COMMISSION EUROPÉENNE

Bruxelles, le 20.7.2010

COM(2010)385 final

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL

Présentation générale de la gestion de l'information dans le domaine de la liberté, de la sécurité et de la justice

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL

Présentation générale de la gestion de l'information dans le domaine de la liberté, de la sécurité et de la justice

1. INTRODUCTION

L'Union européenne a parcouru un long chemin depuis que les dirigeants de cinq pays européens sont convenus, en 1985 à Schengen, de supprimer les contrôles à leurs frontières communes. L'accord conclu à cette occasion a débouché, en 1990, sur la convention de Schengen, qui contenait les germes de nombreuses politiques actuelles de gestion de l'information. La suppression des contrôles aux frontières intérieures a encouragé la mise en place de toute une série de mesures aux frontières extérieures, portant pour la plupart sur la délivrance des visas, la coordination des politiques d'asile et d'immigration et le renforcement de la coopération policière, judiciaire et douanière dans la lutte contre la criminalité transfrontalière. Sans échange de données par-delà les frontières, ni l'espace Schengen ni le marché intérieur de l'UE ne pourraient fonctionner à l'heure actuelle.

Les attentats terroristes perpétrés aux États-Unis en 2001 ainsi que les attentats à la bombe de Madrid en 2004 et de Londres en 2005 ont incité les instances politiques à insuffler une nouvelle dynamique à l'élaboration des politiques européennes de gestion de l'information. En 2006, le Conseil et le Parlement européen ont adopté la directive sur la conservation de données afin de permettre aux autorités nationales de lutter contre les formes graves de criminalité en conservant les données de localisation et les données relatives au trafic des télécommunications[1]. Le Conseil a ensuite adopté l'initiative suédoise visant à simplifier l'échange transfrontalier d'informations dans le cadre d'enquêtes pénales et d'opérations de renseignement. En 2008, il a adopté la décision de Prüm destinée à 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. La coopération transfrontalière entre cellules de renseignement financier, bureaux de recouvrement des avoirs et plateformes de lutte contre la cybercriminalité ainsi que le recours par les États membres à Europol et Eurojust constituent autant de moyens supplémentaires de lutter contre les formes graves de criminalité dans l'espace Schengen.

Au lendemain des attentats terroristes du 11 septembre 2001, le gouvernement américain a mis en place son programme de surveillance du financement du terrorisme (*Terrorist Finance*

[1] À l'heure actuelle, il n'existe pas de définition harmonisée au niveau de l'UE des «formes graves de criminalité». Ainsi, la décision du Conseil habilitant Europol à consulter le VIS (décision 2008/633/JAI, JO L 218 du 13.8.2008, p. 129) définit les «infractions pénales graves» en renvoyant à la liste d'infractions figurant dans la décision relative au mandat d'arrêt européen (décision 2002/584/JAI du Conseil, JO L 190 du 18.7.2002, p. 1). La directive sur la conservation des données (directive 2002/58/CE, JO L 105 du 13.4.2006, p. 54) laisse aux États membres le soin de définir les «formes graves de criminalité». La décision portant création d'Europol (décision 2009/371/JAI du Conseil, JO L 121 du 15.5.2009, p. 37) contient une autre liste d'infractions définies comme constituant des «formes graves de criminalité», qui est très semblable, mais pas identique, à la liste figurant dans la décision sur le mandat d'arrêt européen.

Tracking Program - TFTP) dans le but de déjouer des complots analogues en surveillant les transactions financières suspectes. Le Parlement européen a récemment approuvé la conclusion de l'accord entre l'Union européenne et les États-Unis d'Amérique portant sur le traitement et le transfert des données de messagerie financière de l'Union européenne aux États-Unis aux fins du programme de surveillance du financement du terrorisme (l'accord TFTP UE-États-Unis)[2]. Les échanges avec les pays tiers de données relatives aux passagers aériens (*Passenger Name Records* - PNR) ont également aidé l'UE à lutter contre le terrorisme et d'autres formes graves de criminalité[3]. Après avoir conclu des accords PNR avec les État-Unis, l'Australie et le Canada, la Commission a récemment décidé de repenser totalement son approche de la mise en place d'un système PNR dans l'UE et du partage de ces données avec des pays tiers.

Les mesures présentées ci-dessus ont permis la libre circulation dans l'espace Schengen, contribué à prévenir et combattre les attentats terroristes ainsi que d'autres formes graves de criminalité et soutenu la mise en place d'une politique commune en matière de visas et d'asile.

La présente communication propose, pour la première fois, un panorama complet des mesures qui, au niveau de l'UE, sont en place, en cours de mise en œuvre ou d'examen et qui régissent la collecte, le stockage ou l'échange transfrontalier d'informations à caractère personnel à des fins répressives ou de gestion des flux migratoires. Les citoyens ont le droit de connaître les données à caractère personnel les concernant qui sont traitées et échangées et de savoir par qui elles le sont et à quelle fin. Le présent document apporte une réponse transparente à ces questions. Il précise, pour chacun de ces instruments, son objectif principal, sa structure, le type de données à caractère personnel sur lequel il porte et la liste des services ayant accès à ces données, et rappelle les dispositions régissant la protection et la conservation de données. Il contient en outre un nombre limité d'exemples illustrant la manière dont ces instruments fonctionnent concrètement (voir l'annexe I). Enfin, il énonce les principes fondamentaux qui devraient servir de base à la conception et à l'évaluation des instruments en matière de gestion de l'information dans le domaine de la liberté, de la sécurité et de la justice.

En présentant un panorama des mesures régissant, au niveau de l'UE, la gestion des informations à caractère personnel et en proposant un ensemble de principes à suivre pour mettre au point et évaluer les mesures de ce type, la présente communication contribue à l'émergence d'un dialogue éclairé avec l'ensemble des parties prenantes sur les politiques. Dans le même temps, elle apporte une première réponse aux demandes des États membres de mettre au point une approche plus «cohérente» de l'échange d'informations à caractère personnel à des fins répressives, question qui a récemment été abordée dans la stratégie de gestion de l'information de l'UE[4], et permet de réfléchir à la nécessité éventuelle de concevoir

---

2 Résolution P7_TA-PROV(2010)0279 du Parlement européen du 8.7.2010.

3 Contrairement aux formes graves de criminalité, les «infractions terroristes» sont clairement définies dans la décision-cadre du Conseil relative à la lutte contre le terrorisme (décision-cadre 2002/475/JAI du Conseil, JO L 164 du 22.6.2002, p. 3; modifiée par la décision-cadre 2008/919/JAI du Conseil, JO L 330 du 9.12.2008, p. 21).

