LA PROTECTION DES DROITS FONDAMENTAUX, AU CŒUR DES NOUVELLES PRIORITES DE L'ELSJ (L'ESPACE DE LIBERTE, SECURITE ET JUSTICE DE L'UNION EUROPEENNE): L'EXEMPLE DE LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

Sylvie PEYROU-PISTOULEY[*]

ABSTRACT: *Facing the recent raise of mechanisms for storing and exchanging personal data between public authorities, established in Europe to ensure a wide police cooperation, notably in order to fight against terrorist issues, the personal data protection question arises. The answer of the European Union in this field seems unsatisfying. Indeed, taking into account the framework of the EU pillars construction from Maastricht, this is a fragmented system of protection, gradually built and well-know as insufficient regarding police and judicial cooperation ("third pillar"). However, this legal system is currently evolving. The first evolution factor, completely exogenous, is the European Court of Human Rights, which, notably thanks to its recent case Marper vs. The United Kingdom, becomes the officer of the European Union Area of Freedom, Security and Justice (AFSJ). The endogenous factors from the EU are as much essential, such as the Stockholm Program that defines the new priorities for five years for the AFSJ, or as the Lisbon Treaty, which, eventually, came into force, or as the scheduled EU joining to the European Convention on Human Rights.*

KEYWORD: *storing and exchanging personal data, European Court of Human Rights, personal data protection, police and judicial cooperation*

JEL CLASSIFICATION: *K 00, K 23.*

Introduction

Depuis les attentats du 11 septembre 2001 aux Etats-Unis, toutes les démocraties occidentales ont développé un arsenal juridique propre à organiser la lutte contre le terrorisme. Ceci concerne non seulement les Etats en tant que tels mais aussi l'Union Européenne (UE). La coopération policière mais également judiciaire en matière pénale, qui s'est considérablement développée afin d'édifier un « Espace de liberté, sécurité et justice » (ELSJ) au sein de l'UE, se nourrit en particulier de constitution de fichiers de données personnelles, qui tissent un réseau d'informations indispensables en matière de

[*] Maître de Conférences à la Faculté Pluridisciplinaire de Bayonne, Centre de Documentation et de Recherches Européennes.

lutte contre le terrorisme, mais aussi contre le grand banditisme, voire plus simplement contre l'immigration illégale.

Qu'en est-il dès lors de la protection des droits fondamentaux, et plus particulièrement de la protection des données à caractère personnel, qui alimentent un nombre croissant de fichiers, tant au niveau des Etats que de l'UE ? Si le souci majeur était jusqu'alors de renforcer la sécurité, dans le contexte de la menace terroriste, il semble néanmoins qu'un changement de cap soit en train de s'opérer au sein des instances européennes, dans la construction de l'ELSJ. En effet, le « Programme de Stockholm », adopté par le Conseil européen en décembre 2009 et véritable « feuille de route » pour l'Union dans les cinq ans à venir, a pour ambition désormais de placer le citoyen au centre des prochaines étapes de la construction de cet espace. Ceci signifie concevoir l'ELSJ comme « un espace unique de protection des droits fondamentaux », au sein duquel « le respect de la personne et de la dignité humaine (…) constitue une valeur essentielle »[1].

Deux questions se posent dès lors : celle de savoir, d'abord, quel constat peut être dressé en matière de protection des données à caractère personnel dans l'ELSJ, puis, conséquemment, si le dispositif juridique mis en place répond pleinement aux nouvelles exigences posées par le Programme de Stockholm. Le constat est celui d'un dispositif juridique insatisfaisant, la législation en matière de protection des données étant multiple et d'inégale valeur. C'est en effet au gré de l'ancienne construction en piliers de l'UE que les textes ont été élaborés, et le résultat dans l'ancien troisième pilier semble loin d'être à la hauteur de celui atteint dans le cadre communautaire. Dans le domaine de la coopération policière et judiciaire pénale, la question de la protection des données à caractère personnel a d'abord été réglée au cas par cas, par un certain nombre de textes spécifiques, mettant en place des coopérations spécifiques, dans le cadre des accords de Schengen, par exemple, ou encore d'Europol ou Eurojust etc. C'est donc un paysage morcelé qui s'est peu à peu mis en place. La décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008[2] a eu pour tâche par conséquent de poser un cadre général pour la protection des données dans l'ancien troisième pilier, afin d'harmoniser les dispositions existantes et d'offrir un niveau de protection comparable à celui existant dans le cadre communautaire. Mais ce texte – plus petit dénominateur commun atteint par les Etats dans une négociation où intérêts et égoïsmes nationaux ont prévalu - a manifestement manqué son but, et souffre de nombreuses limites ou insuffisances. Il est loisible de s'interroger au demeurant sur sa compatibilité avec les dispositions générales existantes en matière de protection des droits fondamentaux, à commencer par la Convention européenne des droits de l'homme (CEDH).

Ce sont d'ailleurs les limites intrinsèques au dispositif de protection des données dans l'ELSJ aujourd'hui qui expliquent ses actuelles mutations. La Cour européenne des droits de l'homme, grâce notamment à une très importante jurisprudence récente, va inciter nécessairement les acteurs institutionnels de l'ELSJ à l'évolution, dans un sens plus respectueux des droits individuels. L'évolution apparaît inéluctable par ailleurs suite aux changements induits par l'entrée en vigueur du traité de Lisbonne, en particulier la promotion de la Charte des droits fondamentaux de l'Union. La nouvelle impulsion

[1] V. conclusions du Conseil européen des 10 et 11 décembre 2009, doc. EUCO 6/09, § 27.

[2] Décision-cadre relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, JOUE 30 déc. 2008, L 350/60.

donnée par le Programme de Stockholm s'inscrit donc tout à fait logiquement dans ce nouveau contexte, ce qui va conduire, dans un proche avenir sans doute, à l'adoption d'un nouveau texte général assurant la protection des données au regard de toutes les actions de l'UE. Le dispositif actuel de protection des données à caractère personnel dans l'ELSJ est donc nettement insatisfaisant (I), mais il est en pleine mutation (II).

I Un dispositif juridique insatisfaisant

Il existe au sein de l'Union européenne un certain nombre de textes relatifs à la protection des données à caractère personnel. La construction en piliers de l'U.E. issue du traité de Maastricht a cependant concouru à la fragmentation de la législation en la matière, qui s'avère notoirement insuffisante s'agissant de l'Espace de liberté, sécurité et justice.

A) Un dispositif fragmenté

La dispersion de la réglementation en matière de protection des données résulte, non seulement de la construction en piliers de l'U.E., mais encore de la coexistence de dispositions générales ou spécifiques mal articulées.

