FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

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

Ce rapport porte sur les questions relatives à la protection des données à caractère personnel (article 8) du Titre II « Libertés » de la Charte des droits fondamentaux de l'Union européenne.

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

Un numéro unique gratuit (*):
00 800 6 7 8 9 10 11

(*) Certains opérateurs de téléphonie mobile ne permettent pas l'accès aux numéros 00 800 ou peuvent facturer ces appels.

Crédit photo (couverture): Comstock Images

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

Une fiche catalographique figure à la fin de l'ouvrage.

Luxembourg: Office des publications de l'Union européenne, 2012

ISBN 978-92-9192-510-0
doi:10.2811/47365

Printed in Belgium

Imprimé sur papier recyclé sans chlore (PCF)

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

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

Table des matières

Avant-propos

L'architecture de la protection des droits fondamentaux s'est développée progressivement dans l'Union européenne et elle continue d'évoluer. Le présent rapport, qui fait partie d'une série quatre rapports publiée par l'Agence des droits fondamentaux de l'Union européenne (FRA), examine trois aspects, et institutions, étroitement liés qui contribuent à l'architecture d'ensemble des droits fondamentaux dans l'Union européenne, à savoir les organismes d'égalité, les autorités chargées de la protection des données et les institutions nationales des droits de l'homme.

Pour la FRA, ces trois ensembles d'organismes de surveillance nationaux revêtent une grande importance. L'agence a pour mission spécifique de coopérer avec entre autres les organisations gouvernementales et organismes publics compétents dans le domaine des droits fondamentaux des États membres, y compris les autorités chargées de la protection des données, dans le but d'améliorer la coopération concertée entre le niveau national et le niveau européen. C'est la nécessité de mettre en place une protection et une promotion toujours plus efficaces des droits fondamentaux au niveau national en particulier, associées à des mécanismes européens et internationaux, qui est à la base de l'examen de l'architecture des droits fondamentaux dans l'Union européenne.

Le présent rapport, qui concerne les autorités chargées de la protection des données, offre une analyse de leur rôle crucial en ce qui concerne le droit fondamental à la protection des données à caractère personnel ; il englobe une évaluation de leur efficacité, de leur fonctionnement et de leur indépendance. Ce rapport vient à propos car la protection des données a acquis le statut d'un droit fondamental distinct dans l'UE dans le texte de la Charte des droits fondamentaux (article 8) et elle est désormais liée au droit au respect de la vie privée et familiale, tout en restant distincte de ce dernier. Par ailleurs, la protection des données à caractère personnel représente un domaine politique de plus en plus important dans l'UE, qui a joué un rôle moteur clé pour la mise en place d'une législation dans de nombreux États membres.

La Commissaire à la justice, aux droits fondamentaux et à la citoyenneté, Viviane Reding, a récemment souligné dans une déclaration écrite au Parlement européen que la protection des données occupe une place d'une importance particulière pour l'UE. Elle a déclaré être « intimement convaincue qu'il ne peut y avoir de confiance des citoyens dans l'Europe si nous ne restons pas vigilants pour assurer que les données à caractère personnel soient protégées contre une utilisation non autorisée et que les citoyens aient le droit de décider eux-mêmes du traitement ou non de leur données. » C'est dans cet esprit que la FRA présente ce rapport.

Morten Kjaerum
Directeur

Résumé

L'UE joue un rôle de pionnier à l'échelon mondial pour le droit fondamental à la protection des données à caractère personnel

L'UE a historiquement joué un rôle majeur pour piloter l'élaboration et l'introduction de la législation nationale sur la protection des données à caractère personnel dans un certain nombre de systèmes juridiques dans l'UE, qui ne disposaient auparavant pas d'une telle législation. Un instrument important à cet égard est la directive 95/46/CE 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 (la « directive relative à la protection des données »).

La Charte des droits fondamentaux de l'Union européenne – qui, conformément au nouvel article 6 du Traité de l'Union européenne, a « la même valeur juridique que les traités » – définit, à l'article 8, la protection des données comme un droit fondamental, distinct du respect pour la vie privée et familiale établi à l'article 7. De ce fait, la Charte des droits fondamentaux de l'UE se distingue des autres grands textes internationaux sur les droits de l'homme qui, pour la plupart, traitent essentiellement de la protection des données à caractère personnel en tant qu'extension du droit au respect de la vie privée.

Cette inclusion de la protection des données parmi les droits fondamentaux autonomes représente la reconnaissance par l'UE de l'importance des progrès technologiques ainsi qu'une tentative pour faire en sorte que les droits fondamentaux tiennent compte de ces progrès. Nos vies se caractérisent aujourd'hui par un échange constant d'informations et nous vivons dans un flux constant de données ; leur protection prend donc l'importance et occupe une place de plus en plus centrale dans le système institutionnel et politique. Cette évolution est clairement visible lorsque l'on compare la Charte de l'UE à la Convention européenne des droits de l'homme du Conseil de l'Europe de 1950. Selon l'article 8 de la convention, « toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. » Cette convention ne contient aucun droit explicite ni autonome à la protection des données. Cette dernière se manifeste plutôt, dans la jurisprudence de la Cour européenne des droits de l'homme, à Strasbourg, comme un aspect de la protection de la vie privée. Par comparaison, l'article 8 de la Charte des droits fondamentaux de l'UE reconnaît la place centrale et l'importance acquises par ce droit dans notre société sous l'effet des progrès technologiques.

La présente étude comparative analyse les problèmes et les pratiques encourageantes actuels relatifs aux systèmes de protection des données de l'UE.

Les défis auxquels est confronté le système européen de protection des données

L'Agence des droits fondamentaux de l'Union européenne a recensé les problèmes suivants pour le système de protection des données de l'UE :

Lacunes au niveau des autorités chargées de la protection des données :

Au niveau structurel, le manque d'indépendance de plusieurs autorités chargées de la protection des données représente un problème majeur. Dans un certain nombre d'États membres, on relève des préoccupations concernant la capacité et l'effectivité des délégués[1] au sein des autorités chargées de la protection des données à assumer leur mission de façon autonome. Au niveau du fonctionnement, un manque de personnel et de ressources financières suffisantes suscite de graves difficultés dans plusieurs autorités de protection des données. Sur le plan opérationnel, les pouvoirs limités de plusieurs d'entre elles restent un problème de taille. Dans certains États membres, elles ne disposent pas des pleins pouvoirs pour instruire, intervenir dans le traitement d'opérations, prodiguer des conseils juridiques et ester en justice.

Mise en œuvre déficiente du système de protection des données :

Dans certains États membres, les poursuites et les sanctions pour violation de la législation en matière de protection sont limitées voire inexistantes. Concernant les réparations, dans plusieurs États membres, le système juridique ne laisse, en réalité, aucune possibilité d'obtenir réparation en cas de violation des droits relatifs à la protection des données, en raison d'une combinaison de plusieurs facteurs tels que la charge de la preuve, les difficultés liées à la quantification des dommages et un manque de soutien des autorités de contrôle, qui mènent principalement des activités de promotion « souples » telles que l'enregistrement et la sensibilisation. La tendance générale dans les États membres est de se concentrer sur des méthodes d'influence « souples » pour garantir le respect avec la législation relative à la protection des données, plutôt que d'appliquer et de mettre en œuvre des instruments « stricts » qui permettraient d'identifier les contrevenants aux droits en matière de protection des données, de les sanctionner et leur imposer d'indemniser les victimes. À cet égard, des pratiques encourageantes en matière de coopération des autorités de protection des données et d'autres autorités afin d'améliorer les investigations ont été constatées dans certains États membres.

1 Dans l'intérêt d'une meilleure lisibilité, l'utilisation de la forme grammaticale masculine pour la désignation des personnes et des fonctions doit être comprise comme se référant à toutes personnes sans considération de genre.

Connaissance des droits :

Durant les travaux de recherche menés pour ce rapport, la FRA a pu identifier des enquêtes nationales concernant la protection des données dans 12 des 27 États membres de l'UE. Ces enquêtes ont été dans certain cas commandées par les autorités nationales de protection des données. Les questions posées, le nombre de participants, la méthodologie utilisée et les résultats finaux sont hétérogènes et ne permettent pas toujours d'établir de comparaisons. Toutefois, l'existence même de ces enquêtes nationales constitue une pratique encourageante. En février 2008, deux enquêtes Eurobaromètre sur la protection des données ont été publiées. Les principaux résultats de ces enquêtes étaient qu'une majorité des citoyens de l'UE expriment des inquiétudes par rapport à la protection des données et que les autorités nationales de protection des données restent relativement méconnues de la plupart des citoyens de l'UE.

Le manque de protection des données dans l'ancien troisième pilier de l'UE :

La principale limitation à laquelle l'UE est actuellement confrontée pour assurer une protection des données efficace et exhaustive découle de l'architecture constitutionnelle des anciens piliers de l'UE. Alors que la protection des données est largement développée dans le premier pilier de l'UE, le régime de protection des données dans l'ancien troisième pilier ne peut être jugé satisfaisant. Pourtant, cet ancien troisième pilier de l'UE regroupe des domaines tels que la coopération policière, la lutte contre le terrorisme ou les affaires pénales dans lesquels le besoin de protection des données est particulièrement important. Le Traité de Lisbonne permet de combler ce fossé. La déclaration n° 21 de ce traité note que des règles spécifiques sur la protection des données à caractère personnel et sur la libre circulation de ces données dans les domaines de la coopération judiciaire en matière pénale et de la coopération policière pourraient s'avérer nécessaires en raison de la « nature spécifique » de ces domaines.

Les exceptions aux règles relatives à la protection des données pour des raisons liées à la sécurité et à la défense :

L'article 13, paragraphe 1, de la directive relative à la protection des données prévoit de grandes exceptions et limitations concernant la sécurité publique, la défense, la sûreté de l'État (y compris le bien-être économique de l'État lorsque ces traitements sont liés à des questions de sûreté de l'État) et les activités de l'État relatives à des domaines du droit pénal. L'ampleur de ces exceptions et restrictions manque de clarté. Dans plusieurs États membres, ces domaines sont tous exclus des législations relatives à la protection des données. Cela laisse un domaine extrêmement vaste non réglementé avec des conséquences potentiellement graves pour la protection des droits fondamentaux. La déclaration n° 20 du Traité de Lisbonne indique que chaque fois que doivent être adoptées des règles relatives à la protection des données à caractère personnel qui pourraient avoir une incidence directe sur la sécurité nationale, il devra être « dûment tenu compte » des spécificités de la question.

Le défi de la technologie :

Les avancées technologiques récentes et en cours posent de nouveaux défis qui doivent être relevés de toute urgence. Alors que la vidéosurveillance dans les lieux publics et dans le milieu professionnel est répandue, le cadre législatif reste à la traîne. Le rapport révèle comme exemple que souvent, dans la pratique, les caméras de vidéosurveillance ne sont ni enregistrées ni contrôlées dans certains États membres.

Pratiques encourageantes

La plupart des pratiques encourageantes identifiées par l'Agence des droits fondamentaux de l'UE pour leur contribution effective à la protection des données portent sur des actions de sensibilisation organisées par des autorités nationales de protection des données dans certains États membres, dans le cadre de cours spécifiques, séminaires et conférences, de programmes éducatifs, de guides et de recommandations ou de campagnes d'informations et de conseils. D'autres pratiques encourageantes sont également liées au statut institutionnel des autorités de contrôle, à savoir leur degré d'indépendance, l'application de la législation sur les données à caractère personnel, l'engagement actif dans la préparation de propositions de codes de conduite et leur publication, et le degré de coopération avec les institutions nationales, les ONG et les autorités de protection des données d'autres États membres.

Avis

L'Agence des droits fondamentaux de l'Union européenne a formulé les avis suivants en se basant sur les conclusions et l'analyse comparative du présent rapport :

Élargir le régime de protection des données de l'UE

Le Traité de Lisbonne, qui abolit la structure en piliers de l'UE donne la possibilité à celle-ci d'élargir son régime de protection des données à caractère personnel, qui n'existe actuellement que pour l'ancien premier pilier, à tous les (anciens) piliers de l'UE. L'imposition de limitations à la protection des données pour des raisons de sécurité ou de défense ou à d'autres fins légitimes demeure possible conformément à l'article 52 de la Charte des droits fondamentaux de l'UE. Toutefois, ces limitations doivent être prévues par la loi et doivent respecter le contenu essentiel du droit à la protection des données à caractère personnel et le principe de nécessité et de proportionnalité. L'exclusion complète et totale de certains domaines du champ de la législation sur la protection des données est problématique selon la perspective des droits fondamentaux et doit être évitée.

Assurer l'efficacité de la mise en œuvre

Ce rapport fait apparaître des insuffisances au niveau des effectifs et des ressources financières dans plusieurs autorités de protection des données à caractère personnel. Sur le plan opérationnel, les pouvoirs limités de plusieurs autorités nationales de protection des données représentent un grave problème. Dans certains États membres, elles ne disposent pas des pleins pouvoirs d'investigation, d'intervention, de conseils juridiques et d'ester en justice. Les autorités nationales de protection des données ont besoin de disposer des moyens, des pouvoirs et de l'indépendance nécessaires pour contribuer à l'application efficace du système de protection des données à caractère personnel.

Les garanties concernant la mise en œuvre efficace de la protection des données à caractère personnel ainsi que l'investigation et la détection des auteurs d'infractions jouent un rôle crucial comme moyen de dissuasion et de prévention des violations de la protection des données. L'augmentation des efforts consacrés à la répression contribuerait également à convaincre la population du fait que les questions de protection des données sont prises au sérieux. Le recours exclusif à des mesures « souples » sans application de mesures « strictes » porte atteinte à la crédibilité de l'ensemble du système. Dans ce sens, toute mesure efficace de répression contribuerait également à sensibiliser les citoyens à leurs droits. Les autorités de protection des données doivent jouer un rôle important dans la mise en œuvre du système de protection des données soit parce qu'elles ont directement le pouvoir d'appliquer des sanctions soit parce qu'elles sont habilitées à engager des poursuites qui peuvent conduire à des sanctions d'office. Cela renforcerait leur autorité et leur crédibilité.

Les autorités nationales de protection des données en tant que gardiennes indépendantes

Au niveau structurel, le manque d'indépendance de plusieurs autorités nationales de protection des données pose un grave problème. Dans plusieurs pays, toutefois, différents obstacles d'ordre normatif ou pratique suscitent des préoccupations quant à l'indépendance effective des autorités nationales de protection des données par rapport aux branches politiques du gouvernement. La garantie d'indépendance est en fait principalement assurée par la procédure de nomination et de destitution du personnel des autorités nationales de protection des données. Le contrôle des moyens financiers constitue un second point important pour garantir l'autonomie des autorités de contrôle.

Dans divers États membres, les délégués à la protection des données sont nommés directement par le gouvernement sans l'intervention de l'opposition parlementaire ; dans plusieurs cas, cela a suscité de sérieuses préoccupations quant à l'indépendance effective de l'autorité de protection des données. Des inquiétudes similaires peuvent naître dans les pays où l'autorité de contrôle dépend du Ministère de la Justice. Enfin, d'autre États membres ont prévu une procédure mixte pour la désignation des délégués de l'autorité de protection des données, impliquant à la fois le pouvoir exécutif, législatif et judiciaire ainsi que d'autres groupes organisés de la société. Dans certains cas, toutefois, il est essentiel de garantir que le gouvernement ne contrôle pas de facto, directement ou indirectement, la majorité des personnes désignées, dénaturant ainsi la finalité même d'une procédure de nomination pluraliste.

La directive 95/46/CE relative à la protection des données requiert que les autorités de protection des données « exercent en toute indépendance les missions dont elles sont investies » (article 28, paragraphe 1). Cependant, la nature de cette « indépendance » n'est pas précisée. Il serait utile de décrire dans les détails les garanties de l'indépendance énoncées dans la directive pour garantir une indépendance réelle dans la pratique des autorités de protection des données. Il serait opportun que la directive fasse référence aux principes de Paris et à d'autres normes disponibles lors d'une modification future de la directive afin de proposer une définition plus complète de l'indépendance.

Les autorités nationales de protection des données comme élément de l'architecture émergente des droits fondamentaux de l'UE

Les autorités de protection des données à caractère personnel doivent encourager une coopération plus étroite et une synergie avec d'autres gardiens des droits fondamentaux (tels que les institutions nationales de défense des droits de l'homme et les organismes de promotion de l'égalité, etc.) dans l'architecture émergente des droits fondamentaux de l'UE. Pour contribuer à améliorer la coordination et la synergie, l'UE pourrait notamment ajouter quelques mots à l'article 28 de la directive 95/46/CE relative à la protection des données qui donneraient la possibilité aux États membres de légiférer de manière à ce que leur autorité de protection des données devienne en fait une section spécialisée de leur institution nationale de protection des droits de l'homme (l'article 13 de la directive 2000/43/CE du Conseil offre un exemple intéressant d'un effet semblable).

Les autorités nationales de protection des données en tant que guichets uniques efficaces

Les autorités de protection des données constituent des acteurs clés pour une protection des données effective. Elles servent de point d'accès à bas seuil pour la protection effective des données des citoyens et d'autres personnes. Elles ne doivent pas seulement traiter des questions figurant dans l'ancien premier pilier comme c'est le cas actuellement dans certains États membres mais devraient être agencées sous forme de guichet unique afin de traiter toutes les préoccupations des citoyens et autres personnes concernant la protection des données, notamment les domaines qui faisaient auparavant partie du troisième pilier de l'UE. La prolifération des organismes et autorités chargés de la protection des données n'est pas propice à la sensibilisation des citoyens à leur existence. De plus, la présence d'une multitude d'organismes sème la confusion et crée une complexité inutile.

Connaissance des droits

En février 2008, deux enquêtes Eurobaromètre ont été publiées. Les principaux résultats de ces enquêtes étaient qu'une majorité des citoyens de l'UE expriment des inquiétudes par rapport à la protection des données et que les autorités nationales de protection des données restent relativement méconnues de la plupart des citoyens de l'UE.

Il est recommandé que les autorités de protection des données s'efforcent tout particulièrement de cultiver leur image de gardiennes indépendantes du droit fondamental à la protection des données et qu'elles se concentrent sur la sensibilisation concernant leur existence et leur rôle.

1 Introduction

La Charte des droits fondamentaux de l'UE consacre le droit fondamental à la protection des données dans son article 8. Cette protection représente également l'un des domaines clés des droits fondamentaux dans lesquels l'UE est habilitée à légiférer.

L'agence a établi le présent rapport avec l'assistance du Fralex, le groupe d'experts juridiques de la FRA. Les équipes nationales du Fralex ont produit 27 études nationales et une étude européenne/internationale (qui sont toutes disponibles à titre d'information sur le site web de l'agence http://fra.europa.eu) en respectant des lignes directrices communes élaborées par la FRA. Les études nationales datent de février 2009. Le « Groupe de l'article 29 » a été consulté concernant le projet de rapport comparatif et a soumis ses observations.

Le rapport est étroitement lié aux publications et projets suivants de l'Agence des droits fondamentaux de l'Union européenne :

- Avis sur la proposition de directive relative à l'utilisation des données des dossiers passagers (PNR), octobre 2008[2]
- Contribution de l'agence à une consultation de la Commission européenne sur les scanners corporels de sûreté, janvier 2009[3]
- *National Human Rights Institutions in the European Union Member States (Strengthening the Fundamental Rights Architecture I)* (Rapport sur les institutions nationales des droits de l'homme dans les États membres de l'UE – Renforcement de l'architecture des droits fondamentaux au sein de l'UE), 2010[4]
- *EU-MIDIS, Données en bref 3 : Sensibilisation aux droits et organismes de promotion de l'égalité (Renforcement de l'architecture des droits de l'homme au sein de l'UE III)*, 2010[5]

Le présent rapport dresse pour commencer un état des lieux des normes du droit international concernant la protection des données. Il analyse ensuite la protection des données dans le droit européen et les changements apportés par le Traité de Lisbonne. Il se poursuit par une vue d'ensemble des institutions et pratiques en matière de protection des données dans les États membres. Pour conclure, le rapport recense les lacunes et les pratiques encourageantes.

2 Disponible à l'adresse : http://fra.europa.eu/fraWebsite/attachments/FRA-PNR-Opinion-2011_FR.pdf (Tous les liens ont été consultés au plus tôt le 29 septembre 2008).
3 Contribution non publiée de l'Agence des droits fondamentaux de l'UE à une consultation de la Commission européenne.
4 Disponible à l'adresse : http://fra.europa.eu.
5 Disponible à l'adresse : http://fra.europa.eu/eu-midis.

2 Les normes des droits fondamentaux liés à la protection des données

La protection des données à caractère personnel est reconnue comme un droit fondamental dans divers traités européens et internationaux ; elle est interprétée par la jurisprudence des tribunaux internationaux et régionaux.

2.1. La protection des données dans le cadre des Nations Unies

Le droit fondamental à la protection des données à caractère personnel est également reconnu au niveau international dans différents instruments sur les droits de l'homme adoptés sous l'égide des Nations Unies essentiellement en tant qu'extension du droit au respect de la vie privée.[6]

En particulier, dans le Pacte international relatif aux droits civils et politiques, qui a été ratifié par quatre cinquièmes des États du monde, le droit à la protection de la vie privée, de la famille, du domicile et de la correspondance figure à l'article 17 selon lequel « 1. Nul ne sera 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. 2. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes ». L'observation générale n°16 concernant cet article 17 du Pacte international relatif aux droits civils et politiques[7] se réfère explicitement au droit à la protection des données à caractère personnel. Elle stipule spécifiquement que : « le rassemblement et la conservation, par des autorités publiques, des particuliers ou des organismes privés, de renseignements concernant la vie privée d'individus sur des ordinateurs, dans des banques de données et selon d'autres procédés, doivent être réglementés par la loi. L'État doit prendre des mesures efficaces afin d'assurer que ces renseignements ne tombent pas entre les mains de personnes non autorisées par la loi à les recevoir, les traiter et les exploiter, et ne soient jamais utilisés à des fins incompatibles avec le Pacte. Il serait souhaitable, pour assurer la protection la plus efficace de sa vie privée, que chaque individu ait le droit de déterminer, sous une forme intelligible, si des données personnelles le concernant et, dans l'affirmative, lesquelles, sont stockées dans des fichiers automatiques de données, et à quelles fins. Chaque individu doit également pouvoir déterminer les autorités publiques ou les particuliers ou les organismes privés qui ont ou peuvent avoir le contrôle des fichiers le concernant. Si ces fichiers contiennent des données personnelles incorrectes ou qui ont été recueillies ou traitées en violation des dispositions de la loi, chaque individu doit avoir le droit de réclamer leur rectification ou leur suppression ». En outre, la jurisprudence du Comité des droits de l'homme souligne que la notion de vie privée dans l'observation générale n° 16 ne doit pas donner lieu à une interprétation étroite.[8]

Un autre instrument particulièrement important réside dans les principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel[9] adoptés par l'Assemblée générale des Nations Unies le 14 décembre 1990. Ils établissent un certain nombre de principes concernant les garanties minimales qui devraient être prévues dans les législations nationales pour la protection des données à caractère personnel. Ils prévoient notamment le principe de licéité et de loyauté de la collecte et du traitement des données à caractère personnel, d'exactitude, de finalité, de l'accès par les personnes concernées, de non-discrimination et de sécurité des fichiers. Les dérogations à ces principes « ne peuvent être autorisées que si elles sont nécessaires pour protéger la sécurité nationale, l'ordre public, la santé ou la moralité publiques ainsi que, notamment, les droits et libertés d'autrui, spécialement de personnes persécutées (clause humanitaire), sous réserve que ces dérogations soient expressément prévues par la loi ou par une réglementation équivalente prise en conformité avec le système juridique interne qui en fixe expressément les limites et édicte des garanties appropriées ». Les dérogations au principe de non-discrimination sont encore plus limitées et « ne pourraient être autorisées que dans les limites prévues par la Charte internationale des droits de l'homme et les autres instruments pertinents dans le domaine de la protection des droits de l'homme et de la lutte contre les discriminations ». Les principes y établis « devraient s'appliquer en premier lieu à tous les fichiers informatisés publics et privés et, par voie d'extension facultative et sous réserve des adaptations adéquates, aux fichiers traités manuellement. Des dispositions particulières également facultatives pourraient être prises pour étendre tout ou partie desdits principes aux fichiers de personnes morales, notamment lorsqu'ils contiennent pour partie des informations concernant des personnes physiques ».

Le droit fondamental à la protection des données à caractère personnel est également reconnu au niveau régional dans divers instruments régionaux de protection des droits de l'homme en dehors de l'Europe, principalement en tant qu'extension du droit à la vie privée.[10]

2.2. La protection des données dans le cadre du Conseil de l'Europe

Au niveau régional, la norme pour la protection des données à caractère personnel est établie dans plusieurs conventions adoptées sous l'égide du Conseil de l'Europe. La plupart de ces textes ont été ratifiés par l'ensemble des États membres de l'UE et, dans certains cas, ont été mis en œuvre dans les systèmes juridiques nationaux en tant que normes constitutionnelles suprêmes.

6 L'article 12 de la Déclaration Universelle des Droits de l'Homme protège le droit au respect de la vie privée.

7 Comité des droits de l'homme, Observation générale 16, (23e session, 1988), Récapitulation des observations générales ou des recommandations générales adoptées par les organes créés en vertu d'instruments internationaux relatifs aux droits de l'homme, U.N. Doc. HRI/GEN/1/Rev.1, 21 (1994), paragraphe 10.

8 Voir par exemple l'affaire *Coeriel et Aurik c. Pays-Bas (1994)*, Comm 453/1991.

9 Principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel, adoptés par l'Assemblée générale des Nations Unies dans sa résolution 45/95 du 14 décembre 1990.

10 Le droit au respect de la vie privée figure à l'article V de la Déclaration américaine des droits et devoirs de l'Homme de 1948 et à l'article 11 de la Convention américaine sur les droits de l'homme de 1969. La Charte africaine des droits de l'homme et des peuples de 1981 ne reconnaît pas expressément le droit au respect de la vie privée.

Le principal texte juridique dans le cadre du Conseil de l'Europe, la Convention européenne des droits de l'homme (CEDH) – qui a été ratifiée par tous les États membres de l'UE – ne mentionne pas explicitement la protection des données à caractère personnel en tant que telle. Toutefois, la jurisprudence très fournie de la Cour européenne des droits de l'homme (CouEDH) démontre que le droit à la protection des données est compris dans l'article 8 de la Convention, qui reconnaît expressément le droit au respect de la vie privée et familiale, en indiquant « 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. 2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui ».