4 Conclusions du Conseil concernant une stratégie de gestion de l'information pour la sécurité intérieure de l'UE, Conseil «Justice et affaires intérieures», 30.11.2009 (stratégie de gestion de l'information de l'UE); Liberté, sécurité, protection de la vie privée - Les affaires intérieures européennes dans un monde ouvert - Rapport du groupe consultatif informel de haut niveau sur l'avenir des politiques européennes dans le domaine des affaires intérieures (le «Groupe du futur»), juin 2008.

un modèle européen d'échange d'informations fondé sur une évaluation des mesures actuelles régissant l'échange d'informations[5].

La limitation des finalités est un aspect essentiel pour la plupart des instruments sur lesquels porte la présente communication. Un système d'information unique et global au niveau de l'UE, aux objectifs multiples, permettrait d'atteindre le degré le plus élevé d'échange d'informations. La création d'un tel système serait toutefois synonyme de restriction illégitime et abusive des droits des personnes à la protection des données et au respect de la vie privée et engendrerait de très grandes difficultés concernant sa mise au point et son fonctionnement. En pratique, les politiques dans le domaine de la liberté, de la sécurité et de la justice ont été élaborées progressivement, ce qui a donné naissance à plusieurs instruments et systèmes d'information dont la taille, la portée et la finalité sont variables. La structure compartimentée de la gestion de l'information qui a vu le jour au cours des dernières décennies est plus propice à garantir le respect du droit à la vie privée que tout autre système centralisé.

La présente communication ne porte pas sur les mesures impliquant l'échange de données à caractère non personnel à des fins stratégiques, comme les analyses des risques ou les évaluations des menaces de portée générale; elle n'analyse pas davantage en détail les dispositions en matière de protection des données prévues par les instruments examinés, la Commission procédant actuellement, au titre de l'article 16 du traité sur le fonctionnement de l'Union européenne, à un exercice distinct consacré à un nouveau cadre général de protection des données à caractère personnel dans l'UE. Le Conseil examine à l'heure actuelle le projet de directives de négociation en vue d'un accord UE-États-Unis relatif à la protection des données à caractère personnel lors de leur transfert et de leur traitement aux fins de prévenir les infractions pénales, dont les actes terroristes, d'enquêter en la matière, de les détecter ou de les poursuivre dans le cadre de la coopération policière et de la coopération judiciaire en matière pénale. Ces négociations devant déterminer les modalités selon lesquelles les deux parties peuvent assurer un niveau élevé de protection des libertés et droits fondamentaux lors du transfert ou du traitement des données à caractère personnel plutôt que la teneur proprement dite de ces transferts ou traitements de données, la présente communication ne porte pas sur cette initiative[6].

2. INSTRUMENTS DE L'UE RÉGISSANT LA COLLECTE, LE STOCKAGE OU L'ÉCHANGE DE DONNÉES À CARACTÈRE PERSONNEL À DES FINS RÉPRESSIVES OU DE GESTION DES FLUX MIGRATOIRES

La présente section propose un panorama des instruments adoptés par l'Union européenne et régissant la collecte, le stockage ou l'échange transfrontalier de données à caractère personnel à des fins répressives ou de gestion des flux migratoires. La section 2.1 s'attache plus particulièrement aux mesures actuellement en vigueur ou en cours de mise en œuvre ou d'examen, et la section 2.2 concerne les initiatives annoncées dans le plan d'action mettant en œuvre le programme de Stockholm[7]. Cette section contient, pour chaque instrument, des informations sur les aspects suivants:

---

5 Le programme de Stockholm – Une Europe ouverte et sûre qui sert et protège les citoyens, document 5731/10 du Conseil du 3.3.2010, section 4.2.2.

6 COM(2010) 252 du 26.5.2010.

7 COM(2010) 171 du 20.4.2010 (plan d'action mettant en œuvre le programme de Stockholm).

– contexte (la mesure a-t-elle été proposée par les États membres ou par la Commission)[8];

– finalités(s) pour laquelle/lesquelles les données sont collectées, stockées ou échangées;

– structure (système d'information centralisé ou échange décentralisé de données);

– données à caractère personnel sur lesquelles porte l'instrument;

– services ayant accès aux données;

– dispositions en matière de protection des données;

– règles relatives à la conservation des données;

– degré de mise en œuvre;

– mécanisme de réexamen.

2.1. Instruments actuellement utilisés ou en cours de mise en œuvre ou d'examen

Instruments de l'UE visant à améliorer le fonctionnement de l'espace Schengen et de l'union douanière

Le **système d'information Schengen** (SIS) est né du souhait des États membres de créer un espace sans contrôles aux frontières intérieures tout en facilitant le franchissement par les personnes des frontières extérieures[9]. Fonctionnant depuis 1995, il s'efforce de maintenir la sécurité publique, y compris la sécurité nationale, à l'intérieur de l'espace Schengen et de faciliter la circulation des personnes au moyen des informations qu'il permet de transmettre. Le SIS est un système d'information centralisé doté d'une composante nationale dans chaque État participant et d'une fonction de support technique située en France. Les États membres peuvent signaler les personnes recherchées pour l'arrestation aux fins d'extradition; les ressortissants de pays tiers non admissibles; les personnes disparues; les témoins ou personnes citées à comparaître devant les autorités judiciaires; les personnes et véhicules faisant l'objet d'une surveillance exceptionnelle en raison de la menace qu'ils constituent pour la sécurité publique ou nationale; les armes à feu, documents et véhicules perdus ou volés; et les billets de banque suspects. Les données saisies dans le SIS comprennent les noms et pseudonymes («alias»), les caractéristiques physiques, les date et lieu de naissance, la nationalité et l'indication que la personne concernée est ou non armée et violente. Dans le cadre de procédures pénales, les autorités policières, douanières et judiciaires et celles chargées des contrôles aux frontières peuvent, dans les limites de leurs prérogatives légales respectives, accéder aux informations précitées. Les services d'immigration et les postes consulaires ont

---

[8] Conformément à l'ancien troisième pilier de l'Union européenne, concernant la coopération policière et judiciaire en matière pénale, les États membres et la Commission se partageaient le droit d'initiative. Le traité d'Amsterdam a intégré les domaines des frontières extérieures, des visas, de l'asile et de l'immigration dans le (premier) pilier communautaire, pour lequel la Commission jouissait d'un droit d'initiative exclusif. Le traité de Lisbonne a supprimé la structure en piliers de l'Union, en réaffirmant le droit d'initiative de la Commission. Toutefois, dans les domaines de la coopération policière et judiciaire en matière pénale (y compris la coopération administrative), un acte législatif peut toujours être proposé sur initiative d'un quart des États membres.

