou leur abrogation par une décision de la Commission adoptée conformément aux règles prévues à l'article 45 du RGPD.

À ce jour, la Commission européenne a reconnu qu'Andorre, l'Argentine, le Canada (organisations commerciales relevant du champ d'application de la loi sur les informations personnelles et les documents électroniques, PIPEDA), les îles Féroé, Guernesey, l'île de Man, Israël, Jersey, la Nouvelle-Zélande, la Suisse et l'Uruguay offraient un niveau de protection adéquat. S'agissant des transferts vers les États-Unis, la Commission a adopté une décision d'adéquation en 2000, qui autorisait les transferts vers des entreprises américaines autocertifiant leur niveau de protection des données à caractère personnel transférées à partir de l'UE et leur respect du principe dit de la « sphère de sécurité »[674]. La CJUE a invalidé cette décision en 2015 et une nouvelle décision d'adéquation a été adoptée en juillet 2016, autorisant les entreprises à y adhérer à partir du 1er août 2016.

Exemple : dans l'affaire *Schrems*[675], Maximilian Schrems, un ressortissant autrichien, était un utilisateur de Facebook depuis plusieurs années. Les données fournies par M. Schrems à Facebook ont été transférées, en tout ou en partie, de la filiale irlandaise de Facebook vers des serveurs situés aux États-Unis, où elles ont fait l'objet d'un traitement. M. Schrems a introduit une plainte devant l'autorité irlandaise chargée de la protection des données, considérant que compte tenu des révélations du lanceur d'alerte américain Edward Snowden sur les activités de surveillance menées par les services de renseignement des États-Unis, la loi et les pratiques en vigueur aux États-Unis

674 Décision 2000/520/CE de la Commission du 26 juillet 2000 conforme à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » et par les questions souvent posées y afférentes, publiés par le ministère du commerce des États-Unis d'Amérique, JO L 215. La décision a été déclarée invalide par la CJUE dans l'affaire C-632/14, *Maximilian Schrems c. Data Protection Commissioner* [GC].

675 CJUE, C-362/14, *Maximillian Schrems c. Data Protection Commissioner* [GC], 6 octobre 2015.

ne garantissaient pas une protection suffisante des données transférées vers ce pays. L'autorité irlandaise a rejeté la réclamation au motif que, dans sa décision du 26 juillet 2000, la Commission a considéré que, dans le cadre du système de la « sphère de sécurité », les États-Unis assurent un niveau de protection adéquat des données à caractère personnel transférées. L'affaire a été portée devant la Haute Cour de justice irlandaise, qui a posé une question préjudicielle à la CJUE.

La CJUE a déclaré invalide la décision de la Commission sur l'adéquation du cadre de la sphère de sécurité. La Cour a tout d'abord observé que la décision autorisait la limitation de l'application des principes de la sphère de sécurité en matière de protection des données par des exigences de sécurité nationale, d'intérêt public ou de respect des lois des États-Unis ainsi que par la législation nationale de ce pays. La décision autorisait donc une ingérence dans les droits fondamentaux des personnes dont les données à caractère personnel étaient ou pouvaient être transférées vers les États-Unis[676]. Elle a par ailleurs observé que la décision ne comportait aucune constatation quant à l'existence, aux États-Unis, de règles destinées à limiter de telles ingérences ou à l'existence d'une protection juridique efficace contre des ingérences de cette nature[677]. La Cour a souligné que le niveau de protection des libertés et droits fondamentaux garanti au sein de l'Union exigeait une réglementation comportant une ingérence dans les articles 7 et 8 de la Charte pour prévoir des règles claires et précises régissant la portée et l'application d'une mesure et imposant un minimum de garanties, de dérogations et de limitations en vue de protéger les données à caractère personnel[678]. Étant donné que la décision de la Commission n'indiquait pas que les États-Unis assurent effectivement un tel niveau de protection en raison de leur législation interne ou de leurs engagements internationaux, la CJUE a conclu qu'elle ne remplissait pas les conditions prévues par la disposition pertinente relative au transfert contenue dans la Directive relative à la protection des données et qu'elle était donc invalide[679].

Le niveau de protection assuré par les États-Unis n'était donc pas « substantiellement équivalent » aux libertés et droits fondamentaux garantis

676 *Ibid.*, point 84.

677 *Ibid.*, points 88 et 89.

678 *Ibid.*, points 91 et 92.

679 *Ibid.*, points 96 et 97.

par l'UE[680]. La CJUE a conclu que plusieurs articles de la Charte des droits fondamentaux de l'UE étaient violés. Premièrement, l'essence de l'article 7 n'a pas été respectée, étant donné que la législation américaine « permettait aux autorités publiques d'accéder de manière généralisée au contenu de communications électroniques ». Deuxièmement, l'essence de l'article 47 a également été violée, étant donné que la législation ne prévoyait pas de recours juridictionnel pour les personnes en ce qui concerne l'accès aux données à caractère personnel, leur rectification ou leur effacement. Enfin, dès lors que le système de la sphère de sécurité violait les articles précités, les données à caractère personnel ne faisaient plus l'objet d'un traitement licite, ce qui a conduit à une violation de l'article 8.

Après que la CJUE eut déclaré l'invalidité de l'accord relatif à la sphère de sécurité, la Commission et les États-Unis ont convenu d'un nouveau cadre, le « bouclier de protection des données » UE-États-Unis (« Privacy Shield »). Le 12 juillet 2016, la Commission a adopté une décision constatant que les États-Unis assurent un niveau de protection adéquat pour les données à caractère personnel transférées de l'Union vers des organisations établies aux États-Unis dans le cadre du « bouclier de protection des données »[681].

Tout comme le système de la sphère de sécurité, le cadre du bouclier de protection des données UE-États-Unis a pour but de protéger les données à caractère personnel qui sont transférées de l'UE vers les États-Unis à des fins commerciales[682]. Les entreprises américaines peuvent autocertifier volontairement qu'elles se conforment à la liste du bouclier de protection des données en s'engageant à respecter les normes du cadre en matière de protection des données. Les autorités américaines compétentes surveillent et contrôlent le respect de ces normes par les entreprises certifiées.

680 *Ibid.*, points 73, 74 et 96.

681 Décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis, JO L 207. Le Groupe de travail « Article 29 » s'est réjoui des améliorations apportées par le mécanisme du bouclier de protection des données par rapport à la Décision sur la sphère de sécurité et a salué le fait que la Commission et les autorités américaines avaient pris en considération dans la version finale du document sur le bouclier de protection des données les préoccupations exprimées dans son avis WP 238 sur le projet de décision d'adéquation sur le bouclier de protection des données UE-États-Unis. Il a toutefois souligné que plusieurs préoccupations demeurent. Pour plus de détails, voir Groupe de travail « Article 29 », *Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision*, adopté le 13 avril 2016, 16/EN WP 238.

682 Pour un complément d'informations, voir la fiche d'information sur le bouclier de protection des données UE-États-Unis.

Le mécanisme du bouclier de protection des données prévoit, notamment :

- des obligations à l'égard de la protection des données pour les entreprises qui reçoivent des données à caractère personnel en provenance de l'UE ;

- une protection et une voie de recours pour les particuliers, notamment l'établissement d'un mécanisme de médiation, indépendant des services de renseignement américains et traitant les plaintes de particuliers qui estiment que leurs données à caractère personnel ont été utilisées de façon illicite par les autorités américaines dans le domaine de la sécurité nationale ;

- un examen annuel conjoint de la mise en œuvre du cadre[683] ; le premier examen a eu lieu en septembre 2017[684].

Le gouvernement des États-Unis a pris des engagements écrits et a fourni des assurances qui accompagnent la décision sur le bouclier de protection des données. Ils prévoient des limitations et des garanties quant à l'accès du gouvernement américain aux données à caractère personnel à des fins répressives et de sécurité nationale.

7.3.2. Transferts moyennant des garanties appropriées

Tant le **droit de l'UE** que le **droit du CdE** reconnaissent que des garanties appropriées entre le responsable du traitement qui exporte les données et le destinataire dans le pays tiers ou l'organisation internationale constituent un moyen potentiel d'assurer un niveau suffisant de protection des données pour le destinataire.

Dans le **droit de l'UE**, le transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale est autorisé lorsque le responsable du traitement ou le sous-traitant offre des garanties appropriées et des droits opposables et lorsque des recours juridiques efficaces sont mis à la disposition des personnes

683 Pour un complément d'informations, voir la page web de la Commission européenne sur le bouclier de protection des données UE-États-Unis.

684 Commission européenne, Rapport de la Commission au Parlement européen et au Conseil sur le premier examen annuel du fonctionnement du bouclier de protection des données UE-États-Unis, COM(2017) 611 final, 18 octobre 2017. Voir également Groupe de travail « Article 29 » (2017), *EU – U.S. Privacy Shield – First annual Joint Review*¸ adopté le 28 novembre 2017, 17/EN WP 255.

concernées[685]. La liste des « garanties appropriées » acceptables figure exclusivement dans la législation de l'UE en matière de protection des données. Des garanties appropriées peuvent être fournies par :

- un instrument juridiquement contraignant et exécutoire entre les autorités ou organismes publics ;
- des règles d'entreprise contraignantes ;
- des clauses types de protection des données adoptées soit par la Commission européenne soit par une autorité de contrôle ;
- des codes de conduite ;
- des mécanismes de certification[686].

Des clauses contractuelles personnalisées entre le responsable du traitement ou le sous-traitant de l'UE et le destinataire des données dans un pays tiers sont un autre moyen d'offrir des garanties appropriées. De telles clauses contractuelles doivent, toutefois, être admises par l'autorité de contrôle compétente avant de pouvoir être utilisées comme instrument pour le transfert de données à caractère personnel. De manière similaire, les autorités publiques peuvent recourir aux dispositions relatives à la protection des données qui figurent dans leurs arrangements administratifs, pour autant que l'autorité de contrôle les ait autorisées[687].

Dans le **droit du CdE**, les flux de données vers un État ou une organisation internationale qui n'est pas Partie à la Convention 108 modernisée sont autorisés à condition qu'un niveau de protection approprié soit garanti. Il peut être garanti par :

- les règles de droit de cet État ou de cette organisation internationale ; ou
- des garanties *ad hoc* ou standardisées, incluses dans un instrument juridiquement contraignant[688].

685 RGPD, art. 46.

686 RGPD, art. 46, para. 1, points c) et d), art. 46, para. 2, points a), b), e) et f), et art. 47.

687 *Ibid.*, art. 46, para. 3.

688 Convention 108 modernisée, art. 14, para. 3, point b).

Transferts soumis à des clauses contractuelles

Tant le **droit de l'UE** que le **droit du CdE** reconnaissent que des clauses contractuelles convenues entre le responsable du traitement qui exporte les données et le destinataire dans le pays tiers constituent un moyen potentiel d'assurer un niveau suffisant de protection des données pour le destinataire[689].

Au niveau de l'UE, la Commission européenne, avec l'aide du Groupe de travail « Article 29 », a élaboré des clauses types de protection des données qui ont été officiellement certifiées par une décision de la Commission comme preuve d'une protection adéquate des données[690]. Les décisions de la Commission étant contraignantes dans leur intégralité dans les États membres, les autorités nationales qui contrôlent les transferts de données doivent reconnaître ces clauses contractuelles types dans leurs procédures[691]. Par conséquent, si le responsable du traitement qui exporte les données et le destinataire du pays tiers s'accordent et signent de telles clauses, cela doit suffire à démontrer à l'autorité de contrôle que des garanties adéquates existent. Pourtant, dans l'affaire *Schrems*, la CJUE a conclu que la Commission européenne n'est pas compétente pour restreindre les pouvoirs des autorités nationales de contrôle de superviser le transfert de données à caractère personnel vers un pays tiers ayant fait l'objet d'une décision d'adéquation de la Commission[692]. Dès lors, les autorités nationales de contrôle ne sont pas empêchées d'exercer leurs pouvoirs, y compris celui de suspendre ou d'interdire un transfert de données à caractère personnel lorsque celui-ci est contraire au droit de l'UE ou d'un État membre en matière de protection des données, comme, par exemple, lorsque l'importateur des données ne respecte pas les clauses contractuelles types[693].

L'existence de clauses types de protection des données dans le cadre juridique de l'UE n'empêche pas les responsables du traitement de formuler d'autres clauses contractuelles individuelles *ad hoc*, pour autant que l'autorité de contrôle les

689 RGPD, art. 46, para. 3 ; Convention 108 modernisée, art. 14, para. 3, point b).

690 *Ibid*., art. 46, para. 2, point b), et art. 46, para. 5.

691 *Ibid*., art. 46, para. 2, point c) ; TFUE, art. 288.

692 CJUE, C-362/14, *Maximillian Schrems c. Data Protection Commissioner* [GC], 6 octobre 2015, points 96 à 98 et 102 à 105.

693 Pour tenir compte du point de vue de la CJUE dans l'affaire *Schrems*, la CJUE a modifié sa décision sur les clauses contractuelles types. Décision d'exécution (UE) 2016/2297 de la Commission du 16 décembre 2016 modifiant les décisions 2001/497/CE et 2010/87/UE relatives aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers et vers des sous-traitants établis dans ces pays, en vertu de la directive 95/46/CE du Parlement européen et du Conseil, JO 2016 L 344.

autorise[694]. Elles doivent toutefois garantir le même niveau de protection que celui qu'offrent les clauses types de protection des données. Lorsqu'elles approuvent des clauses *ad hoc*, les autorités de contrôle sont tenues d'appliquer le mécanisme de contrôle de la cohérence afin de garantir une approche réglementaire cohérente dans l'ensemble de l'UE[695]. En d'autres termes, l'autorité de contrôle compétente doit transmettre son projet de décision sur les clauses au Comité européen de la protection des données. Le Comité émet un avis sur la question et l'autorité de contrôle doit tenir le plus grand compte de cet avis lorsqu'elle élabore sa décision. Lorsque l'autorité de contrôle n'entend pas suivre l'avis du Comité, le mécanisme de règlement des litiges du Comité est déclenché et il adopte une décision contraignante[696].

Les principales caractéristiques d'une clause contractuelle type sont les suivantes :

- une clause du tiers bénéficiaire qui permet aux personnes concernées d'exercer des droits contractuels même si elles ne sont pas parties à un contrat ;

- le destinataire ou importateur des données accepte de se soumettre à l'autorité de l'autorité nationale de contrôle et/ou aux tribunaux du pays du responsable du traitement exportateur de données en cas de litige.

Il existe désormais deux ensembles de clauses types pour les transferts de responsable du traitement à responsable du traitement entre lesquels l'exportateur des données peut choisir[697]. Pour les transferts de responsable du traitement à sous-traitant, il n'existe qu'un ensemble de clauses contractuelles types[698]. Ces clauses contractuelles types font toutefois actuellement l'objet d'une procédure judiciaire.

694 RGPD, art. 46, para. 3, point a).

695 *Ibid.*, art. 63 et art. 64, para. 1, point e).

696 *Ibid.*, art. 64 et 65.

697 Le premier ensemble de clauses est contenu à l'annexe de la Décision 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 ; le second ensemble est contenu à l'annexe de la 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.

698 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. Au moment de la rédaction du présent manuel, le recours à des clauses contractuelles types comme base des transferts de données à caractère personnel vers les États-Unis faisait l'objet d'une procédure devant la Haute Cour de justice irlandaise.

Exemple : après que la CJUE a invalidé la Décision sur la sphère de sécurité[699], les transferts de données à caractère personnel vers les États-Unis ne pouvaient plus être fondés sur cette décision d'adéquation. Durant les négociations avec les autorités américaines et dans l'attente de l'adoption d'une nouvelle décision d'adéquation (finalement adoptée le 12 juillet 2016)[700], les transferts ne pouvaient avoir lieu que sur le fondement d'autres bases juridiques, comme des clauses contractuelles types ou des règles d'entreprise contraignantes. Plusieurs entreprises, dont Facebook Ireland (contre laquelle a été engagée l'action qui a abouti à l'invalidation de la Décision sur la sphère de sécurité), se sont tournées vers des clauses contractuelles types afin de poursuivre leurs transferts entre l'UE et les États-Unis.

M. Schrems a déposé une plainte auprès de l'autorité de contrôle irlandaise, lui demandant de suspendre les transferts de données vers les États-Unis fondés sur des clauses contractuelles types. En substance, il alléguait que lorsque des données à caractère personnel le concernant sont transférées de la filiale irlandaise de Facebook vers Facebook Inc. et des serveurs situés aux États-Unis, il n'existe aucune garantie qu'elles seront protégées. Facebook Inc. est régie par le droit américain qui pourrait la contraindre à divulguer des données à caractère personnel aux autorités répressives américaines et il n'existe pas de recours juridictionnel pour les particuliers européens voulant s'opposer à cette pratique[701]. Pour ces motifs, la CJUE a conclu à l'invalidité de la Décision sur la sphère de sécurité et, alors que son arrêt se limitait à l'examen de cette décision, le requérant a considéré que les questions soulevées étaient également pertinentes lorsque le transfert repose sur des clauses contractuelles. Lors de la rédaction du présent manuel, l'affaire était à l'examen devant la Haute Cour de justice irlandaise. Le requérant a, semble-t-il, l'intention de porter l'affaire devant la CJUE, dans le but de contester la validité de la décision de la Commission européenne sur les clauses contractuelles types. Comme expliqué au chapitre 5, la CJUE est seule compétente pour déclarer invalide un instrument de l'UE.

699 CJUE, C-362/14, *Maximillian Schrems c. Data Protection Commissioner* [GC], 6 octobre 2015.

700 Décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis, JO L 207.

701 Pour un complément d'informations, voir la plainte révisée contre Facebook Ireland Ltd soumise à l'Irish Data Protection Commissioner par Maximilian Schrems du 1er décembre 2015.

Transferts soumis à des règles d'entreprise contraignantes

Le **droit de l'UE** autorise également les transferts de données à caractère personnel fondés sur des règles d'entreprise contraignantes pour les transferts internationaux au sein du même groupe d'entreprises ou entre des entreprises engagées dans une activité économique conjointe[702]. Avant que des règles d'entreprise contraignantes puissent être invoquées comme base pour le transfert de données à caractère personnel, l'autorité de contrôle compétente doit les approuver, conformément au mécanisme de contrôle de la cohérence.

Pour être approuvées, les règles d'entreprise contraignantes doivent être juridiquement contraignantes, couvrir tous les principes généraux relatifs à la protection des données et s'appliquer à – et être appliquées par – chaque membre du groupe. Elles doivent expressément conférer aux personnes concernées des droits opposables, couvrir tous les principes généraux relatifs à la protection des données et répondre à certaines exigences formelles, comme préciser la structure de l'entreprise ou décrire les transferts ainsi que la manière dont les principes de la protection seront appliqués. Ceci inclut la fourniture de ces informations aux personnes concernées. Les règles d'entreprise contraignantes doivent notamment préciser les droits des personnes concernées et les dispositions sur la responsabilité en cas de violation des règles[703]. Lors de l'approbation de règles d'entreprise contraignantes, le mécanisme de contrôle de la cohérence est déclenché afin de permettre la coopération entre les autorités de contrôle (voir le chapitre 5).

Dans le cadre du mécanisme de contrôle de la cohérence, l'autorité de contrôle chef de file examine les règles d'entreprise contraignantes proposées, adopte un projet de décision et le soumet au Comité européen de la protection des données. Le Comité émet un avis sur la question et l'autorité de contrôle chef de file peut formellement approuver les règles d'entreprise contraignantes tout en tenant « le plus grand compte » de l'avis du Comité. Cet avis n'est pas juridiquement contraignant, mais si l'autorité de contrôle a l'intention de ne pas en tenir compte, le mécanisme de règlement des litiges est enclenché et le Comité devra se réunir pour adopter une décision juridiquement contraignante à la majorité des deux tiers de ses membres[704].

702 RGPD, art. 47.

703 Pour une description plus détaillée, voir RGPD, art. 47.

704 *Ibid.*, art. 57, para. 1, point s), art. 58, para. 1, point j), art. 64, para. 1, point f), et art. 65, paras. 1 et 2.

Dans le droit du CdE, les garanties types ou *ad hoc*, qui sont incluses dans un instrument juridiquement contraignant[705], couvrent également les règles d'entreprise contraignantes.

7.3.3. Dérogations pour des situations particulières

Dans le droit de l'UE, les transferts de données à caractère personnel vers un pays tiers peuvent être justifiés, même en l'absence d'une décision d'adéquation ou de garanties, telles que des clauses contractuelles types ou des règles d'entreprise contraignantes, dans l'un des cas suivants :

- la personne concernée donne son consentement explicite au transfert des données ;
- la personne concernée s'engage – ou se prépare à s'engager – dans une relation contractuelle nécessitant le transfert de données vers l'étranger ;
- le transfert est nécessaire à la conclusion d'un contrat entre un responsable du traitement et un tiers dans l'intérêt de la personne concernée ;
- le transfert est nécessaire pour des motifs importants d'intérêt public ;
- le transfert est nécessaire à la constatation, à l'exercice ou à la défense de droits en justice ;
- le transfert est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ;
- le transfert a lieu au départ d'un registre public (il s'agit d'un cas d'intérêt prédominant du public à accéder à des informations conservées dans des registres publics)[706].

Lorsqu'aucune de ces conditions ne s'applique et que les transferts ne peuvent se fonder sur une décision d'adéquation ou des garanties appropriées, un transfert ne peut avoir lieu que si ce transfert ne revêt pas de caractère répétitif, ne touche qu'un nombre limité de personnes concernées et est nécessaire aux fins des intérêts

705 Convention 108 modernisée, art. 14, para. 3, point b).

706 Règlement général sur la protection des données, art. 49.

légitimes impérieux poursuivis par le responsable du traitement sur lesquels ne prévalent pas les droits de la personne concernée[707]. Dans de tels cas, le responsable du traitement doit évaluer les circonstances entourant le transfert et offrir des garanties. Il doit également informer l'autorité de contrôle et les personnes concernées du transfert et de l'intérêt légitime le justifiant.

Le fait que les dérogations constituent un dernier recours pour les transferts licites[708] (à n'utiliser qu'en l'absence d'une décision d'adéquation ou d'autres garanties) souligne leur caractère exceptionnel et est également mis en évidence dans l'exposé des motifs du RGPD[709]. En soi, les dérogations sont acceptées comme une possibilité « de transferts dans certains cas » sur la base du consentement de la personne concernée et lorsque « le transfert est occasionnel et nécessaire »[710] dans le cadre d'un contrat ou d'une action en justice.

En outre, conformément aux lignes directrices du Groupe de travail « Article 29 », l'invocation de dérogations pour des situations particulières doit être exceptionnelle, être basée sur des cas individuels et ne pas être utilisée pour des transferts massifs ou répétitifs[711]. Le Contrôleur européen de la protection des données a également souligné le caractère exceptionnel du recours à des dérogations comme base juridique de transferts au titre du Règlement nº 45/2001, en précisant que cette solution devrait être utilisée « dans des cas limités » et pour « des transferts ponctuels »[712].

Exemple : une société de services, Global Distribution System (GDS), dont le siège est établi aux États-Unis, propose un système de réservations en ligne pour des compagnies aériennes, des hôtels et des croisières dans le monde entier et traite les données de dizaines de millions de personnes dans l'UE. Pour le transfert initial des données vers des serveurs situés aux États-Unis, GDS invoque une dérogation comme base licite des transferts,

707 *Ibid.*

708 *Ibid.*, art. 49, para. 1.

709 RGPD, art. 49, para. 1, points a), b) et e), et considérant 113.

710 *Ibid.*, art. 49, para. 1.

711 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.

712 CEPD, *Le transfert de données à caractère personnel à des pays tiers et à des organisations internationales par les institutions et organes de l'Union européenne*, Document d'orientation, Bruxelles, 14 juillet 2014, p. 15.

ceci étant nécessaire à la conclusion d'un contrat. Par conséquent, elle n'offre aucune autre garantie pour les données à caractère personnel en provenance d'Europe, transférées vers les États-Unis et redistribuées ensuite à des hôtels du monde entier (ce qui implique qu'il n'y a pas non plus de garanties pour les transferts ultérieurs). GDS ne respecte pas les exigences du RGPD pour les transferts internationaux licites de données, parce qu'elle se prévaut d'une dérogation comme fondement légitime de transferts massifs.

À moins qu'une décision d'adéquation existe, l'UE ou ses États membres peuvent imposer des limites au transfert de catégories particulières de données à caractère personnel vers un pays tiers, même si d'autres conditions de ces transferts sont remplies, pour des motifs importants d'intérêt public. Ces limitations doivent être considérées comme exceptionnelles et les États membres sont tenus de communiquer les dispositions pertinentes à la Commission[713].

Le droit du CdE autorise les flux de données vers des territoires ne disposant pas d'un niveau approprié de protection des données si :

- la personne concernée a donné son consentement ;
- les intérêts de la personne concernée nécessitent un tel transfert ;
- des intérêts légitimes prépondérants, notamment des intérêts publics importants, sont prévus par la loi ;
- ce transfert constitue une mesure nécessaire et proportionnée dans une société démocratique[714].

7.3.4. Transferts fondés sur des accords internationaux

L'UE peut conclure des accords internationaux avec des pays tiers en vue de réglementer le transfert de données à caractère personnel à des fins spécifiques. Ces accords doivent inclure des garanties appropriées afin d'assurer la protection des

713 RGPD, art. 49, para. 5.

714 Convention 108 modernisée, art. 14, para. 4.

données à caractère personnel des personnes concernées. Le RGPD s'entend sans préjudice de ces accords internationaux[715].

Les États membres peuvent également conclure des accords internationaux avec des pays tiers ou des organisations internationales qui prévoient un niveau approprié de protection des droits fondamentaux des personnes concernées, dans la mesure où ces accords n'affectent pas l'application du RGPD.

Une règle similaire est énoncée à l'article 12, paragraphe 3, point a), de la Convention 108 modernisée.

Les accords sur les dossiers passagers (PNR) sont un exemple d'accords internationaux impliquant le transfert de données à caractère personnel.

Dossiers passagers

Les données PNR sont collectées par des transporteurs aériens pendant le processus de réservation des vols et comprennent, notamment, les noms, adresses, informations sur la carte de crédit et numéros de sièges des passagers aériens. Les transporteurs aériens collectent également ces informations à des fins commerciales qui leur sont propres. L'UE a conclu des accords avec certains pays tiers (Australie, Canada et États-Unis) concernant le transfert de données PNR afin de prévenir, de détecter, d'enquêter et de poursuivre les infractions terroristes et des formes graves de criminalité transnationale. En outre, en 2016, l'Union a adopté la Directive (UE) 2016/681, connue sous le nom de Directive UE-PNR[716]. Cette directive établit un cadre juridique pour le transfert par les États membres de l'UE de données PNR aux autorités compétentes d'autres pays tiers afin de prévenir, de détecter, d'enquêter et de poursuivre les infractions terroristes et les formes graves de criminalité. Les transferts de données PNR aux autorités de pays tiers sont effectués au cas par cas et sont soumis à une évaluation individuelle de la nécessité du transfert pour les finalités mentionnées dans la directive et pour autant que les droits fondamentaux soient respectés.

En ce qui concerne les accords PNR conclus entre l'UE et des pays tiers, leur compatibilité avec les droits fondamentaux au respect de la vie privée et à la protection des

715 RGPD, considérant 102.

716 Directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 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 de la Commission, JO 2016 L 119.

données, garantis par la Charte des droits fondamentaux de l'UE, a été contestée. Lorsque l'UE a signé, à l'issue de négociations avec le Canada, un accord relatif au transfert et au traitement de données PNR en 2014, le Parlement européen a décidé de saisir la CJUE afin qu'elle apprécie la compatibilité de l'accord avec le droit de l'Union et, en particulier, avec les articles 7 et 8 de la Charte.

Exemple : dans son avis sur la légalité de l'accord PNR UE-Canada[717], la CJUE a déclaré que, sous sa forme actuelle, l'accord envisagé était incompatible avec les droits fondamentaux reconnus par la Charte et ne pouvait dès lors pas être conclu. Étant donné qu'il impliquait le traitement de données à caractère personnel, il constituait une ingérence dans le droit à la protection des données à caractère personnel garanti par l'article 8 de la Charte. Dans le même temps, il constitue également une limitation du droit au respect de la vie privée, consacré à l'article 7, étant donné que, considérées globalement, les données PNR peuvent être agrégées et analysées de façon à révéler les habitudes de voyage, les relations entre différentes personnes, des informations sur leur situation financière, leurs habitudes alimentaires et leur état de santé, ce qui porte atteinte à leur vie privée.

L'ingérence dans les droits fondamentaux que constituait l'accord envisagé poursuivait un objectif d'intérêt général, à savoir la sécurité publique et la lutte contre le terrorisme et la criminalité transnationale grave. La Cour a toutefois rappelé que pour être justifiée, une ingérence doit être limitée à ce qui est strictement nécessaire pour atteindre l'objectif poursuivi. Après en avoir analysé le contenu, la CJUE a conclu que l'accord envisagé ne répondait pas au critère de la « stricte nécessité ». Pour aboutir à cette conclusion, la Cour a notamment tenu compte des facteurs suivants :

- le fait que l'accord envisagé impliquait le transfert de données sensibles. Les données PNR collectées au titre de l'accord envisagé pourraient inclure des données sensibles, telles que des informations révélant l'origine raciale ou ethnique, les convictions religieuses ou l'état de santé d'un passager. Le transfert et le traitement de données sensibles par les autorités canadiennes pouvaient constituer un risque pour le principe de non-discrimination et nécessitaient donc une justification précise et solide, tirée de motifs autres que la protection de la sécurité publique et

717 CJUE, *Avis 1/15 de la Cour (grande chambre)*, 26 juillet 2017.

la lutte contre la criminalité grave. En l'occurrence, une telle justification faisait défaut dans l'accord envisagé[718] ;

- la conservation des données PNR de l'ensemble des passagers, pendant cinq ans, même après leur départ du Canada, était également considérée comme excédant les limites du strict nécessaire. La CJUE a estimé que les autorités canadiennes pourraient conserver les données des passagers dont des éléments objectifs peuvent donner à penser qu'ils sont susceptibles de constituer une menace pour la sécurité publique, même après leur départ du Canada. En revanche, la conservation des données à caractère personnel de *tous* les passagers, pour lesquels il n'existe même pas de preuves indirectes qu'ils représentent un risque pour la sécurité publique, n'est pas justifiée[719].

Le Comité consultatif de la Convention 108 a émis un avis sur les implications en matière de protection des données du traitement des dossiers passagers, dans le contexte du droit du CdE[720].

Données de messagerie

La Société de télécommunications interbancaires mondiales (SWIFT) basée en Belgique, qui est le responsable du traitement de la plupart des transferts d'argent mondiaux à partir de banques européennes, opérait avec un « centre jumeau » situé aux États-Unis. SWIFT a reçu une demande de communication de données de la part du Département américain du Trésor aux fins d'une enquête liée au terrorisme au titre de son programme de traçage du financement du terrorisme[721].

Du point de vue de l'UE, il n'existait pas de base légale suffisante pour communiquer ces données, qui concernaient principalement des citoyens de l'UE, qui n'étaient

718 *Ibid.*, para. 165.

719 *Ibid.*, paras. 204 à 207.

720 CdE, *Avis sur les implications en matière de protection des données du traitement des dossiers passagers*, T-PD(2016)18rev, 19 août 2016.

721 Voir, dans ce contexte, Groupe de travail « Article 29 » (2011), *Avis 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.

accessibles aux États-Unis que 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 en vue d'établir la base juridique nécessaire et de garantir une protection adéquate des données[722].

En vertu de cet accord, les données financières conservées par SWIFT continuent d'être communiquées au Département américain du Trésor pour la prévention ou la détection du terrorisme ou de son financement, ainsi que pour les enquêtes ou les poursuites en la matière. Le Département américain du Trésor 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)[723].

Europol doit recevoir une copie de chaque demande du Département américain du Trésor et vérifier si les principes de l'accord SWIFT sont respectés[724]. S'ils le sont, la société SWIFT est tenue de remettre directement les données financières au Département américain du Trésor. Le Département 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 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

722 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 en annexe à cette décision, JO 2010 L 195, p. 5 à 14.

723 *Ibid.*, art. 4, para. 2.

724 L'autorité de contrôle commune d'Europol a effectué des vérifications sur les activités menées par Europol dans ce domaine.

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 Département américain du Trésor peut transférer des informations issues des données reçues de SWIFT à des organismes chargés de l'application de la loi, de la sécurité publique ou de la lutte contre le terrorisme aux États-Unis ou à l'étranger, exclusivement aux fins de la prévention ou de la détection du terrorisme et de son financement ou pour les enquêtes ou poursuites en la matière. Lorsque le transfert ultérieur 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. Ils peuvent examiner en temps réel et rétroactivement toutes les recherches effectuées dans les données fournies, demander des informations complémentaires pour justifier le lien de ces recherches avec le terrorisme et ont le pouvoir de bloquer tout ou partie des recherches qui semblent contraires aux garanties prévues par l'accord.

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 rectification, à l'effacement ou au verrouillage de leurs données collectées et enregistrées par le Département américain du Trésor dans le cadre de l'accord SWIFT. Toutefois, les droits d'accès des personnes concernées peuvent être soumis à 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 et sa première période de validité courait jusqu'en août 2015. Il se prolonge 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. La prolongation automatique s'est appliquée en août 2015, 2016 et 2017 et garantit la validité de l'accord SWIFT au moins jusqu'en août 2018[725].

725 *Ibid.*, art. 23, para. 2.

8

Protection des données dans le contexte de la police et de la justice pénale

UE	Questions traitées	CdE
Directive relative à la protection des données pour les autorités policières et judiciaires en matière pénale	**En général**	Convention 108 modernisée
	Police	Recommandation relative à la police Guide pratique sur l'utilisation de données à caractère personnel dans le secteur de la police
	Surveillance	CouEDH, *B.B. c. France*, nº 5335/06, 2009 CouEDH, *S. et Marper c. Royaume-Uni* [GC], nº 30562/04 et nº 30566/04, 2008 CouEDH, *Allan c. Royaume-Uni*, nº 48539/99, 2002 CouEDH, *Malone c. Royaume-Uni*, nº 8691/79, 1984 CouEDH, *Klass et autres c. Allemagne*, nº 5029/71, 1978 CouEDH, *Szabó et Vissy c. Hongrie*, nº 37138/14, 2016 CouEDH, *Vetter c. France*, nº 59842/00, 2005
	Cybercriminalité	Convention sur la cybercriminalité

UE	Questions traitées	CdE
Autres instruments juridiques spécifiques		
Décision Prüm	**Pour les données spéciales : empreintes digitales, ADN, hooliganisme, informations sur les passagers aériens, données de télécommunication, etc.**	Convention 108 modernisée, art. 6 Recommandation relative à la police, Guide pratique sur l'utilisation de données à caractère personnel dans le secteur de la police
Initiative suédoise (Décision-cadre 2006/960/JAI du Conseil)	**Simplification de l'échange d'informations et de renseignements entre autorités répressives**	CouEDH, *S. et Marper c. Royaume-Uni* [GC], nº 30562/04 et nº 30566/04, 2008
Directive (UE) 2016/681 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 CJUE, affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland* et *Kärntner Landesregierung et autres* [GC], 2014 CJUE, affaires jointes C-203/15 et C-698/15, *Tele2 Sverige* et *Home Department c. Tom Watson et autres* [GC], 2016	**Conservation des données à caractère personnel**	CouEDH, *B.B. c. France*, nº 5335/06, 2009
Règlement Europol Décision Eurojust	**Par des agences spéciales**	Recommandation relative à la police
Décision Schengen II Règlement VIS Règlement Eurodac Décision SID	**Par des systèmes spéciaux d'information communs**	Recommandation relative à la police CouEDH, *Dalea c. France*, nº 964/07, 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 aux fins de lutter contre la criminalité et de garantir la sécurité nationale et la sûreté publique, le CdE et l'UE ont adopté des instruments juridiques spécifiques. Cette section présente un aperçu du droit du CdE (section 8.1) et du droit de l'UE (section 8.2) en ce qui concerne la protection des données dans le domaine de la police et de la justice pénale.