Par ailleurs, au sein du cadre du Conseil de l'Europe, la reconnaissance explicite du droit fondamental à la protection des données à caractère personnel figure dans la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel de 1981 (également désignée « Convention 108 »)[11] qui a été ratifiée par tous les États membres de l'UE. La Convention impose l'obligation aux États parties de garantir, sur leur territoire, à toute personne physique, quelles que soient sa nationalité ou sa résidence, le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant (« protection des données »). La Convention s'applique aux fichiers et aux traitements automatisés de données à caractère personnel dans les secteurs public et privé. Elle définit un certain nombre de principes concernant le traitement des données et fait également référence à la qualité des données, notamment au fait qu'elles doivent être adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées (principe de proportionnalité) ; à leur exactitude ; à la confidentialité des données sensibles ; à l'information de la personne concernée et à son droit à l'accès et à la rectification des données. Toutefois, elle emploie généralement des formulations relativement vagues et générales. Elle n'est pas nécessairement directement applicable et exige que les États parties adoptent des mesures de mise en œuvre : de ce fait, elle ne peut pas être directement invoquée devant les tribunaux. Par ailleurs, la Convention contient une vaste gamme d'exceptions, notamment la possibilité offerte aux États parties de déroger aux dispositions concernant la protection des données lorsqu'une telle dérogation, prévue par la loi de la Partie, constitue une mesure nécessaire dans une société démocratique.

La Convention 108 établit également un comité consultatif composé de représentants des États parties à la Convention ainsi que d'observateurs d'autres États (membres ou non-membres) et d'organisations internationales, qui est chargé d'interpréter les dispositions et d'améliorer la mise en œuvre de la Convention. Ce comité a adopté un Protocole additionnel à la Convention, qui n'a pas encore été ratifié par tous les États membres, concernant les autorités de contrôle et les flux transfrontaliers de données (2001). Il renforce le rôle des autorités de contrôle et interdit le transfert de données à caractère personnel vers un destinataire soumis à la juridiction d'un État ou d'une organisation n'assurant pas un niveau de protection adéquat pour le transfert considéré.

Autre instrument législatif important au sein du cadre du Conseil de l'Europe, la Convention sur les droits de l'homme et la biomédecine (1997)[12] qui n'a pas encore été ratifiée par tous les États membres de l'UE. L'article 10 de cette Convention réaffirme le principe contenu à l'article 8 de la CEDH et repris dans la Convention 108 en établissant que « 1. Toute personne a droit au respect de sa vie privée s'agissant des informations relatives à sa santé. 2. Toute personne a le droit de connaître toute information recueillie sur sa santé. Cependant, la volonté d'une personne de ne pas être informée doit être respectée. 3. À titre exceptionnel, la loi peut prévoir, dans l'intérêt du patient, des restrictions à l'exercice des droits mentionnés au paragraphe 2 ». Par ailleurs, conformément à l'article 6 de la Convention 108, les données à caractère personnel relatives à la santé constituent une catégorie particulière de données, soumises en tant que telles, à un régime spécial. La Convention sur les droits de l'homme et la biomédecine prévoit toutefois certaines restrictions au respect de la vie privée ; ainsi, par exemple, l'autorité judiciaire pourra-t-elle ordonner la réalisation d'un test ayant pour but l'identification de l'auteur d'un crime (exception fondée sur la prévention des infractions pénales) ou détermination de la paternité ou de la maternité (exception fondée sur la protection des droits d'autrui).

Il convient enfin d'indiquer que le Conseil de l'Europe a également eu recours à des recommandations et des résolutions pour préciser davantage les principes de la protection des données à caractère personnel des personnes physiques. Ces instruments sont adoptés à l'unanimité par le Comité des Ministres et, bien qu'ils ne soient pas juridiquement contraignants, ils proposent des normes de référence pour tous les États membres. Depuis 1972, le Conseil de l'Europe a adopté un grand nombre de recommandations et de résolutions sur les questions relatives à la protection des données.[13]

À cet égard, la recommandation R(87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police mérite une mention particulière car elle va au-delà de la « Convention 108 » en garantissant la protection des données sensibles à caractère personnel.[14] En vertu du principe 2.4 des principes de base figurant en annexe à la recommandation, la collecte de données sur des individus pour l'unique motif qu'ils ont telle origine raciale, telles convictions religieuses, tel comportement sexuel ou telles opinions politiques ou qu'ils appartiennent à tels mouvements ou organisations qui ne sont pas interdits par la loi devrait être prohibée. La collecte de données concernant ces facteurs ne peut être effectuée que si elle est absolument nécessaire pour les besoins d'une enquête déterminée. L'annexe à cette recommandation établit également un certain nombre d'autres

11 http://conventions.coe.int/Treaty/FR/Treaties/Html/108.htm.

12 http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=164&CL=FRE.

13 Voir les recommandations suivantes : Recommandation R(95) 4 sur la protection des données à caractère personnel dans le domaine des services de télécommunications, eu égard notamment aux services téléphoniques (7 février 1995) ; Recommandation R(97) 5 sur la protection des données médicales (13 février 1997) ; Recommandation R(97) 18 sur la protection des données à caractère personnel collectées et traitées à des fins statistiques (30 septembre 1997) ; Recommandation R(99) 5 sur la protection de la vie privée sur Internet (23 février 1999) ; et Recommandation R(2002) 9 sur la protection des données à caractère personnel collectées et traitées à des fins d'assurance (18 septembre 2002).

14 Recommandation R(87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police (17 septembre 1987).

principes destinés à réglementer la collecte, l'enregistrement, l'utilisation, la communication et la conservation à des fins de police des données à caractère personnel. Dans son préambule, la recommandation reconnaît la nécessité de concilier l'intérêt de la société à la prévention et à la répression des infractions pénales et au maintien de l'ordre public et, d'autre part, les intérêts de l'individu et le droit au respect de sa vie privée. À cette fin, la jurisprudence en la matière de la Cour européenne des droits de l'homme est prise en considération.

Concernant la jurisprudence de la CouEDH relative au respect de la vie privée, la Cour a également fait référence à plusieurs reprises aux questions relatives à la protection des données. Dans ce contexte, la CouEDH considère que l'article 8 de la CEDH ne se contente pas de commander aux États membres de s'abstenir d'ingérences arbitraires dans la vie privée, mais comporte également des obligations positives qui supposent « l'adoption de mesures visant au respect de la vie privée jusque dans les relations des individus entre eux ».[15]

Dans l'affaire *M.S. c. Suède*, par exemple, la CouEDH indique clairement que « la protection des données à caractère personnel [...] revêt une importance fondamentale pour l'exercice du droit au respect de la vie privée et familiale garanti par l'article 8 de la Convention ».[16] Dans l'affaire *Leander c. Suède*, la Cour indique que la mémorisation de données relatives à la vie privée d'une personne dans le registre secret de la police et la communication de ces informations portent atteinte à son droit au respect de sa vie privée, garanti par l'article 8, paragraphe 1.[17] Elle souligne que « la Cour doit se convaincre de l'existence de garanties adéquates et suffisantes contre les abus car un système de surveillance secrète destiné à protéger la sécurité nationale crée un risque de saper, voire de détruire, la démocratie au motif de la défendre ». Dans l'affaire *Z. c. Finlande*, la CouEDH rappelle le rôle fondamental que joue la protection des données à caractère personnel, les informations relatives à la santé n'en étant pas les moindres, pour l'exercice du droit au respect de la vie privée et familiale garanti par l'article 8 de la Convention.[18] Toutefois, elle admet parallèlement que la protection de la confidentialité des données médicales, qui est dans l'intérêt du patient comme de la collectivité dans son ensemble, peut parfois s'effacer devant la nécessité d'enquêter sur des infractions pénales, d'en poursuivre les auteurs et de protéger la publicité des procédures judiciaires lorsqu'il est prouvé que ces derniers intérêts revêtent une importance encore plus grande.

Dans l'affaire *Rotaru c. Roumanie,* la CouEDH reconnaît expressément que l'article 8 de la CEDH doit être interprété de manière à englober les garanties relatives à la protection des données consacrées dans la Convention 108.[19] Elle réitère le principe énoncé dans l'affaire *Leander* selon lequel tant la mémorisation par une autorité publique de données relatives à la vie privée d'un individu que leur utilisation et le refus d'accorder la faculté de les réfuter constituent une ingérence dans le droit au respect de sa vie privée. Dans l'affaire *Amann c. Suisse,* la Cour relève que l'établissement et la conservation d'une fiche contenant des données relatives à la vie privée d'un individu par une autorité publique, représentent une ingérence dans le droit au respect de la vie privée du requérant sans qu'il lui soit nécessaire de spéculer sur le caractère sensible ou non des éléments recueillis.[20]

La CouEDH a récemment reconnu dans l'affaire *K.U. c. Finlande* que les législateurs nationaux ont le devoir de prévoir un cadre permettant de concilier la confidentialité des services internet avec la défense de l'ordre, la prévention des infractions pénales et la protection des droits et libertés d'autrui. Étant donné qu'un tel cadre n'était pas encore en place au moment des faits, la Cour a considéré que la Finlande, dans cette affaire où le respect de la confidentialité l'a emporté sur le bien-être physique et moral du requérant, a ainsi manqué à protéger le droit de l'intéressé au respect de sa vie privée. Partant, la Cour conclut à la violation de l'article 8.[21] Par ailleurs, dans l'affaire *S. et Marper c. Royaume-Uni,* la CouEDH a statué sur la légalité de la conservation par les autorités britanniques des empreintes digitales, échantillons cellulaires et profils ADN des requérants après la conclusion, respectivement par un acquittement et par une décision de classement sans suite, des poursuites pénales menées contre eux alors que les requérants avaient demandé leur destruction. La CouEDH note que les échantillons cellulaires contiennent beaucoup d'informations sensibles sur un individu et conclut donc que la conservation tant des échantillons cellulaires que des profils ADN des requérants équivaut à une atteinte au droit de ces derniers au respect de leur vie privée au sens de l'article 8, paragraphe 1, de la Convention. Elle observe que la protection offerte par l'article 8 de la Convention serait affaiblie de manière inacceptable si l'usage des techniques scientifiques modernes dans le système de la justice pénale était autorisé à n'importe quel prix et sans une mise en balance attentive des avantages pouvant résulter d'un large recours à ces techniques, d'une part, et des intérêts essentiels s'attachant à la protection de la vie privée, d'autre part.[22]

Dans trois affaires françaises de 2009, tout en réaffirmant le rôle fondamental de la protection des données personnelles soumises à un traitement automatique, surtout à des fins policières, la Cour a conclu que l'inscription des requérants au Fichier judiciaire national automatisé des auteurs d'infractions sexuelles, telle qu'elle leur avait été appliquée, n'était pas contraire à l'article 8.[23]

15 *X et Y c. Pays-Bas*, arrêt du 26 mars 1985, paragraphe 23.
16 *M.S. c. Suède* (requête n° 20837/92), arrêt du 27 août 1997.
17 *Leander c. Suède,* arrêt du 26 mars 1987, paragraphe 48.
18 *Z. c. Finlande*, arrêt du 25 février 1997, paragraphe 95.
19 *Rotaru c. Roumanie*, arrêt du 4 mai 2000, paragraphe 43.
20 *Amann c. Suisse*, arrêt du 16 février 2000, paragraphe 70.
21 *K.U. c. Finlande*, arrêt du 2 décembre 2008.
22 *S. et Marper c. Royaume-Uni*, arrêt du 4 décembre 2008.
23 *Bouchacourt c. France, Gardel c. France, et M.B. c. France*, arrêts du 17 décembre 2009 (non finaux).

3 La protection des données dans le droit de l'UE

La protection des données à caractère personnel est reconnue dans le droit primaire de l'UE en tant que droit fondamental autonome, lié au droit au respect de la vie privée et familiale mais distinct de ce dernier. Selon l'article 8 de la Charte des droits fondamentaux de l'UE : « 1. Toute personne a droit à la protection des données à caractère personnel la concernant. 2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification. 3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante. »[24] Conformément à l'article 6 du Traité sur l'Union européenne (TUE), la Charte des droits fondamentaux de l'UE a « la même valeur juridique que les traités ».

Dans la directive 95/46/CE de l'UE relative à la protection des données, les données à caractère personnel sont définies comme « toute information concernant une personne physique identifiée ou identifiable (personne concernée) ; est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale ».[25]

En traitant la protection des données à caractère personnel en tant que droit autonome, la Charte des droits fondamentaux de l'UE se distingue des autres textes internationaux sur les droits de l'homme qui, pour la plupart, ne mentionnent pas spécifiquement un droit à la protection des données et la considèrent essentiellement comme une extension du droit au respect de la vie privée.

3.1. La protection des données dans l'ancien pilier communautaire

Le régime de protection des données de l'UE a été profondément influencé par l'ancienne structure de division en piliers de l'UE, qui a été aboli par le Traité de Lisbonne. Dans chaque pilier, la protection des données était structurée autour d'ensembles distincts d'instruments. L'ancienne division en pilier suscitait des incertitudes quant aux instruments applicables à des cas spécifiques de traitement des données.

Le principal objectif de l'ancien premier pilier de l'UE, à savoir l'ancien pilier communautaire, est de garantir la libre circulation des données à caractère personnel entre les États membres, dans le fonctionnement du marché intérieur, tout en protégeant les droits fondamentaux des personnes physiques et en particulier leur droit au respect de la vie privée dans le cadre du traitement des données à caractère personnel. La protection des données à caractère personnel n'exige pas simplement que les institutions de l'UE ou les organes des États membres s'abstiennent de toute interférence illégale dans les données personnelles. Il existe également une obligation positive de garantir la protection des données à caractère personnel.

La directive 95/46/CE 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 (ci-après, la directive relative à la protection des données) constitue le principal instrument communautaire en la matière.[26] D'après la Cour de justice de l'Union européenne (CJUE), la directive relative à la protection des données « reprend, au niveau communautaire, les principes généraux qui faisaient déjà partie, en la matière, du droit des États membres. »[27] Le régime communautaire de protection des données est basé sur les principes fondamentaux suivants établis dans la directive relative à la protection des données : les données à caractère personnel doivent être (i) traitées loyalement et licitement (ii) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités ; (iii) adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées. Les données doivent également être exactes et, si nécessaire, mises à jour ; (iv) les données à caractère personnel ne peuvent être traitées licitement que si certains critères de traitement définis dans la directive sont satisfaits (entre autres, que la personne concernée a explicitement donné son consentement). En cas de non-respect des droits des personnes concernées, ces personnes disposent d'un recours juridictionnel qui leur donne un droit d'accès aux données les concernant et de rectification de ces données ; (v) les transferts de données à caractère personnel à destination de pays tiers ne sont autorisés que si ces pays assurent un niveau de protection adéquat ; et (vi) l'UE et ses États membres doivent prévoir qu'une ou plusieurs autorités indépendantes sont chargées de surveiller l'application des dispositions relatives aux données à caractère personnel.

La directive relative à la protection des données s'applique à « toute opération ou ensemble d'opérations [...] appliquées à des données à caractère personnel », désignées « traitement » de données. Conformément à l'article 3, paragraphe 1, elle s'applique « au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier ». L'article 3, paragraphe 2, définit les deux domaines dans lesquels la directive ne s'applique pas. Premièrement le traitement de données à caractère personnel « mis en œuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire, telles que celles prévues aux titres V et VI du Traité sur l'Union européenne, et, en tout état de cause, aux traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État (y compris le bien-être économique de l'État lorsque ces traitements sont liés à des questions de sûreté de l'État) et les activités de l'État relatives à des domaines du droit pénal ». Deuxièmement, le traitement des données « effectué par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques » n'entre pas non plus dans le champ d'application de cette directive.

24 Pour un commentaire sur l'article 8 de la Charte, voir : *Commentary of the Charter of Fundamental Rights of the EU*, Réseau UE d'experts indépendants en matière de droits fondamentaux, juin 2006, p. 90, disponible à l'adresse : http://ec.europa.eu/justice_home/doc_centre/rights/charter/docs/network_commentary_final %20_180706.pdf.

25 Article 2, point a de la directive 95/46/CE relative à la protection des données de l'UE.

26 JO L 281 du 23.11.1995, p. 31.

27 Affaire C-369/98, *The Queen c. Minister of Agriculture, Fisheries & Food ex parte: Trevor Robert Fisher et Penny Fischer* [2000] Rec. n° I-06751, paragraphe 34.

On citera une autre mesure législative communautaire importante, la directive 2002/58/CE[28] 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 »). Elle vise à harmoniser les différentes dispositions des États membres relatives à la protection du droit à la vie privée, en ce qui concerne le traitement des données à caractère personnel dans le secteur des communications électroniques, tout en garantissant la libre circulation de ces données et des équipements et des services de communications électroniques. La directive 2002/58/CE précise et complète la directive 95/46/CE au sujet du traitement des données à caractère personnel de personnes physiques dans le secteur des communications électroniques et prévoit la protection des intérêts légitimes des abonnés qui sont des personnes morales. Cette directive ne s'applique pas aux activités qui ne relèvent pas du Traité instituant la Communauté européenne.

Les directives 95/46/CE et 2002/58/CE s'adressent aux États membres et ne s'appliquent donc pas en tant que telles aux institutions et organes de l'UE. La protection des données à caractère personnel est également un droit résultant des traités dans la mesure où l'article 16 du Traité sur le fonctionnement de l'Union européenne établit les règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, qui sont applicables aux institutions de l'UE elles-mêmes. Le règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 a été adopté à partir de l'ancien article 286 du Traité CE remplacé par l'article 16 du Traité sur le fonctionnement de l'Union européenne concernant 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.[29] Le règlement a pour objectif la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel. Il s'applique au traitement de ces données à caractère personnel par toutes les institutions et tous les organes de l'UE, dans la mesure où ce traitement est mis en œuvre pour l'exercice d'activités qui relèvent en tout ou en partie du champ d'application du droit communautaire. Ce règlement a institué le contrôleur européen de la protection des données (CEPD) en 2004.

Le CEPD est une autorité de contrôle indépendante dont l'objectif est de protéger les données à caractère personnel et la vie privée, et de promouvoir les pratiques encourageantes dans les institutions et organes de l'UE. À cet effet, le CEPD contrôle les traitements de données à caractère personnel effectués par l'administration de l'UE, donne des conseils sur les politiques et les textes législatifs qui touchent à la vie privée et coopère avec les autorités de même nature afin de garantir une protection des données qui soit cohérente. La mission de contrôle consiste à vérifier que les institutions et organes de l'UE traitent licitement les données à caractère personnel des fonctionnaires et autres agents de l'UE. Chaque institution ou organe devrait disposer d'un délégué à la protection des données (DPD). Celui-ci tient un registre des traitements et notifie au CEPD les traitements présentant des risques particuliers. Le CEPD effectue alors des contrôles préalables afin de vérifier si ces traitements respectent les obligations en matière de protection des données. En outre, il reçoit les réclamations et effectue des enquêtes. Ainsi, le CEPD veille au respect du règlement (CE) n° 45/2001 concernant la protection des données. Le CEPD conseille la Commission européenne, le Parlement européen et le Conseil pour les propositions de nouveaux textes législatifs et pour toute une série d'autres questions ayant une incidence sur la protection des données. Le CEPD coopère avec d'autres autorités chargées de la protection des données afin de promouvoir une protection des données qui soit cohérente dans toute l'Europe. L'instance centrale de coopération avec les autorités nationales de contrôle est le Groupe de l'article 29.[30]

La directive 2006/24/CE est une mesure récente 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 (« directive sur la conservation des données »)[31]. Cette directive a pour objectif d'harmoniser les dispositions des États membres relatives aux obligations des fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications en matière de conservation de certaines données qui sont générées ou traitées par ces fournisseurs. Cela garantit la disponibilité de ces données à des fins de recherche, de détection et de poursuite d'infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne.

La CJUE a interprété la directive 95/46/CE dans de nombreux arrêts. La Cour a été invitée à répondre à une première série de questions concernant le champ d'application de cette directive. Dans l'affaire *Österreichischer Rundfunk,* la Cour devait décider si la directive relative à la protection des données était applicable à toutes les activités de contrôle exercées par la Cour des comptes autrichienne à l'égard des salaires versés aux salariés de certaines entités.[32] La CJUE a considéré que la directive était applicable. Selon la Cour « puisque toute donnée à caractère personnel est susceptible de circuler entre les États membres, la directive 95/46 impose en principe le respect des règles de protection de telles données à l'égard de tout traitement de ces dernières tel que défini à son article 3 ». Dans le même sens, dans l'affaire *Satakunnan Markkinapörssi et Satamedia,* la Cour a considéré que les activités de traitement de données à caractère personnel concernant des fichiers des autorités publiques contenant des données à caractère personnel qui ne comprennent que des informations déjà publiées telles quelles dans les médias, relèvent du champ d'application de la directive 95/46.[33]

L'interprétation de certaines dispositions spécifiques de la directive a donné lieu à une deuxième série de problèmes juridiques. Dans l'affaire *Lindqvist*, la CJUE a statué sur la question du traitement des données à caractère personnel sur l'internet.[34] L'opération consistant à faire

28 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 L201 du 31.07.2002, p.37.

29 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 L 8 du 12.1.2001, p. 1-22.

30 Ce groupe de travail est basé sur l'article 29 de la directive 95/46/CE relative à la protection des données. Voir : http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm.

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

32 Affaires jointes C-465/00, C-138/01 et C-139/01, *Österreichischer Rundfunk,* Arrêt du 20 mai 2003, cour plénière, [2003] Rec. I-4989.

33 *Satakunnan Markkinapörssi et Satamedia,* C-73/07, arrêt du 16 décembre 2008.

34 *Bodil Lindqvist* [2003], C-101/01, Rec. I-12971.

figurer ces informations sur une page internet constitue un « traitement de données à caractère personnel, automatisé en tout ou en partie ». Toutefois, la Cour a considéré qu'il n'existe pas de « transfert vers un pays tiers de données » au sens de l'article 25 de la directive 95/46 lorsque des données à caractère personnel sont chargées sur un site internet. Enfin, la Cour a récemment rendu un arrêt très important concernant le principe de non-discrimination en matière de protection des données à caractère personnel dans le cadre de la citoyenneté européenne.[35] La CJUE a considéré que la différence de traitement entre les ressortissants de l'État membre et d'autres citoyens de l'UE, induite par le traitement systématique des données à caractère personnel relatives aux seuls citoyens de l'UE non-ressortissants de l'État membre concerné dans un objectif de lutte contre la criminalité, constitue une discrimination prohibée par l'article 12, paragraphe 1, CE.

La Cour a procédé à un exercice de mise en balance entre le droit au respect de la vie privée et à la protection des données et d'autres droits et libertés fondamentaux protégés par l'ordre juridique communautaire. Elle s'est révélée très attentive dans les affaires concernant la liberté d'expression, et tout particulièrement le journalisme, où elle semble disposée à accepter une exception à la protection des données dans ce cadre. En revanche, la Cour a choisi de ne pas donner de réponse claire en cas de conflit entre le droit à la protection des données et la protection de la propriété intellectuelle.

Dans l'affaire *Lindqvist,*[36] la CJUE a dû trouver un équilibre entre le droit à la protection des données et la liberté d'expression consacrée notamment à l'article 10 de la CEDH et protégée au sein de l'ordre juridique communautaire en tant que principe général du droit de l'Union européenne. La Cour note que « les droits fondamentaux revêtent une importance particulière, ainsi que le démontre l'affaire au principal où il est en substance nécessaire de mettre en balance, d'une part, la liberté d'expression de M^me^ Lindqvist dans le cadre de son travail comme formatrice de communiants ainsi que la liberté d'exercer des activités contribuant à la vie religieuse et, d'autre part, la protection de la vie privée des personnes à propos desquelles Mme Lindqvist a fait figurer des données sur son site internet ». Dans l'affaire *Satakunnan Markkinapörssi et Satamedia,*[37] la CJUE a été invitée à interpréter l'article 9 de la directive relative à la protection des données qui dispose que les États membres prévoient des exemptions et dérogations pour les traitements de données à caractère personnel « effectués aux seules fins de journalisme ou d'expression artistique ou littéraire,[…] 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 ». Plus précisément, Markkinapörssi a collecté auprès des autorités fiscales finlandaises des données publiques afin d'éditer, chaque année, des extraits de ces données dans les éditions régionales du journal Veropörssi et a cédé ces mêmes données à Satamedia en vue de leur diffusion par un système de SMS. La CJUE note l'importance que détient la liberté d'expression dans toute société démocratique et indique qu'il convient d'interpréter les notions y afférentes, dont celle de journalisme, de manière large. Elle précise ensuite que des activités impliquant le traitement de données provenant de documents publics selon la législation nationale, peuvent être qualifiées d'« activités de journalisme », si elles ont pour finalité « la divulgation au public d'informations, d'opinions ou d'idées, sous quelque moyen de transmission que ce soit ». Par ailleurs, la Cour considère que ces activités ne sont pas réservées aux entreprises de média et peuvent être liées à un but lucratif.

La CJUE a traité des questions similaires dans l'affaire *Promusicae.*[38] Elle constate que « la directive 2002/58 n'exclut pas la possibilité, pour les États membres, de prévoir l'obligation de divulguer, dans le cadre d'une procédure civile, des données à caractère personnel » et que la législation relative à la protection de la propriété intellectuelle n'impose pas « aux États membres de prévoir [...] l'obligation de communiquer des données à caractère personnel en vue d'assurer la protection effective du droit d'auteur dans le cadre d'une procédure civile ». Elle conclut à « 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 ».

3.2. La protection des données dans les anciens second et troisième piliers de l'UE

La protection des données à caractère personnel dans le cadre d'activités allant au-delà du champ de l'ancien premier pilier reste source de grandes incertitudes et de lacunes. Bien que le traitement des données à caractère personnel dans le cadre des anciens deuxième et troisième piliers doive respecter les règles fondamentales relatives à la protection des données, un cadre juridique global sur la protection des données à caractère personnel au sein de ces anciens deuxième et troisième piliers fait toujours défaut. En lieu et place, la protection des données est disséminée dans tout un éventail de règles *ad hoc* dans différents instruments sur le traitement des données à caractère personnel dans le cadre, par exemple, de la coopération judiciaire et policière en matière pénale.[39] De plus, un certain nombre de problèmes structurels et d'anomalies liés aux anciens deuxième et troisième piliers sont venus limiter encore davantage les possibilités d'une protection effective des droits fondamentaux. Premièrement, l'ancien troisième pilier a pâti d'anomalies en termes de contrôle démocratique. Le Parlement européen avait essentiellement un rôle consultatif et le Conseil pouvait choisir d'ignorer ses avis s'il le souhaitait. Par ailleurs, la Commission et les États membres se partageaient le droit d'initiative, et la règle de l'unanimité s'appliquait à ce pilier anciennement intergouvernemental. Deuxièmement, le contrôle juridictionnel de la Cour de justice au sein de l'ancien troisième pilier était également limité. Conformément à l'ancien article 35, paragraphe 1, TUE, la Cour de justice était compétente pour statuer à titre préjudiciel sur la validité et l'interprétation des décisions-cadres et des décisions, sur l'interprétation des conventions établies en vertu du présent titre, ainsi que sur la validité et l'interprétation de leurs mesures d'application. Cette compétence était

35 *Huber c. Bundesrepublic Deutschland,* C-524/06, arrêt du 16 décembre 2008.
36 *Bodil Lindqvist* [2003] Rec. I-12971, C-101/01.
37 *Satakunnan Markkinapörssi et Satamedia,* C 73/07, arrêt du 16 décembre 2008.
38 *Productores de Música de España (Promusicae) c. Telefónica de España SAU,* C 275/06, arrêt du 29 janvier 2008.
39 Concernant la protection des données à caractère personnel dans le contexte du titre VI TUE (ledit pilier III), voir par exemple, la Convention d'application de l'accord de Schengen de 1990 comprenant des dispositions spécifiques sur la protection des données applicables au Système d'Information Schengen, JO L 239, 22.9.2000, p. 19 ; la Convention Europol de 1995 et, entre autres, les règles relatives à la transmission de données à caractère personnel par Europol à des États et des instances tierces, JO C 316, 27.11.1995, p. 2 ; la décision instituant Eurojust de 2002, JO L 63, 6.3.2002, p. 1 et les dispositions du règlement intérieur d'Eurojust relatives au traitement et à la protection des données à caractère personnel, JO C 68, 19.3.2005, p. 1 ; la Convention sur l'emploi de l'informatique dans le domaine des douanes de 1995, y compris les dispositions relatives à la protection des données à caractère personnel applicables au système d'information des douanes, JO C 316, 27.11.1995, p. 34 ; et la Convention relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne de 2000, notamment article 23, JO C 197, 12.7.2000, p. 1 et 15.

soumise à l'approbation des États membres qui pouvaient limiter encore la possibilité de demander une décision préjudicielle à certaines cours et tribunaux nationaux. Troisièmement, le rôle consultatif des autorités chargées de la protection des données, tel le contrôleur de la protection des données, était également limité par rapport au premier pilier. Par exemple, même si la Commission européenne confirme qu'elle s'estime tenue de consulter le contrôleur européen de la protection des données lorsqu'elle adopte une proposition de législation pouvant avoir un impact sur la protection des données à caractère personnel (comme elle en a l'obligation en vertu de l'article 28, paragraphe 2, du règlement 45/2001), elle partageait son droit d'initiative dans le cadre du troisième pilier avec les États membres qui n'étaient pas tenus de respecter cette obligation. Au sein du deuxième pilier, la situation était encore pire car il n'existait aucune possibilité de contrôle juridictionnel dans le cadre de la politique étrangère et de sécurité commune.

