LES DEFIS JURIDIQUES LIES A LA MISE EN PLACE DES NOUVELLES TECHNOLOGIES D'IDENTIFICATION DES PERSONNES AU SERVICE DE L'ESPACE DE LIBERTE, DE SECURITE ET DE JUSTICE ?

Mme Isabell Buschel-Verdier
Chercheure à l'Université de Bâle au sein de l'IBMB (Institute for bioethics and medical ethics Base et membre du projet ANR IAAIS.

Si les débuts de l'échange d'informations entre les polices des États souverains en Europe remontent au XVIIIe siècle, il a néanmoins fallu attendre l'entrée en vigueur du traité d'Amsterdam pour que les États membres de l'Union européenne se dotent d'un cadre juridique et d'institutions propres permettant la mise en place de cet espace de liberté, de sécurité et de justice (ci-après « ELSJ »), en jetant les bases à une coopération policière et judiciaire en matière pénale et en créant des agences comme Europol, Eurojust ou le Collège européen de police CEPOL.

Suite à la suppression des contrôles systématiques aux frontières et pour faire face à la criminalité grave transfrontalière tels que le terrorisme, la traite des êtres humains, le trafic de drogues et d'armes, la corruption et la fraude, il s'est en effet avéré nécessaire d'instaurer un niveau élevé de coopération sur les plans national et européen entre la police, les douanes et les autres services répressifs spécialisés, reposant sur une transmission rapide par voie électronique d'informations entre autorités policières et douanières aux fins de la détection des infractions et des enquêtes, ainsi que sur un travail en réseau entre autorités judiciaires au stade du procès[55].

Or, il ne faut pas perdre de vue que contrairement au marché intérieur, créé à l'origine pour faciliter la libre circulation des marchandises, l'ELSJ vise à garantir la libre circulation des personnes. En raison de la dignité inhérente aux personnes qui peuplent cet espace, l'identification de celles-ci doit se faire dans le respect des droits fondamentaux[56], conformément à l'article 67 § 1 TFUE, aux termes duquel « *l'Union constitue un espace de liberté, de sécurité et de justice dans le respect des droits fondamentaux* ». En effet, dans une Union de droit, l'utilisation de données permettant d'identifier une personne au service d'une coopération policière et judiciaire efficace entre les États membres exige non seulement des standards communs quant à la qualité et à la certification scientifique de ces données, mais avant tout le respect des droits fondamentaux de la personne dans le recueil et le traitement de ces données[57]. Tel est le premier défi juridique (I).

Que faut-il entendre par « nouvelles technologies d'identification des personnes » ? Dans le cadre de notre étude, l'identification d'une personne devra être entendue comme la détermination de l'identité d'un individu au sein d'une population, qui nécessite une comparaison de celui-ci avec d'autres personnes enregistrées[58]. Les technologies visées sont

---

[55] Conclusions du Conseil européen de Tampere, 15 et 16 octobre 1999 ; Le programme de La Haye : renforcer la liberté, la sécurité et la justice dans l'Union européenne, JOUE du 3 mars 2005, pp. 1-14 ; Le programme de Stockholm - Une Europe ouverte et sûre qui sert et protège les citoyens, JOUE du 4 mai 2010, n° C 115, pp. 1-38.

[56] DUMORTIER (F.), « L'utilisation de la biométrie et des RFIDs dans le cadre de l'espace européen de liberté, de sécurité et de justice : une affaire de balance ou une question de dignité ? », *ERA Forum*, 2009, pp. 551 et ss.

[57] Considérant n° 17 de la Décision 2008/615/JAI du Conseil du 23 juin 2008 dite "Décision Prüm" relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière, *JOUE* du 6 août 2008, n° L 210, pp. 1-11 : « *Une coopération policière et judiciaire plus étroite en matière pénale doit aller de pair avec le respect des droits fondamentaux, en particulier du droit au respect de la vie privée et du droit à la protection des données à caractère personnel* ».

[58] DUMORTIER (F.), *op. cit.*, p. 547.

celles permettant de recueillir des données à caractère personnel, telles que la prise de photos ou la capture de données biométriques[59] comme par exemple les empreintes digitales (ou « données dactyloscopiques ») et profils ADN. Nous assistons depuis quelques années à un accroissement des moyens biométriques d'identification, puisqu'en sont équipés les passeports et autres documents de voyage délivrés aux ressortissants des États membres, ainsi que les visas et les titres de séjour délivrés aux ressortissants de pays tiers[60].