8.1. Droit du CdE en matière de protection des données dans le domaine de la sécurité nationale, de la police et de la justice pénale

Points clés

- La Convention 108 modernisée et la Recommandation du CdE sur l'utilisation des données à caractère personnel dans le secteur de la police (« Recommandation relative à la police ») s'appliquent à la protection des données dans tous les domaines du travail policier.
- La Convention sur la cybercriminalité (Convention de Budapest) est un instrument juridique international contraignant portant sur les crimes commis contre et à l'aide de réseaux électroniques. Elle est également pertinente pour les enquêtes sur des crimes ne relevant pas de la cybercriminalité, mais impliquant des preuves électroniques.

Il convient d'opérer une distinction importante entre le droit du CdE et celui de l'UE : le **droit du CdE**, à la différence du droit de l'UE, s'applique au domaine de la sécurité nationale. En d'autres termes, les Parties contractantes doivent respecter les limites de l'article 8 de la CEDH même pour des activités en rapport avec la sécurité nationale. Plusieurs arrêts de la CouEDH traitent d'activités de l'État dans les domaines sensibles du droit et de la pratique en matière de sécurité nationale[726].

S'agissant de la police et de la justice pénale, au niveau européen, la Convention 108 modernisée couvre tous les domaines du traitement des données à caractère personnel et ses dispositions visent à réglementer le traitement de données à caractère personnel en général. Par conséquent, la Convention 108 modernisée s'applique à la protection des données dans le domaine de la police et de la justice pénale. Le traitement de données génétiques, de données à caractère personnel concernant des infractions, des procédures et des condamnations pénales et des mesures de sûreté connexes, de données biométriques identifiant un individu de façon unique ainsi que de toute donnée sensible à caractère personnel n'est autorisé qu'à la condition que des garanties appropriées existent contre les risques que le traitement de telles

726 Voir, par exemple, CouEDH, *Klass et autres c. Allemagne*, nº 5029/71, 6 septembre 1978 ; CouEDH, *Rotaru c. Roumanie* [GC], nº 28341/95, 4 mai 2000 ; et CouEDH, *Szabó et Vissy c. Hongrie*, nº 37138/14, 12 janvier 2016.

données peut présenter pour les intérêts, les droits et les libertés fondamentales de la personne concernée, notamment un risque de discrimination[727].

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 relative à la police adoptée par le CdE en 1987 contient des orientations à l'intention des États membres du CdE sur la manière de donner effet aux principes de la Convention 108 dans le contexte du traitement de données à caractère personnel par des autorités de police[728]. La recommandation a été accompagnée d'un guide pratique sur l'utilisation de données à caractère personnel dans le secteur de la police, adopté par le Comité consultatif de la Convention 108.[729]

Exemple : dans l'affaire *D.L. c. Bulgarie*[730], les services sociaux ont placé la requérante dans un internat éducatif privé sur décision de justice. L'ensemble de son courrier et de ses conversations téléphoniques ont fait l'objet d'une surveillance générale et systématique par l'institution. La CouEDH a conclu à une violation de l'article 8 au motif que la mesure en cause n'était pas nécessaire dans une société démocratique. La Cour a déclaré que tout doit être prévu afin que les mineurs placés dans une institution aient suffisamment de contacts extérieurs, car cela fait partie intégrante de leur droit d'être traités dignement et est indispensable pour les préparer à leur retour dans la société. Ceci s'applique aussi bien aux visites qu'au courrier ou aux appels téléphoniques. Par ailleurs, la surveillance ne distinguait pas entre les communications avec des membres de la famille et des ONG de défense des droits de l'enfant ou des avocats. De plus, la décision d'intercepter les communications ne reposait pas sur une étude des situations individuelles mettant en lumière les risques potentiels.

Exemple : dans *Dragojević c. Croatie*[731], le requérant était soupçonné de s'être livré à un trafic de stupéfiants. Il a été reconnu coupable après qu'un

727 Convention 108 modernisée, art. 6.

728 CdE, Comité des Ministres (1987), Recommandation Rec(87)15 aux États membres visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, 17 septembre 1987.

729 Conseil de l'Europe (2018), Comité consultatif de la Convention 108, Guide pratique sur l'utilisation de données à caractère personnel dans le secteur de la police, T-PD(2018)1.

730 CouEDH, *D.L. c. Bulgarie*, nº 7472/14, 19 mai 2016.

731 CouEDH, *Dragojević c. Croatie*, nº 68955/11, 15 janvier 2015.

juge d'instruction eut autorisé le recours à des mesures de surveillance secrète pour écouter les conversations téléphoniques du requérant. La CouEDH a considéré que la mesure, contre laquelle une plainte a été déposée, constituait une ingérence dans le droit au respect de la vie privée et de la correspondance. L'autorisation donnée par le juge d'instruction ne reposait que sur l'affirmation du parquet selon laquelle « l'enquête ne [pouvait] pas être menée autrement ». La CouEDH a également relevé que les juridictions pénales avaient limité leur examen du recours aux mesures de surveillance et que le gouvernement n'avait fourni aucune information sur les recours disponibles. La Cour a donc conclu à une violation de l'article 8.

8.1.1. 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 constituaient une atteinte à l'article 8, paragraphe 1, de la CEDH. De nombreux arrêts de la CouEDH portent sur la justification de telles atteintes[732].

Exemple : dans l'affaire *B.B. c. France*[733], le requérant a été condamné pour agressions sexuelles sur mineurs de quinze ans par personne ayant autorité. Il a fini de purger sa peine d'emprisonnement en 2000. Un an plus tard, il a sollicité l'effacement de la mention de sa condamnation de son casier judiciaire, mais sa demande a été rejetée. En 2004, une loi française a créé le fichier judiciaire national des auteurs d'infractions sexuelles et le requérant a été informé de son inscription dans celui-ci. 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 Cour a donc exclu une violation de l'article 8 de la CEDH.

732 Voir, par exemple, CouEDH, *Leander c. Suède*, nº 9248/81, 26 mars 1987 ; CouEDH, *M.M. c. Royaume-Uni*, nº 24029/07, 13 novembre 2012 ; CouEDH, *M.K. c. France*, nº 19522/09, 18 avril 2013 ; ou CouEDH, *Aycaguer c. France*, nº 8806/12, 22 juin 2017.

733 CouEDH, *B.B. c. France*, nº 5335/06, 17 décembre 2009.

Exemple : dans l'affaire *S. et Marper c. Royaume-Uni*[734], les deux requérants avaient été inculpés pour des infractions pénales, mais n'avaient pas été condamnés. La police avait néanmoins enregistré et conservé leurs empreintes digitales, profils ADN et échantillons cellulaires. La conservation illimitée de données biométriques était autorisée par la loi dans les cas où une personne était suspectée d'une infraction pénale, même si par la suite le suspect était acquitté ou les charges abandonnées. La CouEDH a retenu que la conservation générale et systématique 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 donc conclu à une violation de l'article 8 de la CEDH.

Dans le cadre des communications électroniques, une question cruciale est l'ingérence des autorités publiques dans les droits au respect de la vie privée et à la protection des données. Les moyens de surveillance ou d'interception des communications, comme les dispositifs d'écoutes téléphoniques, ne sont admissibles que s'ils sont prévus par la loi et s'ils constituent une mesure nécessaire dans une société démocratique aux fins :

- de la protection de la sûreté de l'État ;
- de la sécurité publique ;
- des intérêts financiers de l'État ;
- de l'élimination des infractions pénales ; ou
- de la protection de la personne concernée et des droits et libertés d'autrui.

De nombreux autres arrêts de la CouEDH portent sur la justification d'une ingérence par surveillance dans le droit à la protection des données.

734 CouEDH, *S. et Marper c. Royaume-Uni* [GC], nº 30562/04 et nº 30566/04, 4 décembre 2008, paras. 119 et 125.

Exemple : dans l'affaire *Allan c. Royaume-Uni*[735], 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 coaccusé 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 *Roman Zakharov c. Russie*[736], le requérant a engagé une procédure judiciaire contre trois opérateurs de réseaux mobiles. Il a allégué une atteinte à son droit au respect du caractère privé de ses communications téléphoniques au motif que les opérateurs avaient mis en place un dispositif permettant au Service fédéral de sécurité d'intercepter ses communications téléphoniques sans autorisation judiciaire préalable. La CouEDH a considéré que les dispositions du droit national régissant l'interception des communications ne fournissaient pas des garanties suffisantes et adéquates contre l'arbitraire et le risque d'abus. En particulier, le droit national n'imposait pas l'obligation d'effacer les données stockées dès lors que la finalité de la conservation avait été atteinte. Par ailleurs, bien qu'une autorisation judiciaire soit requise, le contrôle juridictionnel était limité.

Exemple : dans l'affaire *Szabó et Vissy c. Hongrie*[737], les requérants alléguaient que la législation hongroise violait l'article 8 de la CEDH au motif qu'elle n'était pas suffisamment détaillée ou précise. Ils affirmaient, en outre, que la législation ne fournissait pas de garanties suffisantes contre les abus et l'arbitraire. La CouEDH a retenu que la législation hongroise ne subordonnait pas la surveillance à une autorisation judiciaire. Elle a toutefois relevé que si la surveillance était soumise à une autorisation du ministre de la Justice, pareil contrôle est éminemment politique et incapable d'assurer l'appréciation requise de la « stricte nécessité ». Par ailleurs, le droit interne ne prévoyait pas de mécanisme de contrôle judiciaire, étant donné qu'aucune notification n'était envoyée aux intéressés. La CouEDH a donc conclu à une violation de l'article 8 de la CEDH.

735 CouEDH, *Allan c. Royaume-Uni*, nº 48539/99, 5 novembre 2002.

736 CouEDH, *Roman Zakharov c. Russie* [GC], nº 47143/06, 4 décembre 2015.

737 CouEDH, *Szabó et Vissy c. Hongrie*, nº 37138/14, 12 janvier 2016.

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 résoudre ce problème en fournissant des orientations sur la façon dont les 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 en place. L'obligation d'offrir une sécurité adéquate des données a également été prise en compte.

La recommandation ne prévoit pas de collecte ouverte et indiscriminée de données à caractère personnel par les autorités de police. Elle limite la collecte de ces données par les autorités de police aux données nécessaires à la prévention d'un danger réel ou à la poursuite 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 ce qui est absolument nécessaire dans le cadre 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 des données dès que leur 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 *Versini-Campinchi et Crasnianski c. France*[738], la requérante, une avocate, avait eu une conversation téléphonique avec un client dont la ligne téléphonique avait été placée sur écoute à la demande d'un juge d'instruction. La transcription de la conversation a montré qu'elle avait divulgué des informations couvertes par le secret professionnel légal. Le procureur a transmis ces informations à l'ordre des avocats, qui a sanctionné la requérante. La CouEDH a reconnu l'existence d'une ingérence dans l'exercice du droit au respect de la vie privée et de la correspondance, non

738 CouEDH, *Versini-Campinchi et Crasnianski c. France*, nº 49176/11, 16 juin 2016.

seulement de la personne dont le téléphone avait été mis sur écoute, mais également de la requérante dont la communication avait été interceptée et transcrite. L'ingérence était prévue par la loi et poursuivait l'objectif légitime de la défense de l'ordre. La requérante avait obtenu un contrôle de la légalité de la présentation de la transcription des écoutes téléphoniques dans le cadre de la procédure disciplinaire conduite contre elle. Bien qu'elle n'ait pas été en mesure de solliciter l'annulation de la transcription de la conversation téléphonique, la CouEDH a estimé qu'il y avait eu un contrôle effectif de nature à limiter l'ingérence alléguée à ce qui était nécessaire dans une société démocratique. La Cour a conclu que la thèse selon laquelle la possibilité de poursuites à l'encontre de l'avocat sur le fondement d'une telle transcription pourrait avoir un effet dissuasif sur la liberté des échanges entre l'avocat et son client et, partant, sur la défense de ce dernier, n'est pas défendable dès lors que les propos tenus par l'avocat lui-même sont susceptibles de caractériser un comportement illégal de celui-ci. Par conséquent, la Cour a exclu une violation de l'article 8.

La Recommandation du CdE relative à la police dispose que, lors de l'enregistrement de données à caractère personnel, une distinction claire doit être opérée entre : les données administratives et les données de police, les différents types de personnes concernées, tels que suspects, condamnés, victimes et témoins, et les données considérées comme des faits établis et celles basées sur des suspicions ou des spéculations.

La finalité pour laquelle des données de police peuvent être utilisées devrait être strictement limitée. Ceci 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.

Exemple : dans l'affaire *Karabeyoğlu c. Turquie*[739], le requérant, un juge, avait fait l'objet d'écoutes téléphoniques dans le cadre d'une enquête pénale sur une organisation criminelle à laquelle il était suspecté d'appartenir ou de fournir aide et soutien. Après un non-lieu, le procureur chargé de l'enquête

739 CouEDH, *Karabeyoğlu c. Turquie*, nº 30083/10, 7 juin 2016.

pénale a détruit les enregistrements en question. Toutefois, les enquêteurs ont conservé les comptes rendus des écoutes et ont ensuite utilisé les éléments pertinents dans le cadre d'une enquête disciplinaire dirigée contre le requérant. La CouEDH a retenu que la législation pertinente avait été violée dans la mesure où les informations avaient été utilisées à des fins autres que celles pour lesquelles elles avaient été collectées et n'avaient pas été détruites dans le délai prévu par la loi. L'ingérence dans le droit du requérant au respect de sa vie privée n'était pas prévue par la loi en ce qui concerne la procédure disciplinaire engagée contre lui.

Les communications ou transferts internationaux devraient être limités aux autorités de police étrangères et être fondés sur des dispositions légales spécifiques, éventuellement des accords internationaux, à moins qu'ils ne soient nécessaires pour prévenir un danger grave et imminent.

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 modernisée. Lorsque les droits d'accès des personnes concernées ont été restreints en application de l'article 9 de la Convention 108 dans l'intérêt de l'efficacité des enquêtes de police et de l'exécution de sanctions pénales, 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.

8.1.2. La Convention de Budapest sur la cybercriminalité

Étant donné que les activités criminelles utilisent de plus en plus les systèmes électroniques de traitement des données et ont un impact croissant sur ceux-ci, de nouvelles dispositions de droit pénal sont nécessaires pour relever ce défi. Le CdE a donc adopté un instrument 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[740]. Cette convention est ouverte à l'adhésion d'États non membres du CdE. Au début de l'année 2018, quatorze États

740 CdE, Comité des Ministres (2001), Convention sur la cybercriminalité, STCE nº 185, Budapest, 23 novembre 2001, entrée en vigueur le 1er juillet 2004.

hors CdE[741] étaient Parties à la Convention et sept autres États non membres avaient été invités à y adhérer.

La Convention sur la cybercriminalité reste le traité international prépondérant en ce qui concerne les violations de la loi qui ont lieu 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 facilitée par l'informatique, la pornographie infantile et d'autres cyberactivités illicites. Elle prévoit également des pouvoirs procéduraux 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 par le biais de réseaux informatiques.

Si la Convention n'est pas véritablement un outil de promotion de la protection des données, elle qualifie de criminelles des activités susceptibles d'entraîner la violation du droit d'une personne concernée à la protection de ses données. En outre, elle impose aux Parties contractantes d'adopter des mesures législatives permettant aux autorités nationales d'intercepter les données relatives au trafic et au contenu[742]. 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[743]. Les Parties contractantes ne sont pas tenues d'adhérer à la Convention 108 également pour signer la Convention de Budapest sur la cybercriminalité.

741 Australie, Canada, Chili, Colombie, États-Unis, Israël, Japon, Maurice, Panama, République dominicaine, Sénégal, Sri Lanka, Tonga et Tunisie. Voir Charte des signatures et ratifications du Traité nº 185, situation en juillet 2017.

742 CdE, Comité des Ministres (2001), Convention sur la cybercriminalité, STCE nº 185, Budapest, 23 novembre 2001, art. 20 et 21.

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

8.2. 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 réglementée dans le contexte du traitement transfrontalier et national par des autorités de police et de justice pénale des États membres et des acteurs de l'UE.
- Au niveau des États membres, la Directive relative à la protection des données pour les autorités policières et judiciaires en matière pénale doit être transposée en droit national.
- Des instruments spécifiques régissent la protection des données dans le domaine de la coopération transfrontalière des autorités policières et répressives, en particulier dans la lutte contre le terrorisme et la criminalité transfrontalière.
- Il existe des régimes spéciaux de protection des données pour l'Office européen de police (Europol), l'unité de coopération judiciaire de l'UE (Eurojust) et le Parquet européen récemment créé, qui sont des organes de l'UE chargés de contribuer à l'application de la loi au-delà des frontières et de la promouvoir.
- Il existe également des régimes spéciaux de protection des données pour les systèmes d'information conjoints qui ont été mis en place au niveau de l'UE pour l'échange transfrontière d'informations entre les autorités policières et judiciaires compétentes. Parmi les principaux exemples figurent le système d'information Schengen II (SIS II), le système d'information sur les visas (VIS) et Eurodac, un système centralisé contenant les empreintes digitales de ressortissants de pays tiers et d'apatrides demandant l'asile dans un État membre de l'UE.
- L'UE met actuellement à jour les dispositions relatives à la protection des données précitées afin de les aligner sur celles de la Directive relative à la protection des données pour les autorités policières et judiciaires en matière pénale.

8.2.1. La Directive relative à la protection des données pour les autorités policières et judiciaires en matière pénale

La Directive (UE) 2016/680 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 relative à la protection des données pour les autorités policières et judiciaires en matière pénale »)[744], a pour objet de protéger les données à caractère personnel collectées et traitées à des fins de justice pénale, qu'il s'agisse de :

- la prévention et la détection des infractions pénales et de poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité et la prévention de telles menaces ;
- l'exécution d'une sanction pénale ; et
- des cas où des autorités policières ou d'autres autorités répressives agissent pour faire appliquer la loi, protéger contre et prévenir les menaces pour la sécurité publique et les droits fondamentaux de la société qui pourraient constituer une infraction pénale.

La Directive relative à la protection des données pour les autorités policières et judiciaires en matière pénale protège les données à caractère personnel de différentes catégories de personnes impliquées dans une procédure pénale, telles que les témoins, les informateurs, les victimes, les suspects et les complices. Les autorités policières et judiciaires sont tenues de se conformer aux dispositions de la directive chaque fois qu'elles traitent des données à caractère personnel à des fins répressives, qu'elles relèvent du champ d'application personnel ou matériel de la directive[745].

L'utilisation de données à une autre fin est toutefois également autorisée à certaines conditions. Le traitement de données pour une finalité répressive autre que celles pour lesquelles elles ont été collectées n'est autorisé qu'à la condition qu'il soit licite, nécessaire et proportionné conformément au droit de l'UE ou au droit d'un État membre[746]. Pour les autres finalités, les dispositions du RGPD s'appliquent. L'une des

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

745 Directive relative à la protection des données pour les autorités policières et judiciaires en matière pénale, art. 2, para. 1.

746 *Ibid*., art. 4, para. 2.

missions spécifiques des autorités compétentes en matière de clarification des responsabilités découlant de réclamations consiste à tenir un journal et à documenter les partages de données.

Les autorités compétentes actives dans le domaine de la police et de la justice pénale sont des autorités publiques ou des autorités auxquelles le droit national et l'autorité publique ont confié des prérogatives de puissance publique[747], par exemple, des prisons privées[748]. Le champ d'application de la directive englobe à la fois le traitement de données au niveau national et le traitement transfrontière entre autorités policières et judiciaires des États membres, ainsi que les transferts internationaux effectués par les autorités vers des pays tiers et des organisations internationales[749]. Il ne couvre pas la sécurité nationale ou le traitement de données à caractère personnel par les institutions, organismes, organes et agences de l'UE[750].

La directive s'appuie, dans une large mesure, sur les principes et définitions énoncés dans le Règlement général sur la protection des données, en tenant compte de la nature spécifique des domaines de la police et de la justice pénale. Le contrôle peut être assuré par les mêmes autorités des États membres que celles qui exercent un contrôle en vertu du RGPD. La désignation de délégués à la protection des données et la réalisation des analyses d'impact relatives à la protection des données ont été introduites dans la directive et constituent de nouvelles obligations pour les autorités de police et de justice pénale[751]. Bien que ces notions s'inspirent du RGPD, la directive les traite sous l'angle spécifique des autorités policières et judiciaires en matière pénale. Par rapport au traitement des données à des fins commerciales, qui est régi par le règlement, le traitement de données liées à la sécurité peut nécessiter un certain degré de flexibilité. Ainsi, la fourniture du même niveau de protection aux personnes concernées en termes de droit à l'information, de droit d'accès à leurs données personnelles ou d'effacement de celles-ci, telle qu'elle est prévue par le

747 *Ibid.*, art. 3, para. 7.

748 Commission européenne (2016), Communication de la Commission au Parlement européen conformément à l'article 294, para. 6, du Traité sur le fonctionnement de l'Union européenne concernant la position du Conseil sur l'adoption d'une 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, et abrogeant la décision-cadre 2008/977/JAI du Conseil, COM(2016) 213 final, Bruxelles, 11 avril 2016.

749 Directive relative à la protection des données pour les autorités policières et judiciaires en matière pénale, chapitre V.

750 *Ibid.*, art. 2, para. 3.

751 *Ibid.*, art. 32 et 27, respectivement.

Règlement général sur la protection des données, pourrait avoir pour conséquence qu'une mission de surveillance menée à des fins répressives deviendrait inefficace dans un contexte répressif. La directive ne fait donc pas référence au principe de la transparence. De même, les principes de minimisation des données et de limitation de la finalité, qui imposent que les données à caractère personnel soient limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées et qu'elles soient traitées pour des finalités déterminées et explicites, doivent aussi être appliqués de manière flexible au traitement de données liées à la sécurité. Les informations collectées et conservées par les autorités compétentes pour une affaire particulière peuvent se révéler extrêmement utiles pour la résolution d'affaires futures.

Principes relatifs au traitement

La Directive relative à la protection des données pour les autorités policières et judiciaires en matière pénale établit plusieurs garanties essentielles concernant l'utilisation des données à caractère personnel. Elle énonce également les principes qui régissent le traitement de ces données. Les États membres doivent veiller à ce que les données à caractère personnel soient :

- traitées de manière licite et loyale ;
- collectées pour des finalités déterminées, explicites et légitimes, et ne soient pas traitées de manière incompatible avec ces finalités ;
- adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées ;
- exactes et, si nécessaire, tenues à jour ; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder ;
- conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ;
- traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite

et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées[752].

Aux termes de la directive, un traitement n'est licite que si et dans la mesure où il est nécessaire à l'exécution de la mission pertinente. En outre, il doit être effectué par une autorité compétente pour les finalités énoncées dans la directive et être fondé sur le droit de l'UE ou sur le droit d'un État membre[753]. Les données ne doivent pas être conservées plus longtemps que nécessaire et elles doivent être effacées ou revues à intervalles réguliers pendant une certaine période. Elles ne doivent être utilisées que par une autorité compétente et pour la finalité pour laquelle elles ont été collectées, communiquées ou mises à disposition.

Droits de la personne concernée

La directive détaille également les droits de la personne concernée. Ils comprennent :

- le droit de recevoir des informations. Les États membres doivent obliger le responsable du traitement à mettre à la disposition de la personne concernée : 1) l'identité et les coordonnées du responsable du traitement, 2) les coordonnées du délégué à la protection des données, 3) les finalités du traitement envisagé, 4) le droit d'introduire une réclamation auprès d'une autorité de contrôle et les coordonnées de ladite autorité et 5) le droit de demander l'accès aux données à caractère personnel, leur rectification ou leur effacement et la limitation du traitement des données[754]. Outre ces exigences générales d'information, la directive prévoit que, dans des cas particuliers, le responsable du traitement doit fournir à la personne concernée des informations sur la base juridique du traitement et la durée de conservation des données afin de lui permettre d'exercer ses droits. Si des données à caractère personnel sont destinées à être communiquées à d'autres destinataires, y compris dans des pays tiers ou des organisations internationales, les personnes concernées doivent recevoir des informations sur les catégories de destinataires. Enfin, le responsable du traitement doit fournir des informations complémentaires, en tenant compte des circonstances spécifiques dans lesquelles les données sont traitées, par exemple lorsque des données à caractère personnel ont été collectées au cours d'une surveillance

752 *Ibid.*, art. 4, para. 1.

753 *Ibid.*, art. 8.

754 *Ibid.*, art. 13, para. 1.

discrète, c'est-à-dire à l'insu de la personne concernée. Ceci garantit un traitement loyal à l'égard de la personne concernée[755] ;

- le droit d'accès aux données à caractère personnel. Les États membres doivent s'assurer que la personne concernée a le droit de savoir si des données à caractère personnel la concernant sont ou ne sont pas traitées. Si tel est le cas, la personne concernée devrait avoir accès à certaines informations, comme les catégories de données traitées[756]. Ce droit peut toutefois être limité, par exemple pour éviter de gêner des enquêtes ou de nuire à la poursuite d'infractions pénales ou pour protéger la sécurité publique et les droits et libertés d'autrui[757] ;

- le droit de rectification des données à caractère personnel. Les États membres sont tenus de veiller à ce qu'une personne concernée puisse obtenir, dans les meilleurs délais, la rectification des données à caractère personnel la concernant qui sont inexactes. Par ailleurs, la personne concernée a également le droit d'obtenir que les données à caractère personnel incomplètes soient complétées[758] ;

- le droit à l'effacement de données à caractère personnel et à la limitation du traitement. Dans certains cas, le responsable du traitement doit effacer des données à caractère personnel. En outre, la personne concernée peut obtenir l'effacement de données à caractère personnel la concernant, mais uniquement lorsque le traitement n'est pas licite[759]. Dans certaines situations, plutôt que de procéder à l'effacement, le traitement de données à caractère personnel peut être limité. Cela peut arriver lorsque : 1) l'exactitude des données à caractère personnel a été contestée mais qu'il est impossible de déterminer si les données sont exactes ou non ou lorsque 2) les données à caractère personnel doivent être conservées à des fins probatoires[760].

Lorsque le responsable du traitement refuse de rectifier ou d'effacer des données à caractère personnel ou de limiter le traitement, la personne concernée doit en être informée par écrit. Les États membres peuvent limiter ce droit d'information,

755 *Ibid.*, art. 13, para. 2.
756 *Ibid.*, art. 14.
757 *Ibid.*, art. 15.
758 *Ibid.*, art. 16, para. 1.
759 *Ibid.*, art. 16, para. 2.
760 *Ibid.*, art. 16, para. 3.

notamment, pour protéger la sécurité publique ou les droits et libertés d'autrui, pour les mêmes motifs qu'ils peuvent limiter le droit d'accès[761].

La personne concernée a normalement le droit d'être informée du traitement de données à caractère personnel la concernant et elle dispose d'un droit d'accès, de rectification ou d'effacement de ces données ainsi que le droit à une limitation du traitement, qu'elle peut exercer directement auprès du responsable du traitement. À titre de solution de secours, l'exercice indirect des droits de la personne concernée par l'intermédiaire de l'autorité de contrôle chargée de la protection des données est également prévu par la Directive relative à la protection des données pour les autorités policières et judiciaires en matière pénale et il prend effet lorsque le responsable du traitement limite le droit de la personne concernée[762]. L'article 17 de la directive impose aux États membres d'adopter des mesures afin que les droits de la personne concernée puissent également être exercés par l'intermédiaire de l'autorité de contrôle. C'est la raison pour laquelle le responsable du traitement doit informer la personne concernée de la possibilité d'un accès indirect à ses données.

Obligations du responsable du traitement et du sous-traitant

Dans le cadre de la Directive relative à la protection des données pour les autorités policières et judiciaires en matière pénale, les responsables du traitement sont des autorités publiques compétentes ou d'autres organismes investis de prérogatives de puissance publique, qui déterminent les finalités et les moyens du traitement de données à caractère personnel. La directive impose plusieurs obligations au responsable du traitement afin d'assurer un niveau élevé de protection des données à caractère personnel traitées à des fins répressives.

Les autorités compétentes doivent tenir un journal des opérations de traitement qu'elles effectuent dans des systèmes de traitement automatisé. Des journaux doivent être tenus à tout le moins pour la collecte, la modification, la consultation, la communication, y compris les transferts, l'interconnexion et l'effacement de données à caractère personnel[763]. La directive prévoit que les journaux des opérations de consultation et de communication doivent permettre d'établir les motifs, la date et l'heure de celles-ci et, dans la mesure du possible, l'identification de la personne qui a consulté le système ou communiqué les données à caractère personnel, ainsi

761 *Ibid.*, art. 16, para. 4.

762 *Ibid.*, art. 17.

763 *Ibid.*, art. 25, para. 1.

que l'identité des destinataires des données à caractère personnel. Les journaux sont utilisés uniquement à des fins de vérification de la licéité du traitement, d'autocontrôle, de garantie de l'intégrité et de la sécurité des données à caractère personnel et à des fins de procédures pénales[764]. Le responsable du traitement et le sous-traitant doivent mettre ces journaux à la disposition de l'autorité de contrôle à la demande de celle-ci.

En particulier, une obligation générale est imposée au responsable du traitement de mettre en œuvre les mesures techniques et organisationnelles appropriées pour s'assurer que le traitement est effectué conformément à la directive et d'être en mesure de le démontrer[765]. Lors de l'élaboration de ces mesures, le responsable du traitement doit tenir compte de la nature, de la portée, du contexte du traitement et, surtout, de tout risque potentiel pour les droits et libertés des personnes physiques. Le responsable du traitement devrait adopter des politiques internes et mettre en œuvre des mesures favorisant le respect des principes de la protection des données, notamment celui de la protection des données dès la conception et par défaut[766]. Lorsque le traitement est susceptible d'engendrer un risque élevé pour les droits des personnes physiques, en raison du recours à de nouvelles technologies, par exemple, le responsable du traitement doit effectuer préalablement au traitement une analyse d'impact sur la protection des données[767]. La directive énumère également les mesures que les responsables du traitement doivent mettre en œuvre pour assurer la sécurité du traitement. Il s'agit notamment de mesures destinées à empêcher toute personne non autorisée d'accéder aux données à caractère personnel traitées par les responsables du traitement, de garantir que les personnes autorisées ne puissent accéder qu'aux données à caractère personnel sur lesquelles porte leur autorisation, de garantir que les fonctions du système de traitement opèrent correctement et que les données à caractère personnel conservées ne puissent pas être corrompues par un dysfonctionnement du système[768]. En cas de violation de données à caractère personnel, le responsable du traitement doit la notifier à l'autorité de contrôle dans les trois jours, en décrivant la nature de la violation, ses conséquences probables, les catégories de données à caractère personnel concernées et le nombre approximatif de personnes concernées touchées. La violation des données à caractère personnel doit également être notifiée à la personne

764 *Ibid.*, art. 25, para. 2.

765 *Ibid.*, art. 19.

766 *Ibid.*, art. 20.

767 *Ibid.*, art. 27.

768 *Ibid.*, art. 29.

concernée « dans les meilleurs délais » lorsqu'elle est susceptible d'engendrer un risque élevé pour ses droits et libertés[769].

La directive mentionne le principe de la responsabilité qui impose aux responsables du traitement de mettre en œuvre des mesures pour en garantir le respect. Les responsables du traitement doivent conserver des registres de toutes les catégories d'activités de traitement effectuées sous leur responsabilité. Le contenu détaillé de ces registres est décrit à l'article 24 de la directive. Les registres doivent être mis à la disposition de l'autorité de contrôle, à sa demande, de sorte qu'elle puisse vérifier les traitements effectués par le responsable du traitement. Une autre mesure importante destinée à renforcer la responsabilité est la désignation d'un délégué à la protection des données (DPD). Le responsable du traitement doit désigner un DPD, bien que la directive permette aux États membres de dispenser de cette obligation les tribunaux et d'autres autorités judiciaires indépendantes[770]. Les missions du DPD ressemblent à celles décrites dans le Règlement général sur la protection des données. Il contrôle le respect de la directive, fournit des informations et dispense des conseils aux employés qui procèdent au traitement sur les obligations qui leur incombent en vertu de la législation relative à la protection des données. Le DPD dispense également des conseils sur la nécessité de réaliser une analyse d'impact relative à la protection des données et il fait office de point de contact pour l'autorité de contrôle.

Transfert vers des pays tiers ou à des organisations internationales

Tout comme le RGPD, la directive fixe les conditions du transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales. Lorsque des données à caractère personnel sont transmises librement en dehors de la juridiction de l'UE, les garanties et le niveau élevé de protection prévus par le droit de l'Union pourraient être mis à mal. Les conditions du transfert sont toutefois assez différentes de celles établies par le RGPD. Le transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales est autorisé lorsque[771] :

- le transfert est nécessaire aux fins de la directive ;

769 *Ibid.*, art. 30 et 31.

770 *Ibid.*, art. 32.

771 *Ibid.*, art. 35.

- les données à caractère personnel sont transférées à une autorité compétente, au sens de la directive, du pays tiers ou de l'organisation internationale, bien qu'il existe une dérogation à cette règle dans des cas particuliers et spécifiques[772] ;

- le transfert vers des pays tiers ou à des organisations internationales de données à caractère personnel reçues dans le cadre d'une coopération transfrontalière exige l'autorisation de l'État membre d'où proviennent les données, bien qu'il existe des exceptions en cas d'urgence ;

- une décision d'adéquation a été adoptée par la Commission européenne, des garanties appropriées ont été mises en place ou des dérogations pour des situations particulières s'appliquent ;

- en cas de transferts ultérieurs de données à caractère personnel vers un autre pays tiers ou à une autre organisation internationale, l'autorité compétente qui a procédé au transfert initial doit autoriser le transfert ultérieur et prendre en considération, notamment, la gravité de l'infraction pénale et le niveau de protection des données dans le pays de destination du second transfert international[773].

Aux termes de la directive, des transferts de données à caractère personnel peuvent avoir lieu lorsque l'une des trois conditions est remplie. La première condition veut que la Commission européenne ait adopté une décision d'adéquation au titre de la directive. La décision peut s'appliquer à l'ensemble du territoire d'un pays tiers ou à des secteurs déterminés d'un pays tiers ou d'une organisation internationale. Cependant, cela n'est possible que si un niveau de protection adéquat est assuré et que les conditions prévues par la directive soient satisfaites[774]. Dans de tels cas, le transfert de données à caractère personnel n'est pas subordonné à l'autorisation de l'État membre[775]. La Commission européenne doit suivre les évolutions qui pourraient porter atteinte au fonctionnement des décisions d'adéquation. De plus, la décision doit inclure un mécanisme d'examen périodique. La Commission peut également abroger, modifier ou suspendre une décision lorsque les informations disponibles révèlent que la situation dans le pays tiers ou l'organisation internationale ne garantit plus un niveau de protection adéquat. Dans ce cas, la Commission doit

772 *Ibid.*, art. 39.

773 *Ibid.*, art. 35, para. 1.

774 *Ibid.*, art. 36.

775 *Ibid.*, art. 36, para. 1.

engager des consultations avec le pays tiers ou l'organisation internationale en vue de remédier à la situation.

En l'absence de décision d'adéquation, les transferts peuvent être basés sur des garanties appropriées. Celles-ci peuvent être fournies dans un instrument juridiquement contraignant ou le responsable du traitement peut procéder à une autoévaluation des circonstances du transfert des données à caractère personnel et conclure à l'existence de garanties appropriées. L'autoévaluation devrait tenir compte des éventuels accords de coopération conclus entre Europol ou Eurojust et le pays tiers ou l'organisation internationale, de l'existence d'obligations de confidentialité et de la limitation de la finalité ainsi que des assurances fournies que les données ne seront pas utilisées pour mettre à exécution toute forme de traitement cruel et inhumain, notamment la peine de mort[776]. Dans ce dernier cas, le responsable du traitement doit notifier à l'autorité de contrôle compétente les catégories de transfert relevant de cette catégorie[777].