Au cours de ces dernières années, l'échange de données à caractère personnel entre les services répressifs dans les différents États membres est devenu une pratique courante dans le cadre de la coopération policière et judiciaire. À cet égard, le « programme de La Haye » adopté le 5 novembre 2004 en réponse à la « guerre contre le terrorisme » comprenait le « principe de disponibilité » selon lequel les informations dont disposent certains services dans un État membre doivent également être mises à disposition des services équivalents dans d'autres États membres. Le « principe de disponibilité » a des implications importantes pour la protection des données à caractère personnel, et des garanties adéquates étaient nécessaires et le demeurent.

Sur cette toile de fond, la décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale[40] était particulièrement la bienvenue. Cette décision constitue le premier instrument horizontal sur la protection des données dans le domaine des données à caractère personnel utilisées par la police et les autorités judiciaires. Cette décision-cadre est applicable aux échanges transfrontaliers de données à caractère personnel dans le cadre de la coopération policière et judiciaire. Ce texte regroupe les règles applicables aux transferts de données à caractère personnel à des États tiers et à la transmission à des personnes privées dans les États membres. La décision permet également aux États membres de l'UE de prévoir des garanties pour la protection des données à caractère personnel plus rigoureuses que celles établies par elle. Toutefois, elle ne peut assurer à elle seule que les garanties du droit au respect de la vie privée et de la protection des données à caractère personnel soient entièrement respectées dans le traitement des données à caractère personnel dans le cadre des deuxième et troisième piliers. Son champ d'application ne couvrant que *les flux transfrontaliers de données entre services répressifs des États membres*, elle ne s'applique pas au traitement des données par les services répressifs au sein de chaque État membre. La décision-cadre doit être mise en œuvre par les États membres d'ici le 27 novembre 2010, en prenant les mesures nécessaires, y compris la désignation d'une ou plusieurs autorités publiques chargées de conseiller et de surveiller son application sur leur territoire.

La protection des données à caractère personnel était également l'un des domaines de l'ancienne structure en piliers de l'UE qui a constamment donné lieu à des avis divergents pour déterminer quel traitement relevait de quel pilier. L'arrêt de la CJUE sur les dossiers des passagers aériens[41] illustre les problèmes découlant de l'ancienne division par piliers pour le régime de protection des données de l'UE. Ces affaires portaient sur l'accord conclu entre les États-Unis et l'UE concernant le transfert des données contenues dans les systèmes informatiques de réservation/contrôle des départs des compagnies aériennes assurant un service à destination ou au départ des États-Unis, désignées « *Passenger Name Records* » (données PNR). Suite à une décision d'adéquation adoptée par la Commission le 14 mai 2004 conformément à l'article 25 de la directive relative à la protection des données, le Conseil a adopté le 17 mai 2004 une décision concernant la conclusion de l'accord avec les États-Unis d'Amérique. Le Parlement européen a entamé une action devant la Cour demandant l'annulation de la décision d'adéquation de la Commission et de la décision du Conseil sur la conclusion de l'accord, en invoquant entre autres une violation des principes essentiels de la directive relative à la protection des données et du droit à la vie privée. La Cour a annulé la décision d'adéquation au seul motif que son contenu ne relevait pas du champ d'application matériel de la directive relative à la protection des données. Elle a considéré que le transfert des données PNR constituait un traitement ayant pour objet «la sécurité publique et les activités de l'État relatives à des domaines du droit pénal» comme il a été dit à l'article 3, paragraphe 2, de la directive 95/46, et que la décision d'adéquation ne pouvait donc être adoptée en vertu de cette directive. De même, la CJUE a annulé la décision du Conseil sur la conclusion de l'accord, considérant que l'article 95 CE ne pouvait constituer une base juridique appropriée de la décision car il « vise le même transfert de données que la décision d'adéquation et donc des traitements de données qui sont exclus du champ d'application de la directive », et la Communauté n'avait donc pas la compétence pour conclure l'accord. En se traduisant par le transfert de l'accord PNR de l'ancien premier pilier à l'ancien troisième pilier, avec des conséquences significatives concernant le contrôle juridictionnel et le contrôle démocratique, l'arrêt de la Cour a créé « une lacune dans le droit à la protection des données »[42] des personnes physiques. Plus important, suite à la décision de la CJUE, l'UE a dû négocier et conclure un nouvel accord avec les États-Unis basé cette fois sur une base juridique correcte. En 2007, la Commission a introduit une proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers PNR à des fins répressives.[43] La FRA a été invitée par la présidence française à émettre un avis sur cette proposition, qu'elle a présenté le 28 octobre 2008.[44] La FRA a estimé que la valeur ajoutée et la nécessité de la proposition concernant l'utilisation des PNR devaient être expliquées, que les termes vagues devaient être évités et qu'il était nécessaire d'établir des garanties procédurales suffisantes. L'agence a également suggéré que le profilage ethnique discriminatoire soit interdit explicitement.

Dans l'affaire *Irlande c. Parlement européen et Conseil de l'Union européenne*, la CJUE a été invitée à nouveau à se prononcer sur le problème de la division en piliers du régime communautaire de la protection des données.[45] Plus précisément, l'Irlande a demandé l'annulation de la directive 2006/24/CE sur la conservation de données générées ou traitées dans le cadre de la

40 Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, JO L 350, 30.12.2008, p. 60.

41 *Parlement européen c. Conseil de l'Union européenne et Commission des Communautés européennes,* Affaires jointes C-317/04 et C-318/04, arrêt de Grande chambre du 30 mai 2006, [2006] Rec. I-4721.

42 E. Guild et E. Brouwer (2006), *The Political Life of Data - The ECJ decision on the PNR Agreement between the EU and the US,* Centre for European Policy Studies, n° 109.

43 COM(2007) 65.

44 http://fra.europa.eu/fraWebsite/attachments/FRA_opinion_PNR_en.pdf.

45 *Irlande c. Parlement européen et Conseil de l'Union européenne,* C-301/06, arrêt de Grande chambre du 10 février 2009.

fourniture de services de communications électroniques au motif que l'article 95 CE n'était pas une base juridique appropriée pour cette mesure législative, car son objectif principal est de faciliter la recherche, la détection et la poursuite d'infractions pénales, y compris en matière de terrorisme et qu'elle aurait donc dû être adoptée dans le cadre du troisième pilier. La Cour ne partage pas cette opinion et considère que la directive a été adoptée sur le fondement d'une base juridique appropriée, étant donné que tant le but que le contenu de cet acte relèvent de l'article 95 CE. La CJUE fait une distinction entre l'affaire *Irlande c. Parlement européen et Conseil de l'Union européenne* et l'arrêt PNR car la directive 2006/24 vise les activités des fournisseurs de services dans le marché intérieur et ne comporte aucune réglementation des activités des pouvoirs publics à des fins répressives comme cela était le cas dans l'affaire *PNR*. Toutefois, la Cour indique expressément que le recours formé par l'Irlande (et donc son arrêt) « porte uniquement sur le choix de la base juridique et non pas sur une éventuelle violation des droits fondamentaux découlant des ingérences dans l'exercice du droit au respect de la vie privée que la directive 2006/24 comporte ».[46] Des doutes ont été émis concernant la conformité de cette directive avec les droits fondamentaux dans certains États membres. En Roumanie, par exemple, un tribunal a saisi la Cour constitutionnelle concernant le caractère non constitutionnel de la loi roumaine sur la conservation des données dans le contexte d'une affaire portée par une ONG contre une société de télécommunications concernant la protection de la vie privée.[47] Le 8 octobre 2009, la Cour constitutionnelle roumaine a déclaré que la loi appliquant la directive sur la conservation des données était contraire à la constitution et violait les droits fondamentaux à la vie privée.[48] Le raisonnement de la cour concerne non seulement la législation de mise en œuvre roumaine, mais conteste également la compatibilité de la directive elle-même avec les droits fondamentaux. En Allemagne, un arrêt contestant la compatibilité de la législation allemande transposant la directive sur la conservation des données avec les droits fondamentaux est actuellement en instance devant la cour constitutionnelle fédérale. La cour a rendu une injonction provisoire qui prévoit la suspension partielle de la législation de mise en œuvre jusqu'à ce qu'une décision finale soit prise.[49] Le 2 mars 2010, la Cour constitutionnelle fédérale allemande a déclaré que la législation allemande transposant la directive de l'UE sur la conservation des données était contraire à la constitution.[50] Dans ce contexte, il pourrait être utile que l'Union européenne examine la conformité de la directive 2006/24/CE de l'UE sur la conservation des données avec les droits fondamentaux de sa propre initiative à la lumière des nouvelles normes en matière de droits fondamentaux du Traité de Lisbonne (voir section 3.3). Un nouvel arrêt de la CJUE concernant la conformité de cette directive avec les droits fondamentaux serait souhaitable dans ce contexte pour garantir une certitude juridique dans tous les États membres de l'UE.

46 *Irlande c. Parlement européen et Conseil de l'Union européenne*, paragraphe 57.

47 www.mondonews.ro/Legea-298-de-stocare-a-datelor-telefonice-ajunge-la-CCR+id-5439.html.

48 Roumanie, Curtea Constituțională, arrêt nº 1258 du 8 octobre 2009 du 8 octobre. Disponible à l'adresse : www.legi-internet.ro/fileadmin/editor_folder/pdf/Decizie_curtea_constitutionala_pastrarea_datelor_de_trafic.pdf.

49 Cour constitutionnelle allemande, communiqué de presse nº 37/2008 du 19 mars 2008

50 Dans sa décision du 2 mars 2010, la Cour constitutionnelle allemande (*1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, Urteil vom 2. März 2010*) a estimé que la loi transposant la directive sur la conservation des données en Allemagne était contraire à la constitution pour le motif que les obligations qu'elle impose sont disproportionnées. En particulier, la cour a considéré que la section 113 de la loi sur les télécommunications ne garantit pas la sécurité des données stockées, qu'elle manque de transparence car elle impose une utilisation directe des données pour l'investigation, la détection et la poursuite de diverses infractions qui ne sont pas précisées clairement et que la protection juridique qu'elle offre au sujet des données n'est pas compatible avec les exigences de la constitution allemande, www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011.html.

La principale limitation à laquelle se heurte actuellement l'UE dans les efforts pour prévoir une protection efficace et complète des données résulte de l'ancienne architecture constitutionnelle des piliers de l'UE. Bien que la protection des données soit très poussée dans l'ancien premier pilier de l'UE, le régime de protection des données établi dans l'ancien troisième pilier ne peut être jugé satisfaisant. Et pourtant, l'ancien troisième pilier englobe des domaines comme la coopération policière, la lutte contre le terrorisme et les questions de droit pénal où la protection des données revêt une importance cruciale.

3.3. Le Traité de Lisbonne

Dans le contexte du droit fondamental à la protection des données à caractère personnel, le Traité de Lisbonne constitue un progrès important pour l'UE car il contient un certain nombre d'améliorations importantes dans ce domaine à l'échelle européenne. La première avancée majeure est que le Traité de Lisbonne confère un statut légal contraignant à la Charte des droits fondamentaux. L'article 8 de la Charte concernant la protection des données à caractère personnel pourra désormais jouer un rôle allant bien au-delà de la proclamation officielle et symbolique d'un droit fondamental. La reconnaissance de la protection des données en tant que droit fondamental autonome ayant une validité juridique pleine et entière et s'inscrivant dans le droit primaire de l'UE permettra de rehausser son importance lorsqu'elle est opposée à d'autres valeurs et intérêts (par exemple, les intérêts en matière de sécurité ou de marché) et lorsque le législateur européen et la CJUE définissent des priorités. La seconde avancée majeure est l'abolition de l'ancienne «structure en piliers». Cela signifie que les problèmes structurels qui se posaient auparavant pour l'ancien troisième pilier, concernant le processus décisionnel et le contrôle judiciaire, sont à présent résolus dans le cadre du Traité de Lisbonne. Ainsi, le vote à la majorité qualifiée est introduit dans l'espace de liberté, de sécurité et de justice, le rôle du Parlement européen a été renforcé et la CJUE est pleinement compétente dans ce domaine. Toutefois, il convient de noter que des dispositions particulières s'appliqueront au Royaume-Uni et à la Pologne en raison du protocole n° 30 du Traité de Lisbonne qui vise à limiter les effets de la Charte européenne dans le droit britannique et polonais. Une intention semblable de limiter les effets de la Charte de l'UE sur le droit tchèque est à la base du point 2 des conclusions de la présidence des 29 et 30 octobre 2009, dans lequel il est convenu qu'un protocole sera joint aux traités de l'UE prévoyant la modification du protocole n° 30 « de manière à ce que la République tchèque y soit visée dans les mêmes termes que la Pologne et le Royaume–Uni ».[51] La déclaration n° 20 annexée au Traité de Lisbonne indique quant à elle que chaque fois que doivent être adoptées des règles relatives à la protection des données à caractère personnel qui pourraient avoir une incidence directe sur la sécurité nationale, il devra être « dûment tenu compte » des spécificités de la question. La déclaration n° 21 note que des règles spécifiques sur la protection des données à caractère personnel et sur la libre circulation de ces données dans les domaines de la coopération judiciaire en matière pénale et de la coopération policière pourraient s'avérer nécessaires en raison de la « nature spécifique » de ces domaines. La question des effets concrets de ces protocoles et déclarations sur la protection des données à caractère personnel reste discutable et ne pourra être clarifiée avant qu'une jurisprudence de la Cour de justice commence à voir le jour.

51 www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/fr/ec/110889.pdf.

4 Aperçu comparatif

Cette partie centrale du rapport présente un aperçu comparatif des autorités nationales de protection des données, des pratiques nationales qui mettent en œuvre les normes relatives à la protection des données, des recours prévus dans les États membres pour sanctionner et réparer les violations à la législation sur la protection des données et la connaissance des droits relatifs à la protection des données parmi les citoyens de l'UE. Les informations présentées ici s'appuient sur les 27 études nationales produites par les équipes du Fralex (toutes disponibles à titre d'information sur le site de la FRA http://fra.europa.eu) conformément à des lignes directrices communes préparées par l'agence. Le présent rapport comparatif a été élaboré en s'appuyant sur ces études, qui datent de février 2009.

4.1. Autorités de protection des données

Tous les États membres de l'UE, en application des dispositions de l'article 28, paragraphe 1, point 1, de la directive relative à la protection des données, ont accordé à une autorité de contrôle nationale le large mandat de surveiller l'application et garantir le respect, sur leur territoire, de la législation relative à la protection des données. Plusieurs États membres (par exemple, l'Autriche, les Pays-Bas) ont désigné une autorité de protection des données disposant d'une compétence générale et plusieurs autres organes de contrôle spécifiques par secteur (par exemple, santé, poste ou télécommunications, etc.). Certains de ces États organises, caractérisés par une organisation fédérale ou dans lesquels des pouvoirs importants sont détenus au niveau régional (tels que l'Allemagne ou l'Espagne) se sont, quant à eux, dotés d'une entité de contrôle nationale et de plusieurs sous-agences infra-étatiques assurant les mêmes fonctions au niveau régional ou fédéral.[52] Par ailleurs, alors que dans beaucoup de pays (tels que la Roumanie), avant la mise en place des autorités de protection des données, les médiateurs étaient chargés de surveiller le respect des droits à la vie privée, dans certains États membres (comme en Finlande), le médiateur conserve encore une fonction relative à la protection des données à caractère personnel.

La présente section contient un aperçu comparatif. Les pratiques encourageantes appliquées dans ce contexte sont présentées dans la section 6.1.

4.1.1. Indépendance

Les États membres de l'UE se sont efforcés positivement de respecter l'article 28, paragraphe 1, section 2, de la directive relative à la protection des données, selon lequel les États membres garantissent que leurs autorités nationales de contrôle en matière de protection des données exercent en toute indépendance les missions dont elles sont investies. L'interprétation de cette disposition de la directive relative à la protection des données a fait l'objet de conclusions de l'avocat général Mazák. Dans ses conclusions, il indique que le terme « indépendance » est un terme relatif, dès lors qu'il convient de préciser à l'égard de qui ou de quoi et à quel niveau cette indépendance doit exister. Concernant les autorités de contrôle en matière de protection des données, il indique qu'il convient de tenir compte de l'objet de leur existence pour évaluer leur niveau d'indépendance.[53]

Dans plusieurs pays toutefois, différents obstacles d'ordre normatif ou pratique suscitent des préoccupations quant à l'indépendance effective des organes de contrôle nationaux par rapport aux branches politiques du gouvernement. La garantie d'indépendance est en fait principalement assurée par la procédure de nomination et de destitution du personnel des autorités de contrôle en matière de protection des données. Le contrôle des moyens financiers constitue un second point important pour garantir l'autonomie des autorités de contrôle.

Dans un certain nombre d'États membres (par exemple, l'Allemagne et la Slovénie), les délégués des autorités de contrôle en matière de protection des données sont élus par les assemblées législatives, parfois même (comme en Grèce) dans le cadre de procédures exigeant un consensus entre la majorité et l'opposition : à quelques exceptions près (par exemple, en Hongrie, où la pratique constitutionnelle permet aux partis représentés au parlement de se répartir les postes disponibles selon le choix de candidat du parti) cela garantit un niveau élevé d'indépendance des délégués élus. Dans d'autres États membres, au contraire, les délégués à la protection des données sont directement nommés par le gouvernement (par exemple, en Irlande et au Luxembourg) sans intervention de l'opposition parlementaire. Dans plusieurs cas, (par exemple, en Estonie, en Lituanie et au Royaume-Uni[54]) cette situation a suscité d'importantes préoccupations quant à l'indépendance effective des autorités de contrôle en matière de protection des données. Des inquiétudes similaires peuvent naître dans les pays où l'autorité de contrôle est rattachée au Ministère de la Justice (par exemple, au Danemark et en Lettonie). Enfin, d'autres

52 À des fins de comparaison, toutefois, le présent rapport analysera uniquement les autorités de contrôle de la protection des données établies au niveau de l'État. À noter qu'en Allemagne, il existe des autorités similaires chargées de la protection des données au niveau des Länder avec des pouvoirs de contrôle sur la sphère publique et privée. En outre, dans certains Länder, il existe des autorités de contrôle compétentes uniquement dans le domaine privé.

53 Conclusions de l'avocat général Mazák, affaire C-518/07, *Commission européenne c. République fédérale d'Allemagne*, présentées le 22 octobre 2009. La Commission a lancé cette procédure en manquement contre l'Allemagne pour transposition erronée de la directive relative à la protection des données de l'UE dans le secteur privé (manque d'indépendance). La Cour (Grande chambre) a rendu l'arrêt concernant l'affaire C 518/07, *Commission européenne c. République fédérale d'Allemagne*, le 9 mars 2010 et déclare ce qui suit aux points 18 et 19 : « S'agissant, en premier lieu, du libellé de l'article 28, paragraphe 1, second alinéa, de la directive 95/46, dès lors que les termes «en toute indépendance» ne sont pas définis par cette dernière, il convient de tenir compte de leur sens habituel. En matière d'organe public, le terme «indépendance» désigne normalement un statut qui assure à l'organe concerné la possibilité d'agir en toute liberté, à l'abri de toute instruction et de toute pression. Contrairement à la position soutenue par la République fédérale d'Allemagne, rien n'indique que l'exigence d'indépendance concerne exclusivement la relation entre les autorités de contrôle et les organismes soumis à leur contrôle. Au contraire, la notion d'»indépendance» est renforcée par l'adjectif «toute», ce qui implique un pouvoir décisionnel soustrait à toute influence extérieure à l'autorité de contrôle, qu'elle soit directe ou indirecte. »

54 Au Royaume-Uni, depuis 2009, le Parlement a un rôle consultatif, et une audience publique des candidats retenus a lieu devant le *Justice Select Committee* avant leur nomination. Les avis de la commission ne sont pas contraignants mais ils sont généralement pris en compte avant la nomination.

États membres (tels que la Belgique, la France, l'Espagne, le Portugal) ont prévu une procédure mixte pour la désignation des délégués de l'autorité nationale de contrôle en matière de protection des données, impliquant à la fois le pouvoir exécutif, législatif et judiciaire ainsi que d'autres groupes organisés de la société (par exemple, le conseil suprême des universités en Espagne). Dans de tels cas, toutefois, il est essentiel de garantir que le gouvernement ne contrôle pas *de facto*, directement ou indirectement, la majorité des personnes désignées, dénaturant ainsi la finalité même d'une procédure de nomination pluraliste.

Dans un certain nombre d'États membres (en Italie par exemple), les délégués des autorités de contrôle en matière de protection des données ont un mandat de sept ans non renouvelable. Dans certains pays (comme en Pologne et en Slovaquie), les délégués des autorités de contrôle en matière de protection des données peuvent être démis de leurs fonctions de façon anticipée uniquement en cas de mauvaise conduite spécifique et en suivant la même procédure que celle adoptée pour leur désignation. Ces solutions techniques garantissent une grande indépendance des organes de contrôle, en limitant l'influence et les pressions des pouvoirs politiques. Dans d'autres États membres (par exemple l'Irlande), au contraire, le gouvernement peut directement destituer de leurs fonctions les commissaires à la protection des données, ce qui suscite des préoccupations quant à l'indépendance réelle de l'organe de contrôle, notamment concernant la surveillance du respect de la législation relative à la protection des données par les autorités gouvernementales.

L'existence et le mandat de l'autorité indépendante chargée de surveiller le respect de la législation relative à la protection des données sont explicitement établis dans la Constitution, comme au Portugal ou en Grèce, ce qui renforce considérablement l'autonomie de cet organe de contrôle. L'attribution d'une personnalité juridique distincte à l'autorité de contrôle en matière de protection des données (par exemple, en Espagne et à Malte) et la possibilité qui lui est offerte d'entamer des poursuites judiciaires devant la Cour constitutionnelle du pays (par exemple, en Slovénie) constituent d'autres garanties importantes d'indépendance institutionnelle.

4.1.2. Ressources

Dans la plupart des États membres, les autorités de protection des données reçoivent les ressources nécessaires à leur fonctionnement à partir du budget de l'État (par exemple, l'Estonie la France, l'Italie, les Pays-Bas) et souvent à partir du budget alloué au Ministère de la Justice. Dans certains États membres, toutefois, les autorités de contrôle peuvent accroître de façon importante leurs ressources financières grâce aux recettes obtenues des notifications des sous-traitants chargés du traitement des données et/ou des sanctions pécuniaires imposées en cas d'infraction à la législation relative à la protection des données (par exemple, au Luxembourg et à Malte). Au Royaume-Uni, les droits de notification représentent la seule source de revenus de l'autorité de contrôle pour les travaux menés en matière de protection des données.

Dans beaucoup d'États membres (notamment en Autriche, en France, en Italie, au Portugal, et en Roumanie), les études nationales ont souligné que le manque de financement des autorités de contrôle posait un problème. Dans d'autres pays, où l'autorité de protection des données bénéficie actuellement d'un financement relativement adéquat, des coupes budgétaires ont été prévues pour les années à venir (par exemple, au Danemark et en Irlande). Compte tenu des tâches confiées aux agences pour la protection des données tant dans les législations communautaire que nationales, le manque de ressources humaines et financières suffisantes représente un défi majeur pour l'efficacité des systèmes de contrôle nationaux, qui pourrait mettre en danger la protection des droits fondamentaux des personnes concernées. De ce fait, les États membres devraient garantir que les autorités nationales de protection des données disposent de ressources suffisantes pour fonctionner correctement.

4.1.3. Pouvoirs

Les États membres de l'UE devaient investir leur autorité nationale de contrôle des pouvoirs généraux spécifiés dans la directive relative à la protection des données, article 28, paragraphe 2 (pouvoir de conseiller les autorités législatives ou administratives lors de l'élaboration des mesures réglementaires ou administratives relatives à la protection des droits et libertés des personnes à l'égard du traitement de données à caractère personnel), paragraphe 3 (pouvoirs d'investigation, d'intervention et d'ester en justice) et paragraphe 4 (pouvoir d'être saisie d'une demande). Comme le montre la vue d'ensemble ci-après, ces dispositions de la directive relative à la protection des données n'ont toutefois pas été entièrement mises en œuvre dans tous les États membres, et certaines autorités nationales ne disposent de ce fait que d'instruments très limités pour remplir leur mission de contrôle. Il s'agit donc d'un problème qui doit être traité dans les pays concernés.

En règle générale, l'analyse des pouvoirs des différentes autorités nationales de protection des données permet de distinguer deux grandes tendances, qui reflètent les approches suivies par les États membres dans la mise en œuvre de la directive relative à la protection des données. Alors que plusieurs pays (par exemple, la Finlande, la Suède, l'Irlande et le Royaume-Uni) ont souligné le rôle préventif et proactif des agences de contrôle, mettant en exergue leur rôle *ex-ante* pour garantir la protection des données à caractère personnel, d'autres États membres (tels que la Lettonie, la République tchèque et la Grèce) ont donné la priorité aux fonctions d'application et de contrôle *a posteriori* des autorités de protection des données et leur ont confié une mission réactive afin de veiller au respect de la législation relative à la protection des données. La nature des pouvoirs conférés aux organes de contrôle varie en conséquence, avec une préférence pour les instruments de prévention « souples » dans le premier cas et pour des mesures «plus strictes» dans le second. Il est important, néanmoins, de pas trop insister sur ces différences, et certains pays (tels que le Danemark, les Pays-Bas, la Slovénie et l'Italie) ont adopté une position intermédiaire, en attribuant à leur autorité nationale de protection des données, des compétences destinées à aider et à garantir un respect actif de la législation relative à la protection des données, tout en les habilitant dans le même temps à poursuivre et sanctionner les cas d'infraction. Par ailleurs, comme le montrent les quatre prochaines sections, on relève également plusieurs caractéristiques communes à travers ces divergences entre pays.