[9] Convention d'application de l'Accord de Schengen du 14 juin 1985 entre les gouvernements des États de l'Union économique Benelux, de la République fédérale d'Allemagne et de la République française relatif à la suppression graduelle des contrôles aux frontières communes, JO L 239 du 22.9.2000, p. 19.

accès aux données relatives aux ressortissants de pays tiers figurant sur la liste des personnes non admissibles ainsi qu'aux signalements concernant les documents perdus ou volés. Europol peut avoir accès à certaines catégories de données figurant dans le SIS, notamment les signalements se rapportant aux personnes recherchées pour l'arrestation aux fins d'extradition et aux personnes faisant l'objet d'une surveillance exceptionnelle en raison de la menace qu'elles constituent pour la sécurité publique ou nationale. Eurojust peut accéder aux signalements se rapportant aux personnes recherchées pour l'arrestation aux fins d'extradition et aux témoins ou personnes citées à comparaître devant les autorités judiciaires. Les données à caractère personnel ne peuvent être utilisées qu'aux fins des signalements spécifiques pour lesquels elles ont été fournies. Les données à caractère personnel saisies dans le SIS à des fins de recherche de personnes ne peuvent être conservées que pendant la durée nécessaire pour atteindre les finalités pour lesquelles elles ont été fournies et doivent être effacées au plus tard trois ans après la date de leur introduction dans le système. Les données relatives aux personnes faisant l'objet d'une surveillance exceptionnelle en raison de la menace qu'elles constituent pour la sécurité publique ou nationale doivent être supprimées après un an. Les États membres doivent adopter des dispositions nationales prévoyant un niveau de protection des données au moins égal à celui résultant de la convention de 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et de la recommandation de 1987 du Comité des ministres du Conseil de l'Europe aux États membres visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police[10]. Bien que la convention de Schengen ne prévoie pas de mécanisme de réexamen, ses signataires peuvent proposer des modifications à la convention, à la suite de quoi le texte modifié doit être approuvé à l'unanimité et ratifié par les parlements nationaux. Le SIS est applicable dans son intégralité dans 22 États membres, ainsi qu'en Suisse, en Norvège et en Islande. Le Royaume-Uni et l'Irlande participent aux aspects liés à la coopération policière de la convention de Schengen et du SIS, sauf pour ce qui est des signalements concernant les ressortissants de pays tiers figurant sur la liste des personnes non admissibles. Chypre a signé la convention de Schengen, mais ne l'a pas encore mise en œuvre. Le Liechtenstein doit la mettre en œuvre en 2010, et la Bulgarie et la Roumanie devraient le faire en 2011. Une recherche effectuée dans le SIS donne lieu à un «résultat positif» (*hit*) lorsque les données relatives à une personne ou un objet recherchés correspondent à celles d'un signalement existant. Lorsqu'elles ont obtenu un résultat positif, les autorités répressives peuvent, par l'intermédiaire de leur réseau de bureaux SIRENE, demander des informations supplémentaires afin de savoir sur qui et/ou sur quoi porte un signalement[11].

L'adhésion de nouveaux États membres à l'espace Schengen a entraîné une croissance correspondante de la taille de la base de données du SIS: entre janvier 2008 et 2010, le nombre total de signalements dans le SIS a augmenté de 22,9 à 31,6 millions[12]. Anticipant cette hausse des volumes de données échangées et les évolutions des besoins des utilisateurs, les États membres ont, en 2001, décidé de mettre au point un **système d'information**

---

10 Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108), Conseil de l'Europe, 28.1.1981 (convention n° 108 du Conseil de l'Europe); recommandation n° R (87) 15 du Comité des ministres aux États membres visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, Conseil de l'Europe, 17.9.1987 (recommandation relative à la police).

11 SIRENE signifie «*Supplementary Information Request at National Entry*» ou «supplément d'information requis à l'entrée nationale».

12 Document 5441/08 du Conseil du 30.1.2008; document 6162/10 du Conseil du 5.2.2010.

Schengen de deuxième génération (SIS II) et confié cette mission à la Commission[13]. Le SIS II, qui est actuellement en cours de mise au point, a pour finalité d'assurer un niveau élevé de sécurité dans le domaine de la liberté, de la sécurité et de la justice en améliorant les fonctionnalités du système de première génération, et de faciliter la circulation des personnes au moyen des informations qu'il permet de transmettre. Outre les catégories initiales de données sur lesquelles portait le système de première génération, le SIS II sera en mesure de traiter les empreintes digitales, les photographies, les copies du mandat d'arrêt européen, les dispositions visant à protéger les intérêts des personnes dont l'identité est usurpée et les liens entre différents signalements. Ainsi, le SIS II sera capable de mettre en relation le signalement concernant une personne recherchée pour enlèvement, celui concernant la victime de cet enlèvement et celui concernant le véhicule utilisé pour commettre cette infraction. La réglementation en matière de droits d'accès et de conservation des données est identique à celle prévue pour le système de première génération. Les données à caractère personnel ne peuvent être utilisées qu'aux fins des signalements spécifiques pour lesquels elles ont été fournies. Les données à caractère personnel se trouvant dans le SIS II doivent être traitées conformément aux dispositions spécifiques figurant dans les actes législatifs de base régissant ce système [règlement (CE) n° 1987/2006 et décision 2007/533/JAI du Conseil], qui précisent les principes énoncés dans la directive 95/46/CE, et conformément au règlement (CE) n° 45/2001, à la convention n° 108 du Conseil de l'Europe et à la recommandation relative à la police[14]. Le SIS II fera usage de s-TESTA, le réseau sécurisé de communication de données de la Commission[15]. Dès qu'il sera opérationnel, ce système sera applicable dans tous les États membres, en Suisse, au Liechtenstein, en Norvège et en Islande[16]. La Commission est tenue de faire parvenir au Parlement européen et au Conseil un rapport semestriel sur l'état d'avancement des travaux concernant le développement du SIS II et la migration éventuelle du système de première génération vers le SIS II[17].

La mise au point d'**EURODAC** remonte à la suppression des frontières intérieures, qui a imposé de définir des règles claires relatives au traitement des demandes d'asile. EURODAC est un système centralisé et automatisé d'identification des empreintes digitales contenant les données dactyloscopiques de certains ressortissants de pays tiers. Il est opérationnel depuis janvier 2003 et son objectif est de contribuer à déterminer l'État membre responsable, au titre du règlement «Dublin», de l'examen d'une demande d'asile[18]. Les personnes âgées de 14 ans

---

13 Règlement (CE) n° 1986/2006, JO L 381 du 28.12.2006, p. 1; règlement (CE) n° 1987/2006, JO L 381 du 28.12.2006, p. 4; décision 2007/533/JAI du Conseil, JO L 205 du 7.8.2007, p. 63.