Lorsqu'aucune décision d'adéquation n'a été adoptée ou qu'il n'existe pas de garanties appropriées, des transferts peuvent néanmoins être autorisés dans les situations particulières prévues par la directive. Elles concernent, notamment, la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne et la prévention d'une menace grave et imminente pour la sécurité publique de l'État membre ou d'un pays tiers[778].

Dans des cas particuliers et déterminés, les autorités compétentes peuvent transférer des données vers des destinataires établis dans des pays tiers qui ne sont pas des autorités compétentes lorsque l'une des trois conditions décrites plus haut est remplie et que les conditions supplémentaires visées à l'article 39 de la directive sont également satisfaites. En particulier, le transfert doit être strictement nécessaire à l'exécution de la mission de l'autorité compétente qui transfère les données, laquelle est également chargée d'établir qu'il n'existe pas de libertés ni de droits fondamentaux de la personne concernée qui prévalent sur l'intérêt public nécessitant le transfert. Ce type de transferts doit être documenté et l'autorité compétente qui effectue le transfert doit en informer l'autorité de contrôle compétente[779].

776 *Ibid.*, considérant 71.

777 *Ibid.*, art. 37, para. 1.

778 *Ibid.*, art. 38, para. 1.

779 *Ibid.*, art. 37, para. 3.

Enfin, s'agissant des pays tiers et des organisations internationales, la directive impose également la mise en place de mécanismes de coopération internationaux destinés à faciliter l'application effective de la législation et elle aide ainsi les autorités de contrôle de la protection des données à coopérer avec leurs homologues étrangers[780].

Contrôle indépendant et voies de recours pour les personnes concernées

Chaque État membre doit faire en sorte qu'une ou plusieurs autorités de contrôle nationales indépendantes soient chargées de surveiller l'application des dispositions adoptées au titre de la directive et de dispenser des conseils en la matière[781]. L'autorité de contrôle établie au titre de la directive peut être la même que celle établie au titre du Règlement général relatif à la protection des données, mais les États membres sont libres de désigner une autorité différente, pour autant qu'elle respecte le principe d'indépendance. Les autorités de contrôle traitent également les réclamations introduites par toute personne au sujet de la protection de ses droits et libertés à l'égard du traitement de données à caractère personnel la concernant par des autorités publiques.

Lorsque l'exercice des droits de la personne concernée est refusé pour des motifs impérieux, celle-ci doit disposer d'un droit de recours devant l'autorité de contrôle nationale compétente et/ou devant un tribunal. Lorsqu'une personne subit un dommage du fait d'une violation des dispositions nationales mettant en œuvre la directive, elle a le droit d'obtenir du responsable du traitement ou de toute autre autorité compétente en vertu du droit national, réparation du préjudice subi[782]. En règle générale, la personne concernée doit avoir accès à un recours juridictionnel pour toute violation de ses droits garantis par les dispositions nationales mettant en œuvre la directive[783].

780 *Ibid.*, art. 40.

781 *Ibid.*, art. 41.

782 *Ibid.*, art. 56.

783 *Ibid.*, art. 54.

8.3. Autres instruments juridiques spécifiques en matière de protection des données dans le domaine répressif

Outre la Directive relative à la protection des données pour les autorités policières et judiciaires en matière pénale, l'échange d'informations détenues par des États membres dans des domaines particuliers est régi par plusieurs instruments juridiques, comme 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, la Décision 2000/642/JAI du Conseil relative aux modalités de coopération entre les cellules de renseignement financier des États membres en ce qui concerne l'échange d'informations et la Décision-cadre 2006/960/JAI du Conseil relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des États membres de l'Union européenne[784].

Il importe de préciser que la coopération transfrontalière[785] entre les autorités compétentes entraîne l'échange croissant de données relatives à l'immigration. Ce domaine du droit n'est pas considéré comme faisant partie des questions de police et de justice pénale, mais, à de nombreux égards, il intéresse le travail de la police et des autorités judiciaires. Il en va de même des données sur les produits importés dans l'UE ou exportés depuis l'UE. La suppression des contrôles aux frontières intérieures au sein de l'espace Schengen a accru le risque de fraude et les États membres ont dû intensifier leur coopération, notamment en renforçant l'échange transfrontalier de données afin de détecter et de poursuivre plus efficacement les violations du droit douanier national et de l'UE. En outre, ces dernières années, le monde a connu une augmentation du terrorisme et de la criminalité grave et organisée, ce qui peut impliquer des déplacements sur le plan international et a mis en

784 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 ; Décision-cadre 2006/960/JAI du Conseil du 18 décembre 2006 relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des États membres de l'Union européenne, JO L 386.

785 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 en matière d'échange d'informations (EIXM)*, COM(2012) 735 final, Bruxelles, 7 décembre 2012.

évidence la nécessité de renforcer la coopération transfrontalière entre autorités policières et répressives dans de nombreuses affaires[786].

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 transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière (« Décision Prüm »), qui a transposé le Traité de Prüm dans le droit de l'UE en 2008[787]. Le Traité de Prüm était un accord international de coopération policière signé en 2005 par l'Allemagne, l'Autriche, la Belgique, l'Espagne, la France, le Luxembourg et les Pays-Bas[788].

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 la migration illégale. À cette fin, la décision prévoit des dispositions concernant :

- l'accès automatisé aux profils ADN, aux données d'empreintes digitales et à 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.

786 Commission européenne (2011), 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 de la Commission, COM(2011) 32 final, Bruxelles, 2 février 2011, p. 1.

787 Conseil de l'Union européenne (2008), Décision 2008/615/JAI du Conseil du 23 juin 2008 relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière, JO 2008 L 210.

788 Traité 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 relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme, la criminalité transfrontalière et la migration illégale.

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, dont la compatibilité avec la Directive relative à la protection des données pour les autorités policières et judiciaires en matière pénale devra être évaluée. Les organes compétents pour le contrôle de ces flux de données sont les autorités nationales de contrôle de la protection des données.

Décision-cadre 2006/960/JAI : l'initiative suédoise

La Décision-cadre 2006/960/JAI (« l'initiative suédoise »)[789] est un autre exemple de coopération transfrontalière en matière d'échange de données nationales par les autorités répressives. L'initiative suédoise porte tout particulièrement sur l'échange d'informations et de renseignements et établit des règles spécifiques pour la protection des données en son article 8.

Cet instrument prévoit que l'utilisation des informations et des renseignements échangés doit être soumise aux dispositions nationales en matière de protection des données de l'État membre qui reçoit les informations, selon les mêmes règles que si elles avaient été collectées dans ledit État. L'article 8 poursuit en précisant que lorsqu'ils transmettent des informations et des renseignements, les services répressifs compétents peuvent, en application de leur droit national, imposer aux services répressifs destinataires des conditions concernant l'usage de ces informations et renseignements. Des conditions peuvent aussi être imposées en ce qui concerne la diffusion des résultats de l'enquête pénale ou de l'opération de renseignement en matière pénale qui a donné lieu à l'échange d'informations et de renseignements. Toutefois, lorsque le droit national prévoit des dérogations aux restrictions d'utilisation (par exemple au profit des autorités judiciaires, des institutions législatives, etc.), les informations et renseignements ne peuvent être utilisés qu'après consultation de l'État membre émetteur.

Les informations et renseignements fournis peuvent être utilisés :

- pour les finalités pour lesquelles ils ont été transmis ; ou
- pour prévenir une menace grave et imminente à la sécurité publique.

789 Conseil de l'Union européenne (2006), Décision-cadre 2006/960/JAI du Conseil du 18 décembre 2006 relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des États membres de l'Union européenne, JO L 386/89 du 29 décembre 2006.

Le traitement à d'autres fins peut être autorisé, mais uniquement moyennant l'autorisation préalable de l'État membre émetteur.

L'initiative suédoise précise également que les données à caractère personnel traitées doivent être protégées conformément aux instruments internationaux applicables, comme :

- la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel[790] ;
- le Protocole additionnel du 8 novembre 2001 à cette Convention concernant les autorités de contrôle et les flux transfrontières de données[791] ;
- la Recommandation R (87) 15 du Conseil de l'Europe visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police[792].

La Directive PNR de l'UE

Les données des dossiers passagers (PNR) concernent les informations sur les passagers aériens qui sont collectées et conservées dans les systèmes de réservation et de contrôle des départs des transporteurs aériens pour leurs propres finalités commerciales. Elles contiennent différents types d'informations, comme les dates du voyage, l'itinéraire, les informations figurant sur le billet, les coordonnées, l'agence de voyages par l'intermédiaire de laquelle le vol a été réservé, le moyen de paiement utilisé, le numéro de siège et les informations sur les bagages[793]. Le traitement des données PNR peut aider les services répressifs à identifier des suspects potentiels ou connus et à analyser leurs schémas de déplacement et d'autres indicateurs généralement associés à des activités criminelles. Une analyse des données

790 Conseil de l'Europe (1981), Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, STCE nº 108.

791 Conseil de l'Europe (2001), 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 nº 108.

792 Conseil de l'Europe (1987), Recommandation nº R (87) 15 du Comité des Ministres aux États membres visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police (adoptée par le Comité des Ministres le 17 septembre 1987 lors de la 410e réunion des Délégués des Ministres).

793 Commission européenne (2011), 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 de la Commission, COM(2011) 32 final, 2 février 2011, p. 1.

PNR permet également de tracer rétroactivement les itinéraires et les contacts de personnes soupçonnées d'être impliquées dans des activités criminelles, ce qui peut permettre aux autorités répressives d'identifier des réseaux criminels[794]. L'UE a conclu différents accords avec des pays tiers en vue d'échanger des données PNR, comme cela a été expliqué au chapitre 7. Elle a également introduit le traitement des données PNR dans l'UE par le biais de la Directive (UE) 2016/681 relative à l'utilisation des données PNR pour la prévention et la détection des infractions terroristes et des formes graves de criminalité (Directive PNR)[795]. Cette directive impose aux transporteurs aériens l'obligation de transmettre les données PNR aux autorités compétentes et établit des garanties strictes en matière de protection pour le traitement et la collecte de ces données. La Directive PNR s'applique aux vols internationaux au départ et à destination de l'UE, mais également aux vols intra-UE si un État membre le décide[796].

Les données PNR collectées ne doivent contenir que les informations autorisées par la Directive PNR. Elles doivent être conservées dans une unité d'informations unique, en un lieu sécurisé dans chaque État membre. Les données PNR doivent être dépersonnalisées six mois après leur transmission par le transporteur aérien et elles peuvent être conservées pendant une période de cinq ans au maximum[797]. Les données PNR sont échangées entre des États membres, entre des États membres et Europol et avec des pays tiers, mais uniquement au cas par cas.

La transmission et le traitement des données PNR et les droits garantis des personnes concernées doivent être conformes à la Directive relative à la protection des données pour les autorités policières et judiciaires en matière pénale et assurer le niveau élevé de protection de la vie privée et des données à caractère personnel qu'exigent la Charte, la Convention 108 modernisée et la CEDH.

Les autorités nationales de contrôle indépendantes et compétentes au titre de la Directive relative à la protection des données pour les autorités policières et judiciaires en matière pénale sont également chargées de surveiller l'application des

794 Commission européenne (2015), Fiche technique de lutte contre le terrorisme au niveau de l'UE, Aperçu des actions, mesures et initiatives de la Commission, Bruxelles, 11 janvier 2015.

795 Directive (UE) 2016/681 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 de la Commission, JO 2016 L 119, p. 132.

796 Directive PNR, JO L 119, p. 132, art. 1er, para. 1, et art. 2, para. 1.

797 *Ibid.*, art. 12, para. 1, et art. 12, para. 2.

dispositions adoptées par les États membres au titre de la Directive PNR et de les conseiller en la matière.

Conservation des données de télécommunications

La Directive sur la conservation des données[798], qui a été déclarée invalide le 8 avril 2014 dans l'arrêt *Digital Rights Ireland*, obligeait les fournisseurs de services de communication à tenir à disposition les données relatives au trafic dans le but spécifique de la lutte contre les formes graves de criminalité pendant une durée minimale de six mois et maximale de deux ans, que le fournisseur ait ou non encore besoin de ces données à des fins de facturation ou pour fournir techniquement le service.

La conservation des données de télécommunications constitue clairement une ingérence dans le droit à la protection des données[799]. La légitimité de cette ingérence a été contestée dans le cadre de plusieurs procédures judiciaires engagées dans des États membres de l'UE[800].

Exemple : dans l'affaire *Digital Rights Ireland* et *Kärntner Landesregierung et autres*[801], le groupe Digital Rights et M. Seitlinger ont engagé une action devant la Haute Cour de justice d'Irlande et la Cour constitutionnelle autrichienne, respectivement, par laquelle ils contestaient la légalité de mesures nationales autorisant la conservation de données de télécommunications électroniques. Digital Rights a demandé à la juridiction irlandaise de déclarer invalide la Directive 2006/24 et la partie du droit pénal national relative aux infractions terroristes. De son côté, M. Seitlinger et plus de 11 000 autres requérants ont contesté et demandé l'annulation d'une

798 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.

799 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.

800 Allemagne, Cour constitutionnelle fédérale (*Bundesverfassungsgericht*), 1 BvR 256/08, 2 mars 2010 ; Roumanie, Cour constitutionnelle fédérale (*Curtea Constituțională a României*), nº 1258, 8 octobre 2009 ; République tchèque, Cour constitutionnelle (Ústavní soud České republiky), 94/2011 Coll., 22 mars 2011.

801 CJUE, affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources et autres* et *Kärntner Landesregierung et autres* [GC], 8 avril 2014, point 65.

disposition de la loi autrichienne sur les télécommunications qui transposait la Directive 2006/24.

En réponse à ces demandes de décisions préjudicielles, la CJUE a déclaré invalide la Directive relative à la conservation des données. De l'avis de la CJUE, les données qui pouvaient être conservées au titre de la directive fournissaient des informations précises sur les personnes physiques lorsqu'elles étaient considérées globalement. En outre, la Cour s'est penchée sur la gravité de l'ingérence dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel. Elle a conclu que la conservation répond à un objectif d'intérêt public, à savoir la lutte contre les formes graves de criminalité et, partant, la sécurité publique. La CJUE a toutefois déclaré que le législateur de l'UE avait violé le principe de proportionnalité en adoptant la directive. Bien que la directive puisse être adéquate pour atteindre l'objectif visé, « cette directive comporte une ingérence dans ces droits fondamentaux [au respect de la vie privée et à la protection des données à caractère personnel] d'une vaste ampleur et d'une gravité particulière [...] sans qu'une telle ingérence soit précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au strict nécessaire ».

En l'absence de législation spécifique sur la conservation des données, celle-ci est autorisée en tant qu'exception à la confidentialité des données de télécommunications en vertu de la Directive 2002/58/CE (Directive « vie privée et communications électroniques »)[802] à titre de mesure préventive, mais uniquement dans le but de lutter contre les formes graves de criminalité. Une telle conservation doit être limitée à ce qui est strictement nécessaire au regard des catégories de données conservées, du mode de communication concerné, des personnes concernées et de la durée de conservation retenue. Les autorités nationales peuvent avoir accès aux données conservées dans des conditions strictes, incluant le contrôle préalable d'une autorité indépendante. Les données doivent être conservées sur le territoire de l'UE.

802 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.

Exemple : après l'arrêt *Digital Rights Ireland* et *Kärntner Landesregierung et autres*[803], la CJUE a été saisie de deux autres affaires se rapportant à l'obligation générale imposée par la Suède et le Royaume-Uni aux fournisseurs de services de communication électronique de conserver les données de télécommunications, comme l'exigeait la directive invalidée relative à la conservation des données. Dans les affaires *Tele2 Sverige* et *Home Department c. Tom Watson et autres*[804], la CJUE a conclu que la législation nationale imposant la conservation généralisée et indifférenciée des données sans exiger de lien entre les données qui doivent être conservées et une menace à la sécurité publique et sans préciser aucune condition – par exemple, la durée de conservation, la zone géographique, le groupe de personnes susceptibles d'être impliquées dans des formes graves de criminalité – va au-delà de ce qui est strictement nécessaire et ne saurait être considérée comme justifiée dans une société démocratique, comme l'exige la Directive 2002/58/CE, lue à la lumière de la Charte des droits fondamentaux.

Perspectives

En janvier 2017, la Commission a publié une proposition de règlement concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques, dont le but est de remplacer la Directive 2002/58/CE[805]. La proposition ne contient aucune disposition spécifique sur la conservation des données. Elle prévoit toutefois que les États membres puissent légiférer afin de limiter certaines obligations et certains droits prévus par le règlement lorsqu'une telle limitation constitue une mesure nécessaire et proportionnée pour préserver certains intérêts publics, comme la sûreté nationale, la défense, la sécurité publique ainsi que la prévention et la détection des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales[806]. Par conséquent, les États membres sont libres de maintenir ou de créer des cadres

803 CJUE, affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources et autres* et *Kärntner Landesregierung et autres* [GC], 8 avril 2014.

804 CJUE, affaires jointes C-203/15 et C-698/15, *Tele2 Sverige AB c. Post- och telestyrelsen et Secretary of State for the Home Department c. Tom Watson et autres* [GC], 21 décembre 2016.

805 Commission européenne (2017), Proposition de règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (Règlement « vie privée et communications électroniques »), COM(2017) 10 final, Bruxelles, 10 janvier 2017.

806 *Ibid*., considérant 26.

nationaux de conservation des données qui prévoient des mesures de conservation ciblées dans la mesure où ces cadres respectent le droit de l'Union, compte tenu de la jurisprudence de la CJUE sur l'interprétation de la Directive « vie privée et communications électroniques » et de la Charte[807]. Au moment de rédiger ce manuel, les discussions sur l'adoption du règlement se poursuivaient.

Accord-cadre UE-États-Unis sur la protection des données à caractère personnel échangées à des fins répressives

Le 1er février 2017, l'accord-cadre UE-USA (*Umbrella Agreement*) sur le traitement de données à caractère personnel à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière est entré en vigueur[808]. L'accord-cadre UE-États-Unis a pour but de garantir un niveau élevé de protection des données aux citoyens de l'UE tout en renforçant la coopération entre les autorités répressives européennes et américaines. Il complète les accords UE-États-Unis et État membre-États-Unis existants conclus entre les autorités répressives, tout en contribuant à mettre en place des règles claires et harmonisées de protection des données pour les accords futurs en la matière. À cet égard, l'accord vise à établir un cadre juridique durable en vue de faciliter l'échange d'informations.

En soi, l'accord ne constitue pas une base juridique adéquate pour l'échange de données à caractère personnel, mais il offre, en revanche, des garanties appropriées en matière de protection des données aux personnes concernées. Il couvre tous les traitements de données à caractère personnel nécessaires à la prévention et à la détection des infractions pénales, y compris le terrorisme, ainsi que les enquêtes et les poursuites en la matière[809].

807 Voir l'exposé des motifs de la Proposition de règlement « vie privée et communications électroniques », COM(2017) 10 final, point 1.3.

808 Voir Conseil de l'UE (2016), « *Enhanced data protection rights for EU citizens in law enforcement cooperation: EU and US sign 'Umbrella agreement'* », communiqué de presse 305/16, 2 juin 2016.

809 Accord entre les États-Unis d'Amérique et l'Union européenne sur la protection des informations à caractère personnel traitées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière du 18 mai 2016 (OR. anglais) 8857/16, art. 3, para. 1. Voir aussi la notification de la Commission sur les négociations de l'accord UE-USA du 26 mai 2010, MEMO/10/2016 et le communiqué de presse de la Commission européenne (2010) sur des normes élevées en matière de respect de la vie privée dans un accord UE-États-Unis relatif à la protection des données du 26 mai 2010, IP/10/609.

L'accord prévoit de multiples garanties afin de faire en sorte que les données à caractère personnel ne soient utilisées qu'aux fins qu'il détermine. En particulier, il prévoit la protection suivante pour les citoyens de l'UE :

- limitations de l'utilisation des données : les données à caractère personnel ne peuvent être utilisées qu'aux fins de la prévention et de la détection des infractions pénales et des enquêtes et poursuites en la matière ;

- la protection contre toute discrimination arbitraire et injustifiable ;

- transferts ultérieurs : tout transfert ultérieur vers un pays tiers de l'UE et des États-Unis ou une organisation internationale doit être soumis à l'autorisation préalable de l'autorité compétente du pays d'où les données ont été exportées initialement ;

- qualité des données : les données à caractère personnel doivent être conservées en tenant compte de leur exactitude, de leur pertinence, de leur caractère opportun et de leur exhaustivité ;

- sécurité du traitement, y compris la notification des violations des données à caractère personnel ;

- le traitement de données sensibles n'est autorisé que moyennant des garanties appropriées prévues par la loi ;

- durées de conservation : les données à caractère personnel ne peuvent pas être conservées plus longtemps que nécessaire ou approprié ;

- droits d'accès et de rectification : toute personne a le droit d'obtenir l'accès aux données à caractère personnel la concernant, sous certaines conditions, et pourra en demander la rectification si elles sont inexactes ;

- les décisions automatisées requièrent des garanties appropriées, notamment la possibilité d'obtenir une intervention humaine ;

- contrôle effectif, y compris la coopération entre les autorités de contrôle américaines et de l'UE ;

- recours juridictionnel et opposabilité : les citoyens de l'UE ont le droit[810] de demander réparation devant des juridictions américaines lorsque les autorités américaines refusent l'accès ou la rectification de données à caractère personnel les concernant ou les divulguent de façon illicite.

L'accord-cadre a également établi un système destiné à informer l'autorité de contrôle compétente dans l'État membre des personnes concernées de toute violation de la protection des données, si nécessaire. Les garanties légales prévues par l'accord assurent l'égalité de traitement des citoyens de l'UE aux États-Unis en cas de violation de la vie privée[811].

8.3.1. Protection des données au sein des agences de l'UE chargées de la justice et de l'application de la loi

Europol

Europol, l'agence de l'UE pour la coopération des services répressifs, a son siège à La Haye et dispose d'unités nationales Europol (UNE) dans chaque État membre. Europol a été créé en 1998 et son statut légal actuel d'institution de l'UE repose sur le Règlement relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (« Règlement Europol »)[812]. 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 I au Règlement Europol, affectant deux ou plusieurs États membres. Pour ce faire, Europol échange des informations et fait fonction de centre d'information de l'UE, fournissant des analyses de renseignements et des évaluations de la menace.

810 Le US Judicial Redress Act a été signé par le Président Obama le 24 février 2016.

811 Le Contrôleur européen de la protection des données a publié un avis sur l'accord UE-États-Unis, dans lequel il recommande, entre autres, les adaptations suivantes : 1) ajout de l'expression « aux fins spécifiques pour lesquelles elles ont été transférées » à l'article relatif à la conservation de données qui ne doit pas être plus longue que nécessaire et approprié et 2) exclure les transferts massifs de données sensibles, qui pourraient être possibles. Voir CEPD, Avis 1/2016, *Avis préliminaire 1/2016 du CEPD relatif à l'accord entre les États-Unis d'Amérique et l'Union européenne concernant la protection des informations à caractère personnel afin de prévenir et de détecter les informations et de procéder aux enquêtes et poursuites en la matière*, para. 35.

812 Règlement (UE) 2016/794 du Parlement européen et du Conseil du 11 mai 2016 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI, JO 2016 L 135, p. 53.

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 des 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. Les organes de l'UE, des pays tiers ou des organisations internationales peuvent également fournir des informations à Europol.

Europol peut également se procurer des informations, y compris des données à caractère personnel, auprès de sources publiques, comme internet. Les transferts de données à caractère personnel vers des organismes de l'UE ne sont autorisés que s'ils sont nécessaires à l'exécution de la mission d'Europol ou de l'organisme de l'UE destinataire. Les transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales ne sont autorisés que si la Commission européenne décide que le pays tiers ou l'organisation internationale en question offre un niveau adéquat de protection des données (« décision d'adéquation ») ou lorsqu'il existe un accord international ou un accord de coopération. Europol peut recevoir et traiter des données à caractère personnel provenant de parties privées et de personnes privées à la stricte condition que ces données soient transférées par une UNE conformément à son droit national, par un point de contact dans un pays tiers ou une organisation internationale avec lequel une coopération a été établie par le biais d'un accord de coopération, ou par une autorité d'un pays tiers ou d'une organisation internationale faisant l'objet d'une décision d'adéquation ou avec laquelle l'UE a conclu un accord international. Tous les échanges d'informations passent par l'application de réseau d'échange sécurisé d'informations (SIENA).

Face aux développements récents, des centres spécialisés ont été créés au sein d'Europol. Le Centre européen de lutte contre la cybercriminalité a été développé au sein de l'agence en 2013[813]. Il sert de plateforme européenne d'information sur la cybercriminalité et contribue à accélérer les réactions en cas de criminalité en ligne, développe et déploie des capacités numériques en matière de criminalistique et

813 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.

élabore des bonnes pratiques en matière d'enquêtes sur la cybercriminalité. L'activité du Centre est axée sur :

- les cybercrimes commis par des groupes organisés dans le but de générer d'importants bénéfices, tels 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 gravement les systèmes critiques de l'UE en matière d'infrastructure et d'information.

Le Centre européen de lutte contre le terrorisme (ECTC) a été créé en janvier 2016 et a pour mission d'apporter un soutien opérationnel aux États membres dans leurs enquêtes sur des infractions terroristes. Il compare les données opérationnelles en temps réel aux données dont Europol dispose déjà, détecte rapidement les liens financiers et analyse tous les détails disponibles des enquêtes afin de cerner l'architecture d'un réseau terroriste[814].

Le Centre européen pour la lutte contre le trafic de migrants (EMSC) a été établi en février 2016, à la suite de la réunion du Conseil de novembre 2015, afin d'aider les États membres à cibler et à démanteler les réseaux criminels impliqués dans le trafic de migrants. Il fait fonction de centre d'échange d'informations au soutien des bureaux des taskforces européennes régionales de Catane (Italie) et du Pirée (Grèce), qui aident les autorités nationales dans plusieurs domaines comme le partage de renseignements, les enquêtes criminelles et la poursuite des réseaux criminels de trafic de personnes[815].

Le régime de protection des données régissant les activités d'Europol a été renforcé et repose sur les principes du Règlement relatif à la protection des données des institutions de l'UE[816] ; il est également compatible avec la Directive relative à la protection des données pour les autorités policières et judiciaires en matière pénale, la Convention 108 modernisée et la Recommandation relative à la police.

814 Voir la page web d'Europol sur l'ECTC.

815 Voir la page web d'Europol sur l'EMSC.

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

Le traitement de données à caractère personnel concernant des victimes d'infraction pénale, des témoins ou d'autres personnes pouvant fournir des informations sur des infractions pénales, ou concernant des personnes de moins de 18 ans, est autorisé s'il est strictement nécessaire et proportionné pour prévenir ou lutter contre les formes de criminalité relevant des objectifs d'Europol[817]. Le traitement de données sensibles est interdit à moins qu'il ne soit strictement nécessaire et proportionné pour prévenir ou lutter contre les formes de criminalité relevant des objectifs d'Europol et à moins que ces données ne complètent d'autres données à caractère personnel traitées par Europol[818]. Dans les deux cas précités, seul Europol peut avoir accès aux données pertinentes[819].

Les données ne sont stockées que pour la durée nécessaire et proportionnée et la poursuite de la conservation est subordonnée à un examen tous les trois ans, sans lequel les données sont effacées automatiquement[820].

Europol peut, à certaines conditions, directement transférer des données à caractère personnel à un organe de l'UE, à une autorité d'un pays tiers ou à une organisation internationale[821]. Les violations de données, lorsqu'elles risquent de porter gravement atteinte aux droits et libertés des personnes concernées, doivent leur être communiquées sans retard injustifié[822]. Au niveau des États membres, une autorité de contrôle nationale sera désignée pour contrôler le traitement de données à caractère personnel par Europol[823].

Le Contrôleur européen de la protection des données est chargé de surveiller et de garantir la protection des libertés et droits fondamentaux des personnes physiques à l'égard des traitements de données à caractère personnel effectués par Europol, ainsi que de conseiller Europol et les personnes concernées sur toute question en rapport avec le traitement de données à caractère personnel. À ces fins, le CEPD joue le rôle d'un organe d'investigation et d'examen des plaintes et agit en étroite coopération avec les autorités de contrôle nationales[824]. Le CEPD et les autorités

817 Règlement Europol, art. 30, para. 1.

818 *Ibid.*, art. 30, para. 2.

819 *Ibid.*, art. 30, para. 3.

820 *Ibid.*, art. 31.

821 *Ibid.*, art. 24 et 25, respectivement.

822 *Ibid.*, art. 35.

823 Règlement Europol, art. 42.

824 *Ibid.*, art. 43 et 44.

nationales de contrôle se réunissent au moins deux fois par an au sein du comité de coopération, qui a un rôle consultatif[825]. Les États membres sont tenus d'établir officiellement une autorité de contrôle chargée de contrôler l'admissibilité du transfert de données à caractère personnel d'un État membre vers Europol ainsi que l'extraction et toute communication à Europol de données à caractère personnel par l'État membre[826]. Les États membres sont également tenus de veiller à ce que l'autorité nationale de contrôle puisse agir en toute indépendance dans l'exécution de ses tâches et obligations au titre du Règlement Europol[827]. Aux fins de vérifier la licéité du traitement des données, d'autoévaluer ses activités et de garantir l'intégrité et la sécurité des données, Europol établit des journaux ou une documentation de ses activités de traitement. Ces journaux contiennent des informations sur les traitements dans des systèmes de traitement automatisés qui concernent la collecte, la modification, la consultation, la divulgation, la combinaison ou l'effacement des données[828].

Toute décision du CEPD peut faire l'objet d'un recours devant la CJUE[829]. Toute personne physique ayant subi un dommage du fait d'une opération de traitement de données illicite a le droit d'obtenir réparation du préjudice subi, soit d'Europol, soit de l'État membre où le fait dommageable s'est produit, en formant un recours devant la CJUE dans le premier cas ou devant une juridiction nationale compétente dans le second cas[830]. En outre, un groupe de contrôle parlementaire conjoint spécialisé (GCPC) des parlements nationaux et du Parlement européen peut contrôler les activités d'Europol[831]. Toute personne physique a le droit d'obtenir l'accès à toute donnée à caractère personnel qu'Europol peut détenir sur elle, en plus du droit de solliciter la vérification, la rectification ou l'effacement de ces données à caractère personnel. Ces droits peuvent être soumis à des dérogations et à des limitations.

Eurojust

Créé en 2002, Eurojust est un organe de l'UE dont le siège est situé à La Haye. Il promeut la coopération judiciaire dans les enquêtes et poursuites relatives aux formes

825 *Ibid.*, art. 45.
826 *Ibid.*, art. 42, para. 1.
827 *Ibid.*, art. 42, para. 1.
828 *Ibid.*, art. 40.
829 *Ibid.*, art. 48.
830 *Ibid.*, art. 50.
831 *Ibid.*, art. 51.

graves de criminalité affectant au moins deux États membres[832]. 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 au sein d'un collège pour exécuter 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 suspectées d'avoir commis une infraction pénale relevant de la compétence d'Eurojust, d'y avoir participé ou d'avoir été condamnées à ce titre. Eurojust peut également traiter certaines informations relatives à des témoins ou victimes d'infractions pénales relevant de sa compétence[833]. 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 peut coopérer avec d'autres institutions, organes et agences de l'UE 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.

832 Conseil de l'Union européenne (2002), Décision 2002/187/JAI du Conseil du 28 février 2002 instituant Eurojust afin de renforcer la lutte contre les formes graves de criminalité, JO L 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 du Conseil 2009/426/JAI 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).

833 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.

S'agissant de la protection des données, Eurojust doit garantir un niveau de protection au moins équivalent aux principes de la Convention 108 modernisée 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 établies par des accords de coopération ou des arrangements de travail conformément aux Décisions Eurojust du Conseil et aux règles d'Eurojust relatives à la protection des données[834].

Une autorité de contrôle conjointe (ACC) indépendante a été établie au sein d'Eurojust et a pour mission de contrôler les traitements de données à caractère personnel effectués par Eurojust. Tout particulier peut former un recours devant l'ACC s'il n'est pas satisfait par une décision d'Eurojust en réponse à une demande d'accès, de rectification, de verrouillage ou d'effacement de données à caractère personnel le concernant. Lorsqu'Eurojust traite des données à caractère personnel de façon illicite, il répond de tout préjudice causé à la personne concernée conformément à la législation nationale de l'État membre dans lequel il a son siège, à savoir les Pays-Bas.

Perspectives

La Commission européenne a présenté une proposition de règlement visant à réformer Eurojust en juillet 2013. Cette proposition était accompagnée d'une proposition visant à créer un parquet européen (voir plus loin). Ce règlement a pour ambition de rationaliser les fonctions et la structure d'Eurojust afin de les aligner sur le Traité de Lisbonne. Par ailleurs, l'objectif de la réforme est d'opérer une distinction claire entre les tâches opérationnelles d'Eurojust, exécutées par le collège, et ses tâches administratives. Cela permettra également aux États membres de se concentrer davantage sur les tâches opérationnelles. Un nouveau directoire sera mis en place afin d'aider le collège dans l'exécution des tâches administratives[835].

Parquet européen

Les États membres disposent d'une compétence exclusive pour poursuivre les infractions pénales en matière de fraude et d'application incorrecte du budget de l'UE ayant également des conséquences transfrontières potentielles. L'importance d'enquêter, de poursuivre et de renvoyer en jugement les auteurs de ces infractions

834 Dispositions du Règlement intérieur d'Eurojust relatives au traitement et à la protection de données à caractère personnel, JO 2005 C 68, 19 mars 2005, p. 1.

835 Voir la page web de la Commission européenne sur Eurojust.

s'est accrue, en particulier du fait de la crise économique actuelle[836]. La Commission européenne a proposé un règlement visant à créer un Parquet européen indépendant[837] pour lutter contre les infractions pénales portant atteinte aux intérêts financiers de l'UE. Le Parquet européen sera établi par la procédure de coopération renforcée, qui permet à neuf États membres au minimum d'établir une coopération renforcée dans un domaine particulier au sein des structures de l'UE, sans la participation des autres États membres de l'UE[838]. L'Allemagne, la Belgique, la Bulgarie, la Croatie, Chypre, et l'Espagne, l'Estonie, la Finlande, la France, la Grèce, la Lettonie, la Lituanie, le Luxembourg, le Portugal, la République tchèque, la Roumanie, la Slovénie, et la Slovaquie ont rejoint la coopération renforcée, tandis que l'Autriche et l'Italie ont fait part de leur intention de le faire[839].

Le Parquet européen sera compétent pour enquêter sur les cas de fraude et d'autres infractions pénales portant atteinte aux intérêts financiers de l'UE, dans le but de coordonner efficacement les enquêtes et les poursuites dans les différents ordres juridiques nationaux et d'optimiser l'utilisation des ressources et l'échange d'informations au niveau européen[840].

Le Parquet européen sera dirigé par un procureur européen, assisté d'au moins un procureur européen délégué dans chaque État membre, qui sera chargé de mener les enquêtes et les poursuites dans cet État membre.

La proposition met en place des garde-fous solides pour garantir les droits des personnes impliquées dans les enquêtes du Parquet européen, conformément au droit national, au droit de l'Union et à la Charte des droits fondamentaux de l'UE. Les mesures d'enquête qui touchent principalement les droits fondamentaux seront

836 Voir Commission européenne (2013), Proposition de règlement du Conseil portant création du Parquet européen, COM(2013) 534 final, Bruxelles, 17 juillet 2013, p. 1, et la page web de la Commission sur le Parquet européen.

837 Commission européenne (2013), Proposition de règlement du Conseil portant création du Parquet européen, COM(2013) 534 final, Bruxelles, 17 juillet 2013.