4.1.3.1. Pouvoirs d'investigation

Conformément à l'article 28, paragraphe 3, section 1, de la directive relative à la protection des données, les autorités de contrôle disposent de pouvoirs d'investigation, tels que le pouvoir d'accéder aux données faisant l'objet d'un traitement et de recueillir toutes les informations nécessaires à l'accomplissement de leur mission de contrôle. Le Tableau 1 indique le degré de mise en œuvre de la disposition ci-dessus dans la législation nationale instituant l'autorité de contrôle en matière de protection des données, en précisant si l'autorité de contrôle est habilitée à : a) demander au sous-traitant/au responsable du traitement des données/à la personne concernée de fournir des informations ou de produire des documents ; b) demander de la part du sous-traitant/responsable du traitement des données d'accéder à des banques de données et des fichiers ; c) mener des perquisitions et des saisies dans les locaux du sous-traitant/responsable du traitement des données sans mandat ; d) mener des perquisitions et des saisies dans les locaux du sous-traitant/responsable du traitement des données après obtention d'un mandat ; e) mener des audits pour contrôler le respect par le sous-traitant/responsable du traitement des données et pour garantir que le traitement des données est mené conformément à la législation en la matière.

Tableau 1 : Pouvoirs d'investigation

État membre	Demander des informations et des documents	Accéder à des banques de données et à des fichiers	Perquisition dans les locaux et saisie sans mandat judiciaire	Perquisition dans les locaux et saisie avec mandat judiciaire	Mener des audits
Allemagne	●	●	●	●*	●
Autriche	●	●	●		●
Belgique	●	●	●		●
Bulgarie	●	●	●		●
Chypre	●	●	●		●
Danemark	●	●	●		●
Espagne	●	●	●		●
Estonie	●	●	●		●
Finlande	●	●	●		●
France	●	●		●	●
Grèce	●	●	●		●
Hongrie	●	●	●		●
Irlande	●	●	●		●
Italie	●	●	●***	●	●
Lettonie	●	●	●		●
Lituanie	●	●	●		●
Luxembourg	●	●	●		●
Malte	●	●		●	●
Pays-Bas	●	●	●		●
Pologne	●	●	●		●
Portugal	●	●	●		●
République tchèque	●	●	●		●
Roumanie	●	●			●
Royaume-Uni	●			●	●***
Slovaquie	●	●	●		●
Slovénie	●	●	●		●
Suède	●	●	●		●

*Notes : * Cette observation est limitée au commissaire fédéral pour la protection des données. Elle ne concerne pas les commissaires pour la protection des données au niveau des Länder, ni les autorités de contrôle dans le domaine privé ;*
*** Normalement, aucun mandat judiciaire n'est nécessaire en Italie, si la perquisition est menée au domicile d'une personne ou dans un autre logement privé avec le consentement de cette personne. Sinon, une autorisation du juge peut être requise ;*
**** L'autorité de protection des données du Royaume-Uni ne peut mener d'audit qu'à la demande du responsable du traitement, et non contre sa volonté. Ce pouvoir ne peut donc être utilisé pour contrôler le respect de la loi.*

Comme l'illustre le Tableau 1, la grande majorité des États membres permettent à leur agence de protection des données de contrôler le respect de la législation relative à la protection des données par les opérateurs privés et publics participant au traitement des données, et plus spécifiquement à auditer les parties intéressées ; mener des examens ; ordonner la fourniture d'informations ; ordonner d'avoir accès aux données et documents professionnels ; et copier les données et documents. Ces pouvoirs peuvent être exercés d'office ou sur demande d'une personne concernée alléguant la violation de ses droits en matière de données à caractère personnel. Dans la grande majorité des États membres, les autorités de contrôle peuvent, dans l'exercice de leurs fonctions, et en vue d'identifier des violations de la législation en matière de protection des données, entrer (au besoin avec l'aide de la police) dans les locaux et dans tout autre lieu où le traitement de données est réalisé, saisir les matériels nécessaires, enquêter et relever des preuves (même sans le consentement des responsables du traitement des données), sans devoir demander au préalable un mandat judiciaire.

4.1.3.2. Pouvoirs d'intervention

Conformément à l'article 28, paragraphe 3, section 1, deuxième tiret, de la directive relative à la protection des données, les autorités de contrôle doivent disposer de pouvoirs effectifs d'intervention, tels que, par exemple, celui de rendre des avis préalablement à la mise en œuvre des traitements de données sensibles, et d'assurer une publication appropriée de ces avis ou celui d'ordonner le verrouillage, l'effacement ou la destruction de données, ou d'interdire temporairement ou définitivement un traitement, ou celui d'adresser un avertissement ou une admonestation au responsable du traitement. Le Tableau 2 suivant présente le degré de mise en œuvre de la disposition ci-dessus dans les différentes législations nationales en précisant si l'autorité de contrôle est habilitée à : a) enregistrer les traitements qui sont notifiés par les responsables du traitement ; b) autoriser les traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées après un contrôle préalable de leur compatibilité avec les spécifications de la législation en matière de protection des données ; c) interrompre les traitements de données à caractère personnel ; d) ordonner l'effacement ou la destruction de données ; e) adresser un avertissement ou une admonestation au responsable du traitement (par exemple, en ordonnant la mise en œuvre de mesures techniques et d'organisation spécifiques en prévention d'infractions à la législation en la matière).

Tableau 2 : Pouvoirs d'intervention

État membre	Enregistrer les traitements	Autoriser les traitements susceptibles de présenter des risques particuliers	Interrompre les traitements	Ordonner l'effacement ou la destruction de données	Adresser un avertissement ou une admonestation au responsable du traitement
Allemagne	●	●	●*		●
Autriche	●	●	●	●	●
Belgique	●	●			
Bulgarie	●	●	●	●	●
Chypre	●		●	●	●
Danemark	●	●	●	●	●
Estonie	●	●	●	●	●
Espagne	●		●	●	●
Finlande	●	●	●	●	●
France	●	●	●	●	●
Grèce	●	●	●	●	●
Hongrie	●	●	●	●	●
Irlande	●	●	●	●	●
Italie	●	●	●	●	●
Lettonie	●		●	●	●
Lituanie	●	●	●	●	●
Luxembourg	●	●	●	●	●
Malte	●	●	●	●	●
Pays-Bas	●	●	●	●	●
Pologne	●	●	●	●	●
Portugal	●	●	●	●	●
République tchèque	●	●	●	●	●
Roumanie	●	●	●	●	●
Royaume-Uni	●		●	●	●
Slovénie	●	●	●	●	●
Slovaquie	●	●	●	●	●
Suède	●	●	●		●

*Note : * Depuis le 1er septembre 2009, les autorités de contrôle ont dans certaines circonstances la possibilité d'interrompre les traitements.*

Le Tableau 2 témoigne d'une certaine convergence entre les autorités de protection des données dans les États membres de l'UE concernant le pouvoir d'intervention. À l'exception du contrôle préalable des traitements des données sensibles, qui n'est pas prévu de droit ou de fait dans certains pays, toutes les autorités de contrôle doivent tenir un registre des notifications des traitements de données. Hormis en Belgique et, en partie, en Allemagne, elles peuvent en outre : ordonner à un responsable privé du traitement des données de cesser un traitement constituant une violation de la loi et rectifier, effacer ou verrouiller des données spécifiques qui sont traitées ; interdire à un responsable privé du traitement des données d'utiliser une procédure spécifique par rapport au traitement des données s'il existe un risque considérable que les données soient traitées en violation de la législation en la matière ; ordonner à un responsable privé du traitement des données de mettre en œuvre des mesures techniques et d'organisation spécifiques afin d'empêcher tout traitement de données illicite, toute destruction ou toute altération accidentelle ou illicite, toute diffusion des données à des personnes non autorisées, tout usage abusif ou toute autre forme de traitement illicite ; et enfin, délivrer des avis d'interdiction ou une injonction de faire à l'encontre des responsables du traitement qui enfreignent la législation en la matière.[55]

4.1.3.3. Pouvoirs d'être saisies d'une demande et d'ester en justice

Conformément à l'article 28, paragraphe 4, section 1, de la directive relative à la protection des données, les autorités de contrôle devraient bénéficier du pouvoir d'être saisies par toute personne, ou par une association les représentant, d'une demande relative à la protection de ses droits et libertés à l'égard du traitement de données à caractère personnel et d'informer la personne concernée des suites données à sa demande. Conformément à l'article 28, paragraphe 3, section 1, troisième tiret, les autorités de protection des données doivent pouvoir ester en justice en cas de violation des dispositions nationales en matière de protection des données ou porter ces violations à la connaissance de l'autorité judiciaire. Enfin, l'article 28, paragraphe 3, section 1, deuxième tiret, permet aux autorités de contrôle de saisir les parlements nationaux ou d'autres institutions politiques. Le Tableau 3 présente le degré de mise en œuvre de la disposition ci-dessus dans les différentes législations nationales en précisant si l'autorité de contrôle est habilitée à : a) entendre et examiner les demandes et réclamations de personnes concernées ; b) porter l'affaire à la connaissance de la police ou des autorités judiciaires ; c) porter directement l'affaire devant les autorités judiciaires en tant que partie à la procédure devant les tribunaux (à savoir, pouvoir d'ester en justice au sens strict) ; d) prendre de son propre chef une décision quant à l'existence ou non d'une violation (avec la possibilité d'infliger une sanction) assurant ainsi une fonction quasi-judiciaire ; et e) saisir le parlement national ou les institutions politiques, notamment en proposant des mesures législatives et réglementaires en vue de modifier la législation correspondante en matière de protection des données pour traiter les problèmes les plus importants découlant de sa demande et refléter l'évolution des techniques informatiques.

55 Cette observation se limite à la compétence des commissaires pour la protection des données au niveau des Länder et/ou aux autorités de contrôle dans le domaine privé et ne concerne pas le commissaire fédéral pour la protection des données.

Tableau 3 : Pouvoirs d'être saisies d'une demande et d'ester en justice

État membre	Entendre et examiner les demandes ou réclamations	Porter l'affaire à la connaissance de la police ou des autorités judiciaires	Porter directement l'affaire devant les autorités judiciaires	Prendre une décision de sa propre initiative concernant le bien-fondé d'une demande	Saisir le parlement national
Allemagne	●	●	●*	●*	●
Autriche	●		●	●	
Belgique	●	●	●	●	●
Bulgarie	●	●	●	●	
Chypre	●	●		●	
Danemark	●	●		●	
Espagne	●	●		●	
Estonie	●			●	●
Finlande	●	●	●	●	●
France	●	●		●	●
Grèce	●	●		●	●
Hongrie	●	●			●
Irlande	●		●		
Italie	●	●		●	●
Lettonie	●		●	●	
Lituanie	●	●		●	●
Luxembourg	●	●	●	●	
Malte	●	●	●	●	●
Pays-Bas	●	●		●	
Pologne	●	●		●	
Portugal	●	●		●	
République tchèque	●	●	●	●	
Roumanie	●	●	●	●	
Royaume-Uni	●	●			
Slovénie	●	●	●	●	
Slovaquie	●	●		●	●
Suède	●	●	●		

*Note : * Cette observation ne concerne pas le commissaire fédéral pour la protection des données en Allemagne, mais les autorités de contrôle au niveau des Länder.*

Le tableau révèle quelques divergences entre les autorités de protection des données des États membres de l'UE. Toutes les autorités de contrôle peuvent être saisies par des parties intéressées alléguant une violation de leurs droits en matière de données à caractère personnel et ont le devoir correspondant de leur apporter une réponse dans un délai donné. Toutefois si, suite à l'examen, la plainte se révèle fondée, seules quelques autorités nationales de protection des données peuvent entamer de façon autonome des poursuites devant un tribunal compétent (notamment pour la Slovénie, devant la Cour constitutionnelle) ou exercer elles-mêmes une fonction quasi-judiciaire en décidant du bien-fondé de l'affaire portée par le requérant (en tant qu'alternative aux tribunaux). Les décisions des autorités de contrôle administratives disposant de pouvoirs quasi-judiciaires peuvent dans tous les cas être révisées par les tribunaux ordinaires : corollaire nécessaire de la règle de droit établie à l'article 28, paragraphe 3, section 2, de la directive relative à la protection des données.

4.1.3.4. Pouvoirs consultatifs

Conformément à l'article 28, paragraphe 2, de la directive relative à la protection des données, les autorités de contrôle sont consultées par les législateurs et administrations nationaux lors de l'élaboration des mesures réglementaires ou administratives relatives à la protection des droits et libertés des personnes à l'égard du traitement de données à caractère personnel. Les finalités mêmes de la directive relative à la protection des données impliquent donc un pouvoir général des autorités de protection des données de donner des avis et d'être consultées par des parties privées concernées par le traitement des données et de fournir des recommandations générales par secteur. Enfin, l'article 25 de la directive relative à la protection des données établit des règles spécifiques sur le transfert de données à caractère personnel vers des pays extérieurs à l'UE (à savoir des pays tiers), avec possibilité d'intervention pour les autorités nationales de contrôle. Le Tableau 4 présente des informations concernant les pouvoirs consultatifs des autorités nationales de contrôle en matière de protection des données, en précisant si elles : a) sont toujours consultées de droit ou de fait par le législateur et/ou les administrations avant d'adopter une législation ou des réglementations ayant trait aux droits individuels en matière de protection des données ; b) peuvent être consultées à la discrétion du législateur et des administrations avant d'adopter une législation ou des réglementations ayant trait aux droits individuels en matière de protection des données ; c) fournissent des avis et des conseils aux parties (par exemple, en les informant de leurs droits et obligations) ; d) soumettent des recommandations et des avis généraux sur la façon d'améliorer la mise en œuvre et le respect de la législation relative à la protection des données dans des secteurs spécifiques (par exemple, en encourageant l'élaboration de codes de conduite) ; e) autorisent le transfert de données à caractère personnel vers des pays tiers.

Tableau 4 : Pouvoirs consultatifs

État membre	Doit être consultée par le législateur ou l'administration	Peut être consultée par le législateur ou l'administration	Fournit des avis et des informations aux parties responsables du traitement des données	Soumet des recommandations et des avis généraux	Autorise le transfert de données à caractère personnel vers des pays tiers
Allemagne	●	●	●	●	●*
Autriche	●		●	●	●
Bulgarie	●		●	●	
Belgique	●	●	●	●	
Chypre	●**		●	●	●
Danemark		●	●	●	●
Espagne	●		●	●	●
Estonie	●		●	●	
Finlande	●	●	●	●	
France	●	●	●	●	●
Grèce	●	●	●	●	●
Hongrie		●	●	●	●***
Irlande		●	●	●	●
Italie	●	●	●	●	●
Lettonie	●		●	●	
Lituanie		●	●	●	●
Luxembourg	●		●	●	●
Malte		●	●	●	●
Pays-Bas	●		●	●	●
Pologne		●	●	●	
Portugal	●		●	●	●
République tchèque		●	●	●	
Roumanie		●	●	●	●
Royaume-Uni		●	●	●	●****
Slovénie		●	●	●	●
Slovaquie		●*****	●	●	●
Suède	●	●	●	●	●

*Notes : * Les autorités de contrôle allemandes peuvent accorder une autorisation, mais cela n'est pas obligatoire ou nécessaire dans tous les cas ;*

*** L'autorité de contrôle en matière de protection des données à Chypre interprète la section 23, point i, de la loi 138(I)/2001 comme accordant un droit d'être consulté des lors qu'un règlement est en discussion. Dans la pratique, le commissaire est invariablement consulté par le législateur et par l'administration des lors que des questions relatives a la protection des données a caractère personnel se posent ;*

*** Certains indices suggèrent que ce pouvoir est limité faute de mise en œuvre efficace ;*

**** Dans la pratique, ce pouvoir semble rarement, voire jamais, utilisé. Voir l'étude thématique nationale sur l'évaluation de mesures de protections des données et des institutions concernées, Royaume-Uni, qui est disponible sur : http://fra.europa.eu ;*

***** En Slovaquie, l'autorité de protection des données est de fait toujours consultée avant l'entrée en vigueur d'une législation affectant la protection des données, même si cela ne constitue pas une obligation légale.*

Comme le montre le Tableau 4, tous les États membres ont habilité leur autorité de contrôle nationale à conseiller des parties privées sur l'application de la législation relative à la protection des données. Les autorités de protection des données disposent également d'un pouvoir quasi-législatif pour élaborer des réglementations générales destinées à des secteurs spécifiques, promouvoir l'élaboration de codes de conduite privés et soumettre des avis et des recommandations à l'attention d'acteurs publics et privés intervenant dans le domaine du traitement des données. La plupart de ces mesures n'ont toutefois aucun caractère juridiquement contraignant. Par ailleurs, beaucoup d'États membres n'accordent à leurs autorités de contrôle qu'une fonction consultative dans le contexte des avis fournis aux pouvoirs législatif et exécutif sur les projets de législation relatifs à la protection des données à caractère personnel. Par conséquent, leurs avis sur les projets de loi et de règlements sont facultatifs, ou (comme en Allemagne, en Autriche, en France, en Grèce, et en Italie) ne sont strictement requis légalement que pour l'élaboration de règlements d'exécution. Cela est regrettable étant donné que les conseils donnés durant la rédaction permettent parfois d'éviter les problèmes à l'avenir. L'absence d'avis des autorités de protection des données avant l'adoption d'une législation ou d'une règlementation qui peuvent avoir un effet négatif sur la protection des données à caractère personnel peut indiquer que l'importance des aspects concernant la protection de la vie privée n'a pas été pleinement appréciée lors de choix politiques. Dans ce cadre, il peut être recommandé que les États membres veillent à une participation plus régulière des autorités de contrôle dans le processus d'élaboration des politiques.

4.1.4. Activités

Les autorités de contrôle des États membres de l'UE participent couramment à toute une série d'activités destinées à évaluer le statut de leur législation nationale en matière de respect de la vie privée mais également à promouvoir la culture de la protection des données à caractère personnel. Premièrement, les autorités de protection des données ont la fonction d'informer le grand public et les institutions de l'État sur les enjeux des droits au respect de la vie privée, les mesures prises par l'autorité de contrôle pour y répondre et les mesures nécessaires pour améliorer leur défense. L'article 28, paragraphe 5, de la directive relative à la protection des données dispose en fait que chaque autorité de contrôle doit établir à intervalles réguliers un rapport sur son activité, qui est ensuite publié. Toutes les autorités de protection des données publient de ce fait un rapport annuel sur la situation de la protection des droits au respect de la vie privée dans leur système juridique national et certaines (par exemple l'Italie) publient également des bulletins mensuels présentant les dernières décisions ou réglementations adoptées. Dans certains pays (par exemple, l'Espagne, la France, l'Italie, et le Royaume-Uni), le rapport annuel est présenté publiquement – parfois devant le législateur – et les médias sont en mesure de couvrir l'événement.

Les autorités de contrôle nationales ont le devoir spécifique de sensibiliser les citoyens de l'UE sur les droits en matière de respect de la vie privée et de données à caractère personnel. Cette mission est particulièrement importante car l'efficacité de la législation relative à la protection des données ne peut être garantie que si les individus connaissent leurs droits fondamentaux et participent activement à leur préservation. Comme nous le verrons plus loin, dans plusieurs États membres, le grand public soit n'a pas connaissance de ses droits (par exemple, à Malte et en Pologne), soit estime que les droits au respect de la vie privée sont bien protégés et qu'il n'est pas véritablement nécessaire d'agir pour améliorer le système (par exemple, au Danemark et en Finlande), soit considère même que d'autres droits, tels que le droit à l'information (par exemple, en Suède), ont plus de poids que les droits en matière de protection des données. Les autorités de protection des données participent donc directement à la sensibilisation. À quelques exceptions près (par exemple, en Bulgarie, en Lituanie, et en Slovaquie), elles proposent un site web convivial spécifique présentant toute la législation pertinente, les avis et les décisions de l'autorité avec des mises à jour régulières. Des conférences, des initiatives et des programmes spéciaux sont également financés par les autorités dans beaucoup de pays (par exemple, aux Pays-Bas et en Slovénie) afin de cibler des segments spécifiques de la population, tels que les étudiants, les salariés, etc.

À l'échelle de l'UE, les autorités nationales de contrôle coopèrent et collaborent dans le cadre du Groupe de protection des personnes à l'égard du traitement des données à caractère personnel établi en vertu de l'article 29, paragraphe 1, section 1, de la directive relative à la protection des données (Groupe de l'article 29). Conformément à l'article 29, paragraphe 2, le groupe se compose du contrôleur européen de la protection des données, d'un représentant de chacune des autorités de contrôle nationales et d'un représentant de la Commission européenne. Ce groupe a un caractère consultatif et indépendant. L'article 30, paragraphe 1, stipule qu'il examine toute question portant sur la mise en œuvre des dispositions nationales prises en application de la directive, en vue de contribuer à leur mise en œuvre homogène ; qu'il donne à la Commission un avis sur le niveau de protection dans la Communauté et dans les pays tiers ; qu'il conseille la Commission sur tout projet de modification de la directive, sur tout projet de mesures additionnelles ou spécifiques à prendre pour sauvegarder les droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel, ainsi que sur tout autre projet de mesures de l'UE ayant une incidence sur ces droits et libertés ; qu'il offre un avis sur les codes de conduite élaborés au niveau de l'UE. Les avis et recommandations du groupe sont généralement pris en considération et cités en référence par les autorités nationales de contrôle en matière de protection des données, et sont particulièrement utiles pour l'élaboration d'une norme européenne sur la protection des données à caractère personnel commune à toutes les autorités nationales de contrôle.[56]

4.2. Respect de la législation

La présente section contient un aperçu comparatif. Les pratiques encourageantes appliquées dans ce contexte sont présentées dans la section 6.2.

4.2.1. Procédures relatives à l'enregistrement et à l'approbation du traitement des données

Conformément à l'article 2 de la directive relative à la protection des données, le « traitement de données à caractère personnel » (ci-après « traitement ») désigne toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des

56 Au Royaume-Uni, les avis et recommandations du groupe ne sont pas considérés comme contraignants par l'autorité britannique de protection des données bien qu'ils soient parfois cités en tant qu'orientations informelles.

données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction. Par ailleurs, les articles 5 à 8 de la directive relative à la protection des données établissent les règles et principes généraux de licéité des traitements de données à caractère personnel, les critères relatifs à la légitimation des traitements de données et les catégories particulières de traitements. À cet égard, les articles 18 à 20 renvoient à l'obligation de notification à l'autorité de contrôle et aux contrôles préalables des traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées.

Les études thématiques nationales ont largement servi de base pour évaluer le respect des normes relatives à la protection des données, telles que les règles concernant les procédures relatives à l'enregistrement et à l'approbation du traitement des données. La plupart d'entre elles comprenaient des données sur le nombre d'enregistrements et d'approbations pour les années 2000-2007. Plusieurs proposaient une analyse et une évaluation qualitative reposant sur ces chiffres ainsi que sur des contacts avec les autorités nationales respectives. Ces données ont servi d'indicateurs pour évaluer le respect de la législation. Parmi les autres indicateurs retenus, on relève la pratique de l'autorité nationale, le degré de conformité avec la législation nationale et les exemples typiques de non-respect de la directive.

La majorité des États membres de l'UE (Allemagne, Autriche, Bulgarie, Chypre, Danemark, Espagne, Estonie, Finlande, Grèce, Irlande, Italie, Lettonie, Lituanie, Luxembourg, Malte, Pays-Bas, Pologne, Portugal, République tchèque, Roumanie, Slovénie, et Suède) ont mis en place un cadre juridique assurant une transposition effective de ces dispositions de la directive relative à la protection des données. On entend par transposition effective le fait que la législation nationale soit, de prime abord, conforme aux dispositions de la directive. La mise en œuvre réelle de la législation nationale est plus ou moins effective selon les États membres et fait l'objet de l'analyse menée dans les prochains paragraphes. D'autre part, des lacunes, qui créent des incohérences entre le système global créé par la directive relative à la protection des données et les dispositions nationales, apparaissent dans la législation de cinq États membres (Belgique, France, Hongrie, Royaume-Uni et Slovaquie). L'évaluation du respect de la législation se révèle toutefois assez problématique. Dans bon nombre de cas, en raison du manque de personnel, les autorités nationales de protection des données ne peuvent fournir un état des lieux systématique et statistique de la situation dans le domaine. Même lorsque des données statistiques existent, leur manque de cohérence et leur insuffisance empêchent de rendre compte fidèlement de la situation. Il a donc été impossible d'évaluer de façon globale agrégée à l'échelle de l'UE le degré de conformité et/ou les domaines problématiques dans la législation ou dans la pratique. Dans le contexte de ce tableau extrêmement incohérent, des exemples manifestes de non-conformité avec la directive tirés des études thématiques nationales sont présentés pour illustrer la nature des problèmes rencontrés.

La Bulgarie a transposé les dispositions appropriées de la directive relative à la protection des données, mais la pratique des responsables du traitement des données à caractère personnel en matière d'enregistrement montre que l'autorité nationale n'était pas prête, dès sa création, à développer suffisamment ses capacités administratives pour accomplir ses missions[57]. L'autorité nationale n'est pas encore en mesure de traiter de façon effective le grand nombre de demandes. Le ratio entre les demandes et les enregistrements est disproportionné dans le sens où le nombre d'enregistrements reste extrêmement faible par rapport au nombre de demandes.[58]

En Pologne, conformément à la loi relative à la protection des données, chaque entité procédant au traitement de données est tenue d'enregistrer un fichier auprès de l'autorité nationale de contrôle qui a des pouvoirs d'investigation limités sur les données traitées par les services spéciaux de l'État (par exemple, les services de renseignement). Les entités qui ne sont pas tenues d'enregistrer les traitements sont néanmoins obligées de satisfaire aux exigences permettant le traitement des données. Le traitement de données sensibles est en règle générale interdit, à quelques exceptions près correspondant largement aux dispositions de la directive relative à la protection des données. Le principal problème identifié est la méconnaissance par les entités de traitement des données de l'obligation d'enregistrement. Dans de nombreux cas, ces entités n'ont pas enregistré les fichiers, tandis que la phase d'enregistrement a donné lieu à de nombreuses erreurs. Le traitement de données sensibles a posé des problèmes dans deux cas significatifs. Le premier concernait la collecte de données sur des enfants roms. Dans cette affaire, l'autorité nationale a ordonné la suppression des données concernant les enfants roms qui étaient traitées sans que ces derniers en aient connaissance et sans leur consentement.[59] La seconde affaire concernait le traitement des données de candidats aux élections issus de différentes minorités nationales et ethniques. L'autorité nationale a ordonné l'arrêt du traitement des données obtenues par des sources non officielles sans le consentement des personnes concernées.[60] Le rapport de 2007 de l'autorité nationale révèle que certains secteurs de l'administration publique n'ont pas respecté les normes relatives à la protection des données.[61] Le secteur de la sécurité publique ne fait état d'aucune lacune particulière dans le domaine de la protection des données et les institutions semblent se conformer à la législation. Les entités assurant le traitement des données dans différents domaines commerciaux, les établissements publics de santé, les banques et les institutions financières, ne respectaient pas entièrement la législation.