1) Des législations propres à chaque pilier de l'UE

Très tôt, dans le domaine strictement communautaire, a été adopté un texte fondamental en matière de protection des données, 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[3]. Le problème majeur concernant ce texte, au demeurant plutôt satisfaisant quant à son contenu, est qu'il ne s'applique pas, par définition, aux activités qui ne relèvent pas du champ d'application du droit communautaire, telles que celles prévues aux titres V et VI du traité UE (l'ancien troisième pilier, l'ELSJ aujourd'hui), ni aux traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'Etat et les activités de l'Etat relatives à des domaines du droit pénal[4]. La même réserve peut être formulée s'agissant du règlement 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[5], qui s'applique au traitement des données par toutes les institutions et organes communautaires, 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[6].

Il manquait un texte équivalent, pour le troisième pilier, jusqu'à l'adoption de 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

[3] V. JOCE L.281 du 23 nov. 1995, p.31-50.

[4] A noter que ce texte prévoit en particulier dans son article 29 la création d'un groupe de travail, appelé « Groupe article 29 » ou G29 », composé des autorités de contrôle nationales des différents Etats membres afin de jouer un rôle consultatif auprès de la Commission sur les questions relatives à la protection des données, et de contribuer à une application uniforme des principes généraux des directives dans l'ensemble des Etats membres.

[5] V. JOCE L 8 du 12 janv. 2001, p. 1-22

[6] C'est sur la base de ce règlement qu'a été instituée une autorité de contrôle indépendante en la personne du Contrôleur Européen de la Protection des Données ou CEPD, qui dispose de pouvoirs étendus en matière de contrôle du traitement des données à caractère personnel par les organes communautaires, et qui a formulé un très grand nombre d'avis.

judiciaire en matière pénale[7]. Avant l'adoption de la décision-cadre, le troisième pilier n'était néanmoins pas vierge de toute disposition de protection des données, ce qui n'a pas manqué au demeurant de contribuer à la complexité, voire à l'absence de cohérence, du cadre législatif existant en la matière. L'analyse est inséparable du contexte sécuritaire, généralisé en Europe, qui favorise la collecte de données personnelles à des fins répressives au niveau des Etats, d'une ampleur aujourd'hui préoccupante. Il existe certes, nécessairement, au sein de tous les Etats membres, des autorités et des mécanismes de contrôle concernant le prélèvement ou la conservation des données personnelles, définis par la législation nationale. Ceci dit, toutes les données collectées au niveau national ne constituent que le premier étage d'une construction plus complexe où le deuxième étage, européen, surajoute ses propres fichiers, afin d'assurer une coopération policière et judiciaire étendue et de lutter contre la criminalité ou le terrorisme. On peut citer à cet égard le SIS (système d'information Schengen), le SID (système d'information des douanes), EURODAC (concernant les demandeurs d'asile et les immigrants clandestins), le VIS (système d'information sur les visas), EUROPOL (Office européen de police), EUROJUST (pour la coopération judiciaire), le dispositif issu du traité de Prüm désormais intégré dans le droit de l'UE[8], sans oublier les accords passés avec les Etats tiers, tel l'accord *PNR* (*Passenger Name Record*) intervenu entre les Etats-Unis et l'UE le 23 juillet 2007[9]. Tout ceci aboutit à un système de fichage complexe, sachant qu'une part de traitement des données purement nationale et une part commune coexistent. Pour la part nationale, il existe des dispositions de protection dans les différentes législations nationales, étant entendu que la place que prend la législation nationale est proportionnelle à l'ampleur de cette part purement nationale de traitement des données[10]. Le danger, manifeste ici, est d'aboutir à des niveaux de protection différents selon les Etats membres. Par ailleurs, tous les systèmes mentionnés de coopération et de collecte de données au niveau de l'UE, comportent des dispositions spécifiques relatives à la protection des données à caractère personnel. Ces dispositions voient naturellement leur champ d'application limité au système d'échange de données qui les a vus naître. Face à la dispersion et à l'hétérogénéité de l'ensemble de ces dispositions, il manquait un cadre général pour la protection des données dans les matières de la coopération policière et judiciaire pénale, que la décision-cadre 2008/977/JAI précitée a précisément pour vocation de remplir. Ce socle général commun a dès lors pour ambition d'harmoniser les règles tout en assurant un niveau de protection élevé, identique à celui existant dans le cadre du premier pilier.

La pertinence de la décision-cadre relative à la protection des données dans le troisième pilier apparaissait d'autant plus grande au surplus, que le « Programme de La Haye »[11] avait mis en exergue le principe de disponibilité[12], dans le but de faciliter la

[7] V. JOUE L. 350/60 du 30 déc. 2008.
[8] V. décision 2008/615/JAI du Conseil du 23 juin 2008, JOUE L. 210 du 6 août 2008, p. 1-11.
[9] Accord relatif à l'obligation des transporteurs aériens assurant des vols au départ ou à destination d'un ou plusieurs Etats membres, de transmettre aux autorités compétentes les données *PNR* afin de prévenir et de combattre les infractions terroristes et la criminalité organisée.
[10] Elle est importante dans le SIS par exemple, elle est plus faible pour EUROPOL ou EURODAC.
[11] Adopté lors du Conseil européen des 4 et 5 novembre 2004 afin de renforcer l'espace de liberté, sécurité et justice.
[12] Il faut l'entendre comme la possibilité, pour les services répressifs d'un Etat membre qui a besoin de certaines informations dans l'exercice de ses fonctions, de les obtenir d'un autre Etat membre qui les détient. L'Etat membre sollicité serait tenu de communiquer les informations requises, sauf refus dûment motivé.

création d'un vaste espace européen au sein duquel les données à caractère personnel, pour les domaines couverts par le troisième pilier, circuleraient sans entrave entre services répressifs. Cette « mutualisation, à l'échelle communautaire, des informations des données des traitements nationaux »[13], prévue par une proposition de décision-cadre[14], posait en effet la question de l'instauration d'une protection appropriée des données à caractère personnel circulant sans frontières. La décision-cadre relative à la protection des données apparaissait ainsi comme la réponse appropriée à ce problème de l'échange d'informations organisé en vertu du principe de disponibilité.