Une mise au service du bon fonctionnement de l'ELSJ de ces nouvelles technologies d'identification des personnes suppose que les données à caractère personnel qu'elles permettent de recueillir puissent être échangées efficacement entre les services répressifs des États membres, voire entre les autorités compétentes des États membres et Europol ou Eurojust. Or, une telle coopération nécessite, sur un plan politique, l'existence d'une confiance mutuelle dans la qualité et l'authenticité de ces données, ainsi que, sur un plan technique, l'interopérabilité des bases dans lesquelles ces données sont enregistrées. La suppression des obstacles à un échange efficace des données constitue le second défi juridique (II).

I. La garantie du respect des droits fondamentaux dans l'utilisation des données

Le respect des droits fondamentaux doit être garanti aussi bien au stade du recueil des données (A) qu'à celui de leur traitement (B).

A. Les droits fondamentaux dont le respect s'impose au moment du recueil des données

Les agents des États membres et des institutions européennes chargés du recueil des données permettant d'identifier des personnes sont tenus au respect du droit à la vie privée (1°), ainsi que du droit à la protection des données à caractère personnel (2°).

1° Le droit au respect de la vie privée

L'exercice du droit à la vie privée est protégé conformément à l'article 8 CEDH, ainsi qu'à l'article 7 de la Charte des droits fondamentaux de l'Union européenne. Or, il ne s'agit pas d'une protection absolue mais soumise à des limitations[61]. Les deux, les juges de Strasbourg et de Luxembourg, lorsqu'ils sont saisis du contrôle des limitations à l'exercice de ce droit, retiennent généralement une interprétation restrictive des dérogations prévues,

---

[59] On entend par « biométrie » la « *technologie d'identification ou d'authentification qui consiste à transformer les caractéristiques biologiques, morphologiques et comportementales d'une personne comme les empreintes digitales, l'empreinte de la rétine, de l'iris, de la voix, la forme du visage et de la main en une empreinte numérique* » : *ibid.*, p. 555, note 61.

[60] Règlement (CE) n° 444/2009 du Parlement européen et du Conseil du 28 mai 2009 modifiant le règlement (CE) n° 2252/2004 du Conseil établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres, *JOUE* du 6 juin 2009, n° L 142, pp. 1-4 ; Règlement (CE) n° 380/2008 du Conseil du 18 avril 2008 modifiant le règlement (CE) n° 1030/2002 du Conseil, du 13 juin 2002, établissant un modèle uniforme de permis de séjour pour les ressortissants de pays tiers, *JOUE* du 29 avril 2008, n° L 115, pp. 1-7.

[61] Si l'article 8 § 2 CEDH et l'article 52 § 1 de la Charte des droits fondamentaux de l'Union européenne prévoient en effet que des limitations peuvent être apportées à l'exercice du droit au respect de la vie privée, la Cour de justice de l'Union européenne a précisé, en application de l'article 52 de la Charte, que "l*es limitations susceptibles d'être légitimement apportées au droit à la protection des données à caractère personnel, correspondent à celles tolérées dans le cadre de l'article 8 de la CEDH*" : CJUE, 9 novembre 2010, *Volker und Markus Schecke GbR* (C-92/09), *Hartmut Eifert* (C-93/09) *c/ Land Hessen*, aff. jtes C-92/09 et C-93/09, pt. 52.

défendant ainsi une position selon laquelle les nouvelles technologies ne sauraient être utilisées à n'importe quel prix dans le cadre de la justice pénale. En effet, la Cour européenne des droits de l'homme a jugé que « *[l]a protection offerte par l'article 8 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* »[62]. Or, dans un arrêt du 2 septembre 2010, elle a admis la surveillance par GPS d'un présumé terroriste dans le cadre d'une enquête pénale, considérant que l'ingérence que constitue celle-ci dans l'exercice du droit au respect de la vie privée et du droit à l'autodétermination dans la sphère de l'information du suspect était proportionnée aux buts poursuivis dans la mesure où « *celui-ci était soupçonné d'infractions extrêmement graves, notamment de participation à des attentats à la bombe commis par une organisation terroriste* »[63]. Ces ingérences seraient d'autant plus tolérables que d'autres méthodes d'enquête n'auraient pas abouti au même résultat puisque le suspect avait réussi à se soustraire à des mesures de surveillance auparavant. Vu les circonstances de l'espèce, la Cour de Strasbourg a jugé que la surveillance par GPS était proportionnée aux buts légitimes poursuivis et, par conséquent, nécessaire dans une société démocratique.