838 Traité sur le fonctionnement de l'Union européenne, art. 86, para. 1, et art. 329, para. 1.

839 Voir Conseil de l'Union européenne (2017), « *20 member states agree on the details of creating the European Public Prosecutor's Office (EPPO)* », communiqué de presse, 8 juin 2017.

840 Commission européenne (2013), Proposition de règlement du Conseil portant création du Parquet européen, COM(2013) 534 final, Bruxelles, 17 juillet 2013, p. 1 et p. 51. Voir également la page web de la Commission européenne sur le Parquet européen.

soumises à l'autorisation d'une juridiction nationale[841]. Les enquêtes du Parquet européen feront l'objet d'un contrôle juridictionnel des juges nationaux[842].

Le Règlement relatif à la protection des données des institutions de l'UE[843] s'appliquera au traitement des données administratives à caractère personnel effectué par le Parquet européen. En ce qui concerne le traitement de données à caractère personnel liées à des questions opérationnelles, à l'instar d'Europol, le Parquet européen disposera d'un régime de protection des données indépendant, similaire à celui qui régit les activités d'Europol et d'Eurojust, étant donné que l'exécution des fonctions du Parquet européen impliquera le traitement de données à caractère personnel par des autorités répressives et judiciaires au niveau national. Les règles du Parquet européen en matière de protection des données sont donc pratiquement identiques à celles visées dans la Directive relative à la protection des données pour les autorités policières et judiciaires en matière pénale. Selon la proposition relative à la création du Parquet européen, le traitement de données à caractère personnel doit suivre les principes de licéité et de loyauté, de limitation de la finalité, de minimisation des données, d'exactitude, d'intégrité et de confidentialité. Le Parquet européen doit, dans la mesure du possible, établir une distinction claire entre les données à caractère personnel de différents types de personnes concernées, tels que les personnes condamnées pour une infraction pénale et les personnes qui sont simplement suspectes, victimes et témoins. Il doit également s'efforcer de vérifier la qualité des données à caractère personnel traitées et distinguer, dans la mesure du possible, les données à caractère personnel reposant sur des faits de celles reposant sur des appréciations personnelles.

La proposition contient des dispositions sur les droits des personnes concernées, notamment le droit à l'information, le droit d'obtenir l'accès, la rectification ou l'effacement de données à caractère personnel les concernant, le droit à la limitation du traitement et elle prévoit que ces droits puissent être exercés indirectement, par l'intermédiaire du CEPD. Elle inclut également les principes de sécurité du traitement et de responsabilité, en imposant au Parquet européen de prendre les mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité adéquat contre les risques posés par le traitement, conserver des registres sur toutes les activités de traitement et réaliser une analyse d'impact relative à la protection des données préalablement au traitement, lorsqu'un type de traitement (par exemple,

841 Commission européenne (2013), Proposition de règlement du Conseil portant création du Parquet européen, COM(2013) 534 final, Bruxelles, 17 juillet 2013, art. 26, para. 4.

842 *Ibid.*, art. 36.

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

le traitement impliquant l'utilisation de nouvelles technologies) est susceptible d'engendrer un risque élevé pour les droits des personnes physiques. Enfin, la proposition prévoit la désignation d'un délégué à la protection des données par le collège, qui doit dûment intervenir dans toutes les questions relatives à la protection des données à caractère personnel et s'assurer que le Parquet européen se conforme à la législation applicable en matière de protection des données.

8.3.2. Protection des données dans les systèmes d'information conjoints au niveau de l'UE

En plus de l'échange de données entre États membres et de la création d'autorités européennes spécialisées dans la lutte contre la criminalité transfrontalière, comme Europol, Eurojust et le Parquet européen, plusieurs systèmes d'information conjoints ont été établis au niveau de l'UE pour servir de plateforme d'échange de données entre les autorités nationales et européennes compétentes à des fins répressives spécifiques dans les domaines de la protection des frontières, de l'immigration et de l'asile ainsi que des douanes. Étant donné que, dans un premier temps, l'espace Schengen a été institué par un accord international indépendant du droit de l'UE, le système d'information Schengen (SIS) s'est développé au travers d'accords multilatéraux et a ensuite été ramené dans le droit de l'Union. Le système d'information sur les visas (VIS), Eurodac, Eurosur et le système d'information des douanes (SID) ont été créés en tant qu'instruments régis par le droit de l'UE.

La supervision de ces systèmes est partagée entre les autorités nationales de contrôle et le CEPD. Afin d'assurer un niveau de protection élevé, ces autorités collaborent au sein de groupes de coordination du contrôle (GCC), qui se rapportent aux systèmes d'information à grande échelle suivants : 1) Eurodac ; 2) le système d'information sur les visas ; 3) le système d'information Schengen ; 4) le système d'information des douanes et 5) le système d'information sur le marché intérieur[844]. Les GCC se réunissent généralement deux fois par an, sous la direction d'un président élu, et ils adoptent des lignes directrices, discutent de dossiers transfrontières ou adoptent des cadres communs pour les inspections.

L'Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle (eu-LISA)[845], créée en 2012, est chargée de la gestion

844 Voir la page web du Contrôleur européen de la protection des données sur la coordination du contrôle.

845 Règlement (UE) nº 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.

opérationnelle du système d'information Schengen de deuxième génération (SIS II), du système d'information sur les visas (VIS) et du système Eurodac. La tâche principale d'eu-LISA consiste à garantir l'exploitation efficace, sécurisée et continue des systèmes d'information. Elle est également chargée de l'adoption des mesures nécessaires pour garantir la sécurité des systèmes et des données.

Le système d'information Schengen

En 1985, plusieurs États membres des anciennes Communautés européennes ont institué un accord rassemblant 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[846]. Pour contrebalancer le risque pour 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.

Du fait 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[847]. 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[848] ainsi que l'Islande, le Liechtenstein, la Norvège et la Suisse[849]. Europol et Eurojust ont accès au SIS II.

Le SIS II est composé d'un système central (C-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 C-SIS contient certaines données saisies

846 Accord entre les gouvernements des États de l'Union économique Benelux, de la République fédérale d'Allemagne et de la République française relatif à la suppression graduelle des contrôles aux frontières communes, JO 2000 L 239.

847 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.

848 La Croatie, Chypre et l'Irlande mettent en œuvre des mesures préparatoires afin d'intégrer le SIS II, mais n'en font pas encore partie. Voir site web de la direction générale chargée de la migration et des affaires intérieures de la Commission européenne pour des informations sur le système d'information Schengen.

849 Règlement (CE) nº 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, 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 (SIS II), JO 2007 L 205.

par les États membres sur des personnes et des objets. Le 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 C-SIS, appelée « système d'information Schengen national » (N-SIS), qui est constamment mis à jour, actualisant ainsi le C-SIS. Il existe différents types d'alertes dans le SIS :

- la personne n'a pas le droit d'entrer ou de séjourner sur le territoire de Schengen ; ou
- la personne ou l'objet est recherché par des autorités judiciaires ou par celles chargées de l'application de la loi (par exemple, mandat d'arrêt européen, demande de vérification discrète) ; ou
- 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 doivent être initiées par l'intermédiaire des bureaux SIRENE. Le SIS II contient de nouvelles fonctionnalités, telles que la possibilité de saisir : des données biométriques, notamment des empreintes digitales et des photos ; ou de nouvelles catégories d'alertes, telles que les 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.

Le SIS II repose sur deux actes complémentaires : la Décision SIS II[850] et le Règlement SIS II[851]. Le législateur de l'UE a utilisé des bases juridiques différentes pour adopter la décision et le règlement. La décision régit l'utilisation de SIS II pour les finalités couvertes par la coopération policière et judiciaire en matière pénale (ancien troisième pilier de l'UE). Le règlement s'applique aux procédures d'alerte relevant des politiques en matière de visa, d'asile, d'immigration et d'autres politiques relatives à la libre circulation des personnes (ancien premier pilier). Les procédures d'alerte de

850 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 (SIS II), JO L 205, 7 août 2007.

851 Règlement (CE) nº 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 L 381, 28 décembre 2006.

chaque pilier devaient être régies par des actes séparés, étant donné que les deux instruments juridiques ont été adoptés avant le Traité de Lisbonne et l'abolition de la structure des piliers.

Les deux instruments contiennent des règles relatives à la protection des données. La Décision SIS II interdit le traitement de données sensibles[852]. Le traitement de données à caractère personnel est couvert par le champ d'application de la Convention 108 modernisée[853]. En outre, les personnes ont le droit d'accéder aux données à caractère personnel les concernant qui ont été introduites dans le SIS II[854].

Le Règlement SIS II établit les conditions et les procédures relatives à l'introduction et au traitement des signalements concernant les refus d'entrée ou de séjour de ressortissants de pays tiers. Il établit également des règles pour l'échange d'informations supplémentaires et de données complémentaires aux fins de l'entrée ou du séjour dans un État membre[855]. Ce règlement contient des règles relatives à la protection des données. Le traitement des catégories de données sensibles visées à l'article 9, paragraphe 1, du Règlement général sur la protection des données est interdit[856]. Le Règlement SIS II énonce également certains droits de la personne concernée, à savoir :

- le droit d'accès aux données à caractère personnel la concernant[857] ;
- le droit de rectification des données inexactes[858] ;
- le droit à l'effacement de données stockées illégalement[859] ; et
- le droit d'être informé en cas de signalement de la personne concernée. Cette information est fournie par écrit, avec une copie ou une référence à la décision nationale qui est à l'origine du signalement[860].

852 Décision SIS II, art. 56 ; Règlement SIS II, art. 40.
853 Décision SIS II, art. 57.
854 Décision SIS II, art. 58 ; Règlement SIS II, art. 41.
855 Règlement SIS II, art. 2.
856 *Ibid.*, art. 40.
857 *Ibid.*, art. 41, para. 1.
858 *Ibid.*, art. 41, para. 5.
859 *Ibid.*, art. 41, para. 5.
860 *Ibid.*, art. 42, para. 1.

Le droit à l'information n'est pas prévu lorsque : 1) les données à caractère personnel n'ont pas été collectées auprès de la personne concernée et pour autant que la communication de l'information soit impossible ou requière des efforts disproportionnés ; 2) la personne concernée a déjà l'information ou 3) la législation nationale permet de déroger au droit d'information, en particulier pour sauvegarder la sécurité nationale ou prévenir les infractions pénales[861].

Tant dans la Décision SIS II que dans le Règlement SIS II, le droit d'accès des personnes physiques aux données introduites dans le système peut s'exercer dans tout État membre et sera traité dans le respect du droit interne de cet État membre[862].

> Exemple : dans l'affaire *Dalea c. France*[863], 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 étant donné qu'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.

L'autorité nationale de contrôle compétente de chaque État membre supervise le N-SIS national. 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[864]. 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 C-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. Le groupe de

861 *Ibid.*, art. 42, para. 2.

862 Règlement SIS II, art. 41, para. 1 ; Décision SIS II, art. 58.

863 CouEDH, *Dalea c. France*, nº 964/07, 2 février 2010.

864 Règlement SIS II, art. 60, para. 2.

coordination du contrôle (GCC) du SIS II a été établi pour assurer la coordination du contrôle du SIS et se réunit jusqu'à deux fois par an. Ce groupe est composé du CEPD et de représentants des autorités de contrôle des États membres qui ont mis en place le SIS II, ainsi que de l'Islande, du Liechtenstein, de la Norvège et de la Suisse, le SIS s'appliquant également à ces pays puisqu'ils sont membres de l'espace Schengen[865]. Chypre, la Croatie et l'Irlande ne font pas encore partie du SIS II et ne participent donc aux réunions du GCC qu'à titre d'observateurs. Dans le cadre du GCC, le CEPD et les autorités nationales de contrôle coopèrent activement en échangeant des informations, en s'assistant mutuellement pour mener les audits et les inspections, en formulant des propositions harmonisées en vue de trouver des solutions communes aux éventuels problèmes et en assurant la sensibilisation aux droits en matière de protection des données[866]. Le GCC du SIS II adopte également des lignes directrices pour aider les personnes concernées. Il a ainsi publié un guide pour aider les personnes concernées à exercer leur droit d'accès[867].

Perspectives

En 2016, la Commission européenne a procédé à une évaluation du SIS[868], dont il est ressorti que des mécanismes nationaux ont été mis en place pour permettre aux personnes concernées d'obtenir un accès aux données à caractère personnel les concernant, leur rectification ou leur effacement ou d'obtenir réparation en cas de données inexactes. Afin d'améliorer l'efficacité du SIS II, la Commission européenne a présenté trois propositions de règlement :

- un règlement concernant l'établissement, l'exploitation et l'utilisation du SIS dans le domaine des contrôles aux frontières, qui abrogera le Règlement SIS II ;

- un règlement concernant l'établissement, l'exploitation et l'utilisation du SIS dans le domaine de la coopération policière et judiciaire en matière pénale, qui abrogera notamment la Décision SIS II ; et

865 Voir la page web du Contrôleur européen de la protection des données sur le système d'information Schengen.

866 Règlement SIS II, art. 46 ; Décision SIS II, art. 62.

867 Voir GCC du SIS II, *Système d'information Schengen II - Guide concernant l'exercice du droit d'accès*, disponible sur le site web du CEPD.

868 Commission européenne (2016), Rapport de la Commission au Parlement européen et au Conseil sur l'évaluation du système d'information Schengen de deuxième génération (SIS II), conformément à l'article 24, paragraphe 5, à l'article 43, paragraphe 3, et à l'article 50, paragraphe 5, du règlement (CE) nº 1987/2006, ainsi qu'à l'article 59, paragraphe 3, et à l'article 66, paragraphe 5, de la décision 2007/533/JAI, COM(2016) 880 final, Bruxelles, 21 décembre 2016.

- un règlement concernant l'utilisation du SIS pour le retour de ressortissants de pays tiers en séjour illégal.

Il est important de souligner que les propositions autorisent le traitement d'autres catégories de données biométriques, en plus des photographies et des empreintes digitales, qui font déjà partie du SIS II actuel. Les images faciales, les empreintes palmaires et les profils ADN seront également stockés dans la base de données SIS. En outre, alors que le Règlement SIS II et la Décision SIS II prévoyaient la possibilité de rechercher les empreintes digitales pour identifier une personne, les propositions rendent cette recherche obligatoire lorsque l'identité de la personne ne peut être établie autrement. Des images faciales, des photographies et des empreintes palmaires seront utilisées pour effectuer une recherche dans le système et identifier des personnes, lorsque cela deviendra techniquement possible. Les nouvelles règles relatives aux identifiants biométriques présentent des risques particuliers pour les droits des personnes physiques. Dans son avis sur les propositions de la Commission[869], le CEPD a observé que les données biométriques sont extrêmement sensibles et que leur introduction dans une base de données aussi vaste devrait être fondée sur une évaluation des éléments de preuve justifiant leur inclusion dans le SIS. En d'autres termes, la nécessité de traiter les nouveaux identifiants devrait être démontrée. Le CEPD a également estimé qu'il convient de clarifier davantage quels types d'informations peuvent être inclus dans le profil ADN. Étant donné que ce profil peut inclure des informations sensibles (l'exemple le plus notable serait les informations révélant des problèmes de santé), les profils ADN conservés dans le SIS ne devraient contenir : « que les informations minimales qui sont strictement nécessaires à l'identification des personnes disparues, et, d'autre part, exclure les informations se rapportant explicitement à la santé, à l'origine raciale et à d'autres renseignements sensibles »[870]. Les propositions mettent toutefois en place des garanties supplémentaires pour limiter la collecte et le traitement des données à ce qui est strictement nécessaire sur le plan opérationnel et pour restreindre l'accès à ces données à caractère personnel aux personnes qui en ont opérationnellement besoin[871]. Les propositions habilitent également l'eu-LISA à produire, à intervalles réguliers,

869 CEPD (2017), avis du CEPD du 2 mai 2017 sur la nouvelle base juridique du système d'information Schengen, avis 7/2017, 2 mai 2017.

870 *Ibid.*, para. 22.

871 Commission européenne (20016), Proposition de règlement du Parlement européen et du Conseil sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, modifiant le règlement (UE) nº 515/2014 et abrogeant le règlement (CE) nº 1986/2006, la décision 2007/533/JAI du Conseil et la décision 2010/261/UE de la Commission, COM(2016) 883 final, Bruxelles, 21 décembre 2016.

des rapports sur la qualité des données à l'intention des États membres afin de revoir régulièrement les signalements et de garantir la qualité des données[872].

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 des visas[873]. Le VIS permet aux États Schengen d'échanger des données sur les visas par l'intermédiaire d'un système qui connecte les consulats et les ambassades des États Schengen situés dans des pays non membres de l'UE avec les points de passage des frontières extérieures de tous les États Schengen. Le VIS traite les données concernant les demandes de visas de court séjour pour visiter l'espace Schengen ou transiter par celui-ci. Le VIS permet aux autorités des frontières de vérifier, à l'aide de données biométriques, notamment les empreintes digitales, si la personne qui présente un visa est son véritable titulaire et d'identifier les personnes sans documents ou porteuses de documents frauduleux.

Le Règlement (CE) nº 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) établit les conditions et les procédures de transfert des données à caractère personnel concernant des demandes de visas de court séjour. Il supervise également les décisions concernant les demandes, y compris les décisions d'annulation, de révocation ou de prolongation d'un visa[874]. Le Règlement VIS couvre essentiellement les données relatives au demandeur, ses visas, ses photographies, ses empreintes digitales, les liens vers des demandes antérieures et les dossiers de demande des personnes qui l'accompagnent ou des données relatives aux personnes qui l'invitent[875]. L'accès au VIS pour saisir, modifier ou supprimer des données est exclusivement limité aux autorités des

872 *Ibid.*, p. 15.

873 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) nº 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 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 2.18

874 Règlement VIS, art. 1er.

875 Règlement (CE) nº 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, art. 5.

États membres en charge des visas, 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 de passage aux frontières extérieures, les contrôles d'immigration et les demandes d'asile.

Dans 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 des infractions pénales ou d'enquêter en la matière[876]. Le VIS ayant été conçu comme un instrument d'aide à la mise en œuvre de la politique commune des visas, le principe de la limitation de la finalité qui exige que, comme expliqué à la section 3.2, les données à caractère personnel ne soient traitées que pour des finalités spécifiques, explicites et légitimes et soient adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées, serait violé si le VIS devenait un instrument répressif. C'est pourquoi les autorités répressives nationales et Europol ne disposent pas d'un accès usuel à la base de données VIS. L'accès ne peut être accordé qu'au cas par cas et doit s'accompagner de garanties strictes. Les conditions et garanties relatives à l'accès et à la consultation du VIS par ces autorités sont réglementées par la Décision 2008/633/JAI du Conseil[877].

Par ailleurs, le Règlement VIS établit des droits pour les personnes concernées, à savoir :

- le droit d'être informées par l'État membre responsable de l'identité et des coordonnées du responsable du traitement chargé du traitement des données à caractère personnel dans ledit État, des finalités pour lesquelles les données à caractère personnel seront traitées dans le VIS, des catégories de destinataires des données et de la durée de conservation des données. De plus, les demandeurs de visa doivent être informés du fait que la collecte de leurs données à caractère personnel dans le cadre du VIS est obligatoire pour l'examen de leur demande, tandis que les États membres doivent également les informer de l'existence de leur droit d'accès à ces données, ainsi que de leur droit d'obtenir leur rectification ou leur effacement et des procédures leur permettant d'exercer lesdits droits[878] ;

876 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 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.

877 *Ibid*.

878 Règlement VIS, art. 37.

- le droit d'accès aux données à caractère personnel les concernant qui ont été introduites dans le VIS[879] ;
- le droit de rectification des données inexactes[880] ;
- le droit à l'effacement de données stockées illégalement[881].

Le GCC du VIS a été mis en place pour assurer la supervision du système. Il est composé de représentants du CEPD et des autorités nationales de contrôle, qui se réunissent jusqu'à deux fois par an. Ce groupe se compose des représentants des 28 États membres de l'UE et de l'Islande, du Liechtenstein, de la Norvège et de la Suisse.

Eurodac

Eurodac est l'abréviation de « European Dactyloscopy » ou « dactyloscopie européenne »[882]. Il s'agit d'un système centralisé contenant des données sur les empreintes digitales de ressortissants de pays tiers qui présentent une demande d'asile dans un État membre de l'UE[883]. Le système est opérationnel depuis janvier 2003 du fait de l'adoption du Règlement (CE) nº 2725/2000 du Conseil et une refonte du règlement est entrée en vigueur en 2015. Il a pour objet principal de contribuer à déterminer l'État membre qui, en vertu du Règlement (CE) nº 604/2013, est responsable de l'examen d'une demande d'asile particulière. Le règlement établit

879 *Ibid.*, art. 38, para. 1.

880 *Ibid.*, art. 38, para. 2.

881 *Ibid.*, art. 38, para. 2.

882 Voir la page web du Contrôleur européen de la protection des données sur Eurodac.

883 Règlement (CE) nº 2725/2000 du Conseil 11 février 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) nº 407/2002 du Conseil du 28 février 2002 fixant certaines modalités d'application du règlement (CE) nº 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) ; Règlement (UE) nº 603/2013 du Parlement européen et du Conseil du 26 juin 2013 relatif à la création d'Eurodac pour la comparaison des empreintes digitales aux fins de l'application efficace du règlement (UE) nº 604/2013 établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale introduite dans l'un des États membres par un ressortissant de pays tiers ou un apatride et relatif aux demandes de comparaison avec les données d'Eurodac présentées par les autorités répressives des États membres et Europol à des fins répressives, et modifiant le règlement (UE) nº 1077/2011 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 (refonte du Règlement Eurodac), JO 2013 L 180, p. 1.

les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale introduite dans l'un des États membres par un ressortissant de pays tiers ou un apatride (Règlement Dublin III)[884]. Les données à caractère personnel figurant dans Eurodac peuvent uniquement être utilisées aux fins de faciliter l'application du Règlement Dublin III[885].

Dans le cadre d'enquêtes pénales, les autorités répressives nationales et Europol sont autorisés à comparer les empreintes digitales avec les données dactyloscopiques contenues dans Eurodac, mais uniquement aux fins de la prévention et de la détection d'infractions terroristes ou d'autres infractions pénales graves ainsi que des enquêtes en la matière. Eurodac ayant été conçu comme un instrument d'appui à la mise en œuvre de la politique de l'UE en matière d'asile et non comme un instrument répressif, les autorités répressives n'ont accès à la base de données que dans des cas déterminés, dans des circonstances spécifiques et dans le respect de conditions strictes[886]. Pour une utilisation ultérieure des données à des fins répressives, la Directive relative à la protection des données pour les autorités policières et judiciaires en matière pénale s'applique, tandis que les données utilisées dans le but principal de faciliter l'application du Règlement Dublin III sont protégées par le Règlement général sur la protection des données. Le transfert ultérieur de données à caractère personnel obtenues par un État membre ou Europol en vertu de la refonte du Règlement Eurodac à un pays tiers, une organisation internationale ou une entité de droit privé établie ou non dans l'UE est interdit[887].

Eurodac est composé d'une unité centrale, exploitée par 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 des ressortissants de pays tiers ou d'apatrides qui séjournent sur leur territoire sans autorisation.

884 Règlement (UE) nº 604/2013 du Parlement européen et du Conseil du 26 juin 2013 établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale introduite dans l'un des États membres par un ressortissant de pays tiers ou un apatride (Règlement Dublin III), JO 2013 L 180.

885 Refonte du Règlement Eurodac, JO 2013 L 180, p. 1, art. 1er, para. 1.

886 *Ibid.*, art. 1er, para. 2.

887 *Ibid.*, art. 35.

Bien que tout État membre puisse consulter Eurodac et demander des comparaisons de données dactyloscopiques, seul l'État membre qui a collecté les empreintes digitales et les a transmises à l'unité centrale a le droit de modifier les données, en les rectifiant, les complétant ou les effaçant[888]. L'eu-LISA conserve des relevés de toutes les opérations de traitement afin de contrôler la protection des données et de garantir leur sécurité[889]. Les autorités nationales de contrôle assistent et conseillent les personnes concernées dans l'exercice de leurs droits[890]. La collecte et la transmission des données dactyloscopiques sont soumises au contrôle juridictionnel des juridictions nationales[891]. Le Règlement relatif à la protection des données des institutions de l'UE[892] et le contrôle par le CEPD s'appliquent aux activités de traitement du système central, qui est géré par eu-LISA en ce qui concerne Eurodac[893]. Toute personne ayant subi un dommage du fait d'un traitement illicite ou de toute action incompatible avec le Règlement Eurodac a le droit d'obtenir de l'État membre responsable réparation du préjudice subi[894]. Il convient toutefois de souligner que les demandeurs d'asile constituent un groupe particulièrement vulnérable de personnes ayant souvent entrepris un voyage long et périlleux. Du fait de leur vulnérabilité et de leur situation précaire, pendant l'examen de leur demande d'asile, ils peuvent souvent éprouver des difficultés à exercer leurs droits, notamment le droit à réparation.

Pour utiliser Eurodac à des fins répressives, les États membres doivent désigner les autorités qui auront le droit de demander l'accès à la base de données, ainsi que celles qui vérifieront que les demandes de comparaison sont licites[895]. L'accès des autorités nationales et d'Europol aux données dactyloscopiques d'Eurodac est soumis à des conditions très strictes. L'autorité requérante doit présenter une demande électronique motivée uniquement après avoir comparé les données avec celles contenues dans d'autres systèmes d'information, comme les fichiers nationaux d'empreintes digitales et le VIS. Il faut qu'il existe un intérêt supérieur de sécurité publique qui rende la comparaison proportionnée. La comparaison doit être

888 *Ibid.*, art. 27.

889 *Ibid.*, art. 28.

890 *Ibid.*, art. 29.

891 *Ibid.*, art. 29.

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

893 Refonte du Règlement Eurodac, JO 2013 L 180, p. 1, art. 31.

894 *Ibid.*, art. 37.

895 Roots, L. (2015), « The New EURODAC Regulation: Fingerprints as a Source of Informal Discrimination », *Baltic Journal of European Studies Tallinn University of Technology*, Vol. 5, nº 2, p. 108 à 129.

véritablement nécessaire, concerner un cas précis et il doit exister des motifs raisonnables de penser que la comparaison contribuera de manière significative à la prévention ou à la détection de l'une des infractions pénales en question ou aux enquêtes en la matière, en particulier lorsqu'il existe des motifs de soupçonner que le suspect, l'auteur ou la victime d'une infraction terroriste ou d'une autre infraction pénale grave relève d'une catégorie soumise à la collecte des empreintes digitales dans le cadre du système Eurodac. La comparaison doit se limiter aux données dactyloscopiques. Europol doit aussi obtenir une autorisation de l'État membre qui a collecté les données dactyloscopiques.

Les données à caractère personnel stockées dans Eurodac qui concernent des demandeurs d'asile sont conservées pendant dix ans à compter de la date où les empreintes digitales ont été relevées, à moins que la personne concernée obtienne la citoyenneté d'un État membre de l'UE. Dans ce cas, les données doivent être effacées immédiatement. Les données relatives aux ressortissants étrangers appréhendés pour avoir franchi une frontière extérieure sans autorisation sont conservées pendant dix-huit mois. Ces données doivent être effacées immédiatement lorsque la personne concernée reçoit un permis de séjour, quitte le territoire de l'UE ou obtient la citoyenneté d'un État membre. Les données des personnes auxquelles l'asile a été accordé restent disponibles à des fins de comparaison dans le cadre de la prévention et de la détection d'infractions terroristes et d'autres infractions pénales graves ainsi que d'enquêtes en la matière pendant trois ans.

Outre tous les États membres de l'UE, l'Islande, la Norvège, le Liechtenstein et la Suisse utilisent également Eurodac sur la base d'accords internationaux.

Le GCC d'Eurodac a été mis en place pour assurer le contrôle du système. Il est composé de représentants du CEPD et des autorités nationales de contrôle, qui se réunissent jusqu'à deux fois par an. Ce groupe se compose des représentants des 28 États membres de l'UE ainsi que de l'Islande, du Liechtenstein, de la Norvège et de la Suisse[896].

896 Voir la page web du Contrôleur européen de la protection des données sur Eurodac.

Perspectives

En mai 2016, la Commission a publié une proposition de nouvelle refonte du Règlement Eurodac, dans le cadre d'une réforme visant à améliorer le fonctionnement du régime d'asile européen commun (RAEC)[897]. La refonte proposée est importante dans la mesure où elle étendra considérablement la portée de la base de données Eurodac initiale. À l'origine, Eurodac a été créé pour soutenir la mise en œuvre du RAEC en fournissant des preuves dactyloscopiques permettant de déterminer l'État membre responsable de l'examen d'une demande d'asile présentée dans l'UE. La refonte proposée étendra la portée de la base de données afin de faciliter le retour des migrants en situation irrégulière[898]. Les autorités nationales seront en mesure de consulter la base de données pour identifier des ressortissants de pays tiers en séjour irrégulier dans l'UE ou entrés de manière irrégulière sur le territoire de l'UE, afin d'obtenir des preuves pour aider les États membres à renvoyer ces personnes dans leur pays. En outre, alors que le régime juridique actuel n'exige que la collecte et le stockage des empreintes digitales, la proposition introduit la collecte des images faciales des personnes[899], qui constituent une autre catégorie de données biométriques. La proposition abaisserait également l'âge minimal des enfants dont les données biométriques peuvent être prises à six ans[900] au lieu de 14 ans, qui est l'âge minimal prévu par le règlement de 2013. Le champ d'application étendu de la

897 Commission européenne, Proposition de règlement du Parlement européen et du Conseil relatif à la création d'« Eurodac » pour la comparaison des empreintes digitales aux fins de l'application efficace du [règlement (UE) nº 604/2013 établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale introduite dans l'un des États membres par un ressortissant de pays tiers ou un apatride], et de l'identification des ressortissants de pays tiers ou apatrides en séjour irrégulier, et relatif aux demandes de comparaison avec les données d'Eurodac présentées par les autorités répressives des États membres et par Europol à des fins répressives (refonte), COM(2016) 272 final, 4 mai 2016.

898 Voir l'exposé des motifs de la proposition, p. 3.

899 Commission européenne, Proposition de règlement du Parlement européen et du Conseil relatif à la création d'« Eurodac » pour la comparaison des empreintes digitales aux fins de l'application efficace du [règlement (UE) nº 604/2013 établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale introduite dans l'un des États membres par un ressortissant de pays tiers ou un apatride], et de l'identification des ressortissants de pays tiers ou apatrides en séjour irrégulier, et relatif aux demandes de comparaison avec les données d'Eurodac présentées par les autorités répressives des États membres et par Europol à des fins répressives (refonte), COM(2016) 272 final, 4 mai 2016, art. 2, para. 1.

900 *Ibid.*, art. 2, para. 2.

proposition signifie qu'elle constituera une ingérence dans les droits au respect de la vie privée et à la protection des données d'un nombre accru de personnes qui pourront être incluses dans la base de données. Pour compenser cette ingérence, la proposition et les amendements proposés par la commission LIBE du Parlement européen[901] visent à renforcer les exigences en matière de protection des données. Au moment de rédiger ce manuel, les discussions sur la proposition se poursuivaient au Parlement et au Conseil.

Eurosur

Le système européen de surveillance des frontières (Eurosur)[902] 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 a pour but d'améliorer l'échange d'informations et la coopération opérationnelle entre les centres de coordination nationaux et Frontex, l'agence de l'UE chargée de développer et d'appliquer le nouveau concept de gestion intégrée des frontières[903]. Ses objectifs généraux sont les suivants :

- réduire le nombre de migrants en situation irrégulière qui entrent dans l'UE sans être détectés ;

- réduire le nombre de décès de migrants en situation irrégulière en sauvant plus de vies en mer ;

901 Parlement européen, *Rapport sur la proposition de règlement du Parlement européen et du Conseil relatif à la création d'« Eurodac » pour la comparaison des empreintes digitales aux fins de l'application efficace du [règlement (UE) nº 604/2013 établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale introduite dans l'un des États membres par un ressortissant de pays tiers ou un apatride], et de l'identification des ressortissants de pays tiers ou apatrides en séjour irrégulier, et relatif aux demandes de comparaison avec les données d'Eurodac présentées par les autorités répressives des États membres et par Europol à des fins répressives (refonte),* PE597.620v03-00, 9 juin 2017.

902 Règlement (UE) nº 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.

903 Règlement (UE) 2016/1624 du Parlement européen et du Conseil du 14 septembre 2016 relatif au corps européen de garde-frontières et de garde-côtes, modifiant le règlement (UE) 2016/399 du Parlement européen et du Conseil et abrogeant le règlement (CE) nº 863/2007 du Parlement européen et du Conseil, le règlement (CE) nº 2007/2004 du Conseil et la décision 2005/267/CE du Conseil, JO L 251.

- accroître la sécurité intérieure de l'UE dans son ensemble en contribuant à la prévention de la criminalité transfrontalière[904].

Eurosur a commencé sa mission le 2 décembre 2013 dans tous les États membres ayant des frontières extérieures et le 1er décembre 2014 dans les autres. Le règlement s'applique à la surveillance des frontières extérieures terrestres, maritimes et aériennes des États membres. Eurosur échange et traite des données à caractère personnel dans une mesure très limitée, étant donné que seuls les États membres et Frontex sont habilités à échanger les numéros d'identification des navires. Eurosur échange des informations opérationnelles, comme la localisation des patrouilles et les incidents et, en principe, les informations échangées ne peuvent contenir aucune donnée à caractère personnel[905]. Dans les cas exceptionnels où des données à caractère personnel sont échangées dans le cadre d'Eurosur, le règlement prévoit que le cadre juridique général de l'UE relatif à la protection des données s'applique pleinement[906].

Eurosur garantit donc le droit à la protection des données, en précisant que les échanges de données à caractère personnel doivent respecter les critères et garanties prévus par la Directive relative à la protection des données pour les autorités policières et judiciaires en matière pénale et le Règlement général sur la protection des données[907].

904 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), *Impact Assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council establishing the European Border Surveillance System (Eurosur)*, Document de travail, SEC(2011) 1536, Bruxelles, 12 décembre 2011, p. 18.

905 Commission européenne, *EUROSUR: Protecting the Schengen external borders – protecting migrants' lives. EUROSUR in a nutshell*, 29 novembre 2013.

906 Règlement (UE) nº 1052/2013, considérant 13 et art. 13.

907 *Ibid.*, considérant 13 et art. 13.

Système d'information des douanes

Un autre système important d'information conjoint établi au niveau de l'UE est le système d'information des douanes (SID)[908]. Dans le cadre de la création du marché intérieur, tous les contrôles et formalités à l'égard des produits circulant sur le territoire européen ont été abolis, ce qui entraîne 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 infractions graves aux réglementations douanière et agricole nationales et européennes, ainsi qu'à mener des enquêtes et des poursuites en la matière. Le SID a été établi par deux instruments juridiques fondés sur des bases juridiques différentes : le Règlement (CE) nº 515/97 du Conseil concerne la coopération entre les différentes autorités administratives nationales aux fins de lutter contre la fraude dans le cadre de l'union douanière et de la politique agricole commune, tandis que la Décision 2009/917/JAI du Conseil vise à contribuer à la prévention des infractions graves à la législation douanière et aux enquêtes et poursuites en la matière. Le SID ne se limite donc pas à des objectifs répressifs.

Les informations contenues dans le SID comprennent des données à caractère personnel se rapportant aux produits, moyens de transport, entreprises, personnes, biens et espèces conservés, saisis ou confisqués. Les catégories de données qui peuvent être traitées sont clairement définies et incluent le nom, la nationalité, le sexe, le lieu et la date de naissance des personnes concernées, le motif de l'inclusion de leurs données dans le système et le numéro d'immatriculation du moyen de transport[909]. Ces informations peuvent uniquement être utilisées dans le but de détecter, de signaler et de réaliser des inspections particulières ou des analyses stratégiques ou opérationnelles concernant des personnes soupçonnées d'avoir enfreint des dispositions douanières.