2) Des dispositions mal articulées

D'abord, par rapport au risque, évoqué ci-dessus, de niveaux de protection des données différents d'un Etat membre à l'autre, et au regard de l'intensification de la circulation des données entre Etats membres en matière répressive, la question s'est posée de l'inclusion, dans le champ d'application de la décision-cadre, des traitements de données opérés dans le cadre national. Le Contrôleur Européen de la Protection des Données (CEPD) a d'ailleurs noté à cet égard que « l'applicabilité de la décision-cadre au traitement national des données est une condition essentielle afin, non seulement d'assurer un niveau de protection suffisant des données à caractère personnel, mais aussi de permettre une collaboration efficace entre les services répressifs »[15], car il estime que « la possibilité d'avoir différents niveaux de protection des données des différents Etats membres dans le cadre du troisième pilier (…) serait incompatible avec la création d'un espace de liberté, de sécurité et de justice au sein duquel les citoyens se déplacent librement et avec un rapprochement approprié des législations »[16]. Le Conseil, durant les négociations de la décision-cadre, semblait du même avis, soulignant que « toute donnée recueillie dans le cadre d'une enquête nationale pourrait, par la suite, être échangée avec des autorités étrangères. Il est difficile, voire impossible, de distinguer les données qui sont susceptibles de faire l'objet à un stade ultérieur d'une transmission transfrontière de celles qui ne le sont pas. Il serait en tout état de cause très coûteux de mettre en place deux types différents de règles de protection des données »[17]. Les réticences d'un certain nombre d'Etats, formulant notamment des doutes quant à l'existence d'une base juridique dans le traité UE qui permettrait de réglementer la protection des données dans des dossiers purement nationaux[18], l'ont cependant emporté. La décision-cadre, dès lors, ne s'applique qu'aux échanges transfrontières de données à caractère personnel, ce qu'on ne peut que regretter. Il semble en effet contreproductif pour la décision-cadre d'ignorer les données traitées dans un cadre strictement national, car la confiance mutuelle, condition pour un échange d'informations efficace, passe par la mise en œuvre de normes communes applicables au traitement des données ; la restriction ainsi introduite dans le

[13] J.M. Delarue, L'Europe des fichiers – Dialogue des juges, des policiers, des autorités administratives indépendantes, in Le dialogue des juges, Mélanges en l'honneur du Président Bruno Genevois, Dalloz, 2009, p. 276.
[14] Proposition de décision-cadre du Conseil relative à l'échange d'informations en vertu du principe de disponibilité, COM(2005)490, qui n'a finalement pas pu être adoptée avant l'entrée en vigueur du traité de Lisbonne.
[15] Troisième avis du CEPD relatif au projet de décision-cadre, 27 avril 2007, JOUE C 139 du 23 juin 2007.
[16] Ibid. § 16 et 18.
[17] V. Note de la Présidence aux conseillers JAI/COREPER/Conseil en date du 17 nov. 2006, N° 15431/06.
[18] V. Note de la Présidence au COREPER/Conseil, du 24 avril 2006, 8175/1/06 REV 1.

champ d'application de la décision-cadre risque par conséquent de nuire à la confiance mutuelle entre les Etats membres, et par la même à l'efficacité de l'action répressive.

Ensuite, il ressort de l'exposé des motifs de la décision-cadre[19], que l'ensemble des dispositions spécifiques relatives à la protection des données à caractère personnel résultant d'actes adoptés sur la base du titre VI du traité UE, tels que EUROPOL, EUROJUST, le SIS, le SID, ou le dispositif du traité de Prüm intégré dans le traité, ne devrait pas être affecté par la décision-cadre. Ce qui signifie que les dispositions spécifiques prévues par ces textes en matière de protection des données, continueront à s'appliquer. La décision-cadre aurait donc vocation à jouer le rôle d'une *lex generalis*, c'est-à-dire à définir un « cadre général pour la protection des données en ce qui concerne des instruments spécifiques »[20]. La mise en place de ce cadre général était nécessaire, en premier lieu, afin de mettre en cohérence les dispositions de protection des données personnelles, dispersées, on l'a dit, dans les différents instruments juridiques qui réglementent les systèmes spécifiques de collecte de données. Elle était non seulement nécessaire mais indispensable, en second lieu, afin d'assurer la cohérence avec les principes de protection des données existant dans le cadre du premier pilier, « dans un contexte où la participation accrue du secteur privé implique que les données à caractère personnel transitent du premier au troisième pilier (comme dans le cas des dossiers des passagers aériens) ou vice-versa », comme l'explique le CEPD[21]. Il apparaît donc au total que coexistent un très grand nombre de règles, spécifiques (autant que de systèmes de stockage ou de collecte de données) et générales (la décision-cadre) ; ainsi, face au nombre de *lex specialis* qui ont vocation à s'appliquer prioritairement, la décision-cadre remplit-elle véritablement son rôle de *lex generalis* ? Il est permis d'en douter surtout eu égard à son contenu, notoirement insuffisant pour assurer une protection complète et efficace dans le cadre de l'ELSJ, on va le voir. La question se pose alors de sa pertinence.

B) Une législation insuffisante pour l'ELSJ

L'étude détaillée des dispositions de la décision-cadre relative à la protection des données traitées dans le cadre de la coopération policière et judiciaire en matière pénale, révèle un grand nombre de lacunes, qui portent à douter de sa capacité à « répondre aux besoins de la création d'un espace de liberté, de sécurité et de justice à l'intérieur duquel les autorités policières et judiciaires pourraient échanger des informations en matière répressive sans tenir compte des frontières nationales »[22].

1) La limitation des finalités

Une question fondamentale en matière de protection des données, est, tout d'abord, celle de la limitation des finalités. L'article 3 § 1 de la décision-cadre précise ici que les données à caractère personnel peuvent être collectées par les autorités compétentes « uniquement pour des finalités déterminées, explicites et licites » et « traitées uniquement pour les finalités pour lesquelles elles ont été collectées ». Par ailleurs, le traitement des données pour une autre finalité est permis, mais seulement dans la mesure où il n'est pas incompatible avec la finalité pour laquelle les données ont été collectées[23]. Ces

[19] V. point 39.
[20] V. le § 20 du premier avis du CEPD, en date du 19 déc. 2005, JOUE C 047 du 25 fév. 2006, p. 27-47.
[21] V. le § 13 du troisième avis, précité.
[22] V. le § 5 du troisième avis du CEPD.
[23] Par exemple, des données collectées, concernant une personne reconnue coupable de trafic de drogue, pourraient être utilisées dans le cadre d'une enquête portant sur un réseau de revendeurs de drogue.

dispositions semblent répondre au souci de limitation de la finalité, tel qu'il résulte par exemple de la Convention européenne des droits de l'homme[24], nous y reviendrons. Toutefois, l'utilisation ultérieure de données collectées pour une finalité qui paraît de prime abord incompatible avec celle pour laquelle elles ont été collectées, peut poser problème. Il est, sans doute, nécessaire de laisser une certaine souplesse aux services de police dans ce domaine, qui respecteront d'autant mieux la limitation de la finalité au niveau de la collecte qu'ils seront assurés ensuite de pouvoir utiliser les données ultérieurement de façon dérogatoire à la finalité originelle. Souplesse ne signifie cependant pas laxisme, et une telle possibilité n'aurait dû être reconnue qu'à la condition que cette utilisation ultérieure pour des finalités autres soit strictement nécessaire, comme le suggérait par exemple le CEPD[25], dans la logique au demeurant de l'article 8 de la CEDH. Or, ce critère de « stricte nécessité », qui figurait au départ dans le texte de la proposition de la Commission[26], a disparu du texte final de la décision-cadre. Cette seule disposition permet de douter, déjà, de la compatibilité de la décision-cadre avec la CEDH.