14 Règlement (CE) n° 1987/2006, JO L 381 du 28.12.2006, p. 4; décision 2007/533/JAI du Conseil, JO L 205 du 7.8.2007, p. 63; directive 95/46/CE, JO L 281 du 23.11.1995, p. 31; règlement (CE) n° 45/2001, JO L 8 du 12.1.2001, p. 1; convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108), Conseil de l'Europe, 28.1.1981 (convention n° 108 du Conseil de l'Europe); recommandation n° R (87) 15 du Comité des ministres aux États membres visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, Conseil de l'Europe, 17.9.1987 (recommandation relative à la police).

15 S-TESTA, qui signifie «*Secure Trans-European Services for Telematics between Administrations*» ou «services télématiques transeuropéens sécurisés entre administrations» est un réseau de communication de données financé par la Commission qui permet l'échange crypté et sécurisé de données entre administrations nationales et institutions, agences, organes et organismes de l'UE.

16 Le Royaume-Uni et l'Irlande participeront au SIS II sauf pour ce qui est des signalements concernant les ressortissants de pays tiers figurant sur la liste des personnes non admissibles.

17 Règlement (CE) n° 1104/2008 du Conseil, JO L 299 du 8.11.2008, p. 1; décision 2008/839/JAI du Conseil, JO L 299 du 8.11.2008, p. 43.

18 Règlement (CE) n° 343/2003 du Conseil, JO L 50 du 25.2.2003, p. 1 (règlement «Dublin») et règlement (CE) n° 2725/2000 du Conseil, JO L 316 du 15.12.2000, p. 1 (règlement EURODAC). Ces instruments se fondent sur la convention de Dublin de 1990 (JO C 254 du 19.8.1997, p. 1), qui avait

ou plus qui introduisent une demande d'asile dans un État membre font automatiquement l'objet d'un relevé d'empreintes digitales, au même titre que les ressortissants de pays tiers appréhendés lors du franchissement irrégulier d'une frontière extérieure. En comparant les empreintes digitales de ces personnes avec celles figurant dans EURODAC, les autorités nationales cherchent à déterminer où cette personne aurait pu avoir présenté une demande d'asile ou par quel pays elle est entrée pour la première fois dans l'Union européenne. Les autorités peuvent aussi comparer aux données figurant dans EURODAC les empreintes digitales de ressortissants de pays tiers se trouvant illégalement sur leur territoire. Les États membres doivent préciser la liste des services ayant accès à cette base de données, parmi lesquelles figurent en général les services chargés de l'asile et des migrations, les gardes-frontières et les services de police. Les États membres transfèrent les données pertinentes à la base de données centrale par l'intermédiaire de leurs points d'accès nationaux. Les données à caractère personnel se trouvant dans EURODAC ne peuvent être utilisées qu'aux fins de faciliter l'application du règlement «Dublin»; toute autre utilisation de ces données est passible de sanctions. Les empreintes digitales des demandeurs d'asile sont conservées pour une durée de dix ans; celles des migrants en situation irrégulière pour une durée de deux ans. Les données des demandeurs d'asile sont supprimées dès lors qu'ils acquièrent la citoyenneté d'un État membre; celles des migrants en situation irrégulière le sont dès lors qu'ils obtiennent un titre de séjour ou la citoyenneté, ou quittent le territoire des États membres. La directive 95/46/CE s'applique au traitement de données à caractère personnel au titre de cet instrument[19]. EURODAC utilise le réseau s-TESTA de la Commission et est applicable dans tous les États membres, ainsi qu'en Norvège, en Islande et en Suisse. Un accord permettant au Liechtenstein d'être connecté devrait être conclu sous peu. La Commission est tenue de soumettre au Parlement européen et au Conseil des rapports annuels sur le fonctionnement de l'unité centrale d'EURODAC.

Au lendemain des attentats du 11 septembre 2001, les États membres ont décidé d'accélérer la mise en œuvre d'une politique commune des visas en créant un système d'échange d'informations pour les visas de court séjour[20]. La suppression des frontières intérieures a également simplifié l'utilisation frauduleuse des régimes de visas des États membres. Le **système d'information sur les visas** (VIS) a pour but de répondre à ces deux préoccupations: il vise à soutenir la mise en œuvre d'une politique commune des visas en simplifiant l'examen des demandes de visa et les contrôles aux frontières extérieures tout en contribuant à la prévention des menaces dirigées contre la sécurité intérieure des États membres[21]. Le VIS sera un système d'information centralisé doté d'une composante nationale dans chaque État participant et d'une fonction de support technique située en France. Il aura recours à un système de correspondance biométrique destiné à garantir la fiabilité des comparaisons d'empreintes digitales et vérifiera l'identité des titulaires de visas aux frontières extérieures. Il comprendra des données concernant les demandes de visas, des photographies, des empreintes digitales, des décisions connexes des services de visas et des liens entre demandes connexes. Les services chargés des visas, de l'asile, de l'immigration et des contrôles aux frontières disposeront d'un accès à cette base de données afin de vérifier l'identité des titulaires de visas

---

pour objectif la détermination de l'État responsable de l'examen d'une demande d'asile présentée dans l'un des États membres. Ce système d'évaluation des demandes d'asile est connu sous le nom de «système de Dublin».

19 Directive 95/46/CE, JO L 281 du 23.11.1995, p. 31.

20 Session extraordinaire du Conseil «Justice et affaires intérieures» du 20.1.2001.

21 Décision 2004/512/CE du Conseil, JO L 213 du 15.6.2004, p. 5; règlement (CE) n° 767/2008, JO L 218 du 13.8.2008, p. 60; décision 2008/633/JAI du Conseil, JO L 218 du 13.8.2008, p. 129. Voir aussi la déclaration sur la lutte contre le terrorisme, Conseil européen, 25.3.2004.

et l'authenticité des visas; les services de police ainsi qu'Europol peuvent la consulter afin de prévenir et combattre le terrorisme et les autres formes graves de criminalité[22]. Les dossiers liés aux demandes peuvent être conservés pour une durée de cinq ans. Les données à caractère personnel se trouvant dans le VIS doivent être traitées conformément aux dispositions spécifiques figurant dans les actes législatifs de base régissant ce système [règlement (CE) n° 767/2006 et décision 2008/633/JAI du Conseil], qui complètent les dispositions de la directive 95/46/CE, du règlement (CE) n° 45/2001, de la décision-cadre 2008/977/JAI du Conseil, de la convention n° 108 du Conseil de l'Europe, de son protocole additionnel n° 181 et de la recommandation relative à la police[23]. Le VIS sera applicable dans tous les États membres (à l'exception du Royaume-Uni et de l'Irlande) ainsi qu'en Suisse, en Norvège et en Islande. Il fonctionnera sur la base du réseau s-TESTA de la Commission. La Commission procédera à l'évaluation du système trois ans après son lancement et ensuite tous les quatre ans.