Bien que les deux droits soient étroitement liés[64], celui à la protection des données à caractère personnel est un droit distinct du droit à la vie privée.

2° Le droit à la protection des données à caractère personnel

Le droit à la protection des données est beaucoup plus récent que le droit au respect de la vie privée, ayant été introduit suite aux évolutions technologiques dans les années 1980. Tandis que « *le droit à la vie privée peut être décrit comme un droit empêchant les autorités publiques de prendre des mesures qui constituent une ingérence dans la vie privée, à moins que certaines conditions soient réunies [...] les principes relatifs à la protection des données visent à établir les conditions dans lesquelles il est légitime et licite de procéder au traitement de données à caractère personnel* »[65]. Le cadre juridique de référence de la protection des données à caractère personnel résulte de normes issues de deux ordres juridiques distincts, le Conseil de l'Europe et l'Union européenne, qui lient les 27 États membres de l'Union européenne dans les deux cas. Sous l'égide du Conseil de l'Europe la Convention n° STE 108

---

[62] Cour EDH, 4 décembre 2008, *S. et Marper c. Royaume-Uni,* requêtes nos 30562/04 et 30566/04, § 112.

[63] Cour EDH, 2 septembre 2010, *Uzun c. Allemagne*, requête n° 35623/05, § 20.

[64] Cour EDH, 17 décembre 2009, *Bouchacourt c. France*, requête n° 5335/06, § 61: "*La protection des données à caractère personnel joue un rôle fondamental dans l'exercice du droit au respect de la vie privée et familiale consacré par l'article 8 de la Convention. La législation interne doit donc ménager des garanties appropriées pour empêcher toute utilisation de données à caractère personnel qui ne serait pas conforme aux garanties prévues par cet article (mutatis mutandis, Z c. Finlande, 25 février 1997, § 95, Recueil 1997-I)*" ; CJCE, 29 janvier 2008, *Productores de Música de España (Promusicae) c/ Telefónica de España SAU*, aff. C-275/06, pt. 63 ; CJUE, 9 novembre 2010, Volker und Markus Schecke GbR (C-92/09), *Hartmut Eifert* (C-93/09) *c/ Land Hessen,* aff. jtes C-92/09 et C-93/09, *op. cit.*, pt. 47 : "*[...l]'article 8, paragraphe 1, de la charte [des droits fondamentaux de l'Union européenne] énonce que « [t]oute personne a droit à la protection des données à caractère personnel la concernant ». Ce droit fondamental est étroitement lié au droit au respect de la vie privée consacré à l'article 7 de cette même charte*". V. aussi les conclusions de Mme l'avocat général E. SHARPSTON sous cet arrêt.

[65] V. site du Contrôleur européen de la protection des données : http://www.edps.europa.eu/EDPSWEB/edps/lang/fr/EDPS/Dataprotection/Legislation (site consulté le 17 mai 2011).

pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel a vu le jour en 1981. La Recommandation n° R (87) 15 visant à réglementer l'utilisation des données à caractère personnel dans le secteur de la police vient compléter la protection offerte par celle-ci. En droit de l'Union européenne, les données à caractère personnel sont protégées d'une manière générale par l'article 8 de la Charte des droits fondamentaux de l'Union européenne. Celles recueillies et transmises au service de l'Espace de liberté, de sécurité et de justice sont régies par la décision-cadre 2008/977/JAI relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale[66], par dérogation aux directives 95/46/CE et 2002/58/CE. À ce régime général – actuellement en cours de révision en vue de remédier aux défaillances le rendant inopérant[67] – se superposent des dispositions spécifiques telles que celles régissant la protection des données applicables au SIS[68] ou celles relatives à la transmission, par Europol, de ces données à des États et instances tiers[69].

B. *Les droits fondamentaux dont le respect s'impose au stade du traitement des données*

Les photos, empreintes digitales et données ADN sont enregistrées dans des bases de données nationales, européennes et internationales et peuvent être échangées entre les services répressifs. Toutefois, le respect du droit à la protection des données à caractère personnel exige que leur stockage et échange soient régis par trois grands principes, à savoir les principes de finalité (1°), de disponibilité (2°) et de responsabilité (3°).