L'accès au SID est accordé aux autorités nationales douanières, fiscales, agricoles, policières et de santé publique, ainsi qu'à Europol et à Eurojust.

908 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), Règlement (CE) nº 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, 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).

909 Voir Décision SID, art. 24, 25 et 28.

Le traitement de données à caractère personnel doit être conforme aux règles spécifiques établies par le Règlement (CE) nº 515/97 et à la Décision 2009/917/JAI du Conseil, ainsi qu'aux dispositions du Règlement général sur la protection des données, du Règlement relatif à la protection des données des institutions de l'UE, de la Convention 108 modernisée et de la Recommandation relative à la police. Le CEPD est chargé du contrôle de la conformité du SID avec le Règlement (CE) nº 45/2001. Il organise au moins une fois par an une réunion avec toutes les autorités nationales de contrôle de la protection des données compétentes en matière de contrôle du SID.

Interopérabilité entre les systèmes d'information de l'UE

La gestion des migrations, la gestion intégrée des frontières extérieures de l'UE et la lutte contre le terrorisme et la criminalité transfrontalière posent des défis importants et sont devenues de plus en plus complexes dans un monde globalisé. Ces dernières années, l'UE a élaboré une nouvelle approche exhaustive de la protection et du maintien de la sécurité sans compromettre les valeurs et libertés fondamentales qu'elle défend. Dans ces efforts, l'échange efficace d'informations est essentiel entre les autorités répressives nationales, entre les États membres et entre ceux-ci et les agences compétentes de l'UE[910]. Les systèmes européens d'information existants dédiés à la gestion des frontières et à la sécurité intérieure ont des objectifs, une structure institutionnelle, des personnes concernées et des utilisateurs qui leur sont propres. L'UE s'est efforcée de combler les lacunes dans les fonctions de la gestion fragmentée des données de l'UE entre les différents systèmes d'information,

910 Commission européenne (2016), Communication de la Commission au Parlement européen et au Conseil – Des systèmes d'information plus robustes et plus intelligents au service des frontières et de la sécurité, Bruxelles, 6 avril 2016 ; Commission européenne (2016), Communication de la Commission au Parlement européen, au Conseil européen et au Conseil – Accroître la sécurité dans un monde de mobilité : améliorer l'échange d'informations dans la lutte contre le terrorisme et renforcer les frontières extérieures, COM(2016) 602 final, Bruxelles, 14 septembre 2016 ; Commission européenne (2016), Proposition de règlement du Parlement européen et du Conseil relatif à l'utilisation du système d'information Schengen aux fins du retour des ressortissants de pays tiers en séjour irrégulier. Voir aussi Communication de la Commission au Parlement européen, au Conseil européen et au Conseil – Septième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective, COM(2017) 261 final, Bruxelles, 16 mai 2017.

tels que le SIS II, le VIS et Eurodac, en étudiant leur potentiel d'interopérabilité[911]. L'objectif principal est de veiller à ce que les autorités policières, douanières et judiciaires compétentes disposent systématiquement des informations nécessaires à l'accomplissement de leurs missions, tout en conservant un équilibre en termes de droit au respect de la vie privée, à la protection des données et d'autres droits fondamentaux.

L'interopérabilité est « la capacité des systèmes d'information à échanger des données et à permettre le partage d'informations »[912]. Cet échange ne doit pas porter atteinte aux règles nécessairement strictes relatives à l'accès et à l'utilisation que garantissent le RGPD, la Directive relative à la protection des données pour les autorités policières et judiciaires en matière pénale, la Charte des droits fondamentaux de l'UE et toutes les autres réglementations pertinentes. Toute solution intégrée de gestion des données ne doit pas affecter les principes de limitation de la finalité, de protection des données dès la conception ou de protection des données par défaut[913].

En plus d'améliorer les fonctionnalités des trois grands systèmes d'information – SIS II, VIS et Eurodac –, la Commission a proposé la création d'un quatrième système centralisé de gestion des frontières concernant les ressortissants de pays tiers : le système d'entrée/sortie (EES)[914], qui devrait être mis en œuvre à l'horizon 2020[915].

911 Conseil de l'Union européenne (2005), Le programme de La Haye : renforcer la liberté, la sécurité et la justice dans l'Union européenne, JO 2005 C 53 ; Commission européenne (2010), Communication de la Commission au Parlement européen et au Conseil – Présentation générale de la gestion de l'information dans le domaine de la liberté, de la sécurité et de la justice, COM(2010) 385 final ; Commission européenne (2016), Communication de la Commission au Parlement européen et au Conseil – Des systèmes d'information plus robustes et plus intelligents au service des frontières et de la sécurité, Bruxelles, 6 avril 2016 ; Commission européenne (2016), Décision de la Commission du 17 juin 2006 instituant le groupe d'experts de haut niveau sur les systèmes d'information et l'interopérabilité, JO 2016 C 257.

912 Commission européenne (2016), Communication de la Commission au Parlement européen et au Conseil – Des systèmes d'information plus robustes et plus intelligents au service des frontières et de la sécurité», COM(2016) 205 final, 6 avril 2016, p. 14.

913 *Ibid*., p. 4 et 5.

914 Commission européenne (2016), Proposition de règlement du Parlement européen et du Conseil portant création d'un système d'entrée/sortie (EES) pour enregistrer les données relatives aux entrées et aux sorties des ressortissants de pays tiers qui franchissent les frontières extérieures des États membres de l'Union européenne ainsi que les données relatives aux refus d'entrée les concernant, portant détermination des conditions d'accès à l'EES à des fins répressives et portant modification du règlement (CE) nº 767/2008 et du règlement (UE) nº 1077/2011, COM/2016/0194 final, Bruxelles, 6 avril 2016.

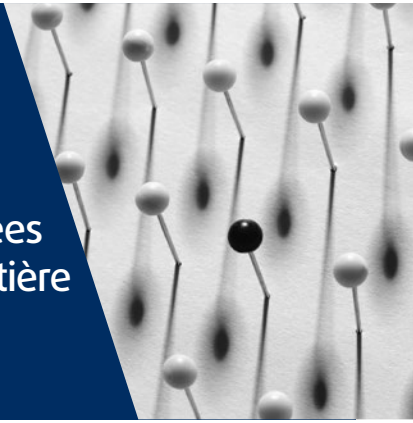
915 Commission européenne (2016), Communication de la Commission au Parlement européen et au Conseil – Des systèmes d'information plus robustes et plus intelligents au service des frontières et de la sécurité, COM(2016) 205 final, 6 avril 2016, p. 5.

La Commission a également publié une proposition visant à créer un système européen d'information et d'autorisation concernant les voyages (ETIAS)[916], qui rassemblera des informations sur les personnes voyageant sans visa à destination de l'UE en vue de permettre de procéder à des contrôles avancés de sécurité et de la migration irrégulière.

916 Commission européenne (2016), Proposition de règlement du Parlement européen et du Conseil portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS) et modifiant les règlements (UE) nº 515/2014, (UE) 2016/399, (UE) 2016/974 et (UE) 2016/1624, COM(2016) 731 final, 16 novembre 2016.

9

Catégories particulières de données et règles correspondantes en matière de protection des données



UE	Questions traitées	CdE
RGPD Directive « vie privée et communications électroniques »	**Communications électroniques**	Convention 108 modernisée Recommandation sur les services de télécommunications
RGPD, art. 89	**Relations de travail**	Convention 108 modernisée Recommandation en matière d'emploi CouEDH, *Copland c. Royaume-Uni*, nº 62617/00, 2007
RGPD, art. 9, para. 2, points h) et i)	**Données médicales**	Convention 108 modernisée Recommandation sur les données médicales CouEDH, *Z c. Finlande*, nº 22009/93, 1997
Règlement relatif aux essais cliniques	**Essais cliniques**	
RGPD, art. 6, para. 4, et art. 89	**Statistiques**	Convention 108 modernisée Recommandation sur les données statistiques

UE	Questions traitées	CdE
Règlement (CE) nº 223/2009 relatif aux statistiques européennes CJUE, C-524/06, *Huber c. Bundesrepublik Deutschland* [GC], 2008	**Statistiques officielles**	Convention 108 modernisée Recommandation sur les données statistiques
Directive (UE) 2014/65 concernant les marchés d'instruments financiers Règlement (UE) nº 648/2012 sur les produits dérivés de gré à gré, les contreparties centrales et les référentiels centraux Règlement (CE) nº 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 modernisée Recommandation R 90 (19) sur la protection des données à caractère personnel utilisées à des fins de paiement et autres opérations connexes CouEDH, *Michaud c. France*, nº 12323/11, 2012

À plusieurs reprises, des actes juridiques spéciaux ont été adoptés au niveau européen pour appliquer de façon plus détaillée les règles générales de la Convention 108 modernisée ou du Règlement général sur la protection des données à des situations particulières.

9.1. 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 localisation (par exemple, l'endroit à partir duquel les données ont été communiquées).

Les réseaux de communication ont un potentiel accru d'ingérence injustifiée dans la sphère personnelle des utilisateurs, étant donné qu'ils offrent de puissants moyens techniques pour écouter et recueillir les communications passant par ces 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[917]. 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, la mise à disposition du 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 un abonné ayant expressément demandé à ne pas en recevoir. Des appareils d'appels 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 de l'UE**, après une première tentative en 1997, la Directive « vie privée et communications électroniques » a été adoptée en 2002 et modifiée en 2009, afin de compléter et de préciser les dispositions de la Directive relative à la protection des données pour le secteur des télécommunications[918].

917 CdE, Comité des Ministres (1995), Recommandation Rec(95)4 sur la protection des données à caractère personnel dans le domaine des services de télécommunication, 7 février 1995.

918 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) nº 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.

La Directive « vie privée et communications électroniques » s'applique uniquement aux services de communication des réseaux électroniques publics.

La Directive « vie privée et communications électroniques » distingue trois grandes catégories de données générées lors d'une communication :

- 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 la localisation du dispositif de communication, appelées « données de localisation » ; ces données portent également sur la localisation des utilisateurs des dispositifs de communication et elles sont particulièrement pertinentes pour les utilisateurs d'appareils mobiles.

Les données relatives au trafic ne peuvent être utilisées que par le fournisseur de services à des fins de facturation et pour la prestation technique du service. Avec le consentement de la personne concernée, ces données peuvent toutefois être divulguées à d'autres responsables du traitement offrant des services à valeur ajoutée, notamment la fourniture d'informations concernant la localisation de l'utilisateur par rapport à la prochaine station de métro ou à une pharmacie, ou les prévisions météo pour 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 doit satisfaire à l'obligation 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 des droits fondamentaux de l'UE. Un tel accès pourrait comprendre un accès à des fins d'enquêtes sur des infractions pénales.

Les modifications apportées en 2009 à la Directive « vie privée et communications électroniques »[919] ont introduit les éléments suivants :

- Les restrictions concernant l'envoi de courriels à des fins de prospection ont été étendues aux services de SMS, aux services de messagerie multimédia et à d'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 les clients antérieurs peuvent être contactés par des courriels publicitaires, s'ils ont communiqué leur adresse électronique et ne s'y opposent pas.

- L'obligation d'offrir des recours juridictionnels contre les violations de l'interdiction de communications non sollicitées a été imposée aux États membres.[920]

- L'utilisation de cookies, des logiciels qui contrôlent et enregistrent 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[921].

En cas de violation de données résultant d'un accès, d'une perte ou d'une destruction non autorisé des données, l'autorité de contrôle compétente doit en être immédiatement informée. Les abonnés doivent être informés de la violation lorsqu'elle peut entraîner un dommage pour ceux-ci[922].

919 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) nº 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 337/2009.

920 Voir Directive modifiée, art. 13.

921 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.

922 Voir aussi Groupe de travail « Article 29 » (2011), *Document de travail 01/2011 sur le cadre européen actuel en matière de violations de données à caractère personnel et recommandations pour les développements politiques futurs*, WP 184, Bruxelles, 5 avril 2011.

La Directive relative à la conservation des données[923] exigeait des fournisseurs de services de communication qu'ils conservent les données relatives au trafic. Cette directive a toutefois été annulée par la CJUE (pour plus de détails, voir la section 8.3).

Perspectives

En janvier 2017, la Commission européenne a adopté une nouvelle proposition de règlement « vie privée et communications électroniques » pour remplacer l'ancienne directive du même nom. L'objectif sera toujours de protéger les « libertés et droits fondamentaux des personnes physiques et morales en ce qui concerne la fourniture et l'utilisation de services de communications électroniques, et notamment le droit au respect de la vie privée et des communications et la protection des personnes physiques à l'égard du traitement des données à caractère personnel ». Cette nouvelle proposition de règlement vise également à garantir la libre circulation des données des communications électroniques et des services de communications électroniques au sein de l'Union[924]. Alors que le Règlement général sur la protection des données traite essentiellement de l'article 8 de la Charte des droits fondamentaux de l'UE, le règlement proposé vise à intégrer l'article 7 de la Charte dans le droit dérivé de l'UE.

Le règlement adaptera les dispositions antérieures de la directive aux nouvelles technologies et à la nouvelle réalité du marché et élaborera un cadre exhaustif et cohérent avec le Règlement général sur la protection des données. Le Règlement « vie privée et communications électroniques » sera donc, en ce sens, une *lex specialis* du RGPD, en l'adaptant aux données de communications électroniques qui sont des données à caractère personnel. Le nouveau règlement couvre le traitement des « données de communications électroniques », notamment le contenu des communications électroniques et les données relatives au trafic qui ne sont pas nécessairement des données à caractère personnel. Le champ d'application territorial est limité à l'UE, y compris lorsque des données recueillies dans l'UE sont traitées en dehors de celle-ci, et couvre les fournisseurs de services de communication d'accès direct (« over-the-top »). Ces fournisseurs de services proposent du contenu, des

923 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.

924 Proposition de règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (Règlement « vie privée et communications électroniques »), COM(2017) 10 final, art. 1er.

services ou des applications par internet, sans la participation directe d'un opérateur de réseau ou d'un fournisseur de services internet (ISP). Skype (appels vocaux et vidéo), WhatsApp (messagerie), Google (recherche), Spotify (musique) ou Netflix (contenu vidéo) en sont des exemples. Les mécanismes de mise en œuvre du Règlement général sur la protection des données s'appliqueront au nouveau règlement.

Le Règlement « vie privée et communications électroniques » devrait être adopté avant le 25 mai 2018, date à laquelle le Règlement général sur la protection des données sera applicable dans les 28 États membres. Cette adoption est toutefois subordonnée à l'accord du Parlement européen et du Conseil[925].

9.2. Données sur l'emploi

Points clés

- Les règles spécifiques relatives à la protection des données dans les relations de travail sont exposées dans la Recommandation du CdE sur les données sur l'emploi.
- Dans le Règlement général sur la protection des données, les relations du travail ne sont spécifiquement mentionnées que dans le contexte du traitement de données sensibles.
- La validité du consentement, qui doit avoir été donné librement, comme base juridique 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 soin.

Le traitement des données dans le contexte de l'emploi est soumis à la législation générale de l'UE sur la protection des données à caractère personnel. Toutefois, un règlement[926] aborde spécifiquement la protection du traitement de données à caractère personnel par les institutions européennes dans le cadre de l'emploi (notamment). Dans le Règlement général sur la protection des données, les relations de

925 Pour en savoir plus, voir Commission européenne (2017), « La Commission propose de resserrer les règles en matière de respect de la vie privée pour toutes les communications électroniques et actualise les règles relatives à la protection des données pour les institutions de l'UE », communiqué de presse, 10 janvier 2017.

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

travail sont spécifiquement mentionnées à l'article 9, paragraphe 2, qui dispose que les données à caractère personnel peuvent être traitées aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail.

Selon le RGPD, le salarié devrait être mis en mesure de distinguer clairement les données pour lesquelles il signifie librement son consentement au traitement et à la conservation et les finalités pour lesquelles les données le concernant sont conservées. Le salarié devrait également être informé de ses droits et du délai de conservation des données avant que le consentement puisse être donné. Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés de personnes physiques, l'employeur doit communiquer la violation au salarié. L'article 88 du règlement permet aux États membres de prévoir des règles plus spécifiques pour assurer la protection des droits et libertés des employés en ce qui concerne le traitement de leurs données à caractère personnel dans le cadre des relations de travail.

Exemple : dans l'affaire *Worten*[927], les données incluaient un registre du temps de travail contenant les périodes journalières de travail et de repos, qui constituent des données à caractère personnel. La législation nationale peut exiger d'un employeur qu'il mette des registres du temps de travail à la disposition des autorités nationales compétentes en matière de surveillance des conditions de travail. Ceci permettrait un accès immédiat aux données à caractère personnel pertinentes. L'accès aux données à caractère personnel est toutefois nécessaire pour permettre à l'autorité nationale de surveiller l'application de la réglementation sur les conditions de travail[928].

S'agissant du **CdE**, la Recommandation sur les données sur l'emploi a été publiée en 1989 et révisée en 2015[929]. Elle couvre le traitement de données à caractère personnel à des fins d'emploi, tant dans le secteur public que privé. Le traitement doit être conforme à certains principes et limitations, tels que le principe de la transparence et la consultation des représentants des salariés avant la mise en place de systèmes de contrôle sur le lieu de travail. La recommandation précise également que

927 CJUE, C-342/12, *Worten – Equipamentos para o Lar SA c. Autoridade para as Condições de Trabalho (ACT)*, 30 mai 2013, point 19.

928 *Ibid.*, point 43.

929 CdE, Comité des Ministres (2015), Recommandation Rec(2015)5 aux États membres sur le traitement des données à caractère personnel dans le cadre de l'emploi, avril 2015.

les employeurs devraient adopter des mesures préventives, telles que l'utilisation de filtres, plutôt que de surveiller l'utilisation d'internet par les salariés.

Une étude des problèmes les plus courants en matière de protection des données dans le cadre de l'emploi est disponible dans un document de travail du Groupe de travail « Article 29 »[930]. Il a analysé l'importance du consentement en tant que base juridique du traitement des données sur l'emploi[931]. Il a constaté que le déséquilibre de pouvoir entre l'employeur qui demande le consentement et l'employé qui le donne aura souvent pour effet de remettre en question la liberté du consentement. Les circonstances dans lesquelles le consentement est invoqué comme base juridique d'un traitement de données devraient donc être étudiées soigneusement lors de l'appréciation de la validité du consentement dans le cadre des relations de travail.

Un problème courant en matière de protection des données dans l'environnement de travail classique actuel est l'étendue légitime du contrôle des communications électroniques des salariés sur le lieu du travail. On entend souvent affirmer que ce problème peut être aisément résolu par l'interdiction de l'utilisation privée des systèmes de communication au travail. Une telle interdiction générale pourrait toutefois être disproportionnée et irréaliste. Les arrêts de la CouEDH dans les affaires *Copland c. Royaume-Uni* et *Bărbulescu c. Roumanie* sont particulièrement intéressants à cet égard.

Exemple : dans l'affaire *Copland c. Royaume-Uni*[932], l'utilisation du téléphone, du courriel et d'internet par une employée d'un établissement d'enseignement postscolaire avait été secrètement surveillée pour déterminer si elle faisait une utilisation abusive des équipements de l'établissement 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

930 Groupe de travail « Article 29 », *Avis 2/2017 sur le traitement des données au travail*, WP 249, Bruxelles, 8 juin 2017.

931 Groupe de travail « Article 29 » (2005), *Document de travail relatif à une interprétation commune des dispositions de l'article 26, para.* 1, de la directive 95/46/CE du 24 octobre 1995, WP 114, Bruxelles, 25 novembre 2005.

932 CouEDH, *Copland c. Royaume-Uni*, nº 62617/00, 3 avril 2007.

par l'article 8 de la CEDH. Dans le cas de la requérante, il n'existait aucune disposition réglementant les conditions dans lesquelles des employeurs pouvaient surveiller l'utilisation du téléphone, du courriel et d'internet par leurs salariés. Partant, l'ingérence n'était pas prévue par la loi. La CouEDH a donc conclu à une violation de l'article 8 de la CEDH.

Exemple : dans l'affaire *Bărbulescu c. Roumanie*[933], le requérant avait été licencié pour avoir utilisé le réseau internet de son lieu de travail pendant ses heures de travail au mépris du règlement intérieur. Son employeur avait surveillé ses communications. Des enregistrements montrant qu'il avait échangé des messages de nature strictement privée ont été produits durant les procédures internes. En jugeant l'article 8 applicable, la CouEDH n'a pas répondu à la question de savoir si le règlement restrictif de l'employeur laissait au requérant une confiance raisonnable dans le respect de sa vie privée, mais a en tout état de cause conclu que les règles d'un employeur ne pouvaient pas réduire à néant la vie sociale privée sur le lieu de travail.

Sur le fond, les États contractants devaient se voir accorder une marge d'appréciation étendue pour déterminer la nécessité d'établir un cadre juridique régissant les conditions dans lesquelles un employeur peut réglementer les communications non professionnelles de ses salariés – sous forme électronique ou autre – sur le lieu de travail. Les juridictions internes devaient toutefois s'assurer que la mise en place par un employeur de mesures de surveillance de la correspondance et des autres communications, quelles qu'en soient l'étendue et la durée, était assortie de garanties adéquates et suffisantes contre les abus. La proportionnalité et les garanties procédurales contre l'arbitraire sont des éléments essentiels et la CouEDH a circonscrit plusieurs facteurs pertinents dans le cas d'espèce. Ils incluaient, notamment, l'étendue de la surveillance des employés par l'employeur et le degré d'intrusion dans la vie privée de l'employé, les conséquences de cette surveillance pour l'employé et l'existence de garanties adéquates. De plus, les autorités internes devaient veiller à ce que les employés dont les communications avaient été surveillées puissent bénéficier d'une voie de recours devant un organe juridictionnel ayant compétence pour statuer, du moins sur le fond, sur le respect des critères énoncés ainsi que sur la licéité des mesures contestées.

933 CouEDH, *Bărbulescu c. Roumanie* [GC], n° 61496/08, 5 septembre 2017, para. 121.

Dans cette affaire, la CouEDH a conclu à une violation de l'article 8 au motif que les autorités nationales n'avaient pas protégé de manière adéquate le droit du requérant au respect de sa vie privée et de sa correspondance et n'avaient dès lors pas ménagé un juste équilibre entre les intérêts en jeu.

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 liées aux performances ou au potentiel de salariés individuels. Les données d'appréciation doivent être basées sur des évaluations justes et honnêtes et ne doivent pas être formulées de façon injurieuse. C'est ce qu'imposent les principes de loyauté du traitement des données et d'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 ces données sont nécessaires pour leur permettre de défendre leurs intérêts ou pour remplir ou superviser les obligations découlant des conventions collectives.

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 des candidats sur leur état de santé ou les soumettre à un examen médical que si cela est nécessaire. Cela pourrait être le cas pour : déterminer leur adéquation au poste ; satisfaire aux exigences de la médecine préventive ; sauvegarder les intérêts vitaux de la personne concernée ou d'autres salariés ou personnes ; permettre le versement de prestations sociales ou répondre à des demandes judiciaires. 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 explicite et informé ou 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 collectées, des entités auxquelles les données sont communiquées régulièrement, ainsi que de la finalité et de la base juridique de ces communications. Sur le lieu de travail, les communications électroniques ne peuvent être consultées que pour des raisons de sécurité ou d'autres motifs légitimes et cette consultation n'est autorisée qu'après avoir informé les salariés que l'employeur peut avoir accès à ce genre de communication.

Les salariés doivent avoir un droit d'accès à leurs données sur l'emploi ainsi qu'un droit de rectification ou 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, le droit de les rectifier ou de les effacer, la législation nationale doit prévoir des procédures appropriées pour contester un tel refus.

9.3. Données relatives à la santé

Point clé

- Les données médicales sont des données sensibles qui bénéficient dès lors d'une protection particulière.

Les données à caractère personnel relatives à l'état de santé de la personne concernée sont qualifiées de données sensibles à l'article 9, paragraphe 1, du Règlement général sur la protection des données et à l'article 6 de la Convention 108 modernisée. Dès lors, le traitement des données médicales est soumis à un régime plus strict que les données non sensibles. Le RGPD interdit le traitement de « données à caractère personnel concernant la santé » (entendues comme « l'ensemble des données se rapportant à l'état de santé d'une personne concernée qui révèlent des informations sur l'état de santé physique ou mentale passé, présent ou futur de la personne concernée »)[934], ainsi que les données génétiques et les données biométriques, à moins que l'article 9, paragraphe 2, ne l'autorise. Ces deux types de données ont été ajoutés à la liste des « catégories particulières de données »[935].

934 RGPD, considérant 35.

935 *Ibid.*, art. 2.

Exemple : dans l'affaire *Z c. Finlande*[936], l'ex-mari de la requérante, qui était séropositif, avait commis un certain nombre d'infractions sexuelles. Il avait ensuite été condamné pour tentative d'homicide au motif qu'il avait délibérément 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 considérée comme 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 relatives à 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 prononcé de l'arrêt, constituerait une violation de l'article 8 de la CEDH.

Dans **le droit de l'UE**, l'article 9, paragraphe 2, point h), du RGPD autorise le traitement des données médicales lorsque celui-ci est nécessaire aux fins de la médecine préventive, de diagnostics médicaux, de la prise en charge sociale ou sanitaire ou de la gestion des services de soins de santé. Le traitement n'est toutefois autorisé que lorsqu'il est effectué par un professionnel de la santé soumis à une obligation de secret professionnel ou par toute autre personne soumise à une obligation équivalente.

Dans **le droit du CdE**, 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[937]. Les règles proposées sont similaires à celles du RGPD en ce qui concerne les finalités légitimes du traitement de données médicales, les obligations nécessaires de secret professionnel pour les personnes utilisant des données médicales et les droits des personnes concernées à la transparence ainsi

936 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.

937 CdE, Comité des Ministres (1997), Recommandation Rec(97)5 aux États membres relative à la protection des données médicales, 13 février 1997. Cette recommandation fait actuellement l'objet d'une révision.

qu'à l'accès, à la rectification et à l'effacement des données. De plus, les données médicales qui font l'objet d'un traitement licite par des professionnels des services de santé ne peuvent pas 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 »[938]. Le droit national doit également être « formulé de façon suffisamment précise et prévoir une protection juridique adéquate contre l'arbitraire »[939].

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 un motif de conserver des données plus longtemps que nécessaire, bien que cela requière 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 2.1.1.

La Recommandation du CdE de 2016 sur les données résultant de tests génétiques s'applique au traitement des données dans le domaine médical[940]. Cette recommandation revêt une grande importance pour la santé en ligne, qui utilise les TIC pour faciliter les soins médicaux. Un exemple est le transfert des résultats du test de paternité d'un patient d'un prestataire de soins à un autre. Cette recommandation a pour but de protéger les droits des personnes dont les données à caractère personnel sont traitées à des fins d'assurance pour couvrir des risques liés à la santé, à l'intégrité physique, à l'âge ou au décès d'une personne. Les assureurs doivent justifier le traitement des données relatives à la santé et celui-ci devrait être proportionné à la nature et à l'importance du risque considéré. Le traitement de ce type de données est subordonné au consentement de la personne concernée. Les assureurs

938 CouEDH, *Avilkina et autres c. Russie*, n° 1585/09, 6 juin 2013, para. 53. Voir également CouEDH, *Biriuk c. Lituanie*, n° 23373/03, 25 novembre 2008.

939 CouEDH, *L.H. c. Lettonie*, n° 52019/07, 29 avril 2014, para. 59.

940 CdE, Comité des Ministres (2016), Recommandation Rec(2016)8 aux États membres sur le traitement des données à caractère personnel relatives à la santé à des fins d'assurance, y compris les données résultant de tests génétiques, 26 octobre 2016.

devraient adopter des mesures de protection pour la conservation des données relatives à la santé.

Les essais cliniques, qui impliquent d'évaluer les effets de nouveaux médicaments sur des patients dans un environnement de recherche documenté, ont des implications considérables sur la protection des données. Les essais cliniques de produits médicaux à usage humain sont réglementés par le Règlement (UE) nº 536/2014 du Parlement européen et du Conseil du 16 avril 2014 relatif aux essais cliniques de médicaments à usage humain et abrogeant la Directive 2001/20/CE (Règlement relatif aux essais cliniques)[941]. Les principaux éléments du Règlement relatif aux essais cliniques sont les suivants :

- une procédure simplifiée de dépôt de demande par le biais du portail de l'UE[942] ;
- des délais pour l'évaluation de la demande d'essais cliniques[943] ;
- un comité d'éthique intervenant dans l'évaluation, conformément au droit des États membres (et au droit de l'UE fixant les délais concernés)[944] ; et
- une transparence accrue des essais cliniques et de leurs résultats[945].

Le RGPD précise qu'aux fins du consentement à la participation à des activités de recherche scientifique dans le cadre d'essais cliniques, le Règlement (UE) nº 536/2014 s'applique[946].

De nombreuses initiatives législatives et autres concernant les données à caractère personnel dans le domaine de la santé sont actuellement examinées au niveau de l'UE[947].

941 Règlement (UE) nº 536/2014 du Parlement européen et du Conseil du 16 avril 2014 relatif aux essais cliniques de médicaments à usage humain et abrogeant la directive 2001/20/CE, JO 2014 L 158.

942 Règlement relatif aux essais cliniques, art. 5, para. 1.

943 *Ibid.*, art. 5, paras. 2 à 5.

944 *Ibid.*, art. 2, para. 2, point 11.

945 *Ibid.*, art. 9, para. 1, et considérant 67.

946 RGPD, considérants 156 et 161.

947 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.

Dossiers médicaux électroniques

Un dossier informatisé de santé s'entend comme « un dossier médical complet ou une documentation similaire sur l'état de santé physique et mental passé et présent d'un individu, présenté sous forme électronique et permettant d'accéder facilement à ces données en vue d'un traitement médical et à d'autres fins étroitement liées »[948]. Les dossiers informatisés de santé sont des versions électroniques de l'historique médical des patients et peuvent inclure des données cliniques relatives à ces personnes, telles que leurs antécédents médicaux, leurs problèmes et maladies, leurs médicaments et traitements ainsi que leurs résultats d'examen et de laboratoire et les rapports médicaux les concernant. Ces dossiers électroniques, qui peuvent aller de dossiers complets à de simples extraits ou à des résumés, peuvent être consultés par le médecin généraliste, le pharmacien et d'autres professionnels de la santé. Le concept de « santé en ligne » concerne également ces dossiers médicaux.

Exemple : M. A a contracté une police d'assurance auprès de la compagnie B, l'assureur. Cette dernière collectera certaines informations relatives à la santé de A, comme les problèmes de santé ou les maladies actuelles. L'assureur devrait conserver les données à caractère personnel relatives à la santé de A séparément d'autres données. Il doit également conserver les données à caractère personnel relatives à la santé séparément d'autres données à caractère personnel. Cela signifie que seul le gestionnaire de dossier de A aura accès aux données concernant la santé de A.

Les dossiers médicaux électroniques posent, toutefois, certains problèmes en termes de protection des données, tels que leur accessibilité, leur conservation adéquate et l'accès de la personne concernée.

Outre les dossiers médicaux électroniques, la Commission européenne a publié, le 10 avril 2014, un livre vert sur la santé mobile (mHealth), la santé mobile étant un nouveau domaine en plein essor, susceptible de faire évoluer les soins de santé et d'en accroître l'efficacité et la qualité. Cette expression recouvre les pratiques médicales et de santé publique reposant sur des dispositifs mobiles tels que téléphones portables, systèmes de surveillance des patients, assistants numériques personnels

948 Recommandation de la Commission du 2 juillet 2008 sur l'interopérabilité transfrontalière des systèmes de dossiers informatisés de santé, point 3(c).

et autres appareils sans fil, ainsi que des applications (par exemple, concernant le bien-être) qui peuvent se connecter à des dispositifs médicaux ou à des capteurs[949]. Le document expose les risques pour le droit à la protection des données à caractère personnel que pourrait poser le développement de la santé mobile et considère que, compte tenu du caractère sensible des données relatives à la santé, les développements devraient intégrer des garanties spécifiques et adéquates en matière de sécurité des données des patients, comme le cryptage, et des mécanismes appropriés d'authentification des patients afin d'atténuer les risques liés à la sécurité. Le respect des règles relatives à la protection des données à caractère personnel, notamment l'obligation d'informer la personne concernée, la sécurité des données et le principe de la licéité du traitement des données à caractère personnel, est essentiel pour instaurer la confiance dans les solutions de santé mobile[950]. À cet effet, un code de conduite a été rédigé par le secteur, sur la base des contributions d'un large éventail de parties prenantes, notamment des représentants spécialisés dans la protection des données, l'autoréglementation et la coréglementation, les TIC et les soins de santé[951]. Au moment de rédiger ce manuel, le projet de code de conduite avait été soumis pour commentaires au Groupe de travail « Article 29 » sur la protection des données, dans l'attente de son approbation formelle.

9.4. Traitement de données à des fins statistiques et de recherche

Points clés

- Les données collectées à des fins statistiques ou de recherche scientifique ou historique 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 ou de recherche scientifique ou historique, à condition que la législation nationale mette en place des garanties adéquates. Dans cette perspective, l'anonymisation ou la pseudonymisation avant la transmission à des tiers devrait être envisagée.

949 Commission européenne (2014), *Livre vert sur la santé mobile*, COM(2014) 219 final, Bruxelles, 10 avril 2014.

950 *Ibid.*, p. 8.

951 Draft Code of Conduct on privacy for mobile health applications, 7 juin 2016.

Le droit de l'UE autorise le traitement de données à des fins statistiques ou à des fins de recherche scientifique ou historique pour autant que soient mises en œuvre des mesures appropriées pour garantir les droits et libertés de la personne concernée. Ces mesures peuvent comprendre la pseudonymisation[952]. Le droit de l'UE ou le droit national peut prévoir certaines dérogations aux droits des personnes concernées dans la mesure où ces droits seraient susceptibles de rendre impossible ou d'entraver sérieusement la réalisation de la finalité légitime de la recherche[953]. Des dérogations peuvent être instaurées en ce qui concerne le droit d'accès de la personne concernée, le droit à la rectification des données, le droit à la limitation du traitement et le droit d'opposition.

Bien que les données qui ont été collectées légalement par un responsable du traitement pour n'importe quelle finalité puissent être réutilisées par ce responsable à ses propres fins statistiques ou de recherche scientifique ou historique, les données devraient, selon les circonstances, être anonymisées ou pseudonymisées avant d'être transmises à un tiers à des fins statistiques ou de recherche scientifique ou historique, à moins que la personne concernée n'y ait consenti ou que cela soit spécifiquement prévu par le droit national. Les données qui ont fait l'objet d'une pseudonymisation restent soumises au RGPD, à la différence des données anonymisées[954].

Le règlement accorde donc à la recherche un traitement spécial par rapport aux règles générales relatives à la protection des données pour éviter de limiter le développement de la recherche et se conformer à l'objectif, mentionné à l'article 179 de TFUE, consistant à réaliser un espace européen de la recherche. Il prévoit une interprétation large du traitement de données à caractère personnel à des fins de recherche scientifique, y compris le développement et la démonstration de technologie, la recherche fondamentale, la recherche appliquée et la recherche financée par le secteur privé. Il reconnaît également l'importance de combiner les données issues des registres à des fins de recherche et la difficulté potentielle de cerner entièrement la finalité ultérieure du traitement des données à caractère personnel à des fins de recherche scientifique au moment de la collecte des données[955]. C'est pourquoi le règlement autorise le traitement de données à ces fins, sans le

952 RGPD, art. 89, para. 1.

953 *Ibid.*, art. 89, para. 2.

954 *Ibid.*, considérant 26.

955 *Ibid.*, considérants 33, 157 et 159.

consentement des personnes concernées, pour autant que soient mises en œuvre les garanties pertinentes.