2) Le traitement des données

Concernant la question du traitement des données ensuite, il semble logique et nécessaire d'opérer une distinction entre les différentes catégories de données. Or, la décision-cadre n'a repris aucune des dispositions, pourtant très protectrices, qui avaient été proposées par la Commission, ce qui est regrettable. Celle-ci avait prévu en effet de distinguer clairement les données à caractère personnel en fonction des différentes catégories de personnes : personnes suspectes, personnes condamnées, témoins, victimes etc. Il convient d'accorder une attention plus particulière ici aux personnes non suspectes, s'agissant par exemple de la durée de conservation de leurs données à caractère personnel. Faute de précautions suffisantes, la question se pose, une fois encore, de la compatibilité de la décision-cadre avec la jurisprudence récente de la Cour européenne des droits de l'homme[27]. Dans le même ordre d'idées, il est également regrettable que la proposition de la Commission qui envisageait un traitement différencié des données en fonction de leurs « degrés d'exactitude et de fiabilité », entraînant un classement des données selon leur nature (distinction entre les données fondées sur des faits et celles fondées sur des opinions ou appréciations personnelles), ait été omise dans la version finale de la décision-cadre. On peut y voir le risque « de porter atteinte aux données échangées entre les services de police étant donné que ceux-ci ne seront pas en mesure de déterminer s'il convient de considérer ces données comme des 'preuves', des 'faits', des 'renseignements confirmés' ou des 'renseignements non confirmés' »[28].

[24] L'article 8 de la CEDH est relatif au droit au respect de la vie privée et familiale, mais a servi de support à une jurisprudence abondante et développée de la Cour européenne des droits de l'homme sur la protection des données à caractère personnel. Voir, par exemple, notre commentaire de l'arrêt *Marper c/ Royaume-Uni* du 4 décembre 2008, et notamment les références jurisprudentielles qui y figurent, RFDA juillet-août 2009, p. 741.

[25] V. le § 64 du premier avis précité.

[26] COM(2005)475 final, 4 oct. 2005, voir l'article 11.

[27] Nous pensons encore une fois à l'affaire *Marper*, relative à la durée de conservation (indéfinie) de données à caractère sensible (données biométriques et profils ADN) de personnes qui avaient été acquittées ou relaxées de leurs poursuites pénales.

[28] V. § 32 du premier avis du CEPD.

Un autre point d'achoppement concerne ensuite la question des données dites sensibles[29]. Leur collecte est interdite par la Convention 108 du Conseil de l'Europe[30], à moins que le droit interne ne prévoie des garanties appropriées, ce qui, ici, n'est pas pertinent puisque l'on se situe dans le cadre de l'UE, et que la décision-cadre a écarté au surplus le droit national de son champ d'application. L'article 6 de la décision-cadre contrevient manifestement à la Convention 108, puisque, dans un renversement de perspective, elle autorise le traitement de telles données sensibles, mais à condition toutefois que ce soit par une loi. Quant aux garanties appropriées, il ne s'agit plus que de simples « mesures garantissant la sauvegarde de l'intérêt légitime de la personne concernée », loin des contraintes qui avaient été prévues par la Commission dans sa proposition[31]. Il apparaît ensuite que la décision-cadre ne contient aucune disposition spécifique relative à la protection des données biométriques et des profils ADN, qui auraient dû être pris en considération compte tenu de leur caractère éminemment sensible. Ainsi, le risque se fait jour de traitements de données qui se révèleront incompatibles avec la jurisprudence récente élaborée par le juge de Strasbourg[32].

3) L'échange de données avec les pays tiers

Une dernière faiblesse majeure de la décision-cadre (pour s'en tenir aux problèmes les plus importants), est relative à l'échange de données avec des pays tiers. Deux points focalisent ici l'attention. Le premier concerne le consentement préalable de l'Etat auprès duquel les données ont été collectées, qui est nécessaire à tout transfert à des pays tiers de données transmises ou mises à disposition par l'autorité compétente d'un autre Etat membre. Or, il est possible de déroger à cette exigence d'accord préalable si « le transfert de données est essentiel pour prévenir un danger immédiat et sérieux pour la sécurité publique d'un Etat membre ou d'un Etat tiers ou pour les intérêts essentiels d'un Etat membre et que l'accord préalable ne peut pas être obtenu en temps utile »[33]. Dans le contexte de lutte contre le terrorisme, qui justifie le transfert d'un certain nombre de données vers des pays tiers (par exemple dans le cadre de l'accord PNR entre l'UE et les Etats-Unis), il est loisible de se demander si l'exception ne risque pas de devenir la règle…Le second est relatif à l'existence d'un niveau de protection adéquat, qui doit être vérifiée avant tout transfert de données vers un pays tiers. Cette nécessité, parfaitement prise en compte par exemple par la directive 95/46/CE précitée, pour le champ strictement communautaire, figure également dans la décision-cadre, ce dont on ne peut que se féliciter. Il convient de remarquer toutefois que cette garantie ne s'applique qu'aux données transmises ou mises à disposition par l'autorité compétente d'un autre Etat membre. Cela ouvre la porte à une différence de traitement en fonction de l'origine des

[29] On entend par « données sensibles » celles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que celles relatives à la santé et à la vie sexuelle.

[30] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Strasbourg 28 janv. 1981, dite Convention 108. Voir l'article 6.

[31] La Commission posait d'ailleurs dans sa proposition le principe de l'interdiction du traitement des données dites sensibles, sauf exception. Quant aux contraintes envisagées, le traitement devait être prévu par un texte de loi et être absolument nécessaire pour l'accomplissement des tâches légitimes de l'autorité concernée aux fins de prévention et de détection des infractions pénales, et d'enquêtes et de poursuites en la matière, ou bien la personne concernée devait avoir consenti au traitement etc.

[32] Nous pensons à l'arrêt *Marper*, évoqué ci-dessus note 25. Nous y reviendrons.

[33] V. article 13 § 2 de la décision-cadre.

données, qui n'est pas acceptable. La limitation des dispositions de protection aux seules dispositions échangées a pour corollaire le risque de « blanchiment de l'information » ; en effet, des données traitées à l'intérieur d'un pays membre pourraient être transférées directement à des pays tiers, à partir desquels ensuite ces données deviendraient accessibles aux autorités compétentes d'autres Etats membres, ce qui constitue naturellement un moyen de contourner les règles communes de protection des données. Par ailleurs, le risque est grand également d'aboutir à un « forum shopping »[34], qui encouragerait les autorités de pays tiers à obtenir les informations souhaitées de la part des Etats ayant le plus bas niveau d'exigences légales en matière de transfert de données. Par conséquent, la décision-cadre n'a pas su ici mettre en place un mécanisme permettant d'apprécier en commun le caractère adéquat du niveau de protection, ainsi que de prendre une décision à cet égard d'un commun accord, avant tout transfert vers un pays tiers. L'évaluation du caractère adéquat du niveau de protection étant laissée à la discrétion de chaque Etat membre, il est patent qu'elle sera amenée à varier d'un Etat à l'autre, ce qui non seulement n'est pas satisfaisant du point de vue de la protection des droits fondamentaux dans l'espace européen, mais encore qui risque de compliquer le fonctionnement de la coopération policière. La décision-cadre a donc manifestement manqué son but.