1° L'échange de données doit se faire dans le respect du principe de finalité

Dans un arrêt *Bouchacourt* du 17 décembre 2009, la Cour européenne des droits de l'homme a jugé que le droit interne relative à la protection des données à caractère personnel soumises à un traitement automatique, en particulier lorsque ces données sont utilisées à des fins policières « *doit notamment assurer que ces données sont pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées, et qu'elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées (voir paragraphes 25 et 26 [...], notamment le préambule et l'article 5 de la Convention sur la protection des données et le principe 7 de la recommandation R (87) 15 du Comité des*

---

[66] 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, *JOUE* du 30 décembre 2008, n° L 350, pp. 60-71.

[67] Opinion of the European Data Protection Supervisor on the communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – A comprehensive Approach on personal data protection in the European Union », §§ 35, 129; S. PEYROU-PISTOULEY conclut que « *la décision-cadre est, au fond, celle d'une occasion manquée [...car] incapable de remplir son rôle de cadre général pour la protection des données dans l'espace de liberté, sécurité et justice. Il ne lui reste plus dès lors qu'à s'effacer, pour laisser place à une nouvelle réglementation qui, forte de la légitimation parlementaire – nouvel acteur invité dans le processus législatif grâce au Traité de Lisbonne -saura garantir une protection des données conforme aux exigences européennes de protection des droits fondamentaux* » : PEYROU-PISTOULEY (S.), « La protection des données à caractère personnel dans l'ELSJ, work in progress… », *RTDE*, 2010, vol. 46, n° 3, pp. 775-790, spéc. p. 790.

[68] En effet, la Convention d'application de l'accord de Schengen contient des dispositions spécifiques sur la protection des données applicables au SIS.

[69] Par exemple, l'article 42 de la Convention Europol prévoit des règles relatives à la transmission de données à caractère personnel à des États et instances tiers.

Ministres visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police) »[70].

2° La transmission des données doit être conforme au principe de disponibilité[71]

En application du principe de disponibilité, l'administration répressive d'un État membre qui détient les informations dont a besoin un agent des services répressifs d'un autre État membre dans l'exercice de ses fonctions met celles-ci à la disposition du requérant.

L'« Initiative suédoise » vise à simplifier l'échange transfrontalier d'informations dans le cadre d'enquêtes pénales et d'opérations de renseignement[72]. La décision de Prüm de 2008 a pour objectif d'accélérer l'échange de profils ADN, d'empreintes digitales et de données relatives à l'immatriculation des véhicules dans le cadre de la lutte contre le terrorisme et d'autres formes de criminalité[73].

3° La sécurité des données doit être assurée au moyen du principe de responsabilité

En vertu de ce principe, tout État membre est responsable de tout dommage causé à une personne, dans lequel interviennent des données entachées d'erreurs de droit ou de fait[74]. Le second défi juridique lié à la mise en place des nouvelles technologies d'identification des personnes au service de l'Espace de liberté, de sécurité et de justice consiste à lever les obstacles à un échange efficace des données.

II. La suppression des obstacles à un échange efficace des données

La confiance dans l'authenticité des données est un préalable indispensable pour que les nouvelles technologies d'identification des personnes puissent servir utilement la réalisation et le bon fonctionnement de l'ELSJ en l'absence de standard commun en matière de certification des données. Pour l'heure actuelle, deux types d'obstacles continuent à entraver l'échange efficace des données, à savoir, les disparités en matière de certification des données (A) ainsi que les défaillances dans la mise en œuvre des textes relatifs à l'interopérabilité des bases de données (B).

---

[70] Cour EDH, 17 décembre 2009, *Bouchacourt c. France*, *op. cit.*, § 61.

[71] Considérant n° 4 de la Décision 2008/615/JAI du Conseil du 23 juin 2008, *op. cit.* : « *Selon ce principe, tout agent des services répressifs d'un État membre qui a besoin de certaines informations dans l'exercice de ses fonctions peut les obtenir d'un autre État membre, les services répressifs de l'autre État membre qui détient ces informations les mettant à sa disposition aux fins indiquées, en tenant compte des exigences des enquêtes en cours dans cet autre État* ».

[72] Décision-cadre 2006/960/JAI du 18 décembre 2006 relative à la simplification de l'échange d'information et de renseignement entre les services répressifs des États membres de l'Union européenne, *JOUE* du 29 décembre 2006, n° L 386, pp. 89-100.