Un exemple important d'utilisation de données à des fins statistiques est celui des statistiques officielles, réalisées par les offices nationaux et européen de la statistique sur la base des législations nationales et européenne relatives aux statistiques officielles. Conformément à ces législations, les citoyens et les entreprises sont généralement tenus de communiquer des données aux autorités compétentes en matière de statistiques. Les fonctionnaires qui travaillent dans les offices de statistiques sont soumis à des obligations spéciales de secret professionnel qu'ils observent avec soin, dans la mesure où elles sont essentielles pour instaurer le niveau élevé de confiance des citoyens qui est nécessaire à la communication de ces données aux autorités statistiques[956].

Le Règlement (CE) nº 223/2009 relatif aux statistiques européennes (Règlement sur les statistiques européennes) établit des règles essentielles pour la protection des données dans les statistiques officielles et il peut donc aussi être considéré comme pertinent pour les dispositions relatives aux statistiques officielles adoptées au niveau national[957]. Le règlement applique le principe selon lequel l'activité statistique requiert une base juridique suffisamment précise[958].

Exemple : dans l'affaire *Huber c. Bundesrepublik Deutschland*[959], un homme d'affaires autrichien résidant en Allemagne s'est plaint que la collecte et la conservation par les autorités allemandes de données à caractère personnel de ressortissants étrangers dans un registre central (AZR) à des fins statistiques violaient ses droits au titre de la Directive relative à la protection des données. Considérant que la Directive 95/46 vise à assurer

956 *Ibid.*, art. 90.

957 Règlement (CE) nº 223/2009 du Parlement européen et du Conseil du 11 mars 2009 relatif aux statistiques européennes et abrogeant le règlement (CE, Euratom) nº 1101/2008 relatif à la transmission à l'Office statistique des Communautés européennes d'informations statistiques couvertes par le secret, le règlement (CE) nº 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 20096 L 87, tel que modifié par le règlement (UE) 2015/759 du Parlement européen et du Conseil du 29 avril 2015 modifiant le règlement (CE) nº 223/2009 relatif aux statistiques européennes, JO 2015 L 123.

958 Ce principe est détaillé dans le Code de bonnes pratiques d'Eurostat, qui, conformément à l'article 11 du Règlement relatif aux statistiques européennes, définit des normes éthiques sur la manière de produire des statistiques officielles, notamment en faisant un usage réfléchi des données à caractère personnel.

959 CJUE, C-524/06, *Heinz Huber c. Bundesrepublik Deutschland* [GC], 16 décembre 2008, voir notamment point 68.

un niveau équivalent de protection des données dans tous les États membres, la CJUE a conclu que, pour garantir un niveau élevé de protection dans l'UE, la notion de nécessité telle qu'elle résulte de l'article 7, point e), ne saurait avoir un contenu variable en fonction des États membres. Dès lors, il s'agit d'une notion autonome du droit de l'UE qui doit recevoir une interprétation de nature à répondre pleinement à l'objet de la Directive 95/46. Notant que seules des informations anonymes devraient être requises à des fins statistiques, la Cour a conclu que le registre allemand n'était pas compatible avec l'obligation de nécessité visée à l'article 7, point e).

Dans le cadre du **CdE**, le traitement ultérieur de données peut être effectué à des fins scientifiques, historiques ou statistiques lorsqu'il sert un motif d'intérêt public et il doit être assorti de garanties appropriées[960]. Les droits des personnes concernées peuvent également être restreints lorsque les données sont traitées à des fins statistiques, pour autant qu'il n'existe pas de risque identifiable de violation de leurs droits et libertés[961].

La Recommandation sur les données statistiques, publiée en 1997, couvre l'exécution d'activités statistiques dans les secteurs public et privé[962].

Les données collectées par un responsable du traitement à des fins statistiques ne peuvent pas être utilisées à d'autres fins. Les données collectées à des fins autres que statistiques peuvent faire l'objet d'une utilisation statistique ultérieure. La Recommandation sur les données statistiques autorise également la communication de données à des tiers si celle-ci poursuit une finalité purement statistique. Dans ce cas, les parties doivent convenir et consigner par écrit le périmètre 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, lorsque celui-ci est nécessaire, il convient de supposer qu'il doit exister des garanties appropriées 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.

960 Convention 108 modernisée, art. 5, para. 4, point b).

961 *Ibid.*, art. 11, para. 2.

962 CdE, 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.

Les professionnels chargés de recherches statistiques doivent être liés par des obligations spéciales de secret professionnel (comme c'est généralement le cas pour les statistiques officielles) en vertu de la législation nationale. Cette obligation doit également s'étendre aux interviewers et aux autres collecteurs de données, dès lors qu'ils travaillent à la collecte des données provenant de personnes concernées ou d'autres personnes.

Lorsqu'une enquête statistique utilisant des données à caractère personnel n'est pas autorisée par la loi, les personnes concernées doivent consentir à l'utilisation de leurs données afin de rendre le traitement légitime, ou avoir 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 non de la divulgation des données en droit national.

Lorsqu'une étude statistique ne peut pas être réalisée sans données anonymes et que 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 permettre l'identification des 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 pareil 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 autres données.

9.5. Données financières

Points clés

- Bien que les données financières ne soient pas considérées comme des données sensibles au sens de la Convention 108 modernisée ou du Règlement général sur la protection des données, leur traitement requiert des garanties particulières pour assurer l'exactitude et la sécurité des données.

- Les systèmes de paiement électronique nécessitent une protection intégrée des données, appelée « respect de la vie privée ou protection des données dès la conception et par défaut ».
- Des problèmes particuliers de protection des données peuvent survenir dans ce domaine du fait de la nécessité de mettre en place des mécanismes d'authentification appropriés.

Exemple : dans l'affaire *Michaud c. France*[963], 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 professionnels 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 des activités de nature tant 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. La CouEDH a exclu la violation de l'article 8 de la CEDH.

Exemple : dans l'affaire *M.N. et autres c. Saint-Marin*[964], le requérant, un citoyen italien, a conclu un accord de fiducie avec une entreprise visée par une enquête. L'entreprise a fait l'objet d'une perquisition qui a conduit à la saisie de copies de documents (électroniques). Le requérant a saisi le tribunal de Saint-Marin au motif qu'il n'était en rien lié aux délits présumés. Le tribunal a toutefois déclaré sa plainte irrecevable au motif qu'il n'était pas une « partie intéressée ». La CouEDH a retenu que le requérant avait été nettement désavantagé du point de vue de la protection de ses droits par rapport à une « partie intéressée », étant donné que ses données étaient toujours soumises aux opérations de perquisition et de saisie. La Cour a donc conclu à une violation de l'article 8.

963 CouEDH, *Michaud c. France*, nº 12323/11, 6 décembre 2012. Voir aussi CouEDH, *Niemietz c. Allemagne*, nº 13710/88, 16 décembre 1992, para. 29 ; CouEDH, *Halford c. Royaume-Uni*, nº 20605/92, 25 juin 1997, para. 42.

964 CouEDH, *M.N. et autres c. Saint-Marin*, nº 28005/12, 7 juillet 2015.

Exemple : dans l'affaire *G.S.B. c. Suisse*[965], les coordonnées bancaires du requérant ont été transmises aux autorités fiscales américaines conformément à un accord de coopération administrative conclu entre la Suisse et les États-Unis. La CouEDH a considéré que la transmission de ces données n'était pas contraire à l'article 8 de la CEDH au motif que l'ingérence dans le droit au respect de la vie privée du requérant était prévue par la loi, poursuivait un but légitime et était proportionnée à l'intérêt public en cause.

L'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 la Recommandation nº R (90) 19 du **CdE** de 1990[966]. Cette recommandation clarifie l'étendue de la collecte et de l'utilisation licites de données dans le contexte des paiements, en particulier à l'aide de cartes de paiement. Elle propose également aux législateurs nationaux des recommandations détaillées sur les règles relatives à la communication de données de paiement à des tiers, les délais de conservation des données, la transparence, la sécurité des données et les flux transfrontières de données et, enfin, sur le contrôle et les voies de recours. Le CdE a également rédigé un avis sur le transfert des données fiscales[967], qui fournit des recommandations et des éléments à prendre en considération lors du transfert de ce type de données.

La CouEDH autorise la transmission de données financières – en particulier, les coordonnées bancaires d'un individu – au titre de l'article 8 de la CEDH, si elle est prévue par la loi, poursuit un but légitime et est proportionnée à l'intérêt public en cause[968].

Dans le droit de l'UE, les systèmes de paiement électronique impliquant le traitement de données à caractère personnel doivent se conformer aux dispositions du Règlement général sur la protection des données. Ces systèmes doivent par conséquent assurer la protection des données dès la conception ainsi que la protection des données par défaut. La protection des données dès la conception oblige le responsable du traitement à prendre les mesures techniques et organisationnelles appropriées pour mettre en œuvre les principes de la protection des données. La

965 CouEDH, *G.S.B. c. Suisse*, nº 28601/11, 22 décembre 2015.

966 CdE, Comité des Ministres (1990), Recommandation nº R (90) 19 sur la protection des données à caractère personnel utilisées à des fins de paiement et autres opérations connexes, 13 septembre 1990.

967 CdE, Comité consultatif de la Convention 108 (2014), Avis sur les implications en matière de protection des données des mécanismes d'échange interétatique et automatique de données à caractère personnel à des fins administratives et fiscales, 4 juin 2014.

968 CouEDH, *G.S.B. c. Suisse*, nº 28601/11, 22 décembre 2015.

protection des données par défaut implique que le responsable du traitement doit veiller à ce que seules les données à caractère personnel qui sont nécessaires à une finalité particulière puissent être traitées par défaut (voir section 4.4). S'agissant des données financières, la CJUE a déclaré que les données fiscales transmises peuvent constituer des données à caractère personnel[969]. Le Groupe de travail « Article 29 » a publié des lignes directrices en la matière à l'intention des États membres, lesquelles prévoient des critères pour assurer le respect des règles relatives à la protection des données lors de l'échange automatique de données à caractère personnel à des fins fiscales par des moyens automatisés[970]. Par ailleurs, un certain nombre d'instruments juridiques ont été adoptés pour réglementer les marchés financiers et les activités des établissements de crédit et des sociétés de placement[971]. D'autres instruments juridiques contribuent à lutter contre les délits d'initiés et la manipulation des cours[972]. Les principaux domaines ayant un impact sur la protection des données sont les suivants :

- la conservation de registres des transactions financières ;
- le transfert de données à caractère personnel vers des pays tiers ;
- l'enregistrement de conversations téléphoniques ou de communications électroniques, y compris le pouvoir conféré aux autorités compétentes de demander les enregistrements d'appels téléphoniques et d'échanges de données ;
- la divulgation d'informations personnelles, notamment la publication de sanctions ;

969 CJUE, C-201/14, *Smaranda Bara et autres c. Casa Națională de Asigurări de Sănătate et autres*, 1er octobre 2015, point 29.

970 Groupe de travail « Article 29 » (2015), déclaration du GT29 sur l'échange interétatique et automatique de données à caractère personnel à des fins fiscales, 14/EN WP 230.

971 Directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant la directive 2002/92/CE et la directive 2011/61/UE, JO 2014 L 173 ; Règlement (UE) nº 600/2014 du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant le règlement (UE) nº 648/2012, JO 2014 L 173 ; Directive 2013/36/UE du Parlement européen et du Conseil du 26 juin 2013 concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement, modifiant la directive 2002/87/CE et abrogeant les directives 2006/48/CE et 2006/49/CE, JO 2013 L 176.

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

- les pouvoirs de contrôle et d'investigation des autorités compétentes, notamment 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 dénonciation ; et

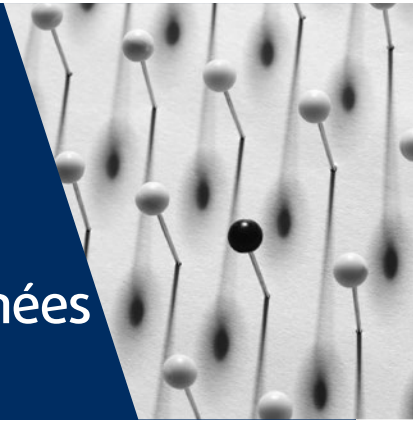
- la coopération entre les autorités compétentes des États membres et l'Autorité européenne des marchés financiers (AEMF).

D'autres problèmes dans ces domaines sont aussi traités de façon spécifique, y compris la collecte des données sur le statut financier des personnes concernées[973] ou le paiement transfrontalier par virements bancaires, qui entraîne inévitablement des flux de données à caractère personnel[974].

973 Règlement (CE) nº 1060/2009 du Parlement européen et du Conseil du 16 septembre 2009 sur les agences de notation de crédit, JO 2009 L 302, modifié en dernier lieu par la directive 2014/51/UE du Parlement européen et du Conseil du 16 avril 2014 modifiant les directives 2003/71/CE et 2009/138/CE et les règlements (CE) nº 1060/2009, (UE) nº 1094/2010 et (UE) nº 1095/2010 en ce qui concerne les compétences de l'Autorité européenne de surveillance (Autorité européenne des assurances et des pensions professionnelles) et de l'Autorité européenne de surveillance (Autorité européenne des marchés financiers), JO 2014 L 153 ; Règlement (UE) nº 462/2013 du Parlement européen et du Conseil du 21 mai 2013 modifiant le règlement (CE) n° 1060/2009 sur les agences de notation de crédit, JO 2013 L 146.

974 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, modifiée par la directive 2009/111/CE du Parlement européen et du Conseil du 16 septembre 2009 modifiant les directives 2006/48/CE, 2006/49/CE et 2007/64/CE en ce qui concerne les banques affiliées à des institutions centrales, certains éléments des fonds propres, les grands risques, les dispositions en matière de surveillance et la gestion des crises, JO 2009 L 302.

10 Les défis modernes de la protection des données à caractère personnel



L'ère du numérique, ou ère des technologies de l'information, se caractérise par l'utilisation généralisée des ordinateurs, d'internet et des technologies numériques. Elle implique la collecte et le traitement de quantités énormes de données, dont des données à caractère personnel. La collecte et le traitement de données à caractère personnel dans une économie mondialisée signifient que les flux transfrontières de données se multiplient. Ces traitements peuvent aboutir à des avantages significatifs et visibles dans la vie quotidienne : les moteurs de recherche facilitent l'accès à des volumes considérables d'informations et de connaissances ; les réseaux sociaux permettent à des personnes du monde entier de communiquer, d'exprimer leurs avis et de sensibiliser à des causes sociales, environnementales et politiques, tandis que les entreprises et leurs clients bénéficient de techniques de marketing efficaces et rentables qui stimulent l'économie. La technologie et le traitement de données à caractère personnel sont également des outils indispensables pour les autorités nationales dans leur lutte contre le crime et le terrorisme. De même, les mégadonnées (« *big data* »), à savoir la collecte, le stockage et l'analyse de grandes quantités d'informations en vue de dégager des tendances et de prévoir des comportements, « peuvent être source de grande valeur et d'innovation pour la société en permettant d'accroître la productivité, les performances du secteur public et la participation sociale »[975].

Malgré ses multiples bienfaits, l'ère du numérique engendre également des défis pour le respect de la vie privée et la protection des données, dans la mesure où d'énormes quantités d'informations personnelles sont collectées et traitées en

975 CdE, Comité consultatif de la Convention 108 (2017), *Lignes directrices sur la protection des personnes à l'égard du traitement des données à caractère personnel à l'ère des mégadonnées*, T-PD(2017)01, Strasbourg, 23 janvier 2017.

recourant à des applications de plus en plus complexes et opaques. Les avancées technologiques ont conduit à l'élaboration d'ensembles de données massives qui peuvent être aisément croisées et analysées de manière plus approfondie pour dégager des tendances ou pour adopter des décisions fondées sur des algorithmes, ce qui peut permettre une compréhension sans précédent des comportements humains et de la vie privée[976].

Les nouvelles technologies sont puissantes et peuvent se révéler particulièrement dangereuses lorsqu'elles tombent entre de mauvaises mains. Des autorités publiques pratiquant une surveillance massive qui peut recourir à ces technologies sont un exemple de l'incidence significative que ces dernières peuvent avoir sur les droits des individus. En 2013, les révélations d'Edward Snowden sur le fonctionnement de programmes de surveillance à grande échelle d'internet et des conversations téléphoniques par les agences de renseignement de certains États ont suscité de vives inquiétudes quant aux dangers que représentent les activités de surveillance pour le respect de la vie privée, la gouvernance et la liberté d'expression. La surveillance de masse et les technologies permettant le stockage et le traitement de données à caractère personnel dans un contexte mondialisé et l'accès à des données de masse peuvent porter atteinte à l'essence même du droit au respect de la vie privée[977]. De plus, elles peuvent affecter négativement la culture politique et avoir un effet dissuasif sur la démocratie, la créativité et l'innovation[978]. La simple crainte que l'État puisse surveiller et analyser en permanence le comportement et les actions de ses citoyens peut dissuader ces derniers d'exprimer leur point de vue sur certaines questions et susciter méfiance et prudence[979]. Ces défis ont incité un certain nombre d'autorités publiques, de centres de recherche et d'organisations de la société civile à analyser les effets potentiels des nouvelles technologies sur la société. En 2015, le Contrôleur européen de la protection des données a lancé plusieurs initiatives visant à évaluer l'impact des données massives et de l'Internet des objets (IdO) sur l'éthique. Il a notamment créé un groupe consultatif

976 Parlement européen (2017), Résolution sur les incidences des mégadonnées pour les droits fondamentaux : respect de la vie privée, protection des données, non-discrimination, sécurité et application de la loi, P8_TA-PROV(2017)0076, Strasbourg, 14 mars 2017.

977 Voir ONU, Assemblée générale, *Rapport du Rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste*, Ben Emmerson, A/69/397, 23 septembre 2014, para. 59. Voir aussi CouEDH, *Fiche thématique - Surveillance de masse*, juillet 2017.

978 CEPD (2015), *Relever les défis des données massives*, Avis nº 7/2015, Bruxelles, 19 novembre 2015.

979 Voir, notamment, CJUE, affaires jointes C-293/12 et C-594/12, *Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources et autres* et *Kärntner Landesregierung et autres*, [GC], 8 avril 2014, point 37.

sur l'éthique, dont le but est d'« encourager un débat ouvert et éclairé sur l'éthique numérique, qui permet à l'Union européenne de concrétiser les avantages de la technologie pour la société et l'économie, tout en renforçant les droits et libertés des personnes, en particulier leurs droits au respect de la vie privée et à la protection des données »[980].

Le traitement de données à caractère personnel est également un outil puissant dans les mains des entreprises. Aujourd'hui, il peut révéler des informations détaillées sur l'état de santé ou la situation financière d'une personne, des informations qui sont ensuite utilisées par des entreprises pour arrêter des décisions importantes pour les individus, comme la prime d'assurance maladie à leur appliquer ou leur solvabilité. Les techniques de traitement des données peuvent, elles aussi, influencer les processus démocratiques, lorsqu'elles sont utilisées par des hommes politiques ou des entreprises pour influencer des éléments, notamment en « microciblant » les communications des électeurs. En d'autres termes, alors qu'à l'origine, le respect de la vie privée était perçu comme le droit de protéger des personnes contre toute immixtion injustifiée des autorités publiques, dans le monde moderne, il peut également être menacé par les pouvoirs d'acteurs privés. Cela soulève des questions sur l'utilisation de la technologie et de l'analyse prédictive dans des décisions qui touchent la vie quotidienne des gens et renforce la nécessité de faire en sorte que tout traitement de données à caractère personnel soit conforme aux exigences des droits fondamentaux.

La protection des données est étroitement liée aux changements technologiques, sociaux et politiques. Il est donc impossible de dresser une liste exhaustive des défis futurs. Le présent chapitre se penche sur des thèmes précis concernant les mégadonnées, les réseaux sociaux en ligne et le marché unique numérique de l'UE. Il ne s'agit pas d'un examen complet de ces domaines du point de vue de la protection des données, mais d'une mise en évidence des multiples interactions possibles entre des activités humaines nouvelles ou modernisées et la protection des données.

980 CEPD, Décision du 3 décembre 2015 instituant un groupe consultatif externe sur les dimensions éthiques de la protection des données (« groupe consultatif sur l'éthique »), 3 décembre 2015, considérant 5.

10.1. Mégadonnées, algorithmes et intelligence artificielle

Points clés

- D'importantes innovations dans les TIC façonnent un nouveau mode de vie, dans lequel les relations sociales, les entreprises, les services publics et privés sont interconnectés numériquement, ce qui génère une quantité toujours plus grande de données, dont une grande partie est constituée de données à caractère personnel.
- Les gouvernements, les entreprises et les citoyens vivent dans une économie de plus en plus basée sur les échanges de données, dans laquelle les données elles-mêmes sont devenues des biens précieux.
- La notion de mégadonnées fait à la fois référence aux données et à leur analyse.
- Les données à caractère personnel traitées par le biais de l'analyse des mégadonnées sont couvertes par la législation de l'UE et du CdE.
- Les dérogations aux règles de la protection des données et aux droits qui en découlent sont limitées à quelques droits bien précis et à des situations spécifiques dans lesquelles l'exercice d'un droit serait impossible ou nécessiterait des efforts disproportionnés de la part des responsables du traitement.
- La règle générale veut que la prise de décisions entièrement automatisée soit interdite, hormis dans des cas spécifiques.
- La prise de conscience et le contrôle par les individus sont essentiels pour garantir le respect de leurs droits.

Dans ce monde de plus en plus numérisé, chaque activité laisse une trace numérique qui peut être collectée, traitée, évaluée ou analysée. Grâce aux nouvelles technologies de l'information et de la communication, un nombre croissant de données sont collectées et enregistrées[981]. Jusqu'à récemment, aucune technologie n'était capable d'analyser ou d'évaluer cette masse de données ou d'en tirer des conclusions utiles. Les données étaient tout simplement trop nombreuses pour permettre leur évaluation et trop complexes, trop peu structurées et trop évolutives pour en dégager des tendances et des habitudes.

981 Commission européenne, Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions – Vers une économie de la donnée prospère, COM(2014) 442 final, Bruxelles, 2 juillet 2014.

10.1.1. Définir les mégadonnées, les algorithmes et l'intelligence artificielle

Mégadonnées

Le terme « mégadonnées » est une expression à la mode qui peut désigner plusieurs concepts en fonction du contexte. Elle recouvre généralement « la capacité technologique croissante de collecter, traiter et extraire très rapidement des connaissances nouvelles et prédictives à partir d'un gros volume et d'une grande variété de données »[982]. La notion de mégadonnées couvre donc à la fois les données proprement dites et leur analyse.

Les **sources** de données sont de différents types et englobent les personnes et leurs données à caractère personnel, des machines ou des capteurs, des informations climatiques, de l'imagerie satellite, des images et vidéos numériques ou des signaux GPS. Une grande partie des données et des informations sont toutefois des données à caractère personnel, depuis un nom, une photo, une adresse électronique, des coordonnées bancaires, des données de traçage GPS, des publications sur des réseaux sociaux ou des informations médicales jusqu'à l'adresse IP d'un ordinateur[983].

Les mégadonnées désignent également le **traitement**, l'analyse et l'évaluation de masses de données et d'informations disponibles, c'est-à-dire l'extraction d'informations utiles aux fins de l'analyse des mégadonnées. En d'autres termes, les données et informations collectées peuvent être utilisées à d'autres fins que celles initialement prévues, par exemple des tendances statistiques, ou pour des services plus adaptés, comme la publicité. En fait, lorsque des technologies permettant de collecter, de traiter et d'évaluer des données massives existent, tout type d'information peut être combiné et réévalué : des transactions financières, la solvabilité, un traitement médical, la consommation privée, l'activité professionnelle, le traçage

982 CdE, Comité consultatif de la Convention 108, Lignes directrices sur la protection des personnes à l'égard du traitement des données à caractère personnel à l'ère des mégadonnées, 23 janvier 2017, p. 2 ; Commission européenne, Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions – Vers une économie de la donnée prospère, COM(2014) 442 final, Bruxelles, 2 juillet 2014, p. 4 ; Union internationale des télécommunications (2015), Recommandation Y.3600 – Exigences et capacités pour les mégadonnées basées sur l'informatique en nuage.

983 Fiche thématique de la Commission européenne sur la réforme de la protection des données dans l'UE et les données massives ; CdE, Comité consultatif de la Convention 108, Lignes directrices sur la protection des personnes à l'égard du traitement des données à caractère personnel à l'ère des mégadonnées, 23 janvier 2017, p. 2.

et les itinéraires empruntés, l'utilisation d'internet, les cartes électroniques et les smartphones, la vidéosurveillance ou la surveillance des communications. L'analyse des données massives apporte une nouvelle dimension quantitative aux données, que l'on peut évaluer et utiliser en temps réel, par exemple pour offrir des services sur mesure aux consommateurs.

Algorithmes et intelligence artificielle

L'intelligence artificielle (IA) désigne l'intelligence de machines agissant comme des « agents intelligents ». En tant qu'agent intelligent, certains dispositifs peuvent, avec l'aide d'un logiciel, percevoir leur environnement et agir selon des algorithmes. L'expression « intelligence artificielle » est utilisée lorsqu'une machine imite des fonctions cognitives, telles que l'apprentissage et la résolution de problèmes, qui seraient normalement associées à des personnes physiques[984]. Pour imiter la prise de décision, les technologies et les logiciels modernes ont recours à des algorithmes que les dispositifs utilisent pour prendre des « décisions automatisées ». On peut définir un algorithme comme une procédure en plusieurs étapes pour le calcul, le traitement de données, l'évaluation, le raisonnement automatisé et la prise de décision.

Tout comme l'analyse des mégadonnées, l'IA et la prise de décisions automatisée qu'elle engendre requièrent la collecte et le traitement de grandes quantités de données. Ces données proviennent du dispositif lui-même (température des freins, carburant, etc.) ou de l'environnement. Le profilage, par exemple, est un processus qui peut reposer sur une prise de décisions automatisée selon des schémas ou des facteurs prédéterminés.

Exemple : Profilage et publicité ciblée

Le profilage basé sur des mégadonnées nécessite de rechercher des schémas qui reflètent des « caractéristiques d'un type de personnalité », par exemple lorsque des sociétés d'achat en ligne proposent des produits que « vous pourriez aussi aimer » sur la base des informations collectées à partir des produits précédemment mis dans le panier d'un client. Plus les données sont nombreuses, plus la mosaïque est révélatrice. Le smartphone, par exemple,

984 Stuart Russel et Peter Norvig, *Artificial Intelligence : A Modern Approach (2nd ed.)*, 2003, Upper Saddle River, New Jersey : Prentice Hall, p. 27, 32 à 58, 968 à 972 ; Stuart Russel et Peter Norvig, *Artificial Intelligence : A Modern Approach (3rd ed.)*, 2009, Upper Saddle River, New Jersey : Prentice Hall, p. 2.

est un questionnaire puissant que les personnes complètent à chaque utilisation, aussi bien consciemment qu'inconsciemment.

La psychographie moderne, la science qui étudie les personnalités, a recours à la méthode OCEAN, grâce à laquelle elle détermine les types de personnalité traités. Les « cinq grands » aspects de la personnalité sont l'ouverture (degré d'ouverture d'une personne à la nouveauté), le sérieux (caractère perfectionniste de la personne), l'extraversion (sociabilité de la personne), l'amabilité (caractère agréable de la personne) et le névrosisme (l'émotivité de la personne). Ces informations profilent la personne, ses besoins et ses craintes, la manière dont elle se comportera, etc. Elles sont ensuite complétées par d'autres informations sur la personne, obtenues auprès de toutes les sources disponibles, depuis les courtiers en données en passant par les réseaux sociaux (y compris les mentions « j'aime » sur les publications et les photos publiées) jusqu'à la musique écoutée en ligne ou les données GPS ou de traçage.

Les multiples profils créés par des techniques d'analyse des mégadonnées sont ensuite comparés afin de dégager des schémas similaires et d'établir des groupes de personnalités. Les informations sur le comportement et les attitudes de certaines personnalités sont donc inversées. Grâce à l'accès aux mégadonnées et à leur utilisation, le test de personnalité est modifié, étant donné que les informations sur le comportement et l'attitude sont désormais utilisées pour décrire la personnalité de l'individu. En disposant des informations combinées sur les mentions « j'aime » sur les réseaux sociaux, les données de traçage, la musique écoutée ou les films visionnés, une image précise de la personnalité d'un individu peut émerger, ce qui permet aux entreprises de communiquer des publicités et/ou des informations personnalisées tenant compte de la « personnalité » de cet individu. Mais surtout, ces informations peuvent être traitées en temps réel[985].

985 Les techniques de traitement et les nouveaux logiciels évaluent les informations sur ce qu'une personne aime, examinent quand elle achète en ligne ou ajoute quelque chose à un panier en ligne en temps réel et peuvent proposer des « produits » susceptibles de l'intéresser sur la base des informations collectées.

10.1.2. Mise en balance des avantages et des risques des mégadonnées

Les techniques de traitement modernes peuvent gérer des masses importantes de données, en importer rapidement de nouvelles, traiter en temps réel les informations avec un temps de réaction court (même dans le cas de demandes complexes), permettre des demandes multiples et simultanées et analyser différents types d'informations (photos, textes ou chiffres). Ces innovations technologiques permettent de structurer, traiter et évaluer des masses de données et d'informations en temps réel[986]. En augmentant de façon exponentielle la quantité de données disponibles et analysées, les résultats que n'aurait pas pu obtenir une analyse à plus petite échelle peuvent désormais être atteints. Les mégadonnées ont également contribué au développement d'un nouveau domaine d'activité, dans lequel de nouveaux services peuvent apparaître pour les entreprises et les consommateurs. La valeur des données à caractère personnel des citoyens de l'UE pourrait atteindre près d'un milliard d'euros par an d'ici 2020[987]. Les mégadonnées peuvent donc offrir de nouvelles **possibilités** résultant de l'évaluation de données massives pour de nouvelles analyses sociales, économiques ou scientifiques susceptibles de présenter des avantages pour les personnes, les entreprises et les gouvernements[988].

L'analyse des mégadonnées peut dégager des schémas entre différentes sources et ensembles de données, qui permettent d'ouvrir des perspectives utiles dans des domaines comme la science ou la médecine. C'est le cas, par exemple, dans des domaines tels que la santé, la sécurité alimentaire, les systèmes de transport

986 Le développement de logiciels pour le traitement des mégadonnées en est toujours à ses balbutiements. Néanmoins, des programmes analytiques ont été récemment développés, notamment pour l'analyse de données massives et d'informations en temps réel en rapport avec les activités des individus. La possibilité d'analyser et de traiter des mégadonnées de façon structurée a créé de nouveaux outils de profilage et de publicité ciblée. Commission européenne, Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions – Vers une économie de la donnée prospère, COM(2014) 442 final, Bruxelles, 2 juillet 2014 ; Commission européenne, Fiche thématique de la Commission européenne sur la réforme de la protection des données dans l'UE et les données massives ; et CdE, Lignes directrices sur la protection des personnes à l'égard du traitement des données à caractère personnel à l'ère des mégadonnées, 23 janvier 2017, p. 2.

987 Fiche thématique de la Commission européenne sur la réforme de la protection des données dans l'UE et les données massives.

988 Conférence internationale des commissaires à la protection des données et de la vie privée (2014), Résolution sur les mégadonnées ; Commission européenne, Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions – Vers une économie de la donnée prospère, COM(2014) 442 final, Bruxelles, 2 juillet 2014 ; Fiche thématique de la Commission européenne sur la réforme de la protection des données dans l'UE et les données massives ; et CdE, Lignes directrices sur la protection des personnes à l'égard du traitement des données à caractère personnel à l'ère des mégadonnées, 23 janvier 2017, p. 1.

intelligents, l'efficacité énergétique ou l'urbanisme. Cette analyse en temps réel des informations peut être mise à profit pour améliorer les systèmes en place. Dans le domaine de la recherche, la combinaison de grandes quantités de données et d'évaluations statistiques, en particulier dans des disciplines dans lesquelles une grande partie des données n'ont jusqu'à présent été analysées que manuellement, peut apporter de nouvelles connaissances. De nouveaux traitements peuvent être développés, adaptés à des patients individuels sur la base de comparaisons avec la masse d'informations disponibles. Les entreprises espèrent que l'analyse des mégadonnées leur permettra de tirer des avantages concurrentiels, de générer des économies potentielles et de créer de nouveaux secteurs d'activité grâce à un service personnalisé et direct à la clientèle. Les agences gouvernementales espèrent améliorer la justice pénale. La Stratégie de la Commission européenne pour le Marché Unique Numérique européen reconnaît le potentiel des technologies et des services fondés sur les données ainsi que des mégadonnées en tant que catalyseurs de croissance économique, d'innovation et de numérisation dans l'Union[989].

Les mégadonnées impliquent toutefois aussi des **risques**, généralement associés aux « trois V » : volume, vitesse et variété des données traitées. Le volume désigne la quantité de données traitées, la variété fait référence au nombre et à la diversité des types de données, tandis que la vitesse concerne la rapidité du traitement des données. Des considérations spécifiques à la protection des données se posent notamment lorsque des analyses de mégadonnées portent sur de grands ensembles de données afin d'en extraire des connaissances nouvelles et prédictives en vue de prendre des décisions concernant des individus et/ou des groupes[990]. Les risques que recèlent les mégadonnées pour la protection des données et le respect de la vie privée ont été mis en évidence dans des avis du CEPD et du Groupe de travail « Article 29 », ainsi que dans des résolutions du Parlement européen et des documents d'orientation du Conseil de l'Europe[991].

989 Résolution du Parlement européen du 14 mars 2017 sur les incidences des mégadonnées pour les droits fondamentaux: respect de la vie privée, protection des données, non-discrimination, sécurité et application de la loi (2016/2225(INI)).

990 CdE, Comité consultatif de la Convention 108, lignes directrices sur la protection des personnes à l'égard du traitement des données à caractère personnel à l'ère des mégadonnées, 23 janvier 2017, p. 2.

991 Voir, par exemple, CEPD (2015), *Relever les défis des données massives*, Avis 7/2015, 19 novembre 2015 ; CEPD (2016), *Application cohérente des droits fondamentaux à l'ère des données massives*, avis 8/2016, 23 septembre 2016 ; Parlement européen (2016), Résolution sur les incidences des mégadonnées pour les droits fondamentaux: respect de la vie privée, protection des données, non-discrimination, sécurité et application de la loi, PA_TA(2017)0076, Strasbourg, 14 mars 2017 ; CdE, Comité consultatif de la Convention 108, Lignes directrices sur la protection des personnes à l'égard du traitement des données à caractère personnel à l'ère des mégadonnées, T-PD(2017)01, Strasbourg, 23 janvier 2017.

Parmi les risques, on compte l'utilisation abusive des mégadonnées par les personnes ayant accès aux informations massives pour manipuler, discriminer ou opprimer des personnes ou des groupes spécifiques de la société[992]. Lorsque des masses de données à caractère personnel ou d'informations sur les comportements individuels sont collectées, traitées et analysées, leur exploitation peut conduire à des violations importantes des droits et libertés fondamentaux, qui dépassent le droit au respect de la vie privée. Il n'est pas possible de quantifier précisément la mesure dans laquelle la vie privée et les données à caractère personnel peuvent être affectées. Le Parlement européen a mis en évidence une lacune de méthodologie pour réaliser une évaluation basée sur des faits démontrés de l'incidence globale des mégadonnées, il est prouvé que l'analyse des mégadonnées peut avoir une incidence horizontale considérable dans le secteur privé comme dans le secteur public[993].

Le RGPD contient des dispositions sur le droit de ne pas faire l'objet d'une décision automatisée, y compris le profilage[994]. La question du respect de la vie privée se pose lorsque l'exercice du droit d'opposition nécessite une intervention humaine, permettant aux personnes concernées de faire valoir leur point de vue et de contester la décision[995]. Il peut être difficile d'assurer un niveau de protection adéquat des données à caractère personnel lorsque, par exemple, une intervention humaine n'est pas possible ou lorsque les algorithmes sont trop complexes et que la quantité de données concernées est trop importante pour fournir aux personnes visées une justification de certaines décisions et/ou des informations préalables pour obtenir leur consentement. Un exemple d'utilisation de l'intelligence artificielle et de décisions automatisées est l'évolution récente observée dans les demandes de crédit hypothécaire ou dans les procédures de recrutement. Des demandes sont refusées ou rejetées au motif que les demandeurs ne répondent pas à des paramètres ou à des facteurs prédéterminés.