La décision-cadre, au total, compte tenu de ses limites et nombreuses faiblesses évoquées, ne semble donc pas répondre aux espérances attendues en matière de protection des données à caractère personnel dans l'espace de liberté, sécurité et justice de l'UE. Néanmoins, ce dispositif, à peine installé, semble menacé ; il ne sera vraisemblablement que transitoire.

II Un dispositif juridique en mutation

La protection des données à caractère personnel au sein de l'ELSJ, si elle n'est pas satisfaisante, n'est néanmoins pas figée. Les facteurs d'évolution sont de deux ordres. Le premier, exogène à l'UE, est constitué par la Cour européenne des droits de l'homme, qui, grâce à sa jurisprudence très protectrice, va jouer un rôle déterminant dans l'avenir, imposant aux différents acteurs, aussi bien nationaux qu'européens, les limites à ne pas franchir en matière d'utilisation de données personnelles en matière pénale ou d'entraide répressive. Le second, endogène à l'UE, est la résultante à la fois des nouvelles priorités définies dans le programme de Stockholm pour l'ELSJ et de l'entrée en vigueur du traité de Lisbonne. Celle-ci va en effet changer considérablement la donne, aussi bien du point de vue de la protection des droits fondamentaux, avec notamment la pleine effectivité de la Charte européenne des droits fondamentaux, que du point de vue institutionnel, avec l'entrée en lice d'un Parlement européen pesant désormais de tout son poids.

A) Un facteur d'évolution exogène : la Cour européenne des droits de l'homme, ordonnateur de l'ELSJ

La Cour européenne des droits de l'homme, par son arrêt rendu le 4 décembre 2008 dans l'affaire *S. et Marper c/ Royaume-Uni*[35], exemplatif de la jurisprudence élaborée à Strasbourg en matière de protection des données, a placé le principe de

[34] Selon les termes du CEPD, dans son deuxième avis, 29 nov. 2006, JOUE C091 du 26 avril 2007, p. 9-14, ici § 22.
[35] Req. N° 30562/04 et 30566/04. Voir notre commentaire à la RFDA, précité note 25.

proportionnalité au cœur de son raisonnement. Ce faisant, elle s'impose comme l'ordonnateur de l'espace de liberté, sécurité et justice, tant les conséquences de l'arrêt sont importantes.

1) Le principe de proportionnalité, principe cardinal en matière de protection des données

Dans cette affaire, il s'agissait du prélèvement d'empreintes digitales et d'échantillons d'ADN des deux requérants à l'occasion de poursuites pénales à leur encontre, l'un, S., inculpé de tentative de vol avec violence alors qu'il était âgé de 11 ans, ayant été relaxé, l'autre, Marper, inculpé de harcèlement à l'égard de sa compagne ayant vu son affaire classée sans suite, après le retrait de la plainte. Les deux requérants, malgré leurs demandes réitérées, aux autorités, puis par voie juridictionnelle, n'ont pu obtenir la destruction de leurs données sensibles ainsi collectées, car elles avaient été stockées sur la base d'une loi de 1984 autorisant leur conservation pour une durée illimitée, dans un objectif de prévention ou détection des infractions pénales. Ils se sont alors adressés à la Cour européenne des droits de l'homme, estimant que la conservation de leurs empreintes digitales et données ADN pour une durée illimitée portait atteinte à leur droit au respect de leur vie privée, garanti par l'article 8 de la Convention européenne des droits de l'homme. Le juge en effet, dans une jurisprudence déjà ancienne et abondante, a subsumé la notion de protection des donnés à caractère personnel sous celle plus générale de droit au respect de la vie privée et familiale[36] garanti par cet article. Toute la question était de savoir ici si la mesure contestée, qui a été considérée comme une atteinte au droit au respect de la vie privée, était justifiée, c'est-à-dire si elle pouvait apparaître comme « nécessaire dans une société démocratique », par référence au § 2 de l'article 8 qui consacre la possibilité d'une ingérence d'une autorité publique dans l'exercice du droit garanti[37]. La Cour a prononcé une condamnation à l'unanimité à l'égard de la législation britannique autorisant la conservation des données mentionnées pour une durée illimitée. Il s'agit en effet pour elle d'une « atteinte disproportionnée au droit des requérants au respect de leur vie privée [qui] ne peut passer pour nécessaire dans une société démocratique »[38]. Le contrôle de proportionnalité, qui met en balance l'intérêt des individus à la protection de leur vie privée et l'intérêt général lié à la prévention des infractions pénales, se trouve ainsi au cœur du raisonnement développé par la Cour. Deux éléments vont emporter la conviction de la Cour dans cette affaire : d'abord le caractère général et indifférencié du pouvoir de conservation des données en cause, quelles que soient la nature et la gravité des infractions dont la personne est soupçonnée et quel que soit son âge, et ensuite le fait que les données en question soient conservées indéfiniment, quelles que soient la nature et la gravité de l'infraction. Rappelons que les requérants n'avaient pas été condamnés, ce qui rendait la mesure de conservation indéfinie de leurs données personnelles encore plus choquante. Si l'on considère les critiques formulées précédemment à l'encontre de la décision-cadre relative à la protection des données dans l'ELSJ, il va sans dire que nombre des

[36] Le § 1 de l'article 8 proclame que « toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance »

[37] Cette possibilité est reconnue « 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 ».

[38] V. § 125 de l'arrêt.

dispositions de ce texte vont directement à l'encontre des principes formulés par la Cour de Strasbourg dans l'arrêt évoqué. La Cour est donc amenée à s'imposer, opportunément, comme l'ordonnateur de l'ELSJ.