[73] DUMORTIER (F.), GAYREL (C.), JOURET (J.), MOREAU (D.), POULLET (Y.), "La protection des données dans l'Espace de liberté, de sécurité et de justice", JDE, 2010, n° 166, pp. 33-46, spéc. pp. 38-39.

[74] V. Titre VI (art. 38-41) de la Convention Europol.

A. La suppression des obstacles résultant de l'existence de disparités en matière de certification des données

Europol déplore pour l'instant l'absence d'accord permettant d'appliquer une norme d'accréditation commune pour l'analyse des preuves scientifiques[75]. L'accroissement de l'échange d'informations concernant les preuves scientifiques, d'une part et la multiplication du recours à des preuves émanant d'un autre État membre dans le cadre de procédures judiciaires d'autre part rendent nécessaire l'établissement de normes communes concernant les prestataires de services de police scientifique au regard notamment du caractère particulièrement sensible de certaines données à caractère personnel telles que les empreintes digitales et profils ADN.

Conformément au plan d'action du Conseil et de la Commission mettant en œuvre le programme de La Haye[76], les États membres ont souligné la nécessité de définir des normes de qualité applicables aux laboratoires médico-légaux. À cet effet, le Conseil a adopté, le 30 novembre 2009, la décision-cadre 2009/905/JAI relative à l'accréditation des prestataires de services de police scientifique menant des activités de laboratoire[77]. Les activités couvertes par ce texte – qui doit être transposé en droit national au plus tard le 30 novembre 2013 en ce qui concerne les profils ADN et deux ans plus tard (le 30 novembre 2015) en ce qui concerne les empreintes digitales –, concernent la détection et la recherche de traces sur des objets, ainsi que l'élaboration, l'analyse et l'interprétation de preuves scientifiques, dans le but d'obtenir des avis d'experts ou d'échanger des preuves scientifiques (article 3a). Si cette décision-cadre a le mérite de créer une obligation de reconnaissance mutuelle des empreintes digitales et profils ADN[78], elle présente néanmoins l'inconvénient d'une part, de ne pas s'appliquer en matière d'appréciation judiciaire des preuves, où les règles nationales demeurent très hétérogènes (art. 5 § 2)[79] et, d'autre part, de ne viser que les mesures prises dans un laboratoire, à l'exclusion des mesures prises sur la scène de l'incident ou la scène de crime (art. 3 a).
Enfin, le dernier défi consiste à lever les obstacles à l'interopérabilité des bases de données.

B. La suppression des obstacles résultant des défaillances dans la mise en œuvre des textes relatifs à l'interopérabilité des bases de données

Nous assistons à une multiplication des bases de données, aussi bien sur le plan national que sur le plan européen : la base EURODAC contient des empreintes digitales et il est prévu que le SIS II et le VIS contiennent des photographies et empreintes digitales. Or, pour l'instant, deux obstacles majeurs s'opposent à une interopérabilité efficace des bases de données :

---

[75] Entretien réalisé au mois d'août 2010 auprès de différents services d'Europol dans le cadre du programme de recherche "IAAIS" financé par l'ANR (2009-2011).
[76] Plan d'action du Conseil et de la Commission mettant en œuvre le programme de La Haye visant à renforcer la liberté, la sécurité et la justice dans l'Union européenne, *JOUE* du 12 août 2005, pp. 1-22, point 3.4, lettre h).
[77] Décision-cadre 2009/905/JAI du Conseil du 30 novembre 2009 relative à l'accréditation des prestataires de services de police scientifique menant des activités de laboratoire, *JOUE* du 9 décembre 2009, n° L 322, pp. 14-16.
[78] Peuvent être prestataire de services de police scientifique toute organisation, publique ou privée, qui mène de telles activités de laboratoire de police scientifique à la demande des autorités répressives ou judiciaires compétentes (article 3c).
[79] BELFIORE (R.), "Movement of Evidence in the EU: The Present Scenario and Possible Future Developments", *European Journal of Crime, Criminal Law and Criminal Justice*, 17 (2009), pp. 1-22.

1° La réticence des Etats membres à alimenter les bases de données

Force est de constater que la coopération bilatérale dans les zones frontalières fonctionne pour l'instant beaucoup mieux que la mise en commun de données dans les bases de données européennes[80].

2° De nombreux problèmes et retards ont eu pour conséquence que le SIS II et le VIS ne sont toujours pas en service[81].