992 Conférence internationale des commissaires à la protection des données et de la vie privée (2014), Résolution sur les mégadonnées.

993 Résolution du Parlement européen du 14 mars 2017 sur les incidences des mégadonnées pour les droits fondamentaux: respect de la vie privée, protection des données, non-discrimination, sécurité et application de la loi (2016/2225(INI)).

994 RGPD, art. 22.

995 *Ibid.*, art. 22, para. 3.

10.1.3. Problèmes liés à la protection des données

En ce qui concerne la protection des données, les principaux problèmes concernent, d'une part, le volume et la variété des données à caractère personnel traitées et, d'autre part, le traitement et ses résultats. L'introduction d'algorithmes et de logiciels complexes pour transformer des données massives en une ressource à des fins décisionnelles a une incidence pour des individus et des groupes particuliers, notamment en cas de profilage ou d'étiquetage, et soulève, en définitive, de nombreux problèmes en termes de protection des données[996].

L'identification des responsables du traitement et des sous-traitants et leur responsabilité

Les mégadonnées et l'intelligence artificielle soulèvent diverses questions quant à l'identification des responsables du traitement et des sous-traitants et à leur responsabilité : lorsque de telles quantités de données sont collectées et traitées, qui est le propriétaire des données ? Lorsque des données sont traitées par des machines et des logiciels intelligents, qui est le responsable du traitement ? Quelles sont les responsabilités exactes de chaque acteur du traitement ? Et pour quelles finalités les mégadonnées peuvent-elles être utilisées ?

La question de la responsabilité dans le contexte de l'intelligence artificielle va se poser de manière plus aiguë lorsqu'une intelligence artificielle prendra une décision fondée sur un traitement de données qu'elle aura conçu elle-même. Le RGPD établit un cadre légal pour la responsabilité du responsable du traitement et du sous-traitant. Le traitement illicite de données à caractère personnel entraîne la responsabilité du responsable du traitement et du sous-traitant[997]. L'intelligence artificielle et la prise de décisions automatisée soulèvent la question de savoir qui est responsable en cas de violations de la vie privée des personnes concernées lorsque la complexité et la quantité de données traitées ne peuvent être déterminées avec certitude. Considérer l'intelligence artificielle et les algorithmes comme des produits soulève la question de la responsabilité personnelle, qui est régie par le RGPD, et celle de la responsabilité du produit, qui ne l'est pas[998]. Il faudrait donc des règles sur la responsabilité afin de combler le vide entre la responsabilité personnelle et la

996 CdE, Comité consultatif de la Convention 108, Lignes directrices sur la protection des personnes à l'égard du traitement des données à caractère personnel à l'ère des mégadonnées, 23 janvier 2017, p. 2.

997 RGPD, art. 77 à 79 et art. 82.

998 Parlement européen, Direction générale des politiques internes, Règles européennes de droit civil en robotique, octobre 2016, p. 14.

responsabilité du produit pour la robotique et l'intelligence artificielle, notamment les décisions automatisées[999].

Incidence sur les principes de la protection des données

La nature, l'analyse et l'utilisation des mégadonnées décrites plus haut vont à l'encontre de l'application de certains des principes fondamentaux et traditionnels du droit européen en matière de protection des données[1000]. Ces défis ont trait essentiellement aux principes de la licéité du traitement, de la minimisation des données, de la limitation de la finalité et de la transparence.

Le principe de la minimisation des données impose que les données à caractère personnel soient adéquates, pertinentes et limitées à ce qui est nécessaire pour les finalités pour lesquelles elles sont traitées. Cependant, le modèle économique des mégadonnées peut être l'antithèse de la minimisation des données, dans la mesure où il réclame de plus en plus de données, souvent pour des finalités non spécifiées.

Il en va de même du principe de la limitation de la finalité, qui impose que les données soient traitées à des fins spécifiques et ne puissent pas être utilisées pour des finalités qui sont incompatibles avec la finalité initiale de la collecte, à moins que ce traitement ne repose sur un fondement juridique, tel que, mais sans s'y limiter, le consentement de la personne concernée (voir section 4.1.1).

Enfin, les mégadonnées s'opposent également au principe de l'exactitude des données, étant donné que les applications de mégadonnées ont tendance à collecter des données auprès de diverses sources sans disposer de la possibilité de vérifier et/ou de préserver l'exactitude des données collectées[1001].

Règles et droits spécifiques

La règle générale reste que les données à caractère personnel traitées par le biais d'une analyse de mégadonnées relèvent du champ d'application de la législation sur

999 Discours de Roberto Viola au séminaire Média sur le droit européen en matière de robotique au Parlement européen, (Discours 16/02/2017) ; Parlement européen, communiqué de presse concernant la demande faite à la Commission de présenter une proposition sur des règles de responsabilité civile en matière de robotique et d'intelligence artificielle.

1000 CdE, *Lignes directrices sur la protection des personnes à l'égard du traitement des données à caractère personnel à l'ère des mégadonnées*, T-PD(2017)01, Strasbourg, 23 janvier 2017.

1001 CEPD (2016), *Avis sur une application cohérente des droits fondamentaux à l'ère des données massives (Big Data)*, avis 8/2016, 23 septembre 2016, p. 8.

la protection des données. Des règles spécifiques ou des dérogations ont toutefois été introduites dans le droit de l'UE et du CdE pour des cas particuliers liés au traitement de données algorithmiques complexes.

Dans le droit du CdE, la Convention 108 modernisée accorde de nouveaux droits aux personnes concernées, pour leur permettre de contrôler plus efficacement leurs données à caractère personnel à l'ère des mégadonnées. Cela est le cas par exemple de l'article 9, paragraphe 1, points a), c) et d) de la Convention modernisée sur le droit de toute personne de ne pas être soumise à une décision l'affectant de manière significative, qui serait prise uniquement sur le fondement d'un traitement automatisé de données, sans que son point de vue soit pris en compte ; le droit d'obtenir, à sa demande, connaissance du raisonnement qui sous-tend le traitement de données, lorsque les résultats de ce traitement lui sont appliqués ; le droit de s'opposer à tout moment à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement. Les autres dispositions de la Convention 108 modernisée, relatives à la transparence et aux obligations additionnelles notamment, sont des éléments complémentaires du mécanisme de protection établi à travers la Convention 108 modernisée pour répondre aux défis numériques.

Dans le droit de l'UE, en dehors des cas énumérés à l'article 23 du RGPD, la **transparence** doit être assurée pour tout traitement de données à caractère personnel. Elle revêt une importance particulière pour les services internet et d'autres traitements de données automatisés et complexes, comme l'utilisation d'algorithmes pour la prise de décisions. Dans ce cas, les caractéristiques des systèmes de traitement de données doivent permettre aux personnes concernées de comprendre réellement ce qu'il va advenir de leurs données. Pour garantir un traitement équitable et transparent, le RGPD impose au responsable du traitement de fournir à la personne concernée des informations significatives concernant la logique sous-jacente de la prise de décisions automatisée, y compris le profilage[1002]. Dans sa Recommandation sur la protection et la promotion du droit à la liberté d'expression et du droit à la vie privée eu égard à la neutralité du réseau, le Comité des Ministres du Conseil de l'Europe a recommandé que les fournisseurs d'accès à internet fournissent « aux usagers des informations claires, complètes et publiques sur toute pratique de gestion du trafic qui pourrait avoir une incidence sur l'accès des usagers aux contenus, applications ou services et sur leur diffusion »[1003]. Les rapports relatifs aux pratiques

1002 RGPD, art. 13, para. 2, point f).

1003 CdE, Comité des Ministres (2016), Recommandation CM/Rec(2016)1 du Comité des Ministres aux États membres sur la protection et la promotion du droit à la liberté d'expression et du droit à la vie privée en lien avec la neutralité du réseau, 13 janvier 2016, para. 5.1.

de gestion du trafic internet, rédigés par les autorités compétentes de chaque État membre, devraient être élaborés de façon ouverte et transparente et mis gratuitement à la disposition du public[1004].

Les responsables du traitement doivent **fournir** aux personnes concernées, que les données aient ou non été collectées auprès d'elles, non seulement **des informations** spécifiques sur les données collectées et le traitement envisagé (voir section 6.1.1), mais aussi, le cas échéant, sur l'existence de processus de prise de décisions automatisée, en leur fournissant des « informations significatives sur la logique sous-jacente »[1005], les objectifs et les conséquences potentielles de ces processus. Le Règlement général sur la protection des données précise également (uniquement lorsque les données à caractère personnel n'ont pas été obtenues auprès de la personne concernée) que le responsable du traitement n'est pas tenu de fournir ces informations à la personne concernée lorsque « la fourniture de telles informations se révèle impossible ou exigerait des efforts disproportionnés »[1006]. Toutefois, ainsi que l'a souligné le Groupe de travail « Article 29 » dans ses *Lignes directrices sur le profilage et la prise de décision individuelle automatisée aux fins du règlement 2016/679*, la complexité du traitement ne devrait pas, en soi, empêcher le responsable du traitement de fournir à la personne concernée des explications claires sur les objectifs et la méthode d'analyse utilisée pour le traitement des données[1007].

Les droits d'**accès**, de **rectification** et d'**effacement** des données à caractère personnel des personnes concernées ainsi que leur droit à la **limitation** du traitement n'incluent pas une telle dérogation. Cependant, l'obligation faite au responsable du traitement de notifier à la personne concernée toute rectification ou tout effacement de données à caractère personnel (voir section 6.1.4) peut également être levée lorsque cette notification « se révèle impossible ou exige des efforts disproportionnés »[1008].

Les personnes concernées ont également le droit de **s'opposer**, à tout traitement de données à caractère personnel les concernant, en vertu de l'article 21 du RGPD (voir section 6.1.6), y compris en cas d'analyse des mégadonnées. Alors que les responsables du traitement peuvent être exemptés de cette obligation s'ils sont en mesure

1004 *Ibid.* para. 5.2.

1005 RGPD, art. 13, para. 2, point f), et art. 14, para. 2, point g).

1006 *Ibid.*, art. 14, para. 5, point b).

1007 Groupe de travail « Article 29 », *Guidelines on Automated Individual Decision-Making and profiling for the purposes of Regulation 2016/679*, WP 251, 3 octobre 2017, p. 14.

1008 RGPD, art. 19.

de démontrer l'existence d'intérêts légitimes impérieux, ils ne peuvent pas bénéficier de cette dérogation pour les traitements à des fins de prospection.

Des dérogations spécifiques à ces droits peuvent également être invoquées par les responsables du traitement lorsqu'ils traitent des données à caractère personnel à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques[1009].

S'agissant du **profilage et de la prise de décisions automatisée**, le RGPD a introduit des règles spécifiques : l'article 22, paragraphe 1, prévoit que la personne concernée « a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé produisant des effets juridiques la concernant ». Comme l'a souligné le Groupe de travail « Article 29 » dans ses lignes directrices, cet article énonce une interdiction générale de la prise de décisions entièrement automatisées[1010]. Les responsables du traitement peuvent être libérés de cette obligation dans trois cas seulement, à savoir lorsque la décision : 1) est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ; 2) est autorisée par le droit de l'UE ou le droit national ou 3) est fondée sur le consentement explicite de la personne concernée[1011].

Contrôle individuel

La complexité et l'opacité de l'analyse des mégadonnées peuvent inciter à reconsidérer les règles du contrôle individuel des données à caractère personnel. Ces règles devraient être adaptées au contexte social et technologique en tenant compte du manque de connaissance des personnes. En ce qui concerne les mégadonnées, la protection des données devrait adopter une conception plus large du contrôle de l'utilisation des données, en vertu de laquelle le contrôle individuel évolue vers un processus plus complexe d'évaluation – sous plusieurs aspects – des risques liés à l'utilisation des données[1012].

1009 *Ibid*., art. 89, paras. 2 et 3.

1010 Groupe de travail « Article 29 », *Guidelines on Automated Individual Decision-Making and profiling for the purposes of Regulation 2016/679*, WP 251, 3 octobre 2017, p. 9.

1011 RGPD, art. 22, para. 2.

1012 CdE, Comité consultatif de la Convention 108, *Lignes directrices sur la protection des personnes à l'égard du traitement des données à caractère personnel à l'ère des mégadonnées*, T-PD(2017)01, Strasbourg, 23 janvier 2017.

La qualité d'une application utilisant des mégadonnées dépend de la mesure dans laquelle elle peut prédire les souhaits ou le comportement de personnes types (ou consommateurs). Les modèles prévisionnels actuels qui reposent sur l'analyse de mégadonnées sont affinés en permanence. Les développements récents permettent non seulement d'utiliser des données pour classer des personnalités (comportement et attitudes), mais aussi d'analyser le comportement en étudiant des schémas vocaux et l'intensité avec laquelle des messages sont rédigés ou en mesurant la température corporelle. Toutes ces informations peuvent être comparées en temps réel avec les connaissances tirées des analyses de mégadonnées pour évaluer la solvabilité pendant une réunion avec un banquier, par exemple. L'analyse ne repose pas sur les qualités de la personne qui demande le crédit, mais sur les caractéristiques de comportement extraites d'une analyse et d'une évaluation d'informations tirées de mégadonnées, c'est-à-dire le fait que le demandeur parle d'une voix forte ou séductrice, son langage corporel ou sa température corporelle.

Le profilage et la publicité ciblée ne posent pas nécessairement de problèmes si les personnes sont **conscientes** qu'elles font l'objet de publicités personnalisées. Le profilage devient problématique lorsqu'il est utilisé pour manipuler des personnes, c'est-à-dire pour rechercher certaines personnalités ou groupes de personnes pour des campagnes politiques. Ainsi, des groupes d'électeurs indécis peuvent être visés par des messages politiques adaptés à leur « personnalité » et à leurs attitudes. Un autre problème pourrait être l'utilisation de ce profilage pour refuser l'accès à des biens et services à certaines personnes. Une mesure de sauvegarde susceptible de protéger contre l'utilisation abusive de mégadonnées et d'informations personnelles est la pseudonymisation (voir section 2.1.1)[1013]. Lorsque les données à caractère personnel sont véritablement anonymisées, c'est-à-dire qu'aucune information ne permet de les relier à la personne concernée, elles ne relèvent plus du champ d'application du Règlement général sur la protection des données. Le consentement des personnes concernées et des personnes au traitement de mégadonnées constitue également un défi pour la législation relative à la protection des données. Il inclut le consentement à être visé par des publicités personnalisées et à faire l'objet d'un profilage, qui peuvent être justifiés par des motifs liés à « l'expérience des clients », et le consentement à l'utilisation de masses de données à caractère personnel afin d'affiner et de développer des outils analytiques basés sur l'information. La prise de conscience, ou l'absence de prise de conscience, du traitement des mégadonnées soulève plusieurs questions quant aux moyens que les personnes concernées peuvent utiliser pour exercer leurs droits, étant donné que le traitement de

1013 *Ibid.*, p. 2.

mégadonnées peut s'appuyer à la fois sur des informations pseudonymisées et sur des informations anonymisées traitées par des algorithmes. Alors que les données pseudonymisées relèvent du champ d'application du RGPD, ce dernier ne s'applique pas aux données anonymisées. Le contrôle individuel et la prise de conscience du traitement des données par les personnes concernées sont capitaux dans l'analyse des mégadonnées. En effet, sans cela, elles ne sauront pas précisément qui est le responsable du traitement ou le sous-traitant, ce qui les empêchera d'exercer effectivement leurs droits.

10.2. Les webs 2.0 et 3.0 : les réseaux sociaux et l'Internet des objets

Points clés

- Les services de réseaux sociaux (SRS) sont des plateformes de communication en ligne permettant à des personnes de rejoindre ou de créer des réseaux d'utilisateurs partageant des intérêts communs.
- L'Internet des objets est la connexion d'objets à internet et l'interconnexion d'objets entre eux.
- Le consentement de la personne concernée est le fondement juridique le plus courant d'un traitement licite de données par des responsables du traitement sur les réseaux sociaux.
- Les utilisateurs de réseaux sociaux sont généralement protégés par l'« exemption domestique » ; celle-ci peut toutefois être levée dans certaines situations.
- Les fournisseurs de services de réseaux sociaux ne sont pas protégés par l'« exemption domestique ».
- Le respect de la vie privée dès la conception et par défaut est donc crucial pour assurer la sécurité des données dans ce domaine.

10.2.1. Définir les Webs 2.0 et 3.0

Services de réseaux sociaux

À l'origine, internet était conçu comme un réseau visant à interconnecter des ordinateurs et à transmettre des messages avec des capacités limitées d'échange de

données, les sites web offrant simplement aux individus la possibilité de consulter passivement leur contenu[1014]. À l'ère du Web 2.0, internet s'est transformé en un forum sur lequel les internautes interagissent, collaborent et génèrent du contenu. L'époque actuelle se caractérise par le succès remarquable et l'utilisation étendue des réseaux sociaux, qui constituent désormais une partie essentielle de la vie quotidienne de millions de personnes.

Les services de réseaux sociaux (SRS) ou « réseaux sociaux » peuvent être globalement définis comme des « plateformes de communication en ligne permettant à des personnes de créer des réseaux d'utilisateurs partageant des intérêts communs »[1015]. Pour devenir membre d'un réseau ou en créer un, les personnes sont invitées à fournir des données à caractère personnel et à créer un profil. Les SRS permettent aux utilisateurs de générer du « contenu » numérique allant de photographies et de vidéogrammes à des liens vers des journaux et des publications personnelles pour donner leur point de vue. Par le biais de ces plateformes de communication en ligne, des utilisateurs peuvent interagir et communiquer avec plusieurs autres utilisateurs. Il est important de souligner que la plupart des SRS populaires ne requièrent pas de droits d'inscription. Plutôt que de demander aux utilisateurs de payer pour rejoindre le réseau, les SRS génèrent la majeure partie de leurs revenus grâce à la publicité ciblée. Les annonceurs peuvent tirer un grand profit des informations personnelles révélées quotidiennement sur ces sites. Le fait de disposer d'informations sur l'âge, le genre, la localisation et les centres d'intérêt des utilisateurs leur permet de cibler les « bonnes » personnes avec leurs publicités.

Le Conseil des Ministres du Conseil de l'Europe a adopté une Recommandation sur la protection des droits de l'homme dans le cadre des services de réseaux sociaux[1016] qui traite de la protection des données dans une section distincte. En 2018, la Recommandation sur les rôles et les responsabilités des intermédiaires d'internet est venue la compléter.[1017]

1014 Commission européenne (2016), *Advancing the Internet of Things in Europe*, SWD(2016) 110 final.

1015 Groupe de travail « Article 29 » (2009), *Avis 5/2009 sur les réseaux sociaux en ligne*, WP 163, 12 juin 2009, p. 4.

1016 CdE, Comité des Ministres, Recommandation CM/Rec(2012)4 du Comité des Ministres aux États membres sur la protection des droits de l'homme dans le cadre des services de réseaux sociaux, 4 avril 2012.

1017 CdE, Comité des Ministres, Recommandation CM/Rec(2018)2 du Comité des Ministres aux États membres sur les rôles et les responsabilités des intermédiaires d'internet, 7 mars 2018.

Exemple : Nora est très heureuse parce que son compagnon lui a demandé de l'épouser. Elle veut partager la bonne nouvelle avec sa famille et ses amis et décide de publier un message émouvant sur un réseau social pour exprimer sa joie et modifier son statut en indiquant qu'elle est « fiancée ». Les jours suivants, lorsqu'elle se connecte à son compte, Nora voit des annonces pour des robes de mariée et des magasins de fleurs. Pourquoi ?

En créant une publicité sur Facebook, les boutiques de robes de mariée et les magasins de fleurs ont sélectionné certains paramètres pour pouvoir cibler des personnes comme Nora. Lorsque le profil de Nora indique qu'elle est une femme, fiancée, vivant à Paris, près de l'endroit où se situent la boutique de robes de mariée et le magasin de fleurs qui ont placé des annonces, elle les voit immédiatement.

L'Internet des objets

L'Internet des objets constitue l'étape suivante dans l'évolution d'internet : l'ère du Web 3.0. Grâce à l'Internet des objets, des dispositifs peuvent être connectés et interagir avec d'autres dispositifs par le biais d'internet. Ceci permet d'interconnecter des objets et des personnes par l'intermédiaire de réseaux de communication, de signaler leur statut et/ou le statut de leur environnement[1018]. L'Internet des objets et les dispositifs connectés sont déjà une réalité et devraient se développer considérablement au cours des prochaines années avec la création et la poursuite du développement de dispositifs intelligents, qui aboutiront à la création de villes intelligentes, de maisons intelligentes et d'entreprises intelligentes.

Exemple : l'Internet des objets peut se révéler particulièrement utile dans le domaine des soins de santé. Des entreprises ont déjà créé des dispositifs, des capteurs et des applications qui permettent de surveiller la santé d'un patient. En utilisant un bouton d'alarme portable et d'autres capteurs sans fil installés dans la maison, il est possible de suivre la routine quotidienne de personnes âgées vivant seules et de générer des alertes si des perturbations graves sont détectées dans leur programme journalier. Des détecteurs de chute, par exemple, sont couramment utilisés par les personnes âgées. Ces capteurs peuvent détecter les chutes avec précision et en avertir le médecin et/ou la famille de la personne.

1018 Commission européenne (2016), Document de travail des services de la Commission, *Advancing the Internet of Things in Europe*, SWD(2016) 110, 19 avril 2016.

Exemple : Barcelone est l'un des exemples les plus connus de ville intelligente. Depuis 2012, la ville utilise des technologies innovantes afin de créer un système intelligent de transport public, de gestion des déchets, de parking et d'éclairage public. Pour améliorer la gestion des déchets, par exemple, la ville a installé des poubelles intelligentes. Elles permettent de surveiller le niveau des déchets en vue d'optimiser les itinéraires de ramassage. Lorsque les poubelles sont presque pleines, elles émettent des signaux via le réseau de communication mobile, qui sont envoyés à l'application utilisée par la société de gestion des déchets. Celle-ci peut ainsi planifier le meilleur itinéraire pour la collecte des déchets, en donnant la priorité et/ou en ne planifiant que le ramassage des poubelles qui doivent effectivement être vidées.

10.2.2. Mise en balance des avantages et des risques

Le large essor et le succès des SRS au cours de la dernière décennie donnent à penser qu'ils présentent des **avantages considérables**. Ainsi, la publicité ciblée (telle que décrite dans l'exemple encadré) est une façon particulièrement novatrice pour les entreprises d'atteindre leur public en leur offrant un marché plus spécifique. Il pourrait également être intéressant pour les consommateurs que les annonces qui leur sont présentées soient plus pertinentes et adaptées. Mais surtout, les SRS et les réseaux sociaux peuvent avoir un effet positif sur la société et sur la mise en œuvre du changement. Ils permettent aux utilisateurs de communiquer, d'interagir et d'organiser des groupes et des événements sur des sujets qui les touchent.

De même, l'Internet des objets devrait présenter des avantages significatifs pour l'économie et fait partie de la stratégie européenne destinée à réaliser un marché unique numérique. Au sein de l'UE, on estime qu'en 2020, le nombre de connexions à l'Internet des objets atteindra les six milliards. L'expansion de la connectivité devrait produire d'importants avantages économiques grâce au développement de services et d'applications innovantes, de meilleurs soins de santé, une meilleure compréhension des besoins des consommateurs et une efficacité accrue.

Dans le même temps, étant donné la quantité énorme d'informations personnelles générées par les utilisateurs des réseaux sociaux et traitées ultérieurement par les exploitants de ces services, l'expansion des réseaux sociaux s'accompagne d'une **préoccupation croissante** quant à la manière dont la vie privée et les données à caractère personnel peuvent être protégées. Les SRS peuvent menacer le

droit au respect de la vie privée et le droit à la liberté d'expression. Ces menaces peuvent notamment découler « de l'absence de garanties juridiques et procédurales, concernant des processus qui peuvent conduire à l'exclusion d'un utilisateur ; d'une protection inadaptée des enfants et des jeunes contre des contenus ou comportements susceptibles de leur être préjudiciables ; d'un manque de respect pour les droits d'autrui ; de l'absence d'une configuration par défaut qui respecte la vie privée ; d'un manque de transparence des finalités pour lesquelles les données à caractère personnel sont collectées et traitées »[1019]. La législation européenne relative à la protection des données a tenté de répondre aux défis que représentent les réseaux sociaux pour la vie privée et la protection des données. Des principes tels que le consentement, le respect de la vie privée et la protection des données dès la conception et par défaut et les droits des personnes sont particulièrement importants dans le contexte des réseaux sociaux et des services de réseautage.

Dans le cadre de l'Internet des objets, l'énorme volume de données à caractère personnel généré par les divers dispositifs interconnectés entraîne également des risques pour la vie privée et la protection des données. Bien que la transparence soit un principe important de la législation européenne en matière de protection des données, du fait de la multitude de dispositifs connectés, il n'est pas toujours évident de savoir qui peut collecter les données collectées par les dispositifs de l'Internet des objets, y accéder et les utiliser[1020]. Dans le droit de l'UE et du CdE, le principe de transparence impose toutefois aux responsables du traitement l'obligation d'informer les personnes concernées de la manière dont leurs données sont utilisées, dans un langage clair et simple. Les risques, les règles, les garanties et les droits relatifs au traitement des données à caractère personnel doivent être clairs pour les personnes concernées. Les dispositifs connectés IdO et les multiples traitements et données concernés pourraient également porter atteinte à l'obligation d'obtenir le consentement explicite et éclairé de la personne concernée au traitement de données, lorsque ledit traitement est fondé sur un consentement. Souvent, les personnes ne comprennent pas le fonctionnement technique de ce traitement ni dès lors les conséquences de leur consentement à celui-ci.

Une autre préoccupation majeure est la sécurité, étant donné que les dispositifs connectés sont particulièrement vulnérables aux atteintes à la sécurité. Ces dispositifs connectés présentent des niveaux de sécurité divers. Dans la mesure où ils

1019 CdE, Recommandation Rec(2012)4 aux États membres sur la protection des droits de l'homme dans le cadre des services de réseaux sociaux, 4 avril 2012.

1020 CEPD (2017), *Understanding the Internet of Things*.

fonctionnent en dehors de l'infrastructure TI standard, il est possible qu'ils ne disposent pas de la puissance de traitement et de la capacité de stockage nécessaires pour héberger un logiciel de sécurité ou recourir à des techniques comme le cryptage, la pseudonymisation ou l'anonymisation afin de protéger les informations personnelles des utilisateurs.

Exemple : en Allemagne, le régulateur a décidé d'interdire un jouet connecté à internet en raison de fortes craintes concernant l'incidence dudit jouet sur le respect de la vie privée des enfants. Le régulateur a jugé qu'une poupée connectée à internet baptisée Cayla constituait effectivement un dispositif espion caché. La poupée fonctionnait en envoyant les questions posées à voix haute par l'enfant jouant avec elle à une application sur un dispositif numérique, qui les traduisait en texte et recherchait la réponse sur internet. L'application envoyait ensuite une réponse à la poupée qui la disait à l'enfant. Les communications de l'enfant et celles des adultes se trouvant à proximité pouvaient être enregistrées et transmises à l'application par l'intermédiaire de cette poupée. Si les fabricants de la poupée n'avaient pas adopté de mesures de sécurité adéquates, la poupée aurait pu être utilisée par n'importe qui pour écouter les conversations.

10.2.3. Problèmes liés à la protection des données

Consentement

En Europe, le traitement de données à caractère personnel n'est licite que s'il est autorisé par la législation européenne relative à la protection des données. Pour les SRS, le consentement des personnes concernées offre généralement un fondement légal au traitement des données. Le consentement doit être donné librement et être spécifique, éclairé et univoque (voir section 4.1.1)[1021]. « Donné librement » signifie essentiellement que les personnes concernées doivent avoir la possibilité d'exercer un choix réel et authentique. Le consentement est « spécifique » et « éclairé » lorsqu'il est compréhensible et fait clairement et précisément référence à l'étendue, aux finalités et aux conséquences du traitement des données. Dans le cadre des réseaux sociaux, on peut douter que le consentement soit libre, spécifique et éclairé pour tous les types de traitement effectués par l'exploitant des SRS et les tiers.

1021 RGPD, art. 4 et 7 ; Convention 108 modernisée, art. 5.

Exemple : pour devenir membre et avoir accès à un réseau social, les personnes doivent fréquemment accepter différents types de traitements de leurs données à caractère personnel, souvent sans recevoir les précisions nécessaires ou d'autres options. Un exemple serait la nécessité d'accepter de recevoir de la publicité comportementale pour devenir membre d'un réseau social. Comme l'observe le Groupe de travail « Article 29 » dans son avis sur la définition du consentement, « compte tenu de l'importance qu'ont pris certains réseaux sociaux, certaines catégories d'utilisateurs (comme les adolescents) consentiront à recevoir de la publicité comportementale pour éviter le risque d'être exclus de certaines interactions sociales. Or l'utilisateur devrait être en mesure de donner un consentement libre et spécifique à la réception de publicités comportementales, indépendamment de son accès au réseau social »[1022].

En vertu du Règlement général sur la protection des données, les données à caractère personnel des enfants de moins de 16 ans ne peuvent, en principe, pas faire l'objet d'un traitement fondé sur leur consentement[1023]. Si un consentement au traitement est nécessaire, il doit être donné par un parent ou un tuteur de l'enfant. Les enfants ont besoin d'une protection spécifique parce qu'ils peuvent être moins conscients des risques et des conséquences qu'implique le traitement des données. Cet élément revêt une grande importance dans le contexte des réseaux sociaux, étant donné que les enfants sont de plus en plus exposés à certains des effets négatifs de l'utilisation de ces réseaux, comme la cyberintimidation, le harcèlement en ligne ou l'usurpation d'identité.

Sécurité et vie privée/protection des données dès la conception et par défaut

Le traitement de données à caractère personnel entraîne, en soi, des risques pour la sécurité en raison de la possibilité permanente d'une violation de la sécurité conduisant à la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel ou l'accès non autorisé à de telles données, de manière accidentelle ou illicite. Conformément à la législation européenne relative à la protection des données, le responsable du traitement et le sous-traitant doivent prendre des

1022 Groupe de travail « Article 29 » (2011), *Avis 15/2011 sur la définition du consentement*, WP 187, 13 juillet 2011, p. 18.

1023 Voir RGPD, art. 8. Les États membres de l'UE peuvent prévoir par la loi un âge inférieur, pour autant que celui-ci ne soit pas en dessous de 13 ans.

mesures techniques et organisationnelles appropriées pour empêcher toute ingérence non autorisée dans des traitements de données. Les fournisseurs de services de réseaux sociaux relevant du champ d'application des règles européennes en matière de protection des données doivent également se soumettre à cette obligation.

Les principes de respect de la vie privée et de protection des données dès la conception et par défaut imposent aux responsables du traitement d'assurer la sécurité lors de la conception de leurs produits et d'appliquer automatiquement des paramètres adéquats de confidentialité et de protection des données. Cela implique que lorsqu'une personne décide de devenir membre d'un réseau social, le fournisseur de services ne peut pas mettre automatiquement toutes les informations sur le nouvel utilisateur du service à la disposition de tous ses utilisateurs. Lors de l'inscription, les paramètres de confidentialité et de protection des données devraient, par défaut, être tels que les informations soient uniquement disponibles pour les contacts choisis de la personne concernée. L'extension de l'accès à des personnes ne figurant pas dans cette liste ne devrait être possible qu'après que l'utilisateur a modifié manuellement les paramètres de confidentialité et de protection des données par défaut. Cela peut aussi avoir des conséquences lorsqu'une violation des données se produit en dépit des mesures de sécurité mises en place. Dans de tels cas, les fournisseurs de services doivent communiquer à la personne concernée toute violation susceptible d'engendrer un risque élevé pour les droits et libertés de celle-ci[1024].

Le respect de la vie privée et la protection des données dès la conception et par défaut sont particulièrement importants dans le cadre des SRS, étant donné qu'outre les risques d'accès non autorisé que soulèvent la plupart des types de traitement, le partage d'informations personnelles sur les réseaux sociaux entraîne des risques supplémentaires en termes de sécurité. Ceux-ci sont souvent dus au fait que les utilisateurs ne savent pas *qui* peut avoir accès à leurs informations et comment ces personnes peuvent les utiliser. Avec l'utilisation généralisée des médias sociaux, le nombre de cas d'usurpation d'identité et de victimes est en augmentation.

Exemple : l'usurpation d'identité est un phénomène par lequel une personne obtient des informations, des données ou des documents appartenant à une autre (la victime) et utilise ces informations pour se faire passer pour la victime afin d'obtenir des produits et des services au nom de la victime. Prenez l'exemple de Paul qui a un compte sur un réseau social. Paul est

1024 *Ibid.*, art. 34.

enseignant et il est un membre actif de sa communauté, très extraverti et pas particulièrement préoccupé par les paramètres de confidentialité et de protection des données de son compte sur ce réseau social. Il a une longue liste de contacts, qui contient même des personnes qu'il ne connaît pas nécessairement personnellement. Étant donné qu'il travaille dans une grande école et qu'il a été très populaire comme entraîneur de l'équipe de football de l'établissement, il pense que ces contacts sont très probablement des parents ou des amis de l'école. L'adresse de courrier électronique et la date d'anniversaire de Paul apparaissent sur son compte. De plus, Paul publie régulièrement des photos de son chien Toby, accompagnées de commentaires du style « Toby et moi lors de notre jogging matinal ». Paul n'a pas compris que l'une des questions de sécurité les plus courantes pour protéger son compte de courrier électronique ou de téléphonie mobile est « quel est le nom de votre animal domestique ». En utilisant les informations publiées sur le profil de Paul sur le réseau social, Nick parvient aisément à pirater les comptes de Paul.

Droits des personnes

Les SRS doivent respecter les droits des individus (voir section 6.1), y compris celui d'être informé de la finalité du traitement et de la façon dont les données à caractère personnel peuvent être utilisées à des fins de prospection. Les personnes doivent également avoir le droit d'accéder aux données à caractère personnel les concernant qu'elles ont générées sur la plateforme de réseautage social et demander leur suppression. Même lorsque des personnes ont consenti au traitement de données à caractère personnel et téléchargé des informations en ligne, elles devraient être en mesure de demander à « être oubliées » si elles ne souhaitent plus bénéficier des services du réseau social. Le droit à la portabilité des données permet également aux utilisateurs d'obtenir une copie des données à caractère personnel qu'ils ont fournies au fournisseur de services de réseaux sociaux dans un format structuré, couramment utilisé et lisible par une machine et de transférer leurs données d'un fournisseur de SRS à un autre[1025].

Responsables du traitement

Une question épineuse qui se pose souvent dans le contexte des médias sociaux est celle de savoir qui est le responsable du traitement, c'est-à-dire qui est la personne

1025 RGPD, art. 21.

qui a l'obligation et la responsabilité de se conformer aux règles relatives à la protection des données. Les fournisseurs de services de réseaux sociaux sont considérés comme les responsables du traitement par la législation européenne relative à la protection des données. Cela ressort clairement de la large définition du « responsable du traitement » et du fait que ces fournisseurs de services déterminent la finalité et les moyens du traitement des données à caractère personnel partagées par les individus. Dans le droit de l'UE, s'ils offrent des services à des personnes concernées établies dans l'Union, les responsables du traitement sont tenus de se conformer aux dispositions du RGPD, même s'ils ne sont pas eux-mêmes établis dans l'UE.

Des utilisateurs de SRS peuvent-ils eux aussi être considérés comme des responsables du traitement ? Lorsque des personnes traitent des données à caractère personnel « au cours d'activités strictement personnelles ou domestiques », les règles de la protection des données ne s'appliquent pas. C'est ce que l'on appelle en droit européen de la protection des données l'« exemption domestique ». Cependant, dans certains cas, l'utilisation du SRS peut ne pas être couverte par cette exemption.