Sur initiative espagnole, le Conseil a adopté en 2004 une directive régissant la transmission d'**informations anticipées sur les passagers** (*Advance Passenger Information* – API) par les transporteurs aériens aux autorités chargées des contrôles aux frontières[24]. Cet instrument a pour but d'améliorer les contrôles aux frontières et de lutter contre les migrations irrégulières. Sur demande, les transporteurs aériens doivent communiquer aux autorités chargées des contrôles aux frontières le nom, la date de naissance, la nationalité, le point d'embarquement et le point de passage frontalier utilisé pour entrer sur le territoire de l'UE des passagers se rendant dans l'UE au départ de pays tiers. Ces données à caractère personnel sont généralement extraites des parties lisibles par machine des passeports des passagers et transmises aux autorités après l'enregistrement. Après l'arrivée d'un vol, les autorités et les transporteurs aériens peuvent conserver les données API pendant 24 heures. Le système API fonctionne de manière décentralisée grâce au partage d'informations entre opérateurs privés et pouvoirs publics. Cet instrument ne permet pas l'échange de données API entre États membres; toutefois, les autorités répressives autres que les gardes-frontières peuvent demander d'avoir accès à ces informations à des fins répressives. Les données à caractère personnel ne peuvent être utilisées que par les pouvoirs publics à des fins de contrôles aux frontières et de lutte contre les migrations irrégulières et doivent être traitées conformément à la directive 95/46/CE[25]. En vigueur dans toute l'UE, cet instrument n'est utilisé que par un faible nombre d'États membres. La Commission procédera à un réexamen de cette directive en 2011.

Une partie importante du programme de la Commission de 1992, qui prévoyait la création du marché intérieur, concernait la suppression de tous les contrôles et formalités concernant les

---

22 Décision 2008/633/JAI du Conseil, JO L 218 du 13.8.2008, p. 129.

23 Règlement (CE) n° 767/2008, JO L 218 du 13.8.2008, p. 60; décision 2008/633/JAI du Conseil, JO L 218 du 13.8.2008, p. 129; directive 95/46/CE, JO L 281 du 23.11.1995, p. 31; règlement (CE) n° 45/2001, JO L 8 du 12.1.2000, p. 1; décision-cadre 2008/977/JAI du Conseil, JO L 350 du 30.12.2008, p. 60; convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108), Conseil de l'Europe, 28.1.1981 (convention n° 108 du Conseil de l'Europe); protocole additionnel à la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel concernant les autorités de contrôle et les flux transfrontières de données (STE n° 181), Conseil de l'Europe, 8.11.2001 (protocole additionnel n° 181); recommandation n° R (87) 15 du Comité des ministres aux États membres visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, Conseil de l'Europe, 17.9.1987 (recommandation relative à la police).

24 Directive 2004/82/CE du Conseil, JO L 261 du 6.8.2004, p. 24.

25 Directive 95/46/CE, JO L 281 du 23.11.1995, p. 31.

marchandises circulant dans la Communauté[26]. La suppression de ces procédures aux frontières intérieures a accru le risque de fraude, ce qui a contraint les États membres à mettre en place, d'une part, un mécanisme d'assistance administrative mutuelle afin de contribuer à la prévention des opérations contraires à la législation douanière et agricole communautaire, ainsi qu'aux enquêtes et aux poursuites en la matière, et, d'autre part, une coopération douanière visant à permettre de détecter et de poursuivre les infractions aux dispositions douanières nationales, notamment en renforçant l'échange transfrontalier d'informations. Sans préjudice de la compétence de l'UE en matière d'union douanière[27], la **convention Naples II** relative à l'assistance mutuelle et à la coopération entre les administrations douanières vise à permettre aux administrations douanières nationales de prévenir et de détecter les infractions aux réglementations douanières nationales et à les aider à poursuivre et réprimer les infractions aux réglementations douanières communautaires et nationales[28]. Au titre de cet instrument, un ensemble de services centraux de coordination peuvent demander par écrit l'assistance de leurs homologues d'autres États membres dans le cadre d'enquêtes pénales concernant des infractions aux réglementations douanières nationales et communautaires. Ces services ne sont autorisés à traiter les données à caractère personnel qu'aux fins prévues par la convention Naples II. Ils peuvent transmettre ces informations aux administrations douanières, autorités de poursuite et instances judiciaires nationales et, moyennant le consentement préalable de l'État membre fournissant les informations, à d'autres autorités. Les données peuvent être conservées pour une durée n'excédant pas celle nécessaire pour atteindre les finalités pour lesquelles elles ont été fournies. Dans l'État membre destinataire, les données à caractère personnel bénéficient au moins du même niveau de protection que dans l'État membre qui les a fournies et leur traitement doit respecter les dispositions de la directive 95/46/CE et de la convention n° 108 du Conseil de l'Europe[29]. La convention Naples II a été ratifiée par tous les États membres. Ceux-ci peuvent proposer des amendements, le texte modifié devant ensuite être adopté par le Conseil des ministres et ratifié par les États membres.

Venant compléter la convention Naples II, la convention SID déploie le **système d'information douanier** (SID) afin d'aider à prévenir, rechercher et poursuivre les infractions graves aux lois nationales en renforçant, par une diffusion plus rapide des informations, l'efficacité des procédures de coopération et de contrôle des administrations douanières des États membres[30]. Le SID, géré par la Commission, est un système d'information centralisé accessible à partir de terminaux dans chacun des États membres et à la Commission, Europol et Eurojust. Il comprend les données à caractère personnel se rapportant à des marchandises, moyens de transports, entreprises, personnes et retenues, saisies ou confiscations d'articles et d'argent liquide. Ces données à caractère personnel sont les noms et noms d'emprunt, les date

---

26 Règlement (CEE) n° 2913/92 du Conseil, JO L 302 du 19.10.1992.

27 Règlement (CE) n° 515/97 du Conseil du 13 mars 1997 relatif à l'assistance mutuelle entre les autorités administratives des États membres et à la collaboration entre celles-ci et la Commission en vue d'assurer la bonne application des réglementations douanière et agricole, JO L 82 du 22.3.1997, p. 1, modifié par le règlement (CE) n° 766/2008, JO L 218 du 13.8.2008, p. 48.

28 Convention établie sur la base de l'article K.3 du traité sur l'Union européenne relative à l'assistance mutuelle et à la coopération entre les administrations douanières, JO C 24 du 23.1.1998, p. 2 (convention Naples II).