La législation grecque a mis en place au départ un système de notification universelle, évitant ainsi toute possibilité d'exceptions ou de simplifications des procédures d'enregistrement et d'approbation proposées par la directive relative à la protection des données. La

57 En décembre 2003, les salariés de l'autorité nationale étaient au nombre de quatre pour faire face à 227 251 demandes. Rapport annuel de la Commission pour la protection des données à caractère personnel de la République de Bulgarie 2002-2003, p. 11-12, disponible en bulgare à l'adresse : www.cpdp.bg/godishniotcheti.html.

58 Par exemple, en 2006, on comptait 274 446 demandes et 31 970 enregistrements. Rapport annuel de la Commission pour la protection des données à caractère personnel de la République de Bulgarie 2006, p.17, disponible en bulgare à l'adresse : www.cpdp.bg/godishniotcheti.html.

59 Décision publiée le 12 octobre 2007, référence : GI-DEC-DOLiS-218/07/5787, 5788.

60 Décision publiée le 23 novembre 2007, référence : GI-DOLiS-430/103/07/6592.

61 Parmi ces lacunes, figuraient les suivantes : stockage des données dans des conditions inappropriées, sur des étagères et dans des tiroirs sans verrous ; utilisation de systèmes informatiques qui souvent ne correspondaient pas aux spécifications techniques établies par la loi ; dans de rares cas, utilisation de systèmes informatiques permettant à des personnes non autorisées d'accéder au fichier ; utilisation de données collectées au cours de procédures administratives à d'autres fins que celle annoncée ; et dans quelques cas, publication de données de personnes sur un site web sans que ces personnes n'aient donné leur consentement.

loi a ensuite été modifiée pour permettre des dérogations, ce qui a conduit à une baisse considérable du nombre de notifications. Le législateur grec n'a pas retenu l'option proposée par la directive relative à la protection des données, qui permet la nomination d'un délégué interne à la protection des données/au respect de la vie privée. En raison de l'asymétrie des pouvoirs caractérisant la relation employeurs - salariés, l'autorité nationale refuse le consentement de la personne concernée en tant que motif permettant la légitimation en soi du traitement des données à caractère personnel.[62] Dans la grande majorité des cas, les responsables du traitement respectent les décisions de l'autorité nationale de protection des données. Un cas important de non-conformité, qui a suscité d'importantes préoccupations et un tollé général, concerne l'utilisation par la police grecque de systèmes de vidéosurveillance pour filmer des manifestations politiques malgré des décisions contraires juridiquement contraignantes de l'autorité nationale sur l'utilisation de caméras dans les espaces publics[63] alors que la décision de l'autorité de protection des données était en instance devant le Conseil d'État en plénière.[64] De plus, les auditeurs de l'autorité n'ont pas été autorisés à accéder aux locaux de la police afin de contrôler le respect des décisions de l'autorité. Cette situation a conduit le président et la plupart des membres de l'autorité à remettre leur démission.

Concernant le Royaume-Uni, il est rapporté que la Commission européenne enquête sur des manquements présumés du Royaume-Uni dans la mise en œuvre de 11 des 34 articles de la directive, soit quasiment un tiers de la directive.[65] Bien que le gouvernement du Royaume-Uni prétende avoir entièrement mis en œuvre la directive, beaucoup de lacunes ont été signalées.[66] Point encore plus problématique, l'autorité nationale en matière de protection des données a clairement fait part de son sentiment qu'il n'était pas de sa compétence d'assurer que la législation nationale soit interprétée conformément à la directive européenne ou d'identifier sur quels points la législation nationale pourrait ne pas satisfaire aux exigences de la directive relative à la protection des données[67].

L'Allemagne a transposé la directive relative à la protection des données dans ses législations fédérale et des *Länder*. Les organes non publics ont le devoir de notifier les traitements automatisés de données avant leur exécution à l'autorité de contrôle ou au commissaire en charge de la protection des données. Les organismes publics de la fédération doivent les annoncer à l'autorité nationale. L'enregistrement obligatoire ne s'applique pas si le responsable du traitement a désigné un délégué interne à la protection des données. Il semble qu'un nombre significatif d'entreprises privées qui sont légalement tenues de désigner des délégués à la protection des données, ne respectent pas cette obligation et que celles qui satisfont l'obligation générale de nomination de délégués à la protection des données ne facilitent souvent pas le travail efficient et efficace des personnes désignées. De plus, on ne peut ignorer que la majorité des moyennes entreprises affichent toujours une série de lacunes en matière de protection des données. Cela est dû au fait que les délégués à la protection des données qui ont été désignés – lorsqu'ils l'ont été – ne peuvent mettre en place les changements nécessaires en matière de protection des données en raison du temps insuffisant qu'ils ont pour suivre la formation nécessaire ou pour s'acquitter comme il se doit de leurs responsabilités. Les récents scandales, concernant des institutions tant privées que publiques, mettent en évidence des cas graves de violations de la protection des données et de la vie privée à grande échelle[68]. Ces cas concernent entre autres, des violations graves des droits au respect de la vie privée, en espionnant ou en observant secrètement des salariés à l'aide de la vidéo ou par des recherches informatisées de profils à l'encontre des salariés sur le lieu de travail. D'autres affaires ont porté sur la commercialisation de données dans des quantités sans précédents sans le consentement préalable des personnes concernées.[69] L'absence de mesures appropriées telles que des poursuites pénales ne fait souvent qu'amplifier le problème.

62 Approche également adoptée par la Commission européenne dans le rapport : *Possible content of a European framework on protection of workers' personal data,* Bruxelles 2002.

63 Décision 58/2005 de l'autorité nationale de contrôle en matière de protection des données *(Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα),* www.dpa.gr/portal/page?_pageid=33,15453&_dad=portal&_schema=PORTAL.

64 Le Ministère grec de l'ordre public a soumis une demande au Conseil d'État en vue de faire annuler les décisions de l'autorité.

65 « Europe claims UK botched one third of Data Protection Directive », *Out-Law News,* 17 septembre 2007, disponible à l'adresse : www.out-law.com/page-8472. Bien qu'il s'agisse d'un article de presse en tant que tel, il repose sur des informations obtenues directement auprès des autorités concernées dans le cadre de la loi sur la liberté de l'information et tant le gouvernement britannique que la Commission ont confirmé que différents points étaient discutés, sans plus de précisions. Toutefois, les informations obtenues par Out-Law montraient que « selon la Commission, les articles 2, 3, 8, 10, 11, 12, 13, 22, 23, 25 et 28 n'auraient pas été correctement mis en œuvre… Ces articles concernent les définitions utilisées dans la directive (par exemple, la signification de données à caractère personnel) ; le champ d'application de la directive aux fichiers manuels ; les conditions dans lesquelles les données sensibles à caractère personnel peuvent être traitées ; les avis de traitement loyal donnés aux personnes ; les droits accordés aux personnes concernées ; l'application de dérogations à ces droits ; les voies de recours dont disposent les personnes en cas de violation ; la responsabilité des organisations en cas de violation de la loi en matière de protection des données, le transfert de données à caractère personnel en dehors de l'Union européenne et les pouvoirs du commissaire à la protection des données. »

66 Par exemple, D. Korff (2008) « UK Data Sharing: European Conflict », *Data Protection Law & Policy,* p.12 et suivantes. D'autres questions ont été soulevées dans l'enquête mentionnée dans la note de bas de page suivante et dans : R. Thomas et M. Walport (2008) *Data Sharing Review Report,* disponible à l'adresse : www.justice.gov.uk/docs/data-sharing-review-report.pdf.

67 Tel qu'indiqué par le vice-commissaire à la protection des données, Jonathan Bamford, en réponse à une question d'une commission d'enquête de la chambre des communes au cours d'auditions sur le dossier médical informatisé introduit au sein du National Health Service, lors d'une séance en mai 2007 : « s'il y a un quelconque doute sur le fait que la loi britannique sur la protection des données met en œuvre correctement la directive européenne relative à la protection des données, il doit être traité par le Ministère de la justice en l'état actuel des choses, car il s'agit de l'instance responsable de garantir la mise en œuvre de la directive dans le droit britannique. S'il y a un souci quant à une éventuelle divergence, c'est le Ministère de la justice qui doit y répondre. Le commissaire à la protection des données est chargé de mettre en œuvre la loi britannique sur la protection des données… Si vous avez une véritable inquiétude [sur un quelconque manquement de la loi à mettre en œuvre correctement la directive], je pense qu'il est important de vous adresser au Ministère de la justice dans le cadre de cette enquête. » Réponse à la question 176 lors de l'audition devant la commission d'enquête le 10 mai 2007. Transcription intégrale disponible sur : www.parliament.the-stationery-office.co.uk/pa/cm200607/cmselect/cmhealth/422/7051002.htm.

68 www.heise.de/tp/r4/artikel/28/28579/1.html, www.dorstenerzeitung.de/nachrichten/politik/blickpunkt/art302,350317, www.tagesschau.de/inland/datenschutz110.html, www.sol.de/news/welt/tagesthema/Datenschutz ;art7325,2705543, www.ruhrnachrichten.de/nachrichten/politik/blickpunkt/art302,433610, http://ez.omg.de/?id=20&nid=29923, www.handelsblatt.com/unternehmen/handel-dienstleister/rasterfahndung-bei-der-bahn ;2136145.

69 www.aufrecht.de/news/view/article/illegaler-handel-mit-adress-und-kontodaten-sprengt-alle-grenzen.html.

4.2.2. Désignation de délégués internes à la protection des données

Concernant la désignation de délégués internes à la protection des données, la plupart des législations nationales prévoient des exigences générales sans qu'aucune connaissance spécifique ni expertise dans le domaine ne soit nécessaire. Au Danemark, en Grèce et en Italie, la législation ne prévoit pas la désignation de délégués à la protection des données. En Belgique, l'arrêté royal correspondant reste muet sur la procédure de désignation des délégués internes à la protection des données. Dans la note explicative relative à l'arrêté royal du 13 février 2001 portant exécution de la loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, le gouvernement indique explicitement que l'idée de désigner une telle personne n'a jamais été soutenue en Belgique. En Autriche, la législation ne crée aucune obligation de désigner des délégués internes à la protection des données mais, dans le secteur public, les syndicats encouragent ces désignations. Concernant les autres États membres, ils se répartissent essentiellement dans deux catégories : a) ceux dont la législation prévoit certaines exigences à respecter et b) ceux qui n'en ont pas. La législation nationale de certains États membres (la Bulgarie, Chypre[70], l'Estonie, la Finlande[71], la Lituanie, l'Irlande, la Roumanie, le Portugal, le Royaume-Uni, la Slovénie et la Suède) ne comporte aucune disposition concernant l'obligation de désigner des délégués à la protection des données. Dans les autres États membres (l'Allemagne, la France, la Hongrie, la Lettonie, le Luxembourg, Malte, les Pays-Bas, la Pologne, la République tchèque et la Slovaquie), la législation nationale contient des dispositions explicites sur l'indépendance des délégués ou leur bonne connaissance/expertise du domaine. Il convient de noter que ces exigences ne sont pas précisées dans plus de détails. Les seules exceptions sont la Hongrie et la Lettonie où le délégué interne à la protection des données doit être titulaire d'un diplôme de l'enseignement supérieur en droit, administration publique ou technologies de l'information ou avoir une qualification équivalente, pour être désigné ou accrédité au sein de l'organisation du responsable du traitement des données ou du sous-traitant technique.

Lors de l'évaluation des exigences en matière de désignation des délégués à la protection des données, il convient de garder à l'esprit que la législation communautaire ne prévoit pas de normes spécifiques à satisfaire. Toutefois, il est évident que la désignation de personnes disposant d'une expertise particulière et/ou un rôle spécial de sensibilisation contribue à garantir que la législation applicable est respectée et entièrement mise en œuvre. Indépendamment des capacités et du niveau de connaissance des délégués à la protection des données, il convient de noter que la pratique de leur recrutement par une branche de l'exécutif n'est pas favorable à l'indépendance des autorités nationales de contrôle en matière de protection des données.

Par ailleurs, un État membre (l'Irlande) a opté pour l'adoption de lignes directrices et deux autres (la Slovaquie et la Suède) pour une formation spécifique des délégués à la protection des données. Enfin, aucun élément probant ne permet de juger de la conformité dans ce domaine.

4.3. Sanctions, réparation et effets juridiques

Tous les États membres ont mis en œuvre dans leur système juridique le Chapitre III de la directive relative à la protection des données sur les « recours juridictionnels, responsabilité et sanctions ». Ce chapitre demande aux autorités nationales de prévoir des recours adéquats et effectifs pour veiller au respect des droits garantis par la législation en matière de protection des données à caractère personnel ; d'adopter des sanctions appropriées et proportionnées à appliquer en cas de violations de la législation en matière de protection des données et de garantir des dommages-intérêts compensatoires pour ceux qui ont subi des dommages suite au traitement illicite des données à caractère personnel les concernant. Du fait toutefois que les dispositions de la directive relative à la protection des données concernant les recours, les sanctions et la responsabilité ne fixent que l'objectif à atteindre par les États membres sans préciser de critères détaillés à respecter, on relève un certain nombre de différences entre les législations nationales sur la protection des données. Celles-ci concernent tant la possibilité d'obtenir réparation et de percevoir des dommages-intérêts que celle que les contrevenants soient condamnés et sanctionnés pour les violations des droits en matière de protection des données à caractère personnel.

4.3.1. Recours

L'article 22 de la directive relative à la protection des données codifie l'obligation générale pour les États membres de prévoir « sans préjudice du recours administratif qui peut être organisé, … que toute personne dispose d'un recours juridictionnel en cas de violation des droits qui lui sont garantis ». Le Tableau 5 présente les différentes méthodes adoptées par les systèmes juridiques nationaux pour garantir le respect du droit de l'UE. Celles-ci sont les suivantes : a) recours administratifs devant l'autorité de protection des données ; b) recours non juridictionnels devant l'autorité de contrôle (en tant qu'alternative à une action judiciaire, qui, une fois commencée, empêchent toute réclamation devant une autorité judiciaire) ; c) recours juridictionnels, disponibles devant un tribunal ordinaire.

70 La législation sur la protection des données à Chypre comprend une disposition selon laquelle le personnel de bureau de l'autorité chypriote de protection des données doit disposer des qualifications énoncées dans le règlement, mais ce règlement n'est pas encore entré en vigueur.

71 Deux lois seulement contiennent des dispositions spécifiques concernant la désignation de délégués à la protection des données : la loi sur le traitement électronique des données de clients au sein des services sociaux et de santé et la loi sur les ordonnances médicales électroniques (*Laki sähköisestä lääkemääräyksestä, Lag om elektroniska recept,* loi n° 61/2007). Ces lois exigent que les prestataires de services sociaux et de santé, les pharmacies, la sécurité sociale finlandaise (KELA) et l'autorité nationale chargée des affaires médico-légales (TEO) désignent des délégués à la protection des données.

Tableau 5 : Recours

État membre	Recours administratifs devant l'autorité de protection des données	Recours non juridictionnels devant l'autorité de protection des données	Recours juridictionnels devant les tribunaux ordinaires
Allemagne	●		●
Autriche	●		●
Belgique		●	●
Bulgarie	●		●
Chypre	●		●
Danemark	●		●
Espagne	●		●
Estonie	●		●
France	●		●
Finlande	●		●
Grèce	●	●	●
Hongrie	●*		●
Irlande	●		●
Italie	●	●	●
Lettonie	●		●
Lituanie	●		●
Luxembourg	●		●
Malte	●		●
Pays-Bas	●		●
Pologne	●		●
Portugal	●		●
République tchèque	●		●
Roumanie	●		●
Royaume-Uni	●		●
Slovénie	●		●
Slovaquie	●		●
Suède	●		●

*Note : * En Hongrie, l'autorité de protection des données est investie de pouvoirs limités pour prévoir des recours administratifs, mais dispose de peu de possibilités pour les appliquer.*

Dans tous les États membres, toute personne peut présenter une réclamation concernant une violation spécifique ou une plainte plus générale devant l'autorité nationale de contrôle, alléguant une violation. Un principe fondamental de la règle de droit est la possibilité, également reconnue dans tous les États membres, d'ester en justice devant des tribunaux ordinaires afin d'obtenir une décision judiciaire sur le litige. Souvent, cela peut être fait grâce à des procédures simplifiées (par exemple, en Belgique et en Italie). Toutefois, dans plusieurs pays (tels qu'en Autriche, en Estonie, en Finlande et en Lettonie), les recours juridictionnels, bien que disponibles en théorie, ne sont pas utilisés par les plaignants dans la pratique. Seules la Belgique, la Grèce, et l'Italie permettent aux personnes concernées de régler des litiges soit devant les tribunaux, soit en présentant une réclamation auprès des autorités de protection des données, qui peuvent offrir un recours rapide et peu coûteux au moyen d'une procédure quasi-judiciaire.

4.3.2. Sanctions

Conformément à l'article 24 de la directive relative à la protection des données, les États membres sont tenus de « déterminer notamment les sanctions à appliquer en cas de violation » de la législation en matière de protection des données. La mise en œuvre de cette disposition générale au niveau national a pourtant donné lieu à des différences significatives. L'influence de la législation et des pratiques nationales en matière de droit pénal et administratif est de fait particulièrement marquée dans ce domaine et a modelé tant l'approche suivie au départ par les législateurs des États membres lors de l'élaboration de la législation en la matière que celle adoptée ensuite par les autorités administratives et judiciaires pour son interprétation et son application. Compte tenu de l'impossibilité d'établir une comparaison exhaustive des législations (administratives et pénales) nationales relatives aux sanctions (et aux peines) en cas de violations de la protection des données, l'analyse se concentrera ici sur les institutions habilitées à prendre des sanctions et sur les principales sanctions qu'elles peuvent adopter.

Diverses sanctions peuvent être imposées par les autorités de protection des données. Outre celles présentées à la section 3.1.3.2 (avertissement ou admonestation au sous-traitant/responsable des traitements, ordre de suspendre le traitement de données à caractère personnel, verrouillage et effacement de données spécifiques), les autorités de contrôle sont habilitées à ordonner des sanctions pécuniaires. Les tribunaux peuvent également ordonner des sanctions pécuniaires, voire des peines d'emprisonnement ou leurs alternatives, telles qu'une peine avec sursis ou des travaux d'intérêt général. Le Tableau 6 illustre l'éventail d'effets que peut avoir le non-respect de la législation en matière de protection des données dans chaque système juridique : a) amendes administratives imposées par les autorités de protection des données ; b) amendes pénales infligées par les tribunaux ; c) emprisonnement ou ses alternatives imposés par les tribunaux. À noter que l'obligation de réparer les pertes et dommages fait l'objet d'une analyse séparée au point 4.3.3.

Tableau 6 : Sanctions

État membre	Amendes administratives imposées par les autorités de protection des données	Amendes pénales infligées par l'autorité judiciaire	Détention imposée par l'autorité judiciaire
Allemagne	●*	●	●
Autriche		●	●
Belgique		●	
Bulgarie	●		
Chypre	●	●	
Danemark		●	●
Espagne	●		
Estonie	●	●	●
Finlande	●	●	●
France	●	●	●
Grèce	●	●	●
Hongrie		●	●
Italie	●	●	●
Irlande	●	●	
Lettonie	●		
Lituanie		●	
Luxembourg	●	●	
Malte	●	●	●
Pays-Bas	●	●	●
Pologne		●	●
Portugal	●		●
République tchèque	●		
Roumanie	●	●	
Royaume-Uni		●	●
Slovénie	●	●	●
Slovaquie	●	●	●
Suède		●	●

*Note : * En 2008, par exemple, des amendes administratives s'élevant à 1,4 million d'euros ont été imposées à l'entreprise commerciale Lidl, qui les a acceptées.*

Comme l'illustre le Tableau 6, les autorités de contrôle en matière de protection des données sont habilitées à imposer des sanctions économiques uniquement dans certains États membres (et leurs décisions sont dans tous les cas toujours susceptibles de recours devant les tribunaux administratifs). Dans d'autres États membres (par exemple, en Belgique et au Royaume-Uni), elles ne sont en mesure que de négocier des solutions à l'amiable avec les contrevenants. L'efficacité des sanctions administratives ordonnées par les organes de contrôle ont toutefois suscité des préoccupations dans un certain nombre d'États membres car les amendes sont trop faibles ou trop rares pour exercer un effet dissuasif. Dans d'autres États membres (tels que l'Autriche, le Danemark, la France et le Royaume-Uni,), ce sont plutôt les pratiques répressives des tribunaux qui se sont avérées dépourvues d'un effet dissuasif. C'est ainsi que, dans certains pays (tels que l'Estonie), les autorités judiciaires n'ont en fait jamais infligé de sanctions pénales.

4.3.3. Réparation

Conformément à l'article 23, paragraphe 1, de la directive relative à la protection des données, les États membres « prévoient que toute personne ayant subi un dommage du fait d'un traitement illicite ou de toute action incompatible avec les dispositions nationales prises en application de la présente directive a le droit d'obtenir du responsable du traitement réparation du préjudice subi ». La législation nationale sur la responsabilité civile varie toutefois selon la décision des États membres d'adopter de réglementer spécifiquement le devoir de réparer les dommages subis dans une affaire relative à la protection des données, ou de prévoir simplement une extension du cadre ordinaire de la responsabilité civile au domaine de la protection des données à caractère personnel. Le Tableau 7 présente les principales solutions retenues par les États membres lors de la mise en œuvre de cette disposition de la directive relative à la protection des données : a) extension du cadre ordinaire de responsabilité civile (le plaignant assumant la charge de la preuve des dommages subis et le risque des coûts du règlement du litige) ; b) extension du cadre existant de responsabilité civile mais avec une inversion de la charge de la preuve (permettant au responsable du traitement d'être exonéré de la responsabilité en tout ou en partie s'il prouve que le fait dommageable ne lui est pas imputable) ; c) mise en œuvre d'un cadre spécial de responsabilité civile.

Tableau 7 : Réparation

État membre	Extension du cadre existant de responsabilité civile	Cadre existant de responsabilité civile avec inversion de la charge de la preuve	Cadre spécial de responsabilité civile
Allemagne		●	●
Autriche	●		
Belgique	●		
Bulgarie	●		
Chypre	●		
Danemark		●	
Espagne	●		
Estonie	●		
Finlande	●		
France	●		
Grèce			●
Hongrie			●
Irlande	●		
Italie		●	
Lettonie	●		
Lituanie	●		
Luxembourg	●		
Malte	●		
Pays-Bas	●		
Pologne	●		
Portugal	●		
République tchèque	●		
Roumanie	●		
Royaume-Uni	●		
Slovénie	●		
Slovaquie	●		
Suède		●*	●

*Note : * La loi suédoise relative à la protection des données comporte des règles spéciales relatives à la réparation, mais la procédure relève du cadre existant s'appliquant aux affaires civiles.*

Comme l'illustre le Tableau 7, des réparations doivent être versées pour tout dommage causé par le non-respect de la législation relative à la protection des données lors du traitement de données à caractère personnel. Dans la plupart des États membres, une action judiciaire ordinaire régie par des dispositions générales relatives à la responsabilité civile peut en théorie permettre d'obtenir réparation même si, dans un certain nombre d'États membres, aucun dommage et intérêt dans les affaires relatives à la protection des données n'a été relevé (par exemple, à Chypre, en Lettonie, à Malte, et au Portugal), ou très peu d'actions en réparation portées devant les tribunaux civils ont été recensées (notamment en Estonie et en Finlande). Dans plusieurs États membres, les règles générales sur la responsabilité s'appliquent aux affaires relatives à la protection des données, à l'exception de l'inversion de la charge de la preuve qui passe du plaignant à la partie défenderesse (le sous-traitant/responsable du traitement). Enfin, dans certains pays, un cadre spécial a été créé pour permettre d'obtenir réparation. En particulier, une règle de responsabilité stricte s'applique aux sous-traitants/responsables du traitement en Allemagne et en Grèce (mais uniquement pour les sous-traitants/responsables du traitement publics). Ainsi, la responsabilité ne dépend pas d'une intention ou d'une négligence, mais découle simplement de l'existence d'un dommage causé par une violation de la législation. En Belgique, il paraît que certains tribunaux accordent des dommages et intérêts au terme d'une procédure rapide devant le président du tribunal de première instance. En Suède, le Ministère de la Justice est habilité à accorder réparation sans action en justice pour des violations commises par des organes gouvernementaux ou administratifs. En Hongrie, les procédures judiciaires en matière de protection des données ne font pas l'objet de droits et taxes des tribunaux, et une règle proche de celle de la responsabilité stricte s'applique aux fins de l'appréciation de la responsabilité du sous-traitant/responsable du traitement.

La quantification procédurale et matérielle des dommages et intérêts à accorder à l'encontre des sous-traitants/responsables du traitement coupables de violations des droits à la protection des données à caractère personnel varie en fonction des États membres suivant la législation et la pratique judiciaire relative à la responsabilité civile et elle ne peut donc être analysée dans le cadre du présent rapport comparatif. La fourchette des indemnités accordées dans les affaires relatives à la protection des données reste par ailleurs inconnue dans la plupart des États membres (Allemagne, Autriche, Belgique, Bulgarie, Chypre, Danemark, Estonie, Finlande, France, Grèce, Hongrie, Irlande, Italie, Lettonie, Lituanie, Luxembourg, Malte, Pays-Bas, Pologne, Portugal, République tchèque, Roumanie, Royaume-Uni, Slovénie, et Suède). Il convient de souligner toutefois que dans la législation ou la pratique judiciaire d'un certain nombre d'États membres (Allemagne, Grèce, Hongrie, Italie, Lituanie, Royaume-Uni, Slovénie, et Suède), des dédommagements pour préjudice immatériel (par exemple, préjudice moral) peuvent également être prononcés, de façon isolée ou avec des dédommagements pour préjudice matériel.

4.3.4. Législation relative à la protection des données spécialisée dans le contexte de la relation d'emploi

La nécessité de garantir le respect des droits fondamentaux et de la dignité de la personne concernée est particulièrement impérieuse dans le domaine de la relation employeur-salarié. D'une part, la protection de la vie privée et des données à caractère personnel des salariés est une condition essentielle et préalable du droit fondamental à participer aux activités des syndicats et aux actions collectives. D'autre part, certaines des technologies les plus avancées permettant de surveiller et de contrôler le comportement des individus (telles que, par exemple, les caméras de surveillance, le contrôle à distance du courrier électronique) sont utilisées essentiellement dans la vie professionnelle. De ce fait, les États membres devraient adopter une législation complémentaire couvrant la protection des données dans le contexte des relations d'emploi afin de compenser l'inégalité inhérente des parties au contrat de travail, en imposant des obligations plus strictes à l'employeur afin qu'il se conforme à la législation en matière de protection des données.