2) La Cour européenne des droits de l'homme, ordonnateur de l'ELSJ en matière de protection des données

Ce sont sans doute un certain nombre de dispositions majeures de la décision-cadre qui risquent d'encourir les foudres strasbourgeoises au regard de la jurisprudence récente. La Cour, d'abord, risque de pointer du doigt l'absence du critère de la stricte nécessité quant à l'utilisation ultérieure de données pour des finalités autres que celles pour lesquelles elles avaient été collectées, qui a été éludé par le texte final, malgré les recommandations du CEPD. La possibilité d'une ingérence dans l'exercice du droit garanti est, on l'a dit, reconnue par l'article 8 § 2 de la CEDH, à la condition d'être « nécessaire » dans une société démocratique à la sécurité nationale, à la sûreté publique, à la défense de l'ordre etc. Ce critère de nécessité, qui est « au cœur du contrôle européen des ingérences »[39], implique « un besoin social impérieux »[40], sachant que la « mesure prise doit être proportionnée au but légitime poursuivi »[41]. Ce principe de proportionnalité, qui « traduit une exigence d'adéquation entre un objectif légitime et les moyens utilisés pour l'atteindre »[42], avait déjà été pris en compte de longue date par la Cour et se trouve placé aujourd'hui au cœur de son raisonnement dans l'affaire *Marper*. L'absence de ce critère de nécessité dans la décision-cadre est donc manifestement problématique.

Ensuite, l'article relatif au traitement des données dites sensibles, non seulement contredit l'interdiction de principe figurant dans la Convention 108 du Conseil de l'Europe, mais en outre ne mentionne même pas les données biométriques ou les profils ADN, sur la spécificité desquelles la Cour a pourtant insisté dans son arrêt *Marper*. Déjà dans un arrêt *Van der Velden*[43], la Cour avait estimé que la « conservation systématique » de données ADN et d'échantillons cellulaires revêtait un caractère suffisamment intrusif pour constituer une atteinte au droit au respect de la vie privée du requérant, « eu égard notamment à l'utilisation ultérieure qui pourrait être faite à l'avenir des échantillons cellulaires en question » ; dans l'arrêt *Marper* ensuite, elle a souligné l'importance des profils ADN, qui, dans la mesure où ils peuvent permettre par exemple de découvrir l'origine ethnique de la personne, constituent une donnée sensible au titre de la Convention 108 précitée, et nécessitent par conséquent une protection accrue. Sur ce point encore, la décision-cadre ne répond manifestement pas aux exigences de la jurisprudence européenne. Enfin, le fait que les données des personnes non suspectes ne bénéficient pas de garanties spécifiques est également en contradiction avec l'arrêt *Marper*, qui a défini la ligne rouge à ne pas franchir concernant les données de personnes non condamnées ou acquittées, pour lesquelles le respect du principe de proportionnalité s'impose de façon plus rigoureuse encore.

Par ailleurs, il n'est pas davantage certain que les textes spécifiques mentionnés ci-dessus, relatifs à EUROPOL, au SIS, au SID etc., (toutes les *lex specialis* par rapport à

[39] V. Coussirat-Coustère, commentaire de l'article 8 § 2 de la CEDH, in La Convention européenne des droits de l'homme, commentaire article par article, sous la direction de L.E. Pettiti, E. Decaux, P.H. Imbert, ECONOMICA 1995, p.337.
[40] Cour européenne des droits de l'homme, *Gillow c/Royaume-Uni*, 24 novembre 1986, A 109, §55.
[41] Ibid.
[42] F. Sudre, Droit européen et international des droits de l'homme, PUF, 9ième éd. 2008, p. 226.
[43] *Van der Velden c/Pays-Bas*, req. N° 29514/05.

la décision-cadre) et contenant leurs propres dispositions de protection des données, ne tombent pas non plus sous le couperet du juge. En effet, s'agissant de la question des délais de conservation en particulier, l'imprécision des formules employées par les différents textes, qui accordent une marge discrétionnaire considérable aux autorités concernées, laisse place au doute quant à leur proportionnalité par rapport au but à atteindre. C'est l'édifice dans son entier relatif à la protection des données dans l'ELSJ qui se trouve dès lors sous l'épée de Damoclès du juge de la Convention. Cela semble un motif suffisant pour remettre en cause l'ensemble des textes et envisager leur remplacement par un dispositif plus respectueux des droits individuels. Il est évident que le législateur européen, à l'avenir, ne pourra faire abstraction des principes posés par le juge de Strasbourg, qui forment d'ores et déjà la trame du futur ouvrage qu'il ne pourra éviter de remettre sur son métier. Le principe de proportionnalité, qui oblige à mettre en balance l'intérêt des individus à la protection de leur vie privée et l'intérêt général lié à la prévention des infractions pénales, en constitue le fil conducteur. L'importance de la jurisprudence de la Cour européenne des droits de l'homme est donc grande, elle le sera plus encore dès lors que l'Union européenne aura adhéré à la CEDH, hypothèse prévue par le traité de Lisbonne, qui a été considérée comme une priorité par le Conseil européen des 10 et 11 décembre 2009[44] et qui est en train de se concrétiser, la Commission ayant présenté des directives de négociation[45]. La Cour de Strasbourg s'impose donc bien comme le grand ordonnateur de l'ELSJ en matière de protection des données.

B) Des facteurs d'évolution endogènes

Le premier facteur d'évolution endogène à l'Union européenne est l'entrée en vigueur du traité de Lisbonne, qui apporte un certain nombre d'innovations, tant du point de vue de la protection des droits fondamentaux que du point de vue institutionnel, qui bouleverseront l'ordre juridique établi. Le second est le Programme de Stockholm, qui a défini les nouvelles priorités de l'ELSJ pour la période 2010-2014, au rang desquelles figure une meilleure protection des droits fondamentaux.

1) Les bouleversements consécutifs à l'entrée en vigueur du traité de Lisbonne

Le premier, et non des moindres, est le « statut constitutionnel »[46] acquis désormais par la Charte des droits fondamentaux de l'Union. Le texte de la Charte n'est, certes, pas formellement incorporé dans les traités, mais le renvoi opéré par l'article 6 TUE[47] lui donne la même valeur que ceux-ci. Il paraît évident que la promotion juridique de la Charte va profondément influencer l'ELSJ, surtout par le fait que « les droits fondamentaux qui sont à l'heure actuelle insuffisamment garantis par la législation de l'Union (…) vont désormais accéder au prétoire du juge »[48]. En effet, la Charte, si elle était déjà utilisée par la Cour de Justice, va bénéficier désormais d'une plus large

[44] Il a été déclaré qu'il était « primordial que l'UE adhère rapidement à la Convention européenne des droits de l'homme », Doc. 17024/09 du 2 décembre 2009.
[45] IP/10/291, 17 mars 2010.
[46] J.P. Jacqué, La protection des droits fondamentaux dans l'Union européenne après Lisbonne, L'Europe des Libertés n°26, mai 2008, p. 2.
[47] « L'Union reconnaît les droits, les libertés et les principes énoncés dans la Charte des droits fondamentaux du 7 décembre 2000, telle qu'adaptée le 12 décembre 2007 à Strasbourg, laquelle a la même valeur juridique que les traités ».
[48] H. Labayle, Le juge de l'espace de liberté, sécurité et justice de l'Union européenne, in Mélanges Genevois, Dalloz, 2009, p. 614.