29 Directive 95/46/CE, JO L 281 du 23.11.1995, p. 31; convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108), Conseil de l'Europe, 28.1.1981 (convention n° 108 du Conseil de l'Europe).

30 Convention établie sur la base de l'article K.3 du traité sur l'Union européenne, sur l'emploi de l'informatique dans le domaine des douanes, JO C 316 du 27.11.1995, p. 34, modifiée par la décision 2009/917/JAI du Conseil, JO L 323 du 10.12.2009, p. 20.

et lieu de naissance, la nationalité, le sexe, les signes particuliers, les documents d'identité, l'adresse, tout antécédent de faits de violence, le motif d'introduction des données dans le SID, l'action suggérée et le numéro d'immatriculation du moyen de transport. Dans le cas des retenues, saisies ou confiscations d'articles et d'argent liquide, seuls les éléments biographiques et l'adresse peuvent être introduits dans le SID. Ces informations peuvent être utilisées uniquement aux fins d'observation ou de compte rendu, d'inspections particulières ou de contrôles spécifiques, ou d'analyses opérationnelles ou stratégiques concernant des personnes suspectées d'avoir enfreint les dispositions douanières nationales. Les autorités douanières, fiscales, agricoles, de santé publique et policières nationales, Europol et Eurojust peuvent accéder aux données du SID[31]. Le traitement des données à caractère personnel doit se faire dans le respect des règles spécifiques arrêtées dans la convention SID et des dispositions de la directive 95/46/CE, du règlement (CE) n° 45/2001, de la convention n° 108 du Conseil de l'Europe et de la recommandation relative à la police[32]. Les données à caractère personnel ne peuvent être copiées du SID dans d'autres systèmes de traitement des données qu'à des fins d'analyses opérationnelles ou de gestion des risques, et seuls les analystes désignés par les États membres peuvent y accéder. Les données à caractère personnel copiées du SID ne peuvent être conservées que pendant la durée nécessaire pour atteindre les finalités pour lesquelles elles ont été copiées et doivent être effacées au plus tard après dix ans. Le SID crée également un **fichier d'identification des dossiers d'enquêtes douanières** (FIDE) afin de contribuer à la prévention des infractions graves aux législations nationales, ainsi qu'aux enquêtes et aux poursuites en la matière[33]. Le FIDE permet aux autorités nationales chargées de mener des enquêtes en matière douanière, lorsqu'elles ouvrent un dossier d'enquête, d'identifier les autres autorités qui auraient pu enquêter sur une personne ou une entreprise donnée. Ces autorités peuvent introduire des données dans le FIDE au départ de leurs dossiers d'enquêtes, y compris les données biographiques des personnes faisant l'objet d'enquêtes ainsi que la raison sociale, la raison commerciale, le numéro de TVA et l'adresse des entreprises faisant l'objet d'enquêtes. Les données provenant des dossiers d'enquêtes dans lesquels aucune fraude douanière n'a été détectée peuvent être conservées pendant trois ans au maximum; celles provenant de dossiers dans lesquels un cas de fraude douanière a été détecté peuvent être conservées pendant six ans au maximum; et celles provenant de dossiers dans lesquels une condamnation ou une sanction ont été prononcées peuvent être conservées pendant dix ans au maximum. Le SID et le FIDE utilisent le réseau commun de communication, l'interface commune des systèmes ou l'accès internet sécurisé que fournit la Commission. Le SID est en vigueur dans tous les États membres. La Commission, en collaboration avec les États membres, présente un rapport annuel au Parlement européen et au Conseil sur le fonctionnement du SID.

---

31 À compter de mai 2011, Europol et Eurojust disposeront d'un accès en lecture au SID en vertu de la décision 2009/917/JAI du Conseil (JO L 323 du 10.12.2009, p. 20).

32 Convention établie sur la base de l'article K.3 du traité sur l'Union européenne, sur l'emploi de l'informatique dans le domaine des douanes, JO C 316 du 27.11.1995, p. 34, modifiée par la décision 2009/917/JAI du Conseil, JO L 323 du 10.12.2009, p. 20; directive 95/46/CE, JO L 281 du 23.11.1995, p. 31; règlement (CE) n° 45/2001, JO L 8 du 12.1.2000, p. 1; convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108), Conseil de l'Europe, 28.1.1981 (convention n° 108 du Conseil de l'Europe); recommandation n° R (87) 15 du Comité des ministres aux États membres visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, Conseil de l'Europe, 17.9.1987 (recommandation relative à la police).

33 Le FIDE se fonde sur le règlement (CE) n° 766/2008 du Parlement européen et du Conseil et sur le protocole établi conformément à l'article 34 du traité sur l'Union européenne et modifiant, en ce qui concerne la création d'un fichier d'identification des dossiers d'enquêtes douanières, la convention sur l'emploi de l'informatique dans le domaine des douanes, JO C 139 du 13.6.2003, p. 1.

Instruments de l'UE visant à prévenir et à combattre le terrorisme et les autres formes graves de criminalité transfrontalière

Les attentats terroristes de mars 2004 à Madrid ont donné lieu à plusieurs nouvelles initiatives au niveau de l'UE. À la demande du Conseil européen, la Commission a présenté, en 2005, une proposition d'instrument régissant l'échange d'informations en vertu du principe de disponibilité[34]. Au lieu d'approuver cette proposition, le Conseil a adopté, en 2006, l'**initiative suédoise**, qui rationalise l'échange entre États membres d'informations ou de renseignements de nature pénale existants, susceptibles d'être nécessaires à des enquêtes pénales ou des opérations de renseignement en matière pénale[35]. Cet instrument se fonde sur le principe politique de l'«accès équivalent», en vertu duquel les conditions applicables aux échanges transfrontaliers de données ne devraient pas être plus strictes que celles régissant l'accès national. L'initiative suédoise prévoit un fonctionnement décentralisé et permet aux autorités policières, douanières et autres habilitées à enquêter sur des infractions pénales (à l'exception des services de renseignement, qui, en général, traitent de renseignements se rapportant à la sécurité publique ou nationale) de partager des informations et des renseignements de nature pénale avec leurs homologues de tous les pays de l'UE. Les États membres doivent désigner des points de contact nationaux pour répondre aux demandes urgentes d'informations. Cet instrument fixe des délais précis pour l'échange d'informations et contraint les États membres à compléter un formulaire lorsqu'ils demandent des informations. Les États membres sont tenus de répondre aux demandes d'informations et de renseignements dans un délai de huit heures dans les cas urgents, dans un délai d'une semaine dans les cas non urgents et dans un délai de deux semaines dans tous les autres cas. L'utilisation d'informations et de renseignements obtenus grâce à cet instrument est soumise au respect des législations nationales en matière de protection de données, tandis que les États membres ne sont pas autorisés à appliquer un traitement différencié aux données selon qu'elles soient d'origine nationale ou qu'elles proviennent d'autres États membres. Un État membre fournisseur peut toutefois soumettre l'utilisation d'informations ou de renseignements dans d'autres États membres au respect de certaines conditions. Le traitement de données à caractère personnel doit être conforme à la législation nationale en matière de protection des données ainsi qu'aux dispositions de la convention n° 108 du Conseil de l'Europe, de son protocole additionnel n° 181 et de la recommandation relative à la police[36]. Douze des trente-et-un signataires de cet instrument (à savoir les États membres de l'UE, ainsi que la Norvège, l'Islande, la Suisse et le Liechtenstein) ont adopté une législation nationale pour le mettre en œuvre; cinq États remplissent régulièrement le formulaire de demande d'informations; mais seuls deux États y ont fréquemment recours pour échanger des