Alors que l'article 8, paragraphe 1, de la directive relative à la protection des données interdit le traitement des données à caractère personnel qui révèlent l'appartenance syndicale, un certain nombre d'États membres (Belgique, Espagne, Finlande, Grèce, Hongrie, Irlande, Italie, Luxembourg, Lettonie, Pays-Bas, Pologne, Portugal, République tchèque, Slovaquie et Slovénie) ont également introduit des dispositions spéciales (que ce soit par le biais de la législation de l'emploi ou dans les lois générales sur la protection des données) en vue de garantir une conformité maximale au droit au respect de la vie privée et à la protection des données à caractère personnel dans le contexte des relations de travail. Ces dispositions donnent un rôle aux autorités de protection des données qui sont autorisées à élaborer des règlements généraux et des lignes directrices, notamment pour les entreprises privées. Les syndicats, outre les services de consultation proposés aux salariés sur les questions concernant la protection des données, sont souvent directement impliqués tant en amont, lors de la négociation des accords avec les employeurs pour la mise en place d'un système de dossiers du personnel qu'en aval, pour surveiller le respect de ceux-ci.

On relève toutefois différentes lacunes évidentes en matière de protection des données dans le contexte de l'emploi. Tout d'abord, plusieurs États membres (Allemagne, Autriche, Bulgarie, Chypre, Danemark, Estonie, France, Lituanie, Malte, Roumanie, Royaume-Uni, et Suède concernant l'emploi privé), ne disposent toujours pas de législation spécifique pour renforcer la protection des salariés. Par ailleurs, même lorsque cette législation existe, elle suscite des préoccupations en raison de l'absence de contrôle par les syndicats (par exemple, en Irlande, en Lettonie et en République tchèque), des pouvoirs discrétionnaires de l'employeur pour décider de l'objectif du traitement des données à caractère personnel (par exemple, en Pologne) mais aussi de l'exemption des petites entreprises de se conformer aux normes strictes relatives au traitement des données dans le domaine de l'emploi (par exemple, aux Pays-Bas). Enfin, dans d'autres pays (comme en Finlande), alors que la protection des données à caractère personnel dans le domaine de l'emploi était jusqu'à présent satisfaisante, des réformes législatives récentes vont sensiblement affaiblir les normes existantes en permettant aux employeurs, dans certaines circonstances, de contrôler les adresses de courrier électronique avec lesquelles les salariés échangent une correspondance, ainsi que le type de pièces jointes liées aux messages, bien que le contenu du message lui-même ne soit pas concerné.[72] Conformément à la loi finlandaise, les entreprises auront le droit de traiter les données d'identification dans leurs réseaux de communications pour détecter les violations du secret professionnel, les utilisations non autorisées, l'espionnage ainsi que certains autres crimes, les prévenir et mener enquête dessus.

72 Voir la loi HE 48/2008 vp du gouvernement finlandais.

4.4. Connaissance des droits

Dans cette sous-section, nous présentons les résultats des enquêtes Eurobaromètre et d'autres études/enquêtes menées dans les États membres pour donner un aperçu comparatif de la connaissance que les citoyens ont de leurs droits en matière de protection des données. Par ailleurs, nous examinons les liens entre la connaissance des droits et les aspects suivants :

- les autorités de contrôle en matière de protection des données, leurs pouvoirs, mandat, ressources et activités,
- les pratiques témoignant du respect de la législation en matière de protection des données,
- les pratiques relatives aux sanctions, à la réparation et aux effets juridiques dans les affaires relatives à la protection des données.

Dans la section 5.1.4, les lacunes constatées dans la connaissance des droits seront présentées, et pratiques encourageantes appliquées dans ce domaine seront recensées dans la section 6.3.

En février 2008, deux enquêtes Flash Eurobaromètre ont été publiées : n° 225 – La protection des données au sein de l'Union européenne : perception des citoyens[73] et n° 226 – Les perceptions des contrôleurs de données.[74]

Parmi les thèmes abordés dans la première enquête figuraient les suivants : les perceptions et inquiétudes des citoyens en matière de confidentialité des données ; la confiance des citoyens dans les différents types d'organismes détenant leurs données personnelles ; la connaissance par les citoyens de leurs droits en matière de protection des données et des autorités nationales chargées de cette protection ; la perception par les citoyens de la sécurité de transmission des données via l'internet, et l'utilisation d'outils visant à améliorer la sécurité des données ; ainsi que les attitudes des citoyens par rapport aux restrictions de leurs droits à la protection des données en raison du terrorisme international. Dans le cadre du sondage, 27 000 personnes ont été interrogées dans les 27 États membres de l'UE (1 000 entretiens par pays), principalement via des lignes téléphoniques fixes (cependant, comme dans neuf États membres, la couverture du réseau téléphonique fixe a été jugée insuffisante, l'échantillon consiste en un mélange d'entretiens téléphoniques et d'entretiens face-à-face.)

Les principaux résultats de l'enquête sont les suivants :

- Une majorité des citoyens de l'UE expriment des inquiétudes fortes ou assez fortes par rapport à la protection de leurs données. Cependant, ce niveau d'inquiétude est identique à celui constaté lors d'un sondage Eurobaromètre mené en 1991.
- C'est aux services médicaux, aux médecins et aux institutions publiques que les répondants accordent le plus de confiance en ce qui concerne la protection des données personnelles.
- La majorité des répondants n'étaient pas sûrs que la législation nationale de leur pays soit adéquate face à l'utilisation d'informations à caractère personnel sur l'internet.
- Bien que la plupart des répondants semblent être au courant de leurs droits concernant l'utilisation des données à caractère personnel et de l'existence de la législation établie dans ce domaine, en moyenne, seulement 28 % des répondants des 27 pays de l'UE connaissent l'existence d'une autorité nationale chargée de la protection des données.

La seconde enquête visait à évaluer les perceptions des contrôleurs de données en matière de protection des données au sein des 27 États membres de l'UE. Parmi les thèmes couverts figuraient les perceptions quant à la législation nationale relative à la protection des données ; les pratiques internes liées à la protection des données et au transfert de données personnelles ; les expériences récentes en matière de confidentialité des données et de protection des données ; l'avenir du cadre légal sur la protection des données ; et la protection des données dans le cadre du terrorisme international.

Les principaux résultats de cette enquête ont été les suivants :

- Une majorité de personnes responsables des questions liées à la protection des données au sein des entreprises (56 %) ont déclaré connaître assez bien les dispositions de la loi de protection des données.
- Une proportion identique (56 %) de répondants a estimé que les lois nationales de protection des données offraient aux citoyens un niveau «moyen» de protection, 28 % ont déclaré que le niveau de protection était «élevé» et seuls 11 % l'ont qualifié de «faible».
- Quelque 50 % des répondants étaient de l'avis que la législation fût plutôt mal adaptée ou pas du tout adaptée pour faire face à la quantité grandissante d'échanges d'informations personnelles.
- Une majorité écrasante (91 %) a estimé que les exigences de la loi de protection des données sont nécessaires. Un tiers des répondants (35 %) ont déclaré qu'à certains égards, les exigences de la loi de protection des données sont trop strictes.
- Les avis étaient partagés concernant l'adéquation de l'harmonisation des lois nationale par rapport à la libre circulation des données personnelles au sein de l'UE et l'existence de différences dans la manière dont les États membres interprètent les lois relatives à la protection des données à travers l'UE (dans les deux cas, une forte proportion des répondants n'avait pas d'opinion clairement définie).
- Au niveau de l'UE-27, 13 % des sondés ont déclaré être régulièrement en contact avec les autorités nationales de protection des données de leur pays – toutefois, ces résultats allaient de 41 % des répondants en Italie à 1 % en Autriche.
- Les répondants ont déclaré majoritairement contacter l'autorité nationale de protection des données pour demander des lignes de conduite (60 % de ceux qui la contactaient régulièrement ont donné cette raison) ou pour effectuer des notifications (56 %).

73 La protection des données au sein de l'Union européenne : Perceptions des citoyens. Flash Eurobaromètre n° 225, http://ec.europa.eu/public_opinion/flash/fl_225_fr.pdf.

74 La protection des données au sein de l'Union européenne : Les perceptions des contrôleurs de données. Flash Eurobaromètre n° 226, http://ec.europa.eu/public_opinion/flash/fl_226_fr.pdf.

- En évaluant les données statistiques disponibles auprès des États membres, il faut noter avant tout que les enquêtes nationales ne sont disponibles que dans 12 des 27 États membres. Ces enquêtes ont dans certain cas été commandées par les autorités nationales de protection des données. Les questions posées, le nombre de répondants, la méthodologie, l'échantillonnage et les résultats finaux sont divers et ne permettent pas toujours de lier les résultats avec les questions examinées dans la présente étude comparative.

Il existe des études nationales sur la connaissance des droits pour certains États membres (Autriche, Danemark, Espagne, Finlande, France, Hongrie, Irlande, Lettonie, Pays-Bas, Royaume-Uni, Slovaquie, Slovénie, et Suède) alors que les autres (Allemagne, Belgique, Bulgarie, Chypre, Estonie, Grèce, Italie, Lituanie, Luxembourg, Malte, Pologne, Portugal, République tchèque, et Roumanie) n'en ont pas réalisé.

Des enquêtes publiques sont régulièrement menées en matière de protection des données à caractère personnel en Slovaquie. Les résultats sont repris dans les rapports publiés par l'autorité nationale en matière de protection des données. Deux de ces enquêtes (effectuées en 2005[75] et en 2007[76]) sont publiées son site internet.[77] Les deux enquêtes ont fait appel à un échantillon aléatoire représentatif au niveau national de répondants âgés d'au moins 18 ans (dans l'enquête de 2005, la taille nette de l'échantillon était de 1 283 répondants, et dans celle de 2007, de 1 531 répondants). D'après les résultats de l'enquête de 2007, 51 % des répondants ont déclaré avoir conscience du droit à la protection des données et quasiment 50 % d'entre eux ont reconnu l'Office pour la protection des données à caractère personnel en tant qu'autorité nationale en la matière (soit 5 % de plus que lors de l'enquête précédente en 2005). Les résultats de l'enquête montrent que le public n'apprécie toujours pas pleinement les problèmes liés aux données à caractère personnel et que ceux-ci font peu l'objet de débats.

En Lettonie, deux enquêtes ont été menées en 2003 et 2005 (toutes deux basées sur un échantillon aléatoire stratifié d'environ 1 000 résidents permanents en Lettonie). Les résultats intéressants dans le cadre de la présente étude comparative sont les suivants : 29,5 % des répondants (23,3 % en 2003) connaissaient l'existence de l'autorité nationale de protection des données ; 19,5 % des répondants (14,5 % en 2003) ont déclaré s'être retrouvés dans une situation où leurs données n'ont pas été traitées correctement, entraînant semble-t-il un préjudice financier ou moral ; 13,5 % des répondants (6,4 % en 2003) ont indiqué avoir été amenés à fournir davantage d'informations les concernant que nécessaire ; 22,9 % des répondants ont tenté d'obtenir des informations les concernant auprès d'institutions ou d'entreprises. La plupart d'entre eux (66,2 %) y sont parvenus mais 32,5 % des répondants se sont vu refuser l'accès à ces informations. Les résultats de l'enquête montrent qu'il convient de sensibiliser sur les questions relatives à la protection des données au sein des institutions de l'État mais aussi du grand public.

En Suède, l'autorité nationale de protection des données mène régulièrement des travaux de recherche sur les secteurs public et privé ainsi que sur des groupes au sein de la société. Trois enquêtes récentes sont disponibles. La première concerne le degré de conscience par les autorités sanitaires provinciales des règles relatives à la protection des données concernant l'accès aux dossiers des patients.[78] La deuxième analyse les questionnaires envoyés à 103 entreprises et autorités publiques, choisies de manière aléatoire, concernant les attitudes des employeurs à l'égard de l'utilisation de l'internet et du courrier électronique par les salariés et la surveillance en place au moyen du traitement de données biométriques et de caméras de surveillance.[79] La troisième, qui porte sur la connaissance de la législation et des droits en matière de protection des données et sur les attitudes à leur égard, ciblait des jeunes de 14 à 18 ans (533 répondants sélectionnés par la méthode des quotas, pour certaines catégories de répondants), qui ont rempli un questionnaire en ligne.[80] Les résultats de ces études n'ont été ni présentés ni analysés dans les études nationales et aucune conclusion ne peut donc en être tirée.

Au Danemark, deux études sont disponibles. La plus récente, qui a été réalisée à l'issue du projet axé sur la protection de la vie privée de la recherche et de la technologie relatives à la sécurité, *Privacy enhancing shaping of security research and Technology,* mené par Privacy and Security Technology (PRISE) conclut à la nécessité d'un débat public sur les questions de mise en œuvre des nouvelles technologies en matière de sécurité. La seconde étude, menée en 2005, qui concerne la télésurveillance par le Conseil pour la prévention de la criminalité (*Det Kriminalpræventive Råd*) et s'appuie sur des entretiens menés auprès de 994 personnes, conclut que « généralement, les Danois ont une perception positive de la télésurveillance. Les femmes semblent plus préoccupées par la criminalité que les hommes. Les citoyens les plus instruits semblent plus inquiets d'une éventuelle ingérence dans leur vie privée ».[81] En général, les études ont montré que la population danoise n'est pas particulièrement inquiète au sujet des questions de respect de la vie privée. Les Danois font en règle générale fondamentalement confiance au gouvernement et aux autorités assurant la protection des données et considèrent que les questions de la prévention de la criminalité et de la sécurité sont plus importantes que la notion intangible et abstraite de vie privée.

L'autorité nationale de protection des données irlandaise a mené une enquête en 2008 (qui faisait suite à des travaux semblables menés en 1997, 2002 et 2005) dans laquelle 1 000 personnes ont été interrogées en face-à-face dans le cadre d'une enquête omnibus.[82] L'un des principaux résultats de l'enquête est que presque les deux tiers de la population (65 %) estiment avoir été personnellement victimes d'une atteinte à la vie privée à un certain niveau – les catégories les plus souvent citées concernaient les messages commerciaux non sollicités.[83] Parmi diverses questions abordées, celles qui présentaient le plus d'importance pour les répondants étaient un bon service de santé (mentionné par 89 % des répondants) et la prévention de la criminalité (87 %), suivies par la confidentialité des informations personnelles (84 %). Si la moitié des répondants estimaient que des contrôles appropriés étaient place dans les organisations des secteurs public et privé pour empêcher les employeurs d'accéder à des informations personnelles à des

75 www.dataprotection.gov.sk/buxus/docs/sprava_5_2005_prieskum_vm1.pdf.
76 www.dataprotection.gov.sk/buxus/docs/zaverecna_sprava_07.pdf.
77 www.dataprotection.gov.sk/buxus/generate_page.php?page_id=421.

78 Résumé du Rapport 2005 en anglais :1 www.datainspektionen.se/Documents/rapport-accessibility-to-patients-data.pdf.
79 Monitoring in Working Life Report 2005:3, Résumé en anglais disponible à l'adresse : www.datainspektionen.se/Documents/rapport-monworklife-summary.pdf.
80 www.datainspektionen.se/Documents/rapport-ungdom-2009-eng.pdf.
81 TV-*overvågning – Fakta om TV-overvågning i Danmark Det Kriminalpræventive Råd Februar 2005*. Disponible en danois à l'adresse : www.dkr.dk/ftp_files/WEBDOX/PDF/dkr_mat_083.pdf.
82 Enquête disponible dans son intégralité à l'adresse : www.dataprotection.ie/docs/Public_Awareness_Survey_2008/794.htm.
83 Rapport présentant les résultats de l'enquête disponible à l'adresse : www.dataprotection.ie/docs/Public_Awareness_Survey_2008_Report/821.htm.

fins inappropriées, environ un sur cinq avait des doutes concernant l'efficacité de ces contrôles. Les répondants estiment que les dossiers médicaux, les historiques financiers et les informations relatives aux cartes de crédit revêtent l'importance la plus haute en ce qui concerne la confidentialité. Quelque 58 % des répondants connaissaient l'existence de l'autorité nationale de protection des données. Cette autorité a déclaré que les résultats de l'enquête seraient repris pour contribuer à planifier les travaux futurs de l'autorité.[84]

En France, la Commission nationale de l'informatique et des libertés (CNIL) commande des sondages annuels pour surveiller sa notoriété ainsi que la connaissance par les citoyens de leurs droits. Ces enquêtes sont menées auprès d'un échantillon de 1 000 personnes représentatif de l'ensemble de la population âgée de 18 ans et plus. Selon l'enquête, en 2007, 61 % des Français pensaient que la constitution de fichiers porte atteinte à leur vie privée et veulent de ce fait davantage se protéger.[85] Par ailleurs, 32 % des personnes interrogées ont déclaré connaître l'autorité nationale de protection des données en juin 2004, 37 % en décembre 2005, 39 % en décembre 2006, et 50 % en novembre 2007.[86] Une personne sur deux connaît ses missions. Cependant, seulement 26 % des personnes interrogées avaient le sentiment d'être suffisamment informées de leurs droits à la protection des données personnelles, tandis que 72 % des répondants pensaient n'être pas suffisamment informés.[87]

Un sondage sur la confiance des Autrichiens à l'égard de la protection des données a été publié en juillet 2008 ; ce sondage (basé sur des quotas) était basé sur des entretiens en face-à-face menés dans la rue auprès de 1 213 répondants.[88] Ses résultats montrent que des questions telles que la protection des données ou la surveillance restent dans une grande mesure méconnues des Autrichiens. Quelque 77 % des répondants ont avoué être plus ou moins ignorants sur ces questions. Quelque 92 % ont indiqué ne pas savoir si des données (à caractère personnel) sont collectées sur eux et le cas échéant, par qui. Quelque 76 % des répondants étaient d'avis que la population autrichienne n'était pas suffisamment informée en matière de protection des données, des risques d'utilisation abusive des données ou de la situation juridique sur le sujet. Concernant la vidéosurveillance, 55 % des répondants ont déclaré être habitués à la présence de caméras vidéo surveillant et enregistrant des événements et le comportement de quasiment tout le monde, et les considéraient plutôt comme une composante de la vie moderne que comme une menace pour les droits fondamentaux. Dans une autre étude, concernant la vidéosurveillance dans les lieux publics (1 237 répondants, méthodologie identique à celle du sondage susmentionné), jusqu'à 81 % des répondants ont déclaré même accepter les caméras dirigées vers les passants. Quelque 90 % ont admis s'être habitués à l'omniprésence des caméras de surveillance.[89]

Deux études sont disponibles en Espagne. La première est intitulée *Étude sur le degré d'adaptation des petites et moyennes entreprises espagnoles à la loi organique sur la protection des données et le nouveau règlement d'application*.[90] Elle affirme que 96 % des petites et moyennes entreprises espagnoles disposent de fichiers contenant des données à caractère personnel et que 78 % les conservent sous forme de fichiers électroniques, de sorte qu'ils relèvent tous de la législation relative à la protection des données (les résultats sont basés sur des entretiens téléphoniques menés auprès d'un échantillon stratifié de 250 petites et moyennes entreprises (moins de 50 salariés)). Les petites et moyennes entreprises espagnoles affichent une attitude positive à l'égard de la protection des données : 82 % des entreprises étudiées affirment qu'elles sont conscientes de la nécessité de se conformer à la législation en la matière, alors que 79 % confirment leur intention d'affecter des moyens économiques et/ou humains pour appliquer la législation en matière de protection des données. Une étude importante (basée sur un échantillon aléatoire stratifié de 600 répondants interrogés au téléphone) a également été menée par l'agence basque sur la protection des données à caractère personnel en juin 2008, qui traite de la perception sociale de la protection des données au Pays basque.[91] Cette étude indique que 37 % de la population de cette Communauté autonome seulement est très ou assez préoccupée de la façon dont les institutions publiques et les entreprises privées utilisent les données à caractère personnel qu'elles possèdent sur eux.

Différentes enquêtes ont examiné les perceptions et la connaissance des questions relatives à la vie privée aux Pays-Bas.[92] Dans une enquête de 1989, les citoyens semblaient d'avis que le respect de la vie privée est tout aussi important que des soins de santé appropriés, la propreté de l'environnement et la lutte contre le chômage et la criminalité.[93] Une étude de 1999 fait la distinction entre trois groupes de citoyens : 1) les citoyens qui estiment que les technologies de l'information sont nécessaires et qui ne voient pas de problèmes liés au respect de la vie privée (19 %) ; 2) les citoyens qui estiment que l'utilisation croissante des technologies de l'information pose de nouveaux problèmes liés au respect de la vie privée (35 %) ; et 3) les citoyens qui estiment que les technologies de l'information constituent une menace pour le respect de la vie privée (47 %).[94] Une étude de 2007 portant sur les libertés et la solidarité a révélé que 51 % des répondants considéraient que le gouvernement néerlandais protégeait suffisamment le droit fondamental au respect de la vie privée, tandis que 43 % estimaient qu'il devrait le protéger davantage. (Les résultats du sondage de 2007 sont basés sur un échantillon aléatoire de ménages d'un panel internet de ménages, et le sondage a été réalisé au moyen d'entretiens auto-administrés sur ordinateur. Les répondants avaient au moins 13 ans et la taille nette de l'échantillon était de 967 personnes).[95] Les résultats d'une étude commandée par l'autorité nationale de protection des données

84 Communiqué de presse du 12.08.08, disponible à l'adresse : www.dataprotection.ie/viewdoc.asp?DocID=815.

85 CNIL, 25/01/2008, « 61 % des Français pensent que la constitution de fichiers porte atteinte à leur vie privée », www.cnil.fr.

86 CNIL, *Rapport annuel 2007*, p.39.

87 CNIL, *Rapport annuel 2007*, p.39.

88 *Vertrauen der ÖsterreicherInnen in den Datenschutz*, disponible à l'adresse : www.oekonsult.eu/datensicherheit2008.pdf.

89 *Big Brother. Gefahr oder Normalität*, disponible à l'adresse : www.oekonsult.at/bigBrother_gesamtergebnisse_final.pdf.

90 Instituto Nacional de Tecnologías de la Comunicación [Institut national des technologies de la communication], *Estudio sobre el grado de adaptación de las Pequeñas y Medianas Empresas españolas a la Ley Orgánica de Protección de Datos y el nuevo Reglamento de Desarrollo*, juillet 2008, disponible à l'adresse : www.inteco.es/Seguridad/Observatorio/Estudios_e_Informes/Estudios_e_Informes_1/estudio_lopd_pymes.

91 « La protección de datos personales ». Cette étude est disponible à l'adresse : www.avpd.euskadi.net/s04- 5249/es/contenidos/informacion/estudio/es_cuali/adjuntos/informe.pdf.

92 Sjaak Nouwt (2005), *Privacy voor doe-het-zelvers*, The Hague: Sdu, ITeR Series Vol. 73. http://arno.uvt.nl/show.cgi?fid=41691.

93 Holvast, Jan, Henny van Dijk et Gerrit Jan Schep (1989), *Privacy Doorgelicht*, Den Haag: SWOKA.

94 Smink, G.C.J., A.M. Hamstra et H.M.L. van Dijk (1999), *Privacybeleving van burgers in de informatiemaatschappij*, Den Haag: Rathenau Instituut, Werkdocument 68.

95 Dieter Verhue, Harmen Binnema & Rogier van Kalmthout (2008), *Nationaal Vrijheidsonderzoek. Meting 2008. Opiniedeel*, avril 2008, p. 36. www.4en5mei.nl/mmbase/attachments/158819/p4751_vrijheidsonderzoek_opiniedeel_v4_read_only.doc.

(basée sur un sondage en ligne mené auprès de 2 016 répondants) ont été publiés en janvier 2009. Le rapport *Rien à cacher mais néanmoins inquiet,* évalue l'attitude des citoyens néerlandais à l'égard de la collecte et du traitement des données à caractère personnel les concernant.[96] Globalement, la plupart des citoyens sont plutôt enclins à divulguer leurs données à caractère personnel. Toutefois, cela ne signifie pas que les citoyens ne soient pas conscients de leur droit au respect de la vie privée. La plupart le sont mais ils acceptent de fournir des informations, plutôt parce que cela est inéluctable et en raison d'une certaine résignation de leur part que parce qu'ils ont confiance que les données sont utilisées à bon escient. En particulier, lors des discussions de groupe, les répondants se sont dits inquiets face aux risques liés au traitement des données à caractère personnel. Toutefois, ils estimaient que les changements de comportement demanderaient trop d'efforts. Le contrôle et la transparence semblaient deux points essentiels pour que le traitement des données soit mieux accepté et les citoyens ont exprimé le désir de pouvoir disposer de comptes rendus réguliers des données personnelles enregistrées les concernant. Par ailleurs, les informations sur les évolutions des technologies et de la société sont jugées importantes et utiles pour favoriser des attitudes veillant davantage au respect de la vie privée. Enfin, les citoyens font beaucoup plus confiance au gouvernement qu'aux entreprises et institutions privées pour l'utilisation et le traitement adéquats des données à caractère personnel.

D'après l'enquête d'opinion slovène, l'autorité nationale de protection des données est considérée comme l'institution publique la plus digne de confiance.[97] Aucune autre enquête n'était disponible sur les questions abordées dans la présente étude comparative.

En Hongrie, une étude sur la conscience et la connaissance de la Constitution a été menée en 2005 (échantillon représentatif de 1 000 personnes).[98] Quelque 8,1 % des répondants estimaient qu'« en vertu de la constitution actuelle, le droit au respect de la vie privée ne peut absolument pas être exercé ; ils étaient 56,5 % à considérer qu'il pouvait être exercé dans une moindre mesure et, selon 33,5 % des répondants, il pouvait être exercé de façon optimale ». À la question de savoir si le niveau de protection de la vie privée devrait être modifié ou non, 38,9 % des répondants étaient d'avis que le niveau de protection était satisfaisant, et 58,3 % souhaitaient un niveau de protection supérieur.[99] En 2008, une étude a été commandée par le bureau du médiateur sur la notoriété et l'évaluation des médiateurs.[100] D'après cette étude (échantillon de 1 000 répondants), la proportion de citoyens connaissant activement les médiateurs, qui était de 15 % en 1998, est passée à 32 % en 2007. Quelque 59 % des citoyens connaissaient l'autorité nationale de protection des données ; 11 % des répondants étaient sûrs qu'ils pourraient se tourner vers le médiateur comme voie de recours en cas de violation de leurs droits et 28 % pensaient pouvoir le faire. Concernant la confiance accordée par le public, les médiateurs occupaient la troisième place parmi les grandes institutions publiques, 52 % des répondants affirmant leur faire confiance.