À la question initialement posée, à savoir « Quels sont les défis juridiques liés à la mise en place des nouvelles technologies d'identification des personnes au service de l'Espace de liberté, de sécurité et de justice ? » nous pouvons répondre qu'il convient de mettre en balance le maintien d'un haut niveau d'ordre et de sécurité publics avec le respect des droits à la libre circulation des personnes, à l'intégrité physique, à la vie privée et à la protection des données à caractère personnel, aussi bien au stade du recueil des données qu'à celui du traitement de celles-ci[82]. Or, de nombreux textes se chevauchent, ce qui rend difficile leur lisibilité et présente le danger d'une protection incomplète du droit à la vie privée. Seule leur refonte dans un instrument unique, actuellement en cours, saura y remédier[83].

De même, il convient de supprimer les obstacles tenant à la disparité des réglementations en matière de certification, ainsi qu'à une mise en œuvre largement défaillante des textes relatifs à l'interopérabilité des bases de données. Or, tant que les modalités de contrôle de l'application des textes sombrent dans l'obscurité[84], il faudra une vraie volonté politique pour relever ces défis, sinon un miracle...

---

[80] Entretien réalisé auprès de différents services d'Europol au mois d'août 2010 dans le cadre du programme de recherche "IAAIS" financé par l'ANR (2009-2011).

[81] Il est désormais prévu que le SIS II ne pourra pas entrer en service avant le dernier trimestre 2011, et la mise en place du VIS est elle aussi repoussée au-delà de septembre 2010, Résolution du Parlement européen du 22 octobre 2009 sur l'état d'avancement du système d'information Schengen de deuxième génération et du système d'information sur les visas (2010/C 265 E/01).

[82] Dans son avis sur la communication de la Commission au Conseil, au Parlement européen et au Comité économique et social européen intitulée « Vers une stratégie européenne en matière d'e-Justice » le Contrôleur européen de la protection des données rappelle que « *garantir un niveau élevé de protection des données traitées dans le cadre de la coopération policière et judiciaire [...] constitue un complément nécessaire à d'autres mesures existantes ou envisages pour faciliter l'échange transfrontalier de données à caractère personnel dans le domaine répressif* ». *Cela ne tient non seulement au droit des citoyens au respect de la protection des données à caractère personnel les concernant, qui est un droit fondamental, mais également à la nécessité que des autorités répressives puissent garantir la qualité des données échangées [...] et, enfin, la validité juridique des preuves recueillies dans un contexte transfrontalier* », *JOUE* du 6 juin 2009, n° C 128, pp. 13-19, spéc. pt. 19. La Cour de justice de l'Union européenne a jugé qu' « *aucune prééminence automatique ne saurait être reconnue à l'objectif de transparence sur le droit à la protection des données à caractère personnel (voir, en ce sens, arrêt Commission/Bavarian Lager, précité, points 75 à 79), même si des intérêts économiques importants sont en jeu* » : CJUE, 9 novembre 2010, *Volker und Markus Schecke GbR* (C-92/09), *Hartmut Eifert* (C-93/09) *c/ Land Hessen*, aff. jtes C-92/09 et C-93/09, pt. 85.

[83] Communication de la Commission au Parlement européen et au Conseil du 20 juillet 2010 intitulée « Présentation générale de la gestion de l'information dans le domaine de la liberté, de la sécurité et de la justice », p. 3; SYMEONIDOU-KASTAIDOU (E.), "DNA Analysis and Criminal Proceedings : The European Institutional Framework", *European Journal of Crime, Criminal Law and Criminal Justice*, 19 (2011), pp. 139-160, spéc. pp. 158-160.

[84] Communication de la Commission au Parlement européen et au Conseil du 20 juillet 2010, *op. cit.*, p. 24 : « *...la structure actuelle de la gestion de l'information dans l'UE n'est pas propice à l'adoption d'un mécanisme d'évaluation unique pour l'ensemble des instruments. En raison de cette diversité, il est essentiel que toute modification future d'un instrument dans le domaine de la gestion de l'information tienne compte de son impact potentiel sur toutes les autres mesures régissant la collecte, le stockage ou l'échange de données à caractère personnel dans le domaine de la liberté, de la sécurité et de la justice* ». Dans ce sens aussi v. BEAUVAIS (P.), « Droit pénal de l'Union européenne (1er septembre 2009 - 31 juillet 2010) », *RTDE*, 2010, pp. 721 et ss.