---

34 COM(2005) 490 du 12.10.2005; Conclusions de la présidence — Le Programme de La Haye, 4/5.11.2004. Voir aussi la déclaration sur la lutte contre le terrorisme, Conseil européen, 25.3.2004.

35 Décision-cadre 2006/960/JAI du Conseil, JO L 386 du 29.12.2006, p. 89.

36 Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108), Conseil de l'Europe, 28.1.1981 (convention n° 108 du Conseil de l'Europe); protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel concernant les autorités de contrôle et les flux transfrontières de données (STE n° 181), Conseil de l'Europe, 8.11.2001 (protocole additionnel n° 181); recommandation n° R (87) 15 du Comité des ministres aux États membres visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, Conseil de l'Europe, 17.9.1987 (recommandation relative à la police).

informations[37]. La Commission est tenue de présenter son rapport d'évaluation au Conseil avant la fin de 2010.

La **décision de Prüm** se fonde sur un accord conclu en 2005 par l'Allemagne, la France, l'Espagne, les pays du Benelux et l'Autriche afin d'approfondir la coopération en matière de lutte contre le terrorisme, la criminalité transfrontalière et la migration illégale. En réponse à l'intérêt exprimé par plusieurs États membres d'adhérer à cet accord, l'Allemagne a proposé, au cours de sa présidence du Conseil de 2007, de le transformer en instrument de l'UE. La décision de Prüm de 2008, qui doit être mise en œuvre d'ici août 2011, énonce les règles applicables à l'échange transfrontalier de profils ADN, d'empreintes digitales, de données relatives à l'immatriculation des véhicules et d'informations relatives aux personnes suspectées de planifier des attentats terroristes[38]. Son objectif est de renforcer la prévention des infractions pénales, en particulier le terrorisme et la criminalité transfrontalière, et de maintenir l'ordre public lors d'événements de grande envergure. Ce système fonctionnera de manière décentralisée en prévoyant l'interconnexion, par l'intermédiaire de points de contact nationaux, des bases de données en matière d'immatriculation des véhicules, d'empreintes digitales et de profils ADN des États participants. En utilisant le réseau s-TESTA de la Commission, les points de contact traiteront les demandes entrantes et sortantes de comparaison de profils ADN, d'empreintes digitales et de données relatives à l'immatriculation des véhicules. Leurs capacités à transmettre ces données aux utilisateurs finaux sont régies par le droit national. À compter d'août 2011, la comparaison de données sera entièrement automatisée. Toutefois, les États membres doivent se soumettre à une procédure rigoureuse d'évaluation (portant, en particulier, sur leur respect des exigences techniques et en matière de protection des données) pour obtenir l'autorisation de commencer l'échange automatisé de données. Les données à caractère personnel ne peuvent pas être échangées au titre de cet instrument tant que les États membres n'ont pas assuré un niveau de protection des données au moins équivalent à celui résultant de l'application de la convention n° 108 du Conseil de l'Europe, de son protocole additionnel n° 181 et de la recommandation relative à la police[39]. Le Conseil statuera à l'unanimité afin de déterminer si cette condition a été remplie. Les informations à caractère personnel ne peuvent être utilisées qu'aux fins pour lesquelles elles ont été communiquées, sauf si l'État membre fournisseur accepte qu'elles soient utilisées à d'autres fins. Les personnes physiques peuvent également s'adresser à leur délégué national à la protection des données, désigné conformément à la directive 95/46/CE, pour faire valoir leurs droits relatifs au traitement des données à caractère personnel au titre de cet instrument. La comparaison des profils ADN et des empreintes digitales se fera selon un système (anonyme) de concordance/non-concordance (*hit/no hit*), en vertu duquel les autorités ne seront en mesure de demander des informations à caractère personnel au sujet d'une personne concernée que si leur recherche initiale a établi l'existence d'une concordance. Ces

---

37 Ces chiffres proviennent des réponses à un questionnaire, dont la présidence espagnole du Conseil a présenté les conclusions lors d'une réunion du groupe de travail ad hoc du Conseil sur l'échange d'informations le 22 juin 2010.

38 Décision 2008/615/JAI du Conseil, JO L 210 du 6.8.2008, p. 1; décision 2008/616/JAI du Conseil, JO L 210 du 6.8.2008, p. 12.

39 Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108), Conseil de l'Europe, 28.1.1981 (convention n° 108 du Conseil de l'Europe); protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel concernant les autorités de contrôle et les flux transfrontières de données (STE n° 181), Conseil de l'Europe, 8.11.2001 (protocole additionnel n° 181); recommandation n° R (87) 15 du Comité des ministres aux États membres visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, Conseil de l'Europe, 17.9.1987 (recommandation relative à la police).

demandes d'informations complémentaires seront d'ordinaire transmises au moyen de l'initiative suédoise. La décision de Prüm est en cours de mise en œuvre dans l'ensemble des 27 États membres, tandis que la Norvège et l'Islande sont sur le point d'y adhérer[40]. La Commission est tenue de présenter son rapport d'évaluation au Conseil en 2012.