Le bureau du commissaire à la protection des données du Royaume-Uni s'est appuyé sur des sondages pour découvrir ce que sait le public concernant la protection des données. Les derniers résultats de ces sondages font apparaître une baisse de dix points de pourcentage (de 49 % en 2006 à 39 % en 2007) dans la part de répondants estimant que la législation existante assure une protection suffisante de leurs informations. Dans le sondage de 2007, 1 223 répondants ont été interrogés par téléphone. Les répondants ont été sélectionnés au moyen de la méthode des quotas pour obtenir un échantillon représentatif sur le plan du sexe, de l'âge, de l'ethnicité et d'autres variables. L'analyse des sondages réalisés de 2004 à 2007 montre que le pourcentage de répondants se déclarant conscients de leur droit à voir les informations conservées sur eux par les organisations (lorsqu'une question leur est posée à ce sujet) est passé de 74 % en 2004 à 90 %. Quelque 17 % des répondants avaient en fait exercé ce droit en demandant à une organisation d'accéder à leurs informations. Lorsque les répondants ont été invités à évaluer une liste d'inquiétudes typiques que pourraient avoir les citoyens concernant le traitement de leurs données personnelles, dans chaque cas, de 83 à 94 % des répondants ont déclaré être très ou assez inquiets. Le point suscitant le plus d'inquiétudes reste la transmission ou la vente d'informations personnelles à d'autres organisations et les problèmes de sécurité relatifs au stockage des informations personnelles.[101]

Complétant les résultats des recherches ci-dessus, une conclusion importante des enquêtes de l'Eurobaromètre est que les autorités nationales restent relativement méconnues de la plupart des citoyens de l'UE. Ce manque de notoriété peut être considéré comme un problème majeur qui explique largement le manque de connaissance des pouvoirs qui leurs sont conférés. De même, cette ignorance conduit à un manque de conscience des droits mais aussi des pouvoirs, mandat, ressources et activités des autorités chargées de la protection des données.

Les informations concernant la connaissance des droits – y compris la connaissance des pratiques démontrant le respect de la législation en matière de protection des données ainsi que des pratiques en matière de sanctions, réparation et effets juridiques – ont pour source principale des enquêtes comme Eurobaromètre. L'étude menée en Espagne par l'Institut national des technologies de la communication, présentée plus haut, donne certains indices sur la connaissance des obligations d'enregistrement en vertu de la législation nationale. Comme il a été dit précédemment, 82 % des entreprises sondées affirmaient savoir qu'elles devaient respecter la législation en la matière, alors que 79 % d'entre elles confirmaient leur intention de consacrer des ressources économiques et/ou humaines pour se conformer à la législation sur la protection des données. Ces chiffres sont encourageants si l'on considère que, d'après l'enquête de l'Eurobaromètre, seulement 56,1 % des responsables des questions liées à la protection des données au sein des entreprises ont déclaré connaître assez bien les dispositions de la loi de protection des données, tandis que 30,2 % d'entre eux ont affirmé ne pas vraiment les connaître et seulement 13,1 % ont dit très bien les connaître.

96 J. Koffijberg *et al.* (2009), *Niets te verbergen en toch bang ; Nederlandse burgers over het gebruik van hun gegevens in de glazen samenleving,* Amsterdam: Regioplan, numéro de publication 1774. www.cbpweb.nl/downloads_rapporten/rap_2009_niets_te_verbergen_en_toch_bang.pdf.

97 www.ip-rs.si/index.php?id=272&tx_ttnews[tt_news]=621.

98 Menée par l'institut Eötvös Károly en coopération avec le département de sociologie juridique de l'université Eötvös Lóránd.

99 László Majtényi, *Az információs szabadságok. Adatvédelem és a közérdekű adatok nyilvánossága.* [La liberté d'information. Protection des données et accès aux données publiques], 2006, Budapest, Complex Kiadó. p. 58-61.

100 Szonda Ipsos Media, Institut d'enquête d'opinion et de marché, www.obh.hu/szonda_ipsos_OBH.doc.

101 *Report on Information Commissioner's Office Annual Track 2007,* p. 7, paragraphe 4.2, disponible à l'adresse : www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/ico_annual_track_2007_individuals_report.pdf. L'ensemble des questions et des réponses de l'enquête figure dans le corps de ce rapport.

5 Analyse des lacunes

Cette section du rapport analyse les principales lacunes résultant du système de protection des données à caractère personnel aux niveaux européen et national. Elle examine tout d'abord les défis que doivent relever les autorités de protection des données, le respect de la législation concernée, les recours, les réparations et les sanctions possibles à l'égard des violations des droits au respect de la vie privée, et les activités de sensibilisation aux droits. Elle recense ensuite les principaux domaines qui sont exclus, exemptés ou non couverts par l'application des lois sur la protection des données.

5.1. Lacunes dans la législation relative à la protection des données

5.1.1. Autorités de protection des données

L'organisation, le fonctionnement et les activités des autorités de protection des données présentent plusieurs lacunes. Au niveau structurel, un problème majeur résulte du manque d'indépendance de plusieurs autorités de contrôle. Dans un certain nombre d'États membres (par exemple, en Lituanie, en Lettonie, en Estonie, en Irlande et au Royaume-Uni), on relève des préoccupations concernant la capacité effective des délégués au sein des autorités nationales de contrôle en matière de protection des données à assumer leur mission en complète autonomie. Ce problème est lié essentiellement à la procédure de nomination ou de désignation des délégués : lorsque le gouvernement détient le pouvoir exclusif de choisir le personnel de direction, sans avis, contrôle ou approbation du législateur, comme nous l'avons observé dans la section 3.1.1, le risque de subordination ou de marginalisation effectives des responsables des données s'accroît considérablement. Il pourrait être éliminé par une réforme de la procédure de nomination/désignation. La directive relative à protection des données pourrait également être modifiée de manière à définir plus spécifiquement et plus précisément l'exigence en matière d'indépendance (établie actuellement à l'article 28, paragraphe 1, de la directive relative à la protection des données).

Au niveau du fonctionnement, le manque de personnel et de ressources financières suffisantes dans plusieurs autorités de contrôle constitue un problème important. Dans beaucoup d'États membres, les autorités de protection des données ne sont pas en mesure de mener intégralement leurs fonctions en raison des ressources économiques et humaines limitées dont elles disposent. C'est le cas en Autriche, en Bulgarie, à Chypre, en France, en Grèce, en Italie, en Lettonie, aux Pays-Bas, au Portugal, en Roumanie, et en Slovaquie. Pour les autorités de contrôle, la capacité à disposer d'une autonomie financière et d'un personnel spécialisé est essentielle non seulement pour garantir une protection effective des droits en matière de données à caractère personnel, mais constitue également un préalable à toute véritable indépendance par rapport à la volonté du gouvernement. Des réformes législatives pourraient être mises en œuvre pour augmenter le contrôle budgétaire et la gestion des ressources humaines des autorités de protection des données (par exemple leur en permettant de recruter directement du personnel spécialisé).

Sur le plan opérationnel, les pouvoirs limités de plusieurs autorités de contrôle suscitent des inquiétudes. Dans certains États membres, les autorités nationales de protection des données ne disposent pas de la totalité des pouvoirs de mener des investigations, d'effectuer des interventions durant les opérations de traitement des données, de donner des conseils juridiques et d'ester en justice qui sont détaillés à l'article 28, paragraphes 2, 3 et 4, de la directive relative à la protection des données. En Autriche, en Hongrie et en Pologne, les autorités de contrôle ne peuvent pas faire appliquer leurs décisions d'avertir le sous-traitant/responsable du traitement de mettre fin à son comportement illicite. En Allemagne et en Belgique, elles ne peuvent pas ordonner le verrouillage, l'effacement ou la destruction des données, ni imposer une interdiction temporaire ou définitive de leur traitement. En France et au Royaume-Uni, elles ne peuvent pénétrer dans des locaux où des données personnelles sont traitées sans avoir obtenu au préalable un mandat judiciaire. D'autre part, dans bon nombre de pays (par exemple, en Autriche, en France, en Grèce, en Hongrie, en Irlande, en Italie, en Lituanie, à Malte, en Pologne, en République tchèque, en Roumanie, au Royaume-Uni, et en Slovénie), les autorités de contrôle ne sont consultées que de façon aléatoire par le législateur lors de l'élaboration de lois susceptibles d'avoir un impact sur les questions liées au respect de la vie privée et à la protection des données car le corps législatif n'est pas concrètement tenu de le faire. Outre qu'elle constitue une violation de la législation communautaire, la mise en œuvre incomplète des spécifications de la directive relative à la protection des données représente une lacune significative dans le système national de protection des données à caractère personnel qui risque de compromettre l'efficacité du système. Puisque le droit communautaire semble être particulièrement clair en ce qui concerne le pouvoir des autorités de protection des données, des amendements devraient être apportés à la législation nationale, le cas échéant, afin de mettre les règles nationales en conformité avec les exigences définies au niveau de l'UE.

5.1.2. Respect de la législation

Diverses lacunes apparaissent lorsque l'on tient compte du niveau de respect effectif de la législation relative à la protection des données pertinente, notamment en ce qui concerne l'obligation d'enregistrement à laquelle sont soumis les acteurs publics et privés responsables des opérations de traitement des données. Alors que dans un certain nombre d'États membres, il est difficile d'évaluer le respect effectif de la législation relative à la protection des données en raison du manque d'informations fiables ou précises, il semble que dans plusieurs pays (par exemple, en Bulgarie, au Danemark, en Lettonie, aux Pays-Bas, au Portugal, en Roumanie et en Slovaquie), il existe un fossé entre la protection des droits liés au respect de la vie privée en théorie, qui peuvent officiellement se conformer aux exigences fixées par le droit européen et international, et leur protection dans la pratique. Ainsi, par exemple, le niveau de respect de la législation relative à la protection des données est étonnamment faible dans les institutions publiques en Estonie et en Roumanie. Par

ailleurs, dans la plupart des pays, l'absence de notions claires (ou d'interprétations communes) sur les concepts pertinents (tels que « données à caractère personnel », « fichier », « traitement », etc.) crée des incertitudes sur les activités qui relèvent des lois sur les données à caractère personnel. Le Groupe de l'article 29 joue un rôle crucial dans les efforts pour établir une interprétation commune de ces termes vagues, mais ce processus dépend également de l'acceptation et de l'application de ces interprétations dans les États membres. La dispersion de la législation relative à la protection des données dans différentes lois spécifiques à des secteurs, comme c'est le cas en Finlande et en Grèce, est également source de complexités et d'incohérences. Par conséquent, alors qu'une meilleure application pratique des normes de protection des données par les parties concernées pourrait suffire à traiter le premier problème, des lois supplémentaires, remplaçant les dispositions vagues et simplifiant le cadre juridique, seraient utiles pour remédier au second. La plupart des lacunes résultant du caractère complexe et imprécis de la législation relative à la protection des données sont liées dans une large mesure à l'énoncé de la directive relative à la protection des données : à cet égard, des solutions doivent être trouvées au niveau de l'UE.

Un problème majeur est le non-respect généralisé, relevé dans plusieurs pays (notamment au Royaume-Uni), de l'obligation de base de s'enregistrer auprès de l'autorité chargée de la protection des données à caractère personnel avant de s'engager dans des opérations de traitement de données. Un exemple récurrent est celui des caméras de surveillance : en Autriche, en Bulgarie, en France, en Lituanie, en République tchèque et en Suède, la grande majorité des caméras de surveillance ne sont pas enregistrées dans la pratique et ne sont donc pas sous la surveillance et le contrôle des autorités nationales de contrôle. L'internet représente un autre domaine de préoccupation majeur (comme en Espagne et en Slovénie). Souvent, le non-respect des obligations d'enregistrement par les sous-traitants/responsables du traitement résulte davantage de la méconnaissance de la législation que de l'intention délibérée de violer la loi. Cette lacune représente un problème particulier pour l'efficacité de la législation relative à la protection des données. Malgré les difficultés auxquelles le droit fait face en tentant de suivre l'évolution des nouvelles technologies, des lois supplémentaires introduisant ou améliorant la législation pour règlementer les technologies ayant un impact sur les droits liés aux données à caractère personnel (tels que la vidéosurveillance, la mise sur écoute des communications, les échantillons de cellules ou la conservation du code ADN, etc.), semblent donc être nécessaires de façon urgente (également afin d'éviter des discriminations dans les droits en matière de données à caractère personnel fondées sur la situation financière, comme cela s'est produit, de façon préoccupante, en République tchèque).[102]

5.1.3. Sanctions, réparation et effets juridiques

Certains problèmes découlent des systèmes nationaux en termes de recours, de sanctions et de réparation, ainsi que de l'application des règles de protection des données dans le contexte de l'emploi. Plusieurs pays présentent des lacunes concernant les sanctions pouvant être imposées par l'autorité chargée de la protection des données à caractère personnel, soit parce que les amendes ont un pouvoir dissuasif limité et/ou sont rarement imposées, soit parce que, tout simplement, les autorités de contrôle n'ont pas mis en place de pratiques pour leur imposition (Autriche, Belgique, Danemark, Finlande, Hongrie, Lituanie, Pologne et Royaume-Uni). L'absence d'obligation légale pour les sous-traitants/responsables du traitement de signaler les violations de données dans certains États membres (comme en Irlande) affaiblit encore davantage le système d'application de la loi. Dans certains pays (par exemple, en Allemagne, en Autriche, en France, en Hongrie, en Lettonie, aux Pays-Bas, en Pologne et au Royaume-Uni), les poursuites et les sanctions pour violation de la loi relative à la protection des données à caractère personnel sont très restreintes. S'agissant des dommages-intérêts dans plusieurs États membres (par exemple, à Chypre, en Estonie, en Finlande, en Irlande, en Lettonie, à Malte, aux Pays-Bas, en Pologne, au Royaume-Uni et en Suède en ce qui concerne les réparations venant d'entités privées), le système juridique national exclut de fait la possibilité de demander réparation pour la violation des droits de protection des données, en raison de la combinaison de plusieurs facteurs tels que la charge de la preuve, les difficultés liées à la quantification des dommages et le rare soutien des autorités de contrôle qui sont principalement engagées dans des activités de promotion. Même si l'utilisation en amont de méthodes « souples » peut être considérée comme une pratique positive en ce qu'elle contribue à garantir la conformité, il est indispensable que les États membres prévoient également des « dispositifs stricts » permettant de punir les contrevenants aux droits au respect de la vie privée et de les obliger à indemniser les victimes. Les réformes législatives, principalement au niveau national, pourraient jouer un rôle pertinent en l'espèce, en prévoyant des voies de recours juridique plus efficaces et complètes à titre de réparation pour violation. En même temps, la sensibilisation à l'importance des droits relatifs à la protection des données des personnes concernées ainsi que des juges et des procureurs permettrait une meilleure application des dispositions déjà en vigueur concernant la punition des violations des lois sur la protection des données.

Un nombre d'États membres (Autriche, Belgique, Bulgarie, Chypre, Danemark, Estonie, France, Lituanie, Malte, Roumanie, Royaume-Uni et Suède) n'ont toujours pas mis en place de législation adaptant les règles relatives à la protection des données spécifiquement à la relation d'emploi, ne reconnaissant pas la nécessité d'adopter des dispositions spécifiques sur la protection des données pour réglementer l'utilisation des données à caractère personnel dans le domaine de l'emploi. En conséquence, des violations des droits personnels de personnes physiques ont été mises en lumière dans certains pays (par exemple, en Allemagne, à Chypre et en Suède et dans le secteur privé) suite à la mise en place de la (vidéo) surveillance secrète des salariés sur leur lieu de travail. Dans d'autres États membres (comme la Finlande), au contraire, si le cadre légal était satisfaisant jusqu'à présent, de récents amendements législatifs ont en fait affaibli la protection dans le contexte de l'emploi.[103] L'UE, fondée sur le principe d'économie sociale de marché, accorde une grande importance au travail, et la libre circulation des travailleurs constitue une liberté fondamentale inscrite dans les traités européens. Les divergences entre les législations nationales pouvant être préjudiciables au fonctionnement du marché interne, une intervention de l'UE dans ce secteur visant à définir une norme minimale relative

102 Pour plus d'informations sur le cas de l'« *Opencard* », voir le site : http://opencard.praha.eu/jnp/en/home/index.html (en anglais) (consulté le 23.01.2009).

103 www.hs.fi/english/article/Lex+Nokia+passes+in+Parliament+-+government+party+ranks+split/1135244038215.

à la protection des données à caractère personnel dans le domaine de l'emploi serait hautement bénéfique. Tout en respectant le principe de subsidiarité, une telle intervention est indispensable pour garantir que les droits fondamentaux des travailleurs, tels qu'ils sont reconnus dans les traditions constitutionnelles communes aux États membres et dans la législation de l'UE, reçoivent une pleine protection.

5.1.4. Connaissance des droits

Un aperçu comparatif relatif à la connaissance des droits a été présenté dans la section 4.4, tandis que les pratiques encourageantes appliquées dans ce domaine sont inventoriées dans la section 6.3. L'implication des autorités de protection des données dans les activités de sensibilisation auprès de diverses parties prenantes s'est avérée d'une manière générale positive.

On a toutefois relevé quelques exemples négatifs où les autorités de protection des données ne se sont pas consacrées aux actions de sensibilisation (par exemple, l'Estonie et la Roumanie). Ainsi, dans certains États membres (comme en Bulgarie, en Lituanie, et en Slovaquie), les autorités de contrôle n'ont pas encore mis en place de site web convivial et/ou complet permettant au grand public d'accéder à toutes les informations sur la protection des données et de consulter facilement les avis et les règlements élaborés par l'autorité de protection des données. En outre, des préoccupations concernant la publicité et la transparence effectives des activités de l'autorité de protection des données ont été soulevées dans certains pays (comme en Bulgarie et à Malte), notamment lorsque l'autorité de contrôle négocie des résolutions à l'amiable des différends avec les contrevenants à la loi relative à la protection des données, sans les rendre accessibles au public (par exemple, au Royaume-Uni). Enfin, dans plusieurs États membres (comme en Autriche et en Grèce), si les performances de l'autorité de contrôle sont globalement satisfaisantes, le délai d'obtention d'informations peut être excessivement long, souvent car les autorités de protection des données ne disposent pas des ressources suffisantes pour répondre rapidement à toutes les demandes reçues des personnes concernées. Dans ces circonstances, il est peu probable qu'une nouvelle législation, que ce soit au niveau européen ou au niveau national, puisse améliorer la situation actuelle. Les autorités nationales de protection des données devraient peut-être plutôt réorganiser leur travail pour fournir rapidement une assistance aux personnes concernées. Un changement d'attitudes serait alors nécessaire pour augmenter la publicité donnée à leurs activités et sensibiliser les parties prenantes aux droits liés à la protection des données. Les autorités de protection des données doivent reconnaître l'importance de leur rôle pratique en matière de sensibilisation aux droits et peuvent facilement tirer des enseignements des pratiques encourageantes d'autres autorités européennes de contrôle pour faire face à ces lacunes.

Point encore plus problématique, dans quelques États membres (par exemple, au Royaume-Uni), les autorités de protection des données ont clairement exprimé qu'il ne leur incombait pas de veiller à ce que la législation nationale relative à la protection des données soit interprétée de manière conforme aux normes européennes et internationales relatives à la protection des données à caractère personnel (même si, dans une large mesure, la législation nationale constitue la transposition nationale des dispositions européennes et internationales concernées).

En effet, le travail des autorités nationales de protection des données est indispensable pour parvenir à une compréhension commune des principes des droits sur la protection des données. Leur convergence (spontanée) doit donc être saluée comme une pratique encourageante non seulement pour garantir une cohérence entre les divers systèmes juridiques, mais également pour définir la norme appropriée en matière de protection des droits au respect de la vie privée. Dans ces circonstances, le pouvoir de la législation est limité : les changements en termes d'approches des autorités nationales de contrôle doivent avoir lieu à un niveau culturel plutôt qu'à un niveau politique/législatif.

5.2. Domaines problématiques concernant la protection des données

La présente sous-section identifie les principaux domaines exclus ou exemptés de l'application de la loi relative à la protection des données, ou qui ne sont pas couverts de manière effective. À cet égard, il existe trois grandes catégories qui doivent être mentionnées : l'exclusion du régime de protection des données des activités liées à la sûreté de l'État (par exemple, les services de renseignements, les activités militaires, etc.) ; la protection des données liées à la santé d'un individu ; et la vidéosurveillance.

5.2.1. Protection des données liées à la sûreté de l'État

L'article 13, paragraphe 1, de la directive relative à la protection des données (concernant les exemptions et limitations) prévoit que « les États membres peuvent prendre des mesures législatives visant à limiter la portée des obligations et des droits prévus à l'article 6, paragraphe 1, à l'article 10, à l'article 11, paragraphe 1, et aux articles 12 et 21, lorsqu'une telle limitation constitue une mesure nécessaire pour sauvegarder : (a) la sûreté de l'État ; (b) la défense ; (c) la sécurité publique ».

Les exceptions visées à l'article 13, paragraphe 1, points a) à c), de la directive relative à la protection des données sont interconnectées. Dans divers États membres (le Danemark, la Grèce, l'Irlande, le Luxembourg, le Portugal, et la Roumanie), ces exceptions sont identifiées comme étant les principaux domaines exclus du cadre de la loi relative à la protection des données. Ceci est prévu en raison du libellé de l'article 13 de la directive relative à la protection des données. Cependant, quatre questions majeures doivent être prises en considération en ce qui concerne l'interprétation de ladite disposition.

Tout d'abord, la formulation prévoit des « limitations » par rapport aux questions de sécurité. Ceci ne doit pas être interprété comme équivalant aux « exceptions » au champ d'application de la directive. Cette analyse grammaticale n'est pas la seule raison pour affirmer que le champ des activités de diverses branches de l'exécutif relève du champ d'application de la directive.

Deuxièmement, conformément au premier considérant du préambule de la directive, le traitement des données à caractère personnel est fondé sur la CEDH. En outre, le troisième considérant du préambule stipule

explicitement que les droits fondamentaux des personnes doivent être conservés. Comme nous l'avons indiqué précédemment dans d'autres parties de la présente étude comparative, la protection des droits de l'homme et de l'intégrité de la personne sont des conditions fondamentales du domaine de protection des données.[104]

Troisièmement, l'essence même de la structure globale de la directive n'est pas de délimiter un champ sans surveillance dans lequel les États seraient exempts des exigences légales. Au contraire, s'agissant des questions de sûreté de l'État, un test de proportionnalité est nécessaire, qui permettra de mettre en balance les droits fondamentaux et les autres intérêts et non pas simplement de passer outre aux premiers.

Quatrièmement, la directive doit être interprétée conformément à l'article 8 de la Charte des droits fondamentaux de l'UE qui, d'après le nouvel article 6 du Traité sur l'Union européenne a « la même valeur juridique que les traités ». L'article 8 ne peut être limité que dans les conditions établies à l'article 52 de la Charte. L'article 13, paragraphe 1, de la directive relative à la protection des données prévoit de grandes exceptions et limitations concernant la sécurité publique, la défense, la sûreté de l'État (y compris le bien-être économique de l'État lorsque ces traitements sont liés à des questions de sûreté de l'État) et les activités de l'État relatives à des domaines du droit pénal. L'ampleur de ces exceptions et restrictions manque de clarté. Dans plusieurs États membres, ces domaines sont tous exclus des législations relatives à la protection des données. Cela laisse un domaine extrêmement vaste non réglementé avec des conséquences potentiellement graves pour la protection des droits fondamentaux. Conformément à l'article 52 de la Charte des droits fondamentaux de l'UE, toute limitation de l'exercice des droits et libertés reconnus par la Charte « doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés ».

C'est pour ces raisons que le choix fait par les législateurs nationaux d'exempter totalement certaines branches de l'exécutif (services de renseignement, Ministère de la Défense, etc.) ne rentre pas dans le cadre normatif de la directive relative à la protection des données.

5.2.2. Protection des données relative à la santé des personnes

Des préoccupations ont été soulevées dans plusieurs pays (comme en Bulgarie, en Suède, et en Slovénie) concernant le cadre de la protection portant sur les données relatives à la santé. L'article 8, paragraphe 2, de la directive relative à la protection des données oblige les États membres à interdire le traitement des données relatives à la santé des individus. L'article 8, paragraphe 3, prévoit une exception au paragraphe 2 « lorsque le traitement des données est nécessaire aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements ou de la gestion de services de santé et que le traitement de ces données est effectué par un praticien de la santé soumis par le droit national ou par des réglementations arrêtées par les autorités nationales compétentes au secret professionnel, ou par une autre personne également soumise à une obligation de secret équivalente ».

Le fait d'autoriser l'ensemble du personnel de santé à accéder à toutes les données des patients permet d'améliorer l'efficacité du service et facilite la prise en charge des urgences médicales où le gain de temps est une question vitale. Toutefois, cela signifie également que davantage de personnes ont accès à des données sensibles (d'où une ingérence plus importante dans la vie privée) ainsi que des risques accrus de fuites de données sensibles. L'accessibilité peut être décidée sur la base, par exemple, du poste, de la spécialité médicale et de la coopération établie. Les divisions qui coopèrent régulièrement car appartenant à la même organisation devraient normalement être en mesure d'accéder aux informations les unes des autres, en supposant que la confidentialité est garantie. Des outils efficaces pour le suivi et la traçabilité sont également nécessaires. L'identification de l'utilisateur doit être conforme aux restrictions en matière de sécurité.

Prévoir une solution forcée à cela, par le biais d'un instrument européen, peut entraîner des répercussions graves sur le secteur des soins de santé dans les États membres. Il semble plus plausible de faire en sorte que les règlements destinés aux professionnels des soins de santé en ce qui concerne le respect de la confidentialité et de la vie privée soient conformes aux objectifs de la directive afin de garantir la protection efficace des droits des individus sans en même temps compromettre leur droit aux soins.[105]

Dans certains États membres, les législatures ont élaboré récemment des lois dans ce domaine. Par exemple, en Belgique, une loi a été proposée concernant la mise en place d'une plateforme « e-santé »[106] à travers laquelle des données médicales et autres seront échangées électroniquement entre les professionnels et les institutions du secteur de la santé, dans le but de simplifier et d'améliorer le système de santé. Ce système permet également la transmission d'ordonnances électroniques de produits pharmaceutiques. Toutefois, étant donné que les médecins, les hôpitaux, les caisses d'assurance maladie et certaines institutions de sécurité sociale y auront accès, la vie privée des patients risque de ne pas être suffisamment protégée. L'élaboration de législations nationales relatives au domaine sensible de la santé et des droits des citoyens devrait être soigneusement équilibrée.

5.2.3. Protection des données en rapport avec la vidéosurveillance

Comme nous l'avons indiqué précédemment, la vidéosurveillance a été signalée parmi les domaines qui pourraient susciter des préoccupations. En Autriche, la grande majorité des caméras de surveillance ne sont pas enregistrées et ne sont donc pas sous la surveillance et le contrôle de l'autorité nationale chargée de la protection des données. En Allemagne, des cas de vidéosurveillance secrète de salariés sur leur lieu de travail ont été signalés. En outre, le droit à l'autodétermination personnelle est souvent violé si les personnes concernées sont insuffisamment informées sur l'utilisation et/ou le traitement de leurs données. Un exemple notoire de vidéosurveillance sur les lieux de travail est le cas de la surveillance

104 Voir la section 2.1 concernant les normes fondamentales en matière de protection des données au niveau du Conseil de l'Europe.

105 Voir aussi le document de travail WP131 du Groupe de l'article 29 du 15 février 2007 : http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp131_fr.pdf.