justiciabilité. Les restrictions aux compétences de la Cour de Justice qui existaient dans le cadre du titre IV CE et du titre VI CE, disparaissent en effet avec le traité de Lisbonne. Toutefois, la clause d'ordre public de l'article 276 du traité sur le fonctionnement de l'Union européenne (TFUE)[49] subsiste, ce qui constitue une limite pour le domaine de la coopération policière et judiciaire en matière pénale. Cela étant, déjà dans l'article 16 du TFUE figure une disposition selon laquelle « Toute personne a droit à la protection des données à caractère personnel la concernant », formule reprise par l'article 8 paragraphe 1 de la Charte, consacré à la protection des données à caractère personnel. Si l'article 8 de la Charte « puise son inspiration à l'article 8 de la Convention européenne des droits de l'homme »[50], la Charte va plus loin dans sa formulation que la CEDH, qui ne proclame pas explicitement le droit à la protection de ses données à caractère personnel[51]. Le juge de Luxembourg, qui, confronté à la problématique de la protection des données, s'appuyait déjà sur l'acquis jurisprudentiel du juge de la Convention[52], ne s'en écartera pas pour autant désormais, d'autant que l'article 53 de la Charte a pour effet « d'exclure toute interprétation de celle-ci qui aboutirait à diminuer le niveau de protection déjà acquis »[53] en vertu du droit international, en particulier la CEDH. Dès lors, la Cour de Justice étant liée à la jurisprudence, très protectrice d'ailleurs, développée par la Cour européenne des droits de l'homme, la promotion juridique de la Charte des droits fondamentaux est-elle d'un intérêt majeur en matière de protection des données ?

La question est d'autant plus pertinente que le traité de Lisbonne a prévu l'adhésion, évoquée plus haut, de l'UE à la CEDH. Un effet bénéfique attendu est de mettre en cohérence les jurisprudences de la Cour de Justice de l'Union et de la Cour européenne des droits de l'homme, ce qui, pour le domaine de la protection des données, ne devrait poser aucun problème. La Cour européenne des droits de l'homme sera incontestablement le chef d'orchestre, qui aura la charge de « garantir l'harmonie entre la Convention et la Charte, en contrôlant l'interprétation de la Convention faite par le juge communautaire à l'occasion de l'application de la Charte »[54].

Cette nouvelle configuration européenne en matière de protection des droits fondamentaux entraîne un certain nombre de conséquences sur la problématique étudiée de la protection des données dans l'ELSJ. En effet, face aux nombreuses faiblesses déplorées de la décision-cadre, le requérant potentiel n'est pas complètement démuni. Il peut, comme première solution, s'adresser à la Cour de Justice de l'Union, par le biais d'un recours individuel en annulation de la décision-cadre, en arguant de la violation de la

[49] « Dans l'exercice de ses attributions concernant les dispositions des chapitres 4 et 5 du titre V de la troisième partie relatives à l'espace de liberté, de sécurité et de justice, la Cour de Justice de l'UE n'est pas compétente pour vérifier la validité ou la proportionnalité d'opérations menées par la police ou d'autres services répressifs dans un Etat membre, ni pour statuer sur l'exercice des responsabilités qui incombent aux Etats membres pour le maintien de l'ordre public et la sauvegarde de la sécurité intérieure ».

[50] O. de Schutter, article II-68, in Traité établissant une Constitution pour l'Europe, Partie II La Charte des droits fondamentaux de l'Union, commentaire article par article, sous la direction de L. Burgorgue-Larsen, A. Levade, F. Picod, Bruylant, 2005, p. 123.

[51] C'est en effet la jurisprudence du juge de Strasbourg qui a subsumé la notion de protection des données sous celle, plus générale, de droit au respect de la vie privée et familiale.

[52] V. par exemple CJCE *Österreichische Rundfunk*, aff. jointes C-465/00, C-138/01, C-139/01, Rec. I-4989.

[53] V. O. de Schutter, op. cit. p. 124.

[54] F. Sudre, L'adhésion de l'Union Européenne à la Convention européenne des droits de l'homme, Annuaire de droit européen 2006, p. 76.

Charte des droits fondamentaux[55]. Les difficultés d'accès au prétoire du juge de Luxembourg pour le particulier sont cependant bien connues, en ce qui concerne par exemple le délai du recours ou, surtout, l'interprétation stricte des conditions posées au droit de recours[56]. La création d'un recours individuel spécifique en matière de droits fondamentaux, tel le *Verfassungsbeschwerde* allemand, aurait été bienvenue[57]… Faute d'aboutir à Luxembourg, le requérant pourra cependant se tourner vers Strasbourg, hypothèse où l'adhésion de l'UE à la CEDH prend tout son relief. En effet, si la Cour européenne des droits de l'homme reconnaît la violation de la Convention au titre de l'article 8, du fait de l'une des dispositions de la décision-cadre, les Institutions de l'Union ne pourront pas ne pas en tenir compte, et seront nécessairement obligées d'en tirer les conséquences, en modifiant voire en supprimant la règle de droit de l'Union jugée incompatible avec la Convention. Il semble donc acquis que, dès à présent, les Institutions de l'Union doivent veiller à « assurer la conformité du droit de l'Union avec les exigences découlant de la CEDH »[58]. Au regard des analyses précédentes, il semble que les jours de la décision-cadre relative à la protection des données dans l'ELSJ, soient comptés…

Cela étant, si le législateur, ce qui est probable, se voit contraint d'adopter un nouveau texte en la matière, l'entrée en vigueur du traité de Lisbonne fait désormais peser sur lui de nouvelles contraintes, en particulier procédurales. La simplification de l'architecture de l'Union par la disparition des « piliers » et des procédures intergouvernementales de décision conduit en effet « au retour à un jeu normal des institutions et à la restauration de leurs prérogatives selon le schéma communautaire, malgré quelques exceptions »[59]. Cela signifie la généralisation de la procédure législative « ordinaire », c'est-à-dire un Parlement Européen jouant pleinement son rôle de co-législateur, ce qui permettra non seulement « de mieux décider, mais aussi [de] décider plus démocratiquement »[60]. Le rejet par le Parlement Européen le 11 février 2010 de l'accord intérimaire SWIFT entre l'UE et les Etats-Unis[61] est l'une des premières manifestations de ce nouveau rapport de forces institutionnel. Les accords internationaux signés par l'UE qui avaient été négociés dans les domaines de la coopération judiciaire et policière pénale (ancien troisième pilier), sont en effet soumis à un vote d'approbation du Parlement Européen. Ce dernier a ainsi, non seulement rejeté l'accord à une large majorité[62], manifestant son inquiétude quant aux lacunes en matière de protection des données, mais il a exigé en outre que le futur accord satisfasse aux exigences de la Charte des droits

[55] L'article 263 alinéa 3 du TFUE permet à un requérant individuel de former un recours en annulation « contre les actes dont [il] est le destinataire ou qui [le] concernent directement et individuellement, ainsi que contre les actes réglementaires qui [le] concernent directement et qui ne comportent pas de mesures d'exécution ».