Les utilisateurs partagent volontairement leurs informations personnelles en ligne. Celles-ci contiennent toutefois souvent des informations personnelles d'autres personnes.

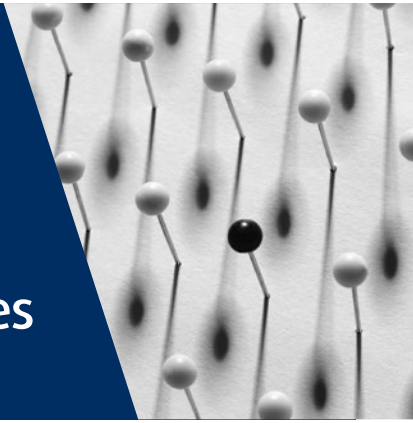
Exemple : Paul a un compte sur une plateforme de réseau social très populaire. Paul veut devenir acteur et utilise son compte pour publier des photos, des vidéogrammes et des textes expliquant sa passion pour l'art. La popularité est importante pour son avenir et il a donc décidé que son profil ne devait pas uniquement être accessible à sa liste de contacts proches, mais à tous les internautes, qu'ils soient ou non membres du réseau. Paul peut-il publier des photos et des vidéos de lui avec son amie Sarah sans son consentement ? Institutrice dans l'enseignement primaire, Sarah s'efforce de tenir sa vie privée à l'abri de son employeur, de ses élèves et de leurs parents. Imaginez que Sarah, qui n'utilise pas les réseaux sociaux, apprenne par leur ami commun Nick qu'une photo d'elle à une fête avec Paul a été mise en ligne. En pareil cas, le traitement de données effectué par Paul ne relèvera pas du droit de l'UE, étant donné qu'il est couvert par l'« exemption domestique ».

Cependant, il est essentiel que les utilisateurs soient conscients et attentifs au fait que le téléchargement d'informations sur d'autres personnes sans leur consentement peut porter atteinte aux droits de ces dernières au respect de la vie privée et à la protection des données. Même lorsque l'exemption domestique s'applique – par exemple, si un utilisateur a un profil qui ne peut être vu que par une liste de contacts qu'il choisit –, la publication d'informations personnelles sur d'autres personnes pourrait néanmoins engager la responsabilité de cet utilisateur. Bien que les règles relatives à la protection des données ne s'appliquent pas lorsque l'exemption domestique s'applique, la responsabilité pourrait résulter de l'application d'autres règles nationales, comme la diffamation ou une violation des droits de la personnalité. Enfin, seuls les utilisateurs de réseaux sociaux sont protégés par l'exemption domestique ; les responsables du traitement et les sous-traitants qui fournissent les moyens de ce traitement privé relèvent, quant à eux, de la législation de l'UE en matière de protection des données[1026].

Si la réforme de la Directive « vie privée et communications électroniques » est adoptée, les règles relatives à la protection des données, à la confidentialité et à la sécurité applicables aux fournisseurs de services de télécommunication au titre du cadre juridique actuel s'appliqueront également aux services de communications de machine à machine et de communications électroniques, y compris, par exemple, aux services « over-the-top ».

1026 *Ibid.*, considérant 18.

Lectures complémentaires



Chapitre 1

Araceli Mangas, M. (éd.) (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.

Docksey, C., « Four fundamental rights: finding the balance », *International Data Privacy Law*, Vol. 6, nº 3, p. 195–209.

González Fuster, G. et Gellert, G. (2012), « The fundamental right of data protection in the European Union: in search of an uncharted right », *International Review of Law, Computers and Technology*, Vol. 26 (1), p. 73–82.

Gutwirth, S., Poullet, Y., de Hert, P., de Terwange, C. et Nouwt, S. (Éd.) (2009), *Reinventing Data Protection*, Springer.

Hijmans, H. (2016), *The European Union as Guardian of Internet Privacy – the Story of Art 16 TFEU*, Springer.

Hustinx, P. (2016), « Le droit de l'Union européenne sur la protection des données : la révision de la directive 95/46/CE et la proposition de règlement général sur la protection des données ».

Kranenborg, H. (2015), « Google and the Right to be Forgotten », *European Data Protection Law Review*, Vol. 1, nº 1, p. 70–79.

Lynskey, O. (2014), « Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order », *International and Comparative Law Quarterly*, Vol. 63, nº 3, p. 569–597.

Lynskey, O. (2015), *The Foundations of EU Data Protection Law*, Oxford, Oxford University Press.

Kokott, J. et Sobotta, C. (2013), « The distinction between privacy and data protection in the case law of the CJEU and the ECtHR », *International Data Privacy Law*, Vol. 3, nº 4, p. 222–228.

EDRi, *An introduction to data protection*, Bruxelles.

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*, Anvers, 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*, Bruxelles, Émile Bruylant.

Simitis, S. (1997), « Die EU-Datenschutz-Richtlinie – Stillstand oder Anreiz? », *Neue Juristische Wochenschrift*, nº 5, p. 281–288.

Warren, S. et Brandeis, L. (1890), « The right to privacy », *Harvard Law Review,* Vol. 4, nº 5, p. 193–220.

White, R. et Ovey, C. (2010), *The European Convention on Human Rights*, Oxford, Oxford University Press.

Chapitre 2

Acquisty, A., et Gross R. (2009), « Predicting Social Security numbers from public data », *Proceedings of the National Academy of Science*, 7 juillet 2009.

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.

de Montjoye, Y.-A., Hidalgo, C. A., Verleysen, M., et Blondel V. D. (2013), « Unique in the Crowd: the Privacy Bounds of Human Mobility », *Nature Scientific Reports*, Vol. 3, 2013.

Desgens-Pasanau, G. (2012), *La protection des données à caractère personnel*, Paris, LexisNexis.

Di Martino, A. (2005), *Datenschutz im europäischen Recht*, Baden-Baden, Nomos.

González Fuster, G. (2014), *The Emergence of Personal Data Protection as a Fundamental Right in the EU*, Springer.

Morgan, R. et Boardman, R. (2012), *Data protection strategy: Implementing data protection compliance*, Londres, Sweet & Maxwell.

Ohm, P. (2010), « Broken promises of privacy: Responding to the surprising failure of anonymization », *UCLA Law Review*, Vol. 57, nº 6, p. 1701–1777.

Samarati, P. et Sweeney, L. (1998), « Protecting Privacy when Disclosing Information: k-Anonymity and Its Enforcement through Generalization and Suppression », rapport technique SRI-CSL-98-04.

Sweeney, L. (2002), « K-Anonymity: A Model for Protecting Privacy », *International Journal of Uncertainty, Fuzziness and Knowledge-based Systems*, Vol. 10, nº 5, p. 557–570.

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*.

Chapitres 3 à 6

Brühann, U. (2012), « Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr » in : Grabitz, E., Hilf, M. et Nettesheim, M. (éds.), *Das Recht der Europäischen Union*, Band IV, A. 30, Munich, C. H. Beck.

Conde Ortiz, C. (2008), *La protección de datos personales*, Cadix, Dykinson.

Coudray, L. (2010), *La protection des données personnelles dans l'Union européenne*, Saarbrucken, Éditions universitaires européennes.

Curren, L. et Kaye, J. (2010), « Revoking consent: a 'blind spot' in data protection law? », *Computer Law & Security Review*, Vol. 26, nº 3, p. 273–283.

Dammann, U. et Simitis, S. (1997), *EG-Datenschutzrichtlinie*, Baden-Baden, Nomos.

De Hert, P. et Papakonstantinou, V. (2012), « The Police and Criminal Justice Data Protection Directive: Comment and Analysis », *Computers & Law Magazine of SCL*, Vol. 22, nº 6, p. 1–5.

De Hert, P. et Papakonstantinou, V. (2012), « The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals », *Computer Law & Security Review*, Vol. 28, nº 2, p. 130–142.

Feretti, Federico (2012), « A European perspective on data processing consent through the re-conceptualization of European data protection's looking glass after the Lisbon treaty: Taking rights seriously », *European Review of Private Law*, Vol. 20, nº 2, p. 473–506.

FRA (Agence des droits fondamentaux de l'Union européenne) (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 (2010), *Developing indicators for the protection, respect and promotion of the rights of the child in the European Union* (édition de la conférence), Vienne, FRA.

FRA (2011), *L'accès à la justice en Europe : présentation des défis à relever et des opportunités à saisir*, Luxembourg, Office des publications.

Irish Health Information and Quality Authority (2010), Guidance on Privacy Impact Assessment in Health and Social Care.

Kierkegaard, S., Waters, N., Greenleaf, G., Bygrave, L. A., Lloyd, I. et Saxby, S. (2011), « 30 years on – The review of the Council of Europe Data Protection Convention 108 », *Computer Law & Security Review*, Vol. 27, nº 3, p. 223–231.

Simitis, S. (2011), *Bundesdatenschutzgesetz*, Baden-Baden, Nomos.

United Kingdom Information Commissioner's Office, *Privacy Impact Assessment*.

Chapitre 7

Contrôleur européen de la protection des données (2014), Document d'orientation – Le transfert de données à caractère personnel à des pays tiers et à des organisations internationales par les institutions et organes de l'Union européenne.

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.

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*.

Chapitre 8

Blasi Casagran, C. (2016) *Global Data Protection in the Field of Law Enforcement, an EU Perspective*, Londres, Routledge.

Boehm, F. (2012), *Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Towards Harmonised Data Protection Principles for Information Exchange at EU-level,* Berlin, Springer.

Europol (2012), *Data Protection at Europol*, Luxembourg, Office des publications.

Eurojust, *Data protection at Eurojust: A robust, effective and tailor-made regime*, La Haye, Eurojust.

De Hert, P. et Papakonstantinou, V. (2012), 'The Police and Criminal Justice Data Protection Directive: Comment and Analysis', *Computers & Law Magazine of SCL*, Vol. 22, nº 6, p. 1–5.

Drewer, D. et Ellermann, J. (2012), « Europol's data protection framework as an asset in the fight against cybercrime », *ERA Forum*, Vol. 13, nº 3, p. 381–395.

Gutiérrez Zarza, A. (2015), *Exchange of Information and Data Protection in Cross-border Criminal Proceedings in Europe*, Berlin, 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, nº 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.

Chapitre 9

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, nº 5, p. 722–776.

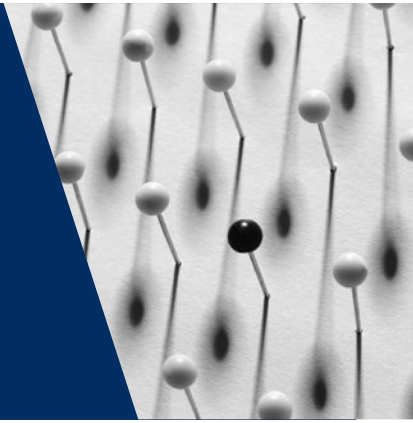
Rosemary, J. et Hamilton, A. (2012), *Data protection law and practice*, Londres, Sweet & Maxwell.

Chapitre 10

El Emam, K. et Álvarez, C. (2015), « A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques », *International Data Privacy Law*, Vol. 5, nº 1, p. 73–87.

Mayer-Schönberger, V. et Cate, F. (2013), « Notice and consent in a world of Big Data », *International Data Privacy Law*, Vol. 3, nº 2, p. 67–73.

Rubistein, I. (2013), « Big Data: The End of Privacy or a New Beginning? », *International Data Privacy Law*, Vol. 3, nº 2, p. 74–87.



Jurisprudence

Jurisprudence choisie 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
M.K. c. France, n° 19522/09, 18 avril 2013
Odièvre c. France [GC], n° 42326/98, 13 février 2003

Mise en balance de la protection des données avec la liberté d'expression et le droit à l'information

Axel Springer AG c. Allemagne [GC], n° 39954/08, 7 février 2012
Bohlen c. Allemagne, n° 53495/09, 19 février 2015
Coudec et Hachette Filipacchi Associés c. France [GC], n° 40454/07, 10 novembre 2015
Magyar Helsinki Bizottság c. Hongrie [GC], n° 18030/11, 8 novembre 2016
Müller et autres c. Suisse, n° 10737/84, 24 mai 1988
Satakunnan Markkinapörssi Oy et Satamedia Oy c. Finlande [GC], n° 931/13, 27 juin 2017
Vereinigung bildender Künstler c. Autriche, n° 68345/01, 25 janvier 2007
Von Hannover c. Allemagne (n° 2), n° 40660/08 et n° 60641/08, 7 février 2012

Mise en balance de la protection des données avec la liberté de religion

Sinan Işık c. Turquie, nº 21924/05, 2 février 2010

Défis de la protection des données en ligne

K.U. c. Finlande, nº 2872/02, 2 décembre 2008

Consentement de la personne concernée

Elberte c. Lettonie, nº 61243/08, 13 janvier 2015
Sinan Işık c. Turquie, nº 21924/05, 2 février 2010
Y c. Turquie, nº 648/10, 17 février 2015

Correspondance

Amann c. Suisse [GC], nº 27798/95, 16 février 2000
Association for European Integration and Human Rights et Ekimdzhiev c. Bulgarie, nº 62540/00, 28 juin 2007
Bernh Larsen Holding AS et autres c. Norvège, nº 24117/08, 14 mars 2013
Cemalettin Canlı c. Turquie, nº 22427/04, 18 novembre 2008
D.L. c. Bulgarie, nº 7472/14, 19 mai 2016
Dalea c. France, nº 964/07, 2 février 2010
Gaskin c. Royaume-Uni, nº 10454/83, 7 juillet 1989
Haralambie c. Roumanie, nº 21737/03, 27 octobre 2009
Khelili c. Suisse, nº 16188/07, 18 octobre 2011
Leander c. Suède, nº 9248/81, 26 mars 1987
Malone c. Royaume-Uni, nº 8691/79, 2 août 1984
Rotaru c. Roumanie [GC], nº 28341/95, 4 mai 2000
S. et Marper c. Royaume-Uni [GC], nº 30562/04 et 30566/04, 4 décembre 2008
Shimovolos c. Russie, nº 30194/09, 21 juin 2011
Silver et autres c. Royaume-Uni, nº 5947/72, 6205/73, 7052/75, 7061/75, 7107/75 et 7113/75, 25 mars 1983
The Sunday Times c. Royaume-Uni, nº 6538/74, 26 avril 1979

Bases de données des casiers judiciaires

Aycaguer c. France, nº 8806/12, 22 juin 2017
B.B. c. France, nº 5335/06, 17 décembre 2009
Brunet c. France, nº 21010/10, 18 septembre 2014
M.K. c. France, nº 19522/09, 18 avril 2013
M.M. c. Royaume-Uni, nº 24029/07, 13 novembre 2012

Sécurité des données

Haralambie c. Roumanie, n° 21737/03, 27 octobre 2009
K.H. et autres c. Slovaquie, n° 32881/04, 28 avril 2009

Bases de données d'ADN

S. et Marper c. Royaume-Uni [GC], n° 30562/04 et n° 30566/04, 4 décembre 2008

Données GPS

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

Données relatives à la santé

Avilkina et autres c. Russie, n° 1585/09, 6 juin 2013
Biriuk c. Lituanie, n° 23373/03, 25 novembre 2008
I c. Finlande, n° 20511/03, 17 juillet 2008
L.H. c. Lettonie, n° 52019/07, 29 avril 2014
L.L. c. France, n° 7508/02, 10 octobre 2006
M.S. c. Suède, n° 20837/92, 27 août 1997
Szuluk c. Royaume-Uni, n° 36936/05, 2 juin 2009
Y c. Turquie, n° 648/10, 17 février 2015
Z c. Finlande, n° 22009/93, 25 février 1997

Identité

Ciubotaru c. Moldova, 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 relatives aux activités professionnelles

G.S.B. c. Suisse, n° 28601/11, 22 décembre 2015
M.N. et autres c. Saint-Marin, n° 28005/12, 7 juillet 2015
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
Brito Ferrinho Bexiga Villa-Nova c. Portugal, n° 69436/10, 1er décembre 2015
Copland c. Royaume-Uni, n° 62617/00, 3 avril 2007

Halford c. Royaume-Uni, nº 20605/92, 25 juin 1997
Iordachi et autres c. Moldova, nº 25198/02, 10 février 2009
Kopp c. Suisse, nº 23224/94, 25 mars 1998
Liberty et autres c. Royaume-Uni, nº 58243/00, 1er juillet 2008
Malone c. Royaume-Uni, nº 8691/79, 2 août 1984
Mustafa Sezgin Tanrıkulu c. Turquie, nº 27473/06, 18 juillet 2017
Pruteanu c. Roumanie, nº 30181/05, 3 février 2015
Szuluk c. Royaume-Uni, nº 36936/05, 2 juin 2009

Obligations des détenteurs de droits

B.B. c. France, nº 5335/06, 17 décembre 2009
I c. Finlande, nº 20511/03, 17 juillet 2008
Mosley c. Royaume-Uni, nº 48009/08, 10 mai 2011

Données à caractère personnel

Amann c. Suisse [GC], nº 27798/95, 16 février 2000
Bernh Larsen Holding AS et autres c. Norvège, nº 24117/08, 14 mars 2013
Uzun c. Allemagne, nº 35623/05, 2 septembre 2010

Photos

Sciacca c. Italie, nº 50774/99, 11 janvier 2005
Von Hannover c. Allemagne, nº 59320/00, 24 juin 2004

Droit à l'oubli

Satakunnan Markkinapörssi Oy et Satamedia Oy c. Finlande [GC], nº 931/13, 27 juin 2017
Segerstedt-Wiberg et autres c. Suède, nº 62332/00, 6 juin 2006

Droit d'opposition

Leander c. Suède, nº 9248/81, 26 mars 1987
M.S. c. Suède, nº 20837/92, 27 août 1997
Mosley c. Royaume-Uni, nº 48009/08, 10 mai 2011
Rotaru c. Roumanie [GC], nº 28341/95, 4 mai 2000
Sinan Işık c. Turquie, nº 21924/05, 2 février 2010

Catégories sensibles de données

Brunet c. France, nº 21010/10, 18 septembre 2014

I c. Finlande, nº 20511/03, 17 juillet 2008
Michaud c. France, nº 12323/11, 6 décembre 2012
S. et Marper c. Royaume-Uni [GC], nº 30562/04 et nº 30566/04, 4 décembre 2008

Contrôle et application de la loi (rôle des différents acteurs, y compris les autorités de contrôle)

I c. Finlande, nº 20511/03, 17 juillet 2008
K.U. c. Finlande, nº 2872/02, 2 décembre 2008
Von Hannover c. Allemagne, nº 59320/00, 24 juin 2004
Von Hannover c. Allemagne (nº 2), nº 40660/08 et nº 60641/08, 7 février 2012

Méthodes de surveillance

Allan c. Royaume-Uni, nº 48539/99, 5 novembre 2002
Association for European Integration and Human Rights et Ekimdzhiev c. Bulgarie, nº 62540/00, 28 juin 2007
Bărbulescu c. Roumanie [GC], nº 61496/08, 5 septembre 2017
D.L. c. Bulgarie, nº 7472/14, 19 mai 2016
Dragojević c. Croatie, nº 68955/11, 15 janvier 2015
Karabeyoğlu c. Turquie, nº 30083/10, 7 juin 2016
Klass et autres c. Allemagne, nº 5029/71, 6 septembre 1978
Roman Zakharov c. Russie [GC], nº 47143/06, 4 décembre 2015
Rotaru c. Roumanie [GC], nº 28341/95, 4 mai 2000
Szabó et Vissy c. Hongrie, nº 37138/14, 12 janvier 2016
Taylor-Sabori c. Royaume-Uni, nº 47114/99, 22 octobre 2002
Uzun c. Allemagne, nº 35623/05, 2 septembre 2010
Versini-Campinchi et Crasnianski c. France, nº 49176/11, 16 juin 2016
Vetter c. France, nº 59842/00, 31 mai 2005
Vukota-Bojić c. Suisse, nº 61838/10, 18 octobre 2016

Vidéosurveillance

Köpke c. Allemagne, nº 420/07, 5 octobre 2010
Peck c. Royaume-Uni, nº 44647/98, 28 janvier 2003

Échantillons de voix

P.G. et J.H. c. Royaume-Uni, nº 44787/98, 25 septembre 2001
Wisse c. France, nº 71611/01, 20 décembre 2005

Jurisprudence choisie de la Cour de justice de l'Union européenne

Jurisprudence liée à la Directive relative à la protection des données

C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde c. Rīgas pašvaldības SIA « Rīgas satiksme »*, 4 mai 2017
[Principe de licéité du traitement : intérêt légitime d'un tiers]

C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce c. Salvatore Manni*, 9 mars 2017
[Droit à l'effacement des données à caractère personnel ; droit d'opposition au traitement]

Affaires jointes C-203/15 et C-698/15, *Tele2 Sverige AB c. Post- och telestyrelsen* et *Secretary of State for the Home Department c. Tom Watson et autres* [GC], 21 décembre 2016
[Confidentialité des communications électroniques ; fournisseurs de services de communications électroniques ; obligation portant sur la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation ; absence de contrôle préalable par une juridiction ou une autorité administrative indépendante ; Charte des droits fondamentaux de l'Union européenne ; compatibilité avec le droit de l'Union]

C-582/14, *Patrick Breyer c. Bundesrepublik Deutschland*, 19 octobre 2016
[Notion de « données à caractère personnel » ; adresses IP ; conservation par un fournisseur de services de médias en ligne ; réglementation nationale ne permettant pas la prise en compte de l'intérêt légitime poursuivi par le responsable du traitement]

C-362/14, *Maximillian Schrems c. Data Protection Commissioner* [GC], 6 octobre 2015
[Principe de licéité du traitement ; droits fondamentaux ; nullité de la Décision relative à la sphère de sécurité ; pouvoirs des autorités de contrôle indépendantes]

C-230/14, *Weltimmo s. r. o. c. Nemzeti Adatvédelmi és Információszabadság Hatóság*, 1er octobre 2015
[Pouvoirs des autorités nationales de contrôle]

C-201/14, *Smaranda Bara et autres c. Casa Națională de Asigurări de Sănătate et autres*, 1er octobre 2015
[Droit d'être informé du traitement de données à caractère personnel]

C-212/13, *František Ryneš c. Úřad pro ochranu osobních údajů*, 11 décembre 2014
[Notions de « traitement des données » et de « responsable du traitement »]

C-473/12, *Institut professionnel des agents immobiliers (IPI) c. Geoffrey Englebert et autres*, 7 novembre 2013
[Droit d'être informé du traitement de données à caractère personnel]

T-462/12 R, *Pilkington Group Ltd c. Commission européenn*e, ordonnance du président du Tribunal, 11 mars 2013

C-342/12, *Worten – Equipamentos para o Lar SA c. Autoridade para as Condições de Trabalho (ACT)*, 30 mai 2013
[Notion de « données à caractère personnel » ; registre du temps de travail ; principes relatifs à la qualité des données et à la légitimation des traitements de données ; accès de l'autorité nationale compétente en matière de surveillance des conditions de travail ; obligation pour l'employeur de mettre à disposition le registre du temps de travail de façon à en permettre la consultation immédiate]

Affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources et autres* et *Kärntner Landesregierung et autres* [GC], 8 avril 2014
[Violation du droit primaire de l'UE par la Directive relative à la conservation des données ; traitement licite ; limitation de la finalité et de la conservation des données]

C-288/12, *Commission européenne c. Hongrie* [GC], 8 avril 2014
[Légitimité de la législation mettant fin au mandat du contrôleur national de la protection des données]

Affaires jointes C-141/12 et C-372/12, *YS c. Minister voor Immigratie, Integratie en Asiel* et *Minister voor Immigratie, Integratie en Asiel c. M et S*, 17 juillet 2014
[Étendue du droit d'accès de la personne concernée ; protection des personnes à l'égard du traitement de données à caractère personnel ; notion de « données à caractère personnel » ; données relatives au demandeur d'un titre de séjour et analyse juridique contenues dans un document administratif préparatoire à la décision ; Charte des droits fondamentaux de l'Union européenne]

C-131/12, *Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 13 mai 2014
[Obligations des fournisseurs de moteurs de recherche de s'abstenir, à la demande de la personne concernée, de faire apparaître des données à caractère personnel dans les résultats de recherche ; applicabilité de la Directive relative à la protection des données ; notion de « traitement des données » ; sens de « responsables du traitement » ; mise en balance de la protection des données et de la liberté d'expression ; droit à l'oubli]

C-614/10, *Commission européenne c. République d'Autriche* [GC], 16 octobre 2012
[Indépendance d'une autorité nationale de contrôle]

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) contre Administración del Estado*, 24 novembre 2011
[Transposition correcte de l'article 7, point f), de la Directive relative à la protection des données – « intérêts légitimes d'autrui » – dans le droit national]

C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) c. Netlog NV*, 16 février 2012
[Obligation faite aux fournisseurs de services de réseaux sociaux d'empêcher l'utilisation illicite d'œuvres musicales et audiovisuelles par les utilisateurs du réseau]

C-70/10, *Scarlet Extended SA c. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24 novembre 2011
[Société de l'information ; droit d'auteur ; internet ; logiciels « peer-to-peer » ; fournisseurs d'accès à internet ; mise en place d'un système de filtrage des communications électroniques afin d'empêcher l'échange des fichiers portant atteinte aux droits d'auteur ; absence d'obligation générale de surveiller les informations transmises]

C-543/09, *Deutsche Telekom AG c. Bundesrepublik Deutschland*, 5 mai 2011
[Nécessité de renouveler le consentement]

Affaires jointes C-92/09 et C-93/09, *Volker und Markus Schecke GbR et Hartmut Eifert c. Land Hessen* [GC], 9 novembre 2010
[Notion de « données à caractère personnel » ; proportionnalité de l'obligation légale de publier des données à caractère personnel sur les bénéficiaires de certains fonds agricoles de l'UE]

C-553/07, *College van burgemeester en wethouders van Rotterdam c. M. E. E. Rijkeboer*, 7 mai 2009
[Droit d'accès de la personne concernée]

C-518/07, *Commission européenne c. République fédérale d'Allemagne* [GC], 9 mars 2010
[Indépendance d'une autorité nationale de contrôle]

C-73/07, *Tietosuojavaltuutettu c. Satakunnan Markkinapörssi Oy et Satamedia Oy* [GC], 16 décembre 2008
[Notion d'« activités journalistiques » au sens de l'article 9 de la Directive relative à la protection des données]

C-524/06, *Heinz Huber c. Bundesrepublik Deutschland* [GC], 16 décembre 2008
[Légitimité de la conservation de données sur des ressortissants étrangers dans un registre statistique]

C-275/06, *Productores de Música de España (Promusicae) c. Telefónica de España SAU* [GC], 29 janvier 2008
[Notion de « données à caractère personnel » ; obligation faite aux fournisseurs d'accès internet de divulguer l'identité des utilisateurs de programmes d'échange de fichiers KaZaA à une association de protection de la propriété intellectuelle]

C-101/01, *Procédure pénale contre Bodil Lindqvist*, 6 novembre 2003
[Catégories particulières de données à caractère personnel]

Affaires jointes C-465/00, C-138/01 et C-139/01, *Rechnungshof c. Österreichischer Rundfunk et autres* et *Christa Neukomm et Joseph Lauermann c. Österreichischer Rundfunk*, 20 mai 2003
[Proportionnalité de l'obligation légale de publier des données à caractère personnel sur les revenus de salariés de certaines catégories d'institutions liées au secteur public]

C-434/16, *Peter Nowak c. Data Protection Commissioner*, conclusions de l'avocat général Kokott, 20 juillet 2017
[Notion de données à caractère personnel ; accès à sa propre copie d'examen ; corrections de l'examinateur]

C-291/12, *Michael Schwarz c. Stadt Bochum*, 17 octobre 2013
[Demande de décision préjudicielle ; espace de liberté, de sécurité et de justice ; passeport biométrique ; empreintes digitales ; base juridique ; proportionnalité]

Jurisprudence liée à la Directive 2016/681/CE

Avis 1/15 de la Cour [GC], 26 juillet 2017
[Base juridique ; projet d'accord entre le Canada et l'Union européenne sur le transfert et le traitement des données des dossiers passagers ; compatibilité du projet d'accord avec l'article 16 du TFUE et les articles 7 et 8 et l'article 52, paragraphe 7, de la Charte des droits fondamentaux de l'Union européenne]

Jurisprudence liée au Règlement relatif à la protection des données des institutions de l'UE

C-615/13 P, *ClientEarth, Pesticide Action Network Europe (PAN Europe) c. Autorité européenne de sécurité des aliments (EFSA), Commission européenne*, 16 juillet 2015
[Accès aux documents]

C-28/08 P, *Commission européenne c. The Bavarian Lager Co. Ltd* [GC], 29 juin 2010
[Accès aux documents]

Jurisprudence relative à la Directive 2002/58/CE

C-536/15, *Tele2 (Netherlands) BV et autres c. Autoriteit Consument en Markt (AMC)*, 15 mars 2017
[Principe de non-discrimination ; mise à disposition des données à caractère personnel concernant les abonnés aux fins de la fourniture de services de renseignements téléphoniques accessibles au public et d'annuaire ; consentement de l'abonné ; distinction selon l'État membre dans lequel les services de renseignements téléphoniques accessibles au public et d'annuaire sont fournis]

Affaires jointes C-203/15 et C-698/15, *Tele2 Sverige AB c. Post- och telestyrelsen* et *Secretary of State for the Home Department c. Tom Watson et autres* [GC], 21 décembre 2016
[Confidentialité des communications électroniques ; fournisseurs de services de communications électroniques ; obligation portant sur la conservation généralisée et

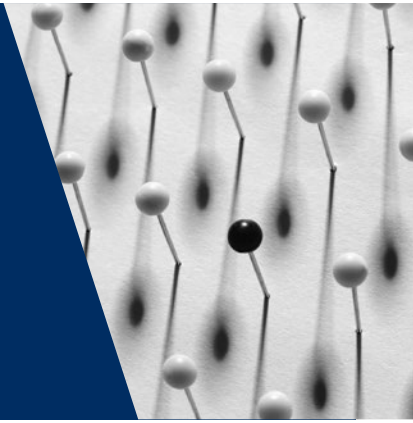
indifférenciée des données relatives au trafic et des données de localisation ; absence de contrôle préalable par une juridiction ou une autorité administrative indépendante ; Charte des droits fondamentaux de l'Union européenne ; compatibilité avec le droit de l'Union]

C-70/10, *Scarlet Extended SA c. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24 novembre 2011

[Société de l'information ; droit d'auteur ; internet ; logiciels « peer-to-peer » ; fournisseurs d'accès à internet ; mise en place d'un système de filtrage des communications électroniques afin d'empêcher l'échange des fichiers portant atteinte aux droits d'auteur ; absence d'obligation générale de surveiller les informations transmises]

C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB et Storyside AB c. Perfect Communication Sweden AB*, 19 avril 2012

[Droit d'auteur et droits voisins ; traitement de données par internet ; atteinte à un droit exclusif ; livres audio rendus accessibles par l'intermédiaire d'un serveur FTP au moyen d'internet par une adresse IP fournie par l'opérateur internet ; injonction adressée à l'opérateur internet de fournir le nom et l'adresse de l'utilisateur de l'adresse IP]



Index

Jurisprudence de la Cour de justice de l'Union européenne

Jurisprudence de la Cour européenne des droits de l'homme

Jurisprudence des juridictions nationales

De nombreuses informations sur l'Agence des droits fondamentaux de l'Union européenne sont disponibles sur le site web de la FRA (fra.europa.eu).

D'autres informations sur la jurisprudence de la Cour européenne des droits de l'homme sont disponibles sur le site web 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: http://hudoc.echr.coe.int.

Comment obtenir des publications du Conseil de l'Europe?

Les Éditions du Conseil de l'Europe publient des ouvrages dans tous les domaines d'activité de l'organisation, notamment les droits de l'homme, le droit, la santé, l'éthique, les affaires sociales, l'environnement, l'éducation, la culture, les sports, la jeunesse et le patrimoine architectural. Chaque livre ou produit électronique peut être commandé directement en ligne à partir du site web: http://book.coe.int.

Une salle de lecture virtuelle permet aux utilisateurs de consulter gratuitement des extraits des principaux ouvrages publiés récemment ou l'intégralité de certains documents officiels.

Le texte intégral des Conventions du Conseil de l'Europe et diverses informations sur celles-ci sont disponibles sur le site officiel du Bureau des Traités du Conseil de l'Europe: http://conventions.coe.int.

Comment prendre contact avec l'Union européenne?

En personne

Dans toute l'Union européenne, des centaines de centres d'information Europe Direct sont à votre disposition. Pour connaître l'adresse du centre le plus proche, visitez la page suivante: https://europa.eu/european-union/contact_fr

Par téléphone ou courrier électronique

Europe Direct est un service qui répond à vos questions sur l'Union européenne. Vous pouvez prendre contact avec ce service:

- par téléphone:
  - via un numéro gratuit: 00 800 6 7 8 9 10 11 (certains opérateurs facturent cependant ces appels),
  - au numéro de standard suivant: +32 22999696;
- par courrier électronique via la page https://europa.eu/european-union/contact_fr

Comment trouver des informations sur l'Union européenne?

En ligne

Des informations sur l'Union européenne sont disponibles, dans toutes les langues officielles de l'UE, sur le site web Europa à l'adresse https://europa.eu/european-union/index_fr

Publications de l'Union européenne

Vous pouvez télécharger ou commander des publications gratuites et payantes sur le site EU Bookshop à l'adresse suivante: https://publications.europa.eu/fr/publications. Vous pouvez obtenir plusieurs exemplaires de publications gratuites en contactant Europe Direct ou votre centre d'information local (https://europa.eu/european-union/contact_fr).

Droit de l'Union européenne et documents connexes

Pour accéder aux informations juridiques de l'Union, y compris à l'ensemble du droit de l'UE depuis 1952 dans toutes les versions linguistiques officielles, consultez EUR-Lex à l'adresse suivante: http://eur-lex.europa.eu

Données ouvertes de l'Union européenne

Le portail des données ouvertes de l'Union européenne (http://data.europa.eu/euodp/fr) donne accès à des ensembles de données provenant de l'UE. Les données peuvent être téléchargées et réutilisées gratuitement, à des fins commerciales ou non commerciales.

doi:10.2811/091298 TK-05-17-225-FR-N

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

EDPS

L'évolution rapide des technologies de l'information souligne la nécessité d'une protection solide 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 repoussent notamment les frontières de la surveillance, de l'interception des communications et de la conservation des données, ce qui met 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 dans la protection des données de se familiariser avec ce nouveau domaine du droit. Il présente un aperçu des cadres légaux applicables de l'UE et du CdE. Il explique la jurisprudence essentielle et résume les principaux arrêts de la Cour de justice de l'Union européenne et de la Cour européenne des droits de l'homme. Il propose, en outre, des illustrations pratiques basées sur des scénarios hypothétiques des divers problèmes rencontrés dans ce domaine en évolution constante.

AGENCE DES DROITS FONDAMENTAUX DE L'UNION EUROPÉENNE
Schwarzenbergplatz 11 – 1040 Vienne – Autriche
Tél. +43 (1) 580 30-0 – Fax +43 (1) 580 30-699
fra.europa.eu – info@fra.europa.eu – @EURightsAgency

COUR EUROPÉENNE DES DROITS DE L'HOMME
CONSEIL DE L'EUROPE
67075 Strasbourg Cedex – France
Tél. +33 (0) 3 88 41 20 18 – Fax +33 (0) 3 88 41 27 30
echr.coe.int – publishing@echr.coe.int – @ECHRPublication

CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES
Rue Wiertz 60 – 1047 Bruxelles – Belgique
Tél. +32 2 283 19 00
www.edps.europa.eu – edps@edps.europa.eu – @EU_EDPS

Office des publications

ISBN 978-92-871-9850-1 (CdE)
ISBN 978-92-9491-900-7 (FRA)