106 Belgique/Commissie voor de bescherming van de persoonlijke levenssfeer, Advies nr. 33/2008, disponible à l'adresse : www.privacycommission.be/nl/docs/Commission/2008/advies_33_2008.pdf ; Commission de la protection de la vie privée, Avis n° 33/2008 (24 septembre 2008), disponible à l'adresse : www.privacycommission.be/fr/docs/Commission/2008/avis_33_2008.pdf.

des administrateurs de l'autorité nationale de concurrence de Chypre par le chef de l'autorité, qui a finalement conduit à sa démission. Il est rappelé qu'en Grèce, l'autorité nationale chargée de la protection des données s'est vu refuser l'accès aux locaux de la police où le traitement des données avait lieu. Au Royaume-Uni, il existe quelques restrictions sur l'utilisation de caméras de vidéosurveillance pour surveiller les lieux publics, mais le Royaume-Uni est, de tous les pays du monde, celui qui en compte le plus grand nombre.[107]

La directive relative à la protection des données n'offre aucune orientation détaillée concernant la vidéosurveillance. L'énoncé du quatorzième considérant du préambule est le suivant : « compte tenu de l'importance du développement en cours, dans le cadre de la société de l'information, des techniques pour capter, transmettre, manipuler, enregistrer, conserver ou communiquer les données constituées par des sons et des images, relatives aux personnes physiques, la présente directive est appelée à s'appliquer aux traitements portant sur ces données ». Il peut être entendu que ces données peuvent largement relever de la définition des « données à caractère personnel », tel que prévu par l'article 2 de la directive relative à la protection des données et par conséquent, une personne peut se prévaloir de la protection prévue par le droit communautaire.

Toutefois, l'article 33 de la directive relative à la protection des données stipule que : « La Commission examine, en particulier, l'application de la présente directive aux traitements de données constituées par des sons et des images, relatives aux personnes physiques, et elle présente les propositions appropriées qui pourraient s'avérer nécessaires en tenant compte des développements de la technologie de l'information et à la lumière de l'état des travaux sur la société de l'information ». Il ressort de cette référence que l'UE accorde un intérêt particulier à la vidéosurveillance. Il convient de noter que le Groupe de l'article 29 a fourni des avis à cet égard.[108] Compte tenu des particularités techniques intrinsèques des données de son et d'image et des multiples effets possibles sur les droits des personnes, une mesure législative européenne distincte doit être considérée à l'avenir.

Le corps législatif de certains pays a été récemment impliqué dans ce domaine, mais on peut se demander si la voie engagée est appropriée. Deux lois relatives à la vidéosurveillance ont été adoptées au Danemark en juin 2007. La première loi confère aux entreprises privées des pouvoirs étendus pour effectuer des activités de surveillance dans les domaines liés à leur propriété. Elles ne sont plus obligées de notifier à l'autorité chargée de la protection des données l'installation d'équipements de surveillance. La seconde loi confère aux services de renseignements de la police davantage de pouvoirs pour échanger des informations avec les services de renseignements militaires et recueillir des informations auprès d'autres autorités publiques, telles que les hôpitaux, les écoles, les bibliothèques, les services sociaux, etc. sans ordonnance judiciaire. Elle renforce également les pouvoirs de la police de demander aux institutions publiques et aux particuliers d'installer et d'effectuer une vidéosurveillance.

La question de la protection des données dans le contexte de la vidéosurveillance s'inscrit dans le cadre d'un débat plus général : la nécessité d'actualiser la législation de protection des données pour lui permettre de tenir compte des avancées technologiques. Les progrès récents et actuels (y compris informatique dématérialisée, informatique autonomique, implants TIC dans le corps humain, interface cerveau-machine) posent de nouveaux défis qui doivent être relevés de toute urgence. Les implications de l'internet et de nouvelles technologies de réseaux sociaux, comme facebook et twitter, pour la protection des droits fondamentaux relatifs aux données à caractère personnel doivent également être pris en considération : l'importance de « l'identité numérique » de chacun ne saurait être sous-estimée.[109] De nos jours, elle représente une composante essentielle de l'identité et de la personnalité globale d'une personne. En tant que telle, elle mérite un niveau de protection équivalent à d'autres facettes « traditionnelles » de la personnalité. L'«identité numérique» est inextricablement liée à l'« existence numérique » d'un individu. Dans le vaste cyberespace, un individu peut établir sa présence et mener des activités qui étaient auparavant concevables uniquement dans le domaine public « réel ». Une attention particulière doit être accordée à cet égard aux travaux du forum sur la gouvernance de l'internet et la «charte internet», mentionnée dans une recommandation du Parlement européen sur le renforcement de la sécurité et des libertés fondamentales sur l'internet.[110]

107 www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/1806.htm#a41, au paragraphe 213.

108 Voir le document de travail WP 67 du 25 novembre 2002 : http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp67_fr.pdf ; avis 4/2004, WP 89 du 11 février 2004 : http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp89_fr.pdf.

109 Rapport contenant une proposition de recommandation du Parlement européen à l'intention du Conseil sur le renforcement de la sécurité et des libertés fondamentales sur Internet (2008/2160(INI)), *Commission des libertés civiles, de la justice et des affaires intérieures,* (en anglais uniquement) www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/a6-0103_2009_/a6-0103_2009_en.pdf.

110 T6-0194/2009 du 26 mars 2009.

6 Pratiques encourageantes

Cette section du rapport présente un bref compte rendu des pratiques encourageantes les plus pertinentes en matière de protection des données dans les États membres, mettant en lumière des exemples nationaux positifs concernant les autorités de protection des données, le respect de la législation, les recours et les activités de sensibilisation. L'identification d'exemples de « pratiques encourageantes » permet de reconnaître la valeur de pratiques particulières et contribue à favoriser une culture de progrès constants. Cependant, l'identification d'une pratique comme telle n'implique pas que celle-ci a été examinée directement en profondeur par l'agence.

6.1. Autorités de protection des données

S'agissant des autorités nationales de protection des données, les pratiques encourageantes concernent l'organisation des autorités de contrôle ou leur travail. D'une part, plusieurs États membres ont doté leurs agences nationales chargées de la protection des données de pouvoirs spécifiques et leur assurent un degré d'autonomie élevé. D'autre part, les autorités de protection des données ont établi une coopération avec trois catégories de parties prenantes : les institutions publiques, les ONG actives sur le terrain et les autorités de protection des données d'autres États membres.

L'indépendance des autorités de protection des données est un facteur essentiel pour assurer un niveau élevé de protection des données. De ce point de vue, des mesures structurelles telles que l'attribution à l'autorité de contrôle d'une personnalité juridique distincte (comme c'est le cas en Espagne et à Malte) ou la codification constitutionnelle de ses pouvoirs et de ses compétences (comme c'est le cas en Grèce et au Portugal) constituent donc des exemples positifs qui renforcent l'indépendance des autorités de contrôle. Même si l'élection par le Parlement ne garantit pas nécessairement l'indépendance des délégués de l'autorité de contrôle, les procédures exigeant un consensus entre la majorité et l'opposition (comme en Grèce) doivent être considérées comme une pratique encourageante. Un autre exemple de pratique encourageante garantissant un degré d'autonomie élevé à l'autorité chargée de la protection des données est celui de la Slovénie où l'agence nationale a qualité pour agir pour contester la constitutionnalité de la législation devant la cour constitutionnelle.

Le pouvoir des autorités de protection des données à s'engager activement dans la préparation et la proposition de codes de conduite représente une pratique positive. La participation à l'élaboration de codes de conduite en matière de protection des données non seulement contribue à améliorer la protection générale des citoyens, mais également à augmenter la visibilité des autorités nationales dans la société, et les autorités de protection des données devraient s'y employer de manière proactive. En Irlande, en particulier, la législation nationale confère à l'autorité nationale chargée de la protection des données le pouvoir de proposer et d'élaborer des codes qui, s'ils sont approuvés par le Parlement, auront des effets contraignants.[111]

La coopération et la communication régulière entre différents organismes publics et les autorités de protection des données ont la capacité de garantir un meilleur fonctionnement du système de protection des données dans son ensemble. En Allemagne, par exemple, des programmes de formation intensifs sont dispensés sous la forme d'une académie de protection des données qui a développé des programmes de formation complets et systématiques pour tous les domaines de l'administration.

Une coopération étroite et une communication avec les ONG qui sont actives dans le domaine de la protection des données offrent plusieurs avantages. Tout d'abord, les ONG sont en mesure de signaler aux autorités nationales et à la société civile les violations systématiques et/ou flagrantes des lois relatives à la protection des données. Ainsi, une autorité de contrôle supplémentaire et informelle est en place. Dans certains cas, elles contribuent efficacement à la surveillance complète de la protection des données sur le terrain. Deuxièmement, les ONG assurent un canal de communication « ascendant », en permettant aux citoyens actifs de proposer des amendements au cadre juridique. Dans cette perspective, l'autorité chargée de la protection des données en Hongrie aurait accepté d'aider et de coopérer avec des ONG. Par exemple, en 2000, elle a revu le plan de protection des données d'un projet de recherche sur les droits des Roms réalisé par le Comité Helsinki de Hongrie et en 2004, le personnel de l'autorité, en collaboration avec l'Union hongroise pour les libertés civiles, a testé plusieurs locaux de santé publique pour vérifier si des tests de dépistage VIH étaient réalisés de façon anonyme et gratuite comme annoncé. Sur la base des conclusions, une recommandation a été émise.[112]

Enfin, une coopération et une communication permanente entre les autorités de protection des données d'autres États (membres de l'UE ou non) sont également utiles. Au niveau de l'UE, cela est réalisé principalement dans le cadre du groupe de travail établi par l'article 29 de la directive relative à la protection des données. Ce forum prévoit l'environnement institutionnel nécessaire aux autorités de protection des données pour harmoniser l'application de leurs lois respectives. La coopération bilatérale ou multilatérale, sur la base d'affinités régionales ou linguistiques, doit également être encouragée au sein des pays de l'UE et avec les pays tiers. Un bon exemple est celui du Portugal où une réunion annuelle et informelle est organisée avec la partie homologue espagnole pour discuter des développements les plus importants en matière de protection de données.

111 Loi irlandaise relative à la protection des données (*Ireland Data Protection Act*) (1988-2003), section 13.

112 http://beszelo.c3.hu/03/11/04zadori.htm ; http://abiweb.obh.hu/dpc/index.php?menu=reports/2004/lll/2&dok=reports/2004/27.

6.2. Respect de la législation

S'agissant du respect de la législation, les pratiques encourageantes découlent de la capacité accrue des autorités de protection des données à détecter les violations et à poursuivre ceux qui ont enfreint la loi. Une caractéristique intéressante des pratiques encourageantes mises en œuvre en Italie est la coopération entre l'agence nationale et les organes de police, dans le cadre d'un protocole ad hoc avec la police financière. Un exemple de pratiques encourageantes a également été relevé en Roumanie où l'autorité chargée de la protection des données a signé des accords de coopération avec des institutions publiques comme l'autorité nationale chargée de la protection des consommateurs, l'inspection générale de la police roumaine, la brigade financière, le Ministère des Communications et des Technologies de l'Information, et l'Office national du registre du commerce.

Un aspect intéressant du système néerlandais est l'obligation du gouvernement, dans un délai de cinq ans après l'entrée en vigueur de la législation nationale, de présenter un rapport au parlement néerlandais sur l'efficacité et les effets de la loi dans la pratique. Cette évaluation de l'autorité néerlandaise en matière de protection des données a été menée en deux phases. La première phase d'évaluation, une étude de sources secondaires, a eu lieu en 2007 et a été présentée dans le rapport intitulé Première phase d'évaluation de loi relative à la protection des données à caractère personnel (*Eerste fase evaluatie Wet bescherming persoonsgegevens*).[113] La seconde phase de l'évaluation comprend des études de cas et des entretiens, concernant l'efficacité de la loi relative à la protection des données à caractère personnel dans la pratique. Le rapport a été publié en février 2009.[114]

6.3. Connaissance des droits

La section 4.4 a donné un aperçu comparatif relatif à la connaissance des droits, tandis que la section 5.1.4, a été consacrée aux lacunes apparaissant dans ce domaine. Les activités de sensibilisation aux droits menées par les autorités de protection des données ont donné lieu à un large éventail de pratiques encourageantes. Tout d'abord, bon nombre d'agences nationales ont mis en place des sites web conviviaux contenant les informations pertinentes relatives à la protection des données. Ces sites web se déclinent souvent en plusieurs langues. Une seconde série de pratiques encourageantes concerne les activités éducatives menées par les agences pour favoriser la culture du respect de la vie privée notamment, mais pas exclusivement, chez les jeunes. Des cours spécifiques, des séminaires et des conférences peuvent être organisés à l'intention des acteurs impliqués dans les opérations de traitement de données. Dispenser des conseils à ces acteurs constitue une autre pratique encourageante importante mise en œuvre par les autorités de protection des données. Enfin, des prix spéciaux peuvent être attribués pour promouvoir le respect de la législation relative à la protection des données.

Dans le but de faire appliquer la loi de la manière la plus efficace et de faciliter l'accès à des recours efficaces, bon nombre d'autorités de protection des données ont créé des sites et des pages web grâce auxquels il est possible de soumettre des documents officiels prévus par la législation, d'enregistrer ou de notifier le traitement de données à caractère personnel, de demander et de recevoir des conseils et/ou des informations et de déposer une plainte. En Allemagne, par exemple, le centre indépendant pour la protection des données du Schleswig-Holstein (soutenu par presque toutes les autorités de protection des données germanophones), a créé un site web contenant des informations détaillées sur les derniers développements, des affaires judiciaires, des rapports et des communiqués de presse, et une base de données sur les concepts clés.[115] Une page d'accueil contenant des informations exhaustives sur la façon de se protéger contre les violations de protection des données, destinées en particulier aux éducateurs et à d'autres personnes occupant des postes de « multiplicateurs de l'information », a également été développée.[116] En Espagne[117] comme en Italie, un système de transmission de données permet de notifier à l'autorité chargée de la protection des données des dossiers via l'internet.

Dans de nombreux cas, la page web officielle est multilingue, en raison du régime linguistique en vigueur dans un État membre donné où plusieurs langues sont utilisées ou parce qu'une version anglaise (internationale) est fournie en vue d'élargir l'accès. Les autorités de protection des données devraient envisager sérieusement d'adopter cette caractéristique d'accès compte tenu de la libre circulation des citoyens européens dans les 27 États membres. Au Luxembourg, par exemple, les documents du site web multilingue de l'autorité nationale chargée de la protection des données sont relativement détaillés et offrent une multitude d'informations aux personnes concernées, aux responsables du traitement, aux sous-traitants et aux législateurs.[118] En Finlande également, le site web de l'autorité chargée de la protection des données constitue un autre moyen majeur qui fournit des informations en plusieurs langues.[119]

La politique éducative élaborée par certaines autorités nationales chargées de la protection des données est un élément innovant présentant de multiples aspects. D'une part, proposer des programmes éducatifs à tous les niveaux de l'enseignement, à savoir de l'école primaire à l'université, favorise la sensibilisation aux questions de protection des données. D'autre part, le fait de cibler des segments d'âge différents de la société par le biais de programmes adaptés à chaque public peut assurer un retour d'informations utile sur les particularités et les besoins des différents niveaux de nos sociétés. Les médias offrent l'espace nécessaire pour élaborer des programmes de télévision, des pages web interactives et d'autres initiatives visant à sensibiliser le public. En République tchèque, par exemple, l'autorité nationale gère un projet ciblant les enfants et les jeunes ainsi qu'un programme éducatif intitulé « Protection des données à caractère personnel dans l'éducation ». L'autorité nationale a également coopéré en ce qui concerne la réalisation en 2006 d'une série télévisée sur la protection des données intitulée « La méconnaissance n'est pas une excuse – Nous avons tous

113 G. Zwenne *et al.* (2007), *Eerste fase evaluatie Wet bescherming persoonsgegevens,* disponible à l'adresse : www.wodc.nl/images/1382a_volledige_tekst_tcm44-61969. Un résumé figure à la page 207.

114 H.B. Winter *et al.* (2008), *Wat niet weet wat niet deert,* WODC 2008, www.wodc.nl/onderzoeksdatabase/evaluatie-wet-bescherming-persoonsgegevens-wbp-2e-fase.aspx#.

115 www.datenschutz.de.

116 www.datenparty.de.

117 https://212.170.242.196/portalweb/canalresponsable/inscripcion_ficheros/Notificaciones_tele/que_es/index-ides- idphp.php.

118 www.cnpd.lu/fr.

119 www.tietosuoja.fi.

des secrets » (selon le rapport annuel 2006, chaque épisode a été regardé par environ 160 000 à 310 000 personnes).[120] La participation d'experts de l'autorité chargée de la protection des données à des conférences et séminaires organisés à l'intention de membres de groupes d'intérêt dans le domaine de la protection des données constituent d'autres pratiques encourageantes dans le domaine de l'éducation. C'est le cas de la Finlande où un magazine destiné en particulier aux responsables du traitement est publié quatre fois par an par l'autorité. En outre, des conseils sont également donnés par téléphone. Au Portugal et en Belgique, l'autorité organise des programmes de stages permettant à des étudiants et des diplômés en droit d'effectuer une période de formation pratique afin de se familiariser avec ses travaux. En Italie, des initiatives de communication spécifiques ont été lancées à l'intention des jeunes en particulier (parmi ces initiatives, l'autorité chargée de la protection des données a collaboré avec le Ministère de l'Éducation à la rédaction de lignes directrices relatives à l'utilisation appropriée de téléphones portables et de leurs caméras vidéo pendant les cours).

La fourniture de conseils et d'informations concernant divers projets de système de données représentent une tâche importante et en expansion constante. L'autorité nationale en Espagne a déployé des efforts pour publier des guides concernant de nombreux domaines qui ont des implications pour les questions de protection des données : les droits des enfants et les obligations des parents ;[121] les mesures de sécurité en matière de données ;[122] les fichiers ;[123] la protection des données à caractère personnel en tant que droit fondamental ;[124] et la protection des données à caractère personnel dans les municipalités,[125] les écoles et universités publiques, les associations professionnelles, les services de santé publics et les services sociaux publics. C'est également le cas en Estonie[126] et en Italie[127]. En France et au Royaume-Uni, les autorités de protection des données ont publié des guides sur la protection des données dans le domaine de l'emploi.

S'agissant des activités de sensibilisation, une pratique encourageante à mettre en évidence est la campagne d'information et de consultation menée par l'autorité nationale chargée de la protection des données en ce qui concerne la lutte contre le « spam » ou courriel indésirable. En France, par exemple, l'objectif de l'autorité chargée de la protection des données est de recueillir et de traiter les plaintes des utilisateurs de l'internet, et de les diriger vers les différents acteurs impliqués dans la lutte contre le « spam », tels que les autorités publiques et politiques et les professionnels, selon leurs diverses missions et capacités.[128]

Par ailleurs, en Espagne, l'autorité nationale chargée de la protection des données a été directement engagée pour élaborer des guides d'information[129] et un décalogue de recommandations[130] visant à lutter contre le spam.

Parmi les pratiques encourageantes, figure également la création de prix spéciaux attribués par les autorités de protection des données. En Slovénie, chaque année, à l'occasion de la journée européenne de la protection des données, l'autorité nationale de contrôle sélectionne l'entreprise privée ou l'organisme public qui, selon elle, a le mieux réussi à assurer la protection des données à caractère personnel. Le prix de « pratique encourageante » est décerné et recommandé en tant que modèle dans le domaine.[131] En France, un prix de doctorat intitulé « Traitement des données, fichiers de données et libertés individuelles », d'un montant de 7 000 euros, a été créé par l'autorité nationale de contrôle. Dans le même esprit, une proposition pour la création d'un prix Nobel dans le domaine de la protection des données et des libertés a été approuvée en 2008, ce prix devant être décerné pour la première fois en 2010.[132] En outre, un prix récompensant les meilleures pratiques en matière de protection des données dans les services publics européens a été institué en Espagne.

120 *Výroční zpráva za rok 2006* (rapport annuel 2006), p. 2 disponible à l'adresse : www.uoou.cz/vz_2006.pdf.
121 www.agpd.es/portalweb/canal_joven/common/pdfs/recomendaciones_menores_2008.pdf.
122 www.agpd.es/portalweb/canaldocumentacion/publicaciones/common/pdfs/guia_seguridad_datos_2008.pdf.
123 https://212.170.242.196/portalweb/canaldocumentacion/publicaciones/common/pdfs/guia_responsable_ficheros.pdf.
124 https://212.170.242.196/portalweb/canal_joven/common/pdfs/FOLLETO.pdf.
125 www.madrid.org/cs/Satellite?c=CM_Publicacion_FA&cid=1114180060765&idPage=1109266885968&language=es&pagename=APDCM %2FCM_Publicacion_FA %2FfichaPublicacionAPDCM.
126 www.aki.ee/est/?part=html&id=56.
127 Parmi les lignes directrices les plus pertinentes, figurent les lignes directrices pratiques destinées aux PME, sur les relations employeur-employé dans le secteur privé et le secteur public, sur les relations avec les clients dans le secteur bancaire, sur la publication et la diffusion de documents par les autorités locales, sur le traitement des données dans le cadre des essais cliniques pharmaceutiques, sur les cartes de fidélité.
128 Voir l'accord de partenariat signé le 30.10.2007 entre la CNIL et l'association Signal Spam.
129 www.agpd.es/portalweb/canaldocumentacion/lucha_contra_spam/common/pdfs/INFORMACI-OO-N- SPAM--ap-V.-30-mayo-cp-.pdf.
130 https://212.170.242.196/portalweb/canaldocumentacion/lucha_contra_spam/common/pdfs/CONSEJOS-para-prevenir-el-Spam_guia.pdf.
131 www.lek.si/slo/mediji/sporocila-za-javnost/3849/ et http://www.ip-rs.si/novice/detajl/nagrajenca-ob-2-evropskem-dnevu-varstva-osebnih-podatkov-sta-zavod-za-zdravstveno-zavarovanje-slove.
132 Déclaration de l'IPA (*International Privacy Association*) sur la création d'un prix Nobel dans le domaine de la protection des données et des libertés, à décerner tous les ans par la conférence mondiale des commissaires à la protection des données www.privacyconference2008.org/index.php?langue=2&page_id=1.

7 Conclusion

Certains des problèmes les plus urgents auxquels se heurte le régime de protection des données actuel ont plusieurs solutions. Bien que des mesures nationales puissent manifestement être adoptées, il est possible que l'application d'une approche coordonnée et harmonisée à l'échelle de l'UE s'avère plus efficace pour renforcer la protection des données à caractère personnel.

Les institutions de l'UE jouent un rôle particulièrement important à cet égard, et le Parlement européen a manifesté un vif intérêt concernant la protection des données.[133] Le Parlement européen ainsi que le Conseil de l'UE et la Commission européenne sont invités à introduire des réformes législatives afin de garantir l'efficacité du régime de protection des données. À cet égard, il est rassurant de constater que la commissaire à la justice, aux droits fondamentaux et à la citoyenneté a souligné l'importance de la protection des données et son intention de regrouper les règles de l'UE relatives à la protection des données au sein d'un instrument juridique moderne et exhaustif.[134] La CJUE, à son tour, a adopté une attitude proactive concernant la protection des données. Ainsi, jusqu'à présent, elle a interprété un instrument d'harmonisation du marché intérieur (la directive relative à la protection des données) de manière à favoriser la protection d'un droit fondamental au sein de la Communauté. À cet égard, elle a adopté une interprétation étendue du champ de protection de la directive relative à la protection des données, qui dépasse l'exercice d'activités économiques, et une interprétation restrictive des domaines exempts de protection.

Les améliorations de la législation existante relative à la protection des données peuvent être réalisées par une coopération entre les autorités nationales de protection des données et le Groupe de l'article 29. En particulier, les avis et recommandations du groupe de travail, dans la mesure où ils sont pris en considération par les autorités nationales de protection des données, contribuent à l'élaboration d'une norme commune de l'UE offrant un niveau élevé de protection des données à caractère personnel. Le contrôleur européen de la protection des données est chargé de veiller à ce que les droits fondamentaux et les libertés des personnes physiques, et en particulier le droit à la protection de leur vie privée, soient respectés par les institutions et organismes de l'UE. La tâche de consultation du contrôleur européen de la protection des données revêt une importance particulière en ce qu'elle contribue efficacement à la protection des libertés fondamentales des citoyens de l'UE chaque fois qu'une nouvelle législation est adoptée.

Des améliorations sont également nécessaires concernant l'indépendance, l'efficacité, les ressources et les pouvoirs des autorités de protection des données. Elles jouent un rôle crucial de gardiennes de la protection des données aux yeux du public. L'ensemble du système de la protection des données dépend de la confiance accordée par le public à ces autorités. Il sera difficile de convaincre les citoyens du sérieux avec lequel sont traitées leurs inquiétudes concernant la protection des données et de la vie privée, si des doutes persistent quant à l'indépendance des autorités de protection des données ou si les ressources qui leur sont attribuées sont jugées insuffisantes pour leur permettre de s'acquitter de manière efficace et efficiente de leurs obligations.

Les autorités de protection des données sont également un élément crucial de l'architecture des droits fondamentaux de l'UE car cette dernière joue un rôle de pionnier dans la protection des données en tant que droit fondamental et qu'elle a contribué à stimuler le développement des systèmes de protection des données dans de nombreux États membres. La protection des données est également pour l'UE un domaine politique clé, dans lequel elle est habilitée à légiférer concernant les droits fondamentaux. Pour cette raison, l'efficacité d'ensemble du système de protection des données pourrait également avoir un effet positif sur la perception de l'UE en tant que gardienne des droits fondamentaux par le public.

133 Par exemple, la proposition de la Commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen concernant une Recommandation du Parlement européen à l'intention du Conseil sur le renforcement de la sécurité et des libertés fondamentales sur Internet (2008/2160(INI)).

134 Communication aux membres du Parlement européen, 7.1.2010, doc. PE431.139v02-00, www.europarl.europa.eu/hearings/static/commissioners/answers/reding_replies_fr.pdf.

Ces quatre rapports élaborés par l'Agence des droits fondamentaux de l'Union européenne (FRA) examinent des questions, des institutions et des législations communautaires étroitement liées, qui contribuent à l'architecture globale des droits fondamentaux au sein de l'Union européenne. Les composantes de ce paysage des droits fondamentaux sont les autorités chargées de la protection des données et les institutions nationales de défense des droits de l'homme (INDH), ainsi que les organismes de promotion de l'égalité mis en place dans le cadre de la directive sur l'égalité raciale (2000/43/CE).

Agence des droits fondamentaux de l'Union européenne

La protection des données à caractère personnel dans l'Union européenne : le rôle des autorités nationales chargées de la protection des données

Luxembourg: Office des publications de l'Union européenne, 2012

2012 – 50 p. – 21 x 29,7 cm

ISBN 978-92-9192-510-0
doi:10.2811/47365

De nombreuses informations sur l'Agence des droits fondamentaux de l'Union européenne sont disponibles sur le site internet de la FRA (fra.europa.eu).

TK-31-09-265-FR-C

doi:10.2811/47365

FRA – Agence des droits fondamentaux de l'Union européenne
Schwarzenbergplatz 11
1040 Vienne
Autriche
Tél. : +43 (0) 1 580 30 - 0
Fax : +43 (0) 1 580 30 - 699
E-mail : information@fra.europa.eu
http://fra.europa.eu

Office des publications

ISBN 978-92-9192-510-0