[56] Le fait pour le requérant d'être « directement et individuellement concerné » par l'acte attaqué (cf. CJCE 15 juillet 1963 *Plaumann*, 25/62, Rec. 199). Il eût suffi de remplacer le « et » par « ou » dans le texte pour élargir les possibilités de recours…

[57] Il avait été envisagé mais n'a finalement pas été retenu. V. F.-X. Priollaud et D. Siritzky, Le Traité de Lisbonne, article par article, La Documentation Française 2008, p. 344.

[58] F. Sudre, op. cit. p. 79.

[59] H. Labayle, L'espace de liberté, sécurité et justice : la nouvelle frontière ?, EUROPE, juillet 2008, dossier 10, § 9.

[60] V. Constantinesco, Le processus de décision : vers une nouvelle gouvernance ? EUROPE, juillet 2008, dossier 8, § 5.

[61] Accord provisoire pour neuf mois signé par les Ministres des 27 sur les transferts de données bancaires vers les Etats-Unis aux fins de la lutte anti-terroriste. Ce rejet prive l'accord d'effet juridique. Voir le communiqué de presse du Parlement Européen du 11 février 2010.

[62] A savoir, 378 voix pour, 196 contre, 31 abstentions.

fondamentaux. Les députés ont plus particulièrement demandé dans leur résolution que les données ne soient collectées « qu'aux fins de la lutte contre le terrorisme » et « qu'un juste équilibre » soit trouvé entre les mesures de sécurité et la protection des libertés. Ce débat, symptomatique de la réorientation actuelle des priorités de l'Union, en particulier depuis la publication du Programme de Stockholm, montre que le Conseil des Ministres sera à l'avenir contraint d'entendre la voix du Parlement, ce qui ne pourra être que favorable à l'adoption d'un nouveau texte à portée générale assurant la protection des données au sein de l'UE.

2) Les nouvelles priorités pour l'ELSJ définies par le Programme de Stockholm

Le « programme de La Haye » arrivant à expiration, il s'agissait de définir les nouvelles priorités pour l'Espace de liberté, sécurité et justice de l'UE pour la période 2010-2014. C'est ce à quoi s'est attaché le « programme de Stockholm », formellement adopté lors du Conseil européen des 10 et 11 décembre 2009[63]. Si la programmation précédente avait été marquée par le souci de renforcer la sécurité dans le contexte de menace terroriste[64], la nouvelle priorité est en revanche de développer le cadre juridique de la protection des droits fondamentaux. La Commission européenne a en effet souligné son ambition de promouvoir les droits du citoyen, l'ELSJ devant être « avant tout un espace unique de protection des droits fondamentaux au sein duquel le respect de la personne et de la dignité humaine ainsi que des autres droits consacrés dans la Charte des droits fondamentaux constitue une valeur essentielle »[65]. La thématique de la protection des données personnelles y est particulièrement mise en valeur : « L'Union doit répondre au défi posé par un échange accru de données personnelles en respectant pleinement la protection de la vie privée. Les droits à la vie privée et à la protection des données à caractère personnel sont garantis par la Charte. *Un régime complet de protection devrait être mis en place*[66] » ; elle a insisté de plus sur la nécessité de « réaffirmer un certain nombre de principes : finalité, proportionnalité et légitimité du traitement, durée limitée de conservation, sécurité et confidentialité, respect du droit des personnes et contrôle par une autorité indépendante[67] », autant de points qui, dans l'état actuel de la protection des données dans l'ELSJ posent problème, on l'a vu.

Le message a été entendu et relayé par le Conseil européen de décembre 2009[68], et la Commission européenne vient d'adresser une communication au Parlement Européen et au Conseil, présentant son plan d'action pour mettre en œuvre le programme de Stockholm[69]. Est ainsi prévue la proposition d'un nouveau cadre juridique global en matière de protection des données (la possibilité en est désormais offerte par l'article 16 TFUE[70]), la Commission prenant acte de la nécessité d'adapter la

[63] Conclusions du Conseil européen, EUCO 6/09 du 11 décembre 2009.
[64] Idée soulignée par exemple dans le rapport d'information du Sénat, n°107, du 19 novembre 2009, p. 44.
[65] Communication de la Commission au Parlement Européen et au Conseil, intitulée « Un espace de liberté, de sécurité et de justice au service des citoyens », COM(2009)262/4, point 1.
[66] C'est nous qui soulignons.
[67] COM(2009262/4, point 2.3.
[68] EUCO 6/09 du 11 décembre 2009, § 27 par exemple.
[69] Bruxelles, 20 avril 2010, COM(2010)171 final.
[70] Cette nouvelle disposition, très importante, est en effet désormais la base juridique unique pour les matières relevant précédemment des premier et troisième piliers. Sur cette base pourra ainsi être adopté un nouveau régime général de protection des données applicable à l'ensemble de l'Union, PESC exceptée.

directive de 1995 pour tenir compte des nouveaux développements technologiques, et surtout pour assurer la protection des données au regard de toutes les actions de l'UE[71]. Le dispositif existant de protection des données dans l'ELSJ a donc vécu. Quant au législateur européen, sa voie est toute tracée à l'avenir : les insuffisances soulignées de la décision-cadre par rapport au dispositif européen de protection des droits fondamentaux lui serviront en effet de contre-modèle.

Conclusion Le thème, complexe et technique, de la protection des données dans l'ELSJ cristallise les grandes évolutions en cours qui marquent l'UE, dans un monde globalisé qui, après les attentats du 11 septembre 2001 aux Etats-Unis, a essayé d'organiser une défense crédible contre le terrorisme, au prix d'une réduction alarmante des droits fondamentaux. Mais si cette page là n'est pas définitivement tournée, le retour de balancier s'enclenche progressivement vers une meilleure protection des droits fondamentaux. Ainsi, si le dispositif actuel de protection des données dans l'ELSJ - essentiellement constitué par la décision-cadre et les multiples dispositions spécifiques évoquées - se révèle notoirement insatisfaisant, il est d'ores et déjà remis en question. Son remplacement par un texte général relatif à la protection des données dans l'UE rénovée par le traité de Lisbonne, se profile. Il ne fait aucun doute que, sous la pression conjointe du juge (de Luxembourg ou de Strasbourg) et du Parlement européen (nouvel acteur invité dans le processus législatif grâce au traité de Lisbonne), le futur texte saura éviter les écueils de son prédécesseur.

[71] « The EU Data Protection Directive (1995) needs to be adapted to new technological developments and in addition to ensure data protection with regard all EU actions, as foreseen by the Lisbon Treaty (art. 16) and the Charter of fundamental rights », MEMO/10/39, 20/04/2010, p. 5.