À la suite des attentats à la bombe de Londres de juillet 2005, la Grande-Bretagne, l'Irlande, la Suède et la France ont proposé l'adoption d'un instrument de l'UE harmonisant les dispositions nationales applicables à la conservation de données. La **directive sur la conservation de données** de 2006 oblige les fournisseurs de services de téléphonie et d'accès à l'internet à conserver, à des fins de recherche, de détection et de poursuite d'infractions graves, les données de localisation et les données relatives au trafic des communications électroniques, ainsi que des renseignements sur les abonnés (y compris leur numéro de téléphone, leur adresse IP et l'identifiant de leur équipement mobile)[41]. La directive sur la conservation de données ne réglemente ni l'accès aux données conservées par les autorités nationales ni leur utilisation. Son champ d'application exclut explicitement le contenu des communications électroniques; en d'autres termes, elle ne permet pas la mise sur écoute. Cet instrument laisse aux États membres le soin de définir les «infractions graves». Les États membres peuvent aussi spécifier les autorités nationales qui peuvent accéder à ces données au cas par cas ainsi que les procédures permettant d'accorder l'accès à ces informations et les conditions de cet accès. Les durées de conservation de données varient de six à vingt-quatre mois. La directive 95/46/CE et la directive 2002/58/CE régissent la protection des données à caractère personnel au titre de cet instrument[42]. Six États membres n'ont pas encore totalement transposé cette mesure, et les Cours constitutionnelles allemande et roumaine ont déclaré inconstitutionnelle la législation nationale d'exécution adoptée par ces pays. La Cour constitutionnelle allemande a estimé que les dispositions régissant l'accès aux données ainsi que leur utilisation, telles que figurant dans la législation nationale, étaient anticonstitutionnelles[43]. La Cour constitutionnelle roumaine a jugé que la conservation de données était en soi contraire à l'article 8 de la convention de sauvegarde des droits de l'homme et des libertés fondamentales (convention européenne des droits de l'homme) et était donc anticonstitutionnelle[44]. La Commission procède actuellement à l'évaluation de cet instrument et doit présenter son rapport d'évaluation au Parlement européen et au Conseil à la fin 2010.

La mise en place, toujours en cours, d'un **système européen d'information sur les casiers judiciaires** (ECRIS), remonte à une initiative belge de 2004, dont l'objectif était de retirer aux délinquants sexuels ayant été condamnés le droit de travailler avec des enfants dans d'autres États membres. Par le passé, les États membres se fondaient sur la convention du Conseil de l'Europe d'entraide judiciaire en matière pénale afin d'échanger des informations relatives aux condamnations de leurs ressortissants, mais ce système s'est avéré inefficace[45]. Le Conseil a effectué un premier pas sur la voie de la réforme en adoptant la

---

40 À ce jour, dix États membres ont été autorisés à commencer à échanger de manière automatisée des profils ADN, cinq ont été autorisés à le faire pour les empreintes digitales et sept pour les données relatives à l'immatriculation des véhicules. L'Allemagne, l'Autriche, l'Espagne et les Pays-Bas ont fourni à la Commission des statistiques partielles sur l'utilisation qu'ils font de cet instrument.

41 Directive 2006/24/CE, JO L 105 du 13.4.2006, p. 54.

42 Directive 95/46/CE, JO L 281 du 23.11.1995, p. 31; directive 2002/58/CE, JO L 201 du 31.7.2002, p. 37 (directive vie privée et communications électroniques).

43 Arrêt de la Cour constitutionnelle allemande, Bundesverfassunggericht 1 BvR 256/08, 11.3.2008.

44 Arrêt n° 1258 de la Cour constitutionnelle roumaine, 8.10.2009.

45 Convention européenne d'entraide judiciaire en matière pénale (STE n° 3), Conseil de l'Europe, 20.4.1959. Voir aussi COM(2005) 10 du 25.1.2005.

décision 2005/876/JAI du Conseil, qui obligeait chaque État membre à mettre en place une autorité centrale qui transmettrait, à intervalles réguliers, aux autres États membres les condamnations prononcées à l'égard des ressortissants de ces autres États membres[46]. Cet instrument permettait aussi aux États membres d'obtenir, pour la première fois et sous réserve des dispositions législatives nationales, les condamnations prononcées antérieurement à l'encontre de leurs ressortissants dans d'autres États membres. Les États membres pouvaient demander ces informations en complétant un formulaire type plutôt qu'en recourant aux procédures d'entraide judiciaire. En 2006 et 2007, la Commission a présenté un ensemble complet de mesures législatives composé de trois instruments: la décision-cadre 2008/675/JAI du Conseil obligeant les États membres à prendre en compte les décisions de condamnation antérieures à l'occasion d'une nouvelle procédure pénale; la décision-cadre 2009/315/JAI du Conseil concernant l'organisation et le contenu des échanges d'informations extraites des casiers judiciaires; et la décision 2009/316/JAI du Conseil relative à la création de l'ECRIS comme moyen technique d'échanger des informations extraites des casiers judiciaires[47]. Devant être mises en œuvre au plus tard en avril 2012, les décisions-cadres 2009/315/JAI et 2009/316/JAI du Conseil visent à définir les procédures selon lesquelles un État membre prononçant une condamnation doit transmettre les informations relatives à une nouvelle condamnation à l'État membre ou aux États membres de nationalité de la personne condamnée, à préciser les obligations en matière de stockage et à arrêter un cadre pour un système informatisé d'échange d'informations. L'ECRIS sera un système d'information décentralisé permettant l'interconnexion des casiers judiciaires des États membres grâce au réseau s-TESTA de la Commission. Un ensemble d'autorités centrales échangeront des données relatives aux antécédents judiciaires et aux nouvelles condamnations des citoyens. Les données seront cryptées et structurées selon un format prédéfini, et comprendront les éléments suivants: éléments biographiques; condamnation, peine et infraction sous-jacente; et informations complémentaires (y compris les empreintes digitales, le cas échéant). À compter d'avril 2012, des extraits de casier judiciaire doivent être fournis pour les procédures pénales en cours et transmises aux autorités judiciaires ou administratives compétentes, telles que les instances habilitées à évaluer les personnes souhaitant occuper un poste sensible ou détenir une arme à feu. Les données à caractère personnel communiquées pour des procédures pénales ne peuvent être utilisées qu'à cette seule fin; leur utilisation à d'autres fins nécessite l'accord de l'État membre fournisseur. Le traitement de données à caractère personnel doit être conforme aux dispositions spécifiques de la décision-cadre 2009/315/JAI, qui intègre les dispositions de la décision 2005/876/JAI du Conseil, ainsi qu'à la décision-cadre 2009/977/JAI du Conseil et à la convention n° 108 du Conseil de l'Europe[48]. Le règlement (CE) n° 45/2001[49] s'applique à tout traitement de données à caractère personnel effectué par les institutions de l'UE au moyen de l'ECRIS, par exemple pour garantir la sécurité des données. Ce paquet législatif ne contient pas de dispositions relatives à la conservation des données, le stockage des informations relatives aux condamnations pénales étant régi par le droit national. Quinze États membres participent actuellement à un projet

---

46 Décision 2005/876/JAI du Conseil, JO L 322 du 9.12.2005, p. 33.

47 Décision-cadre 2008/675/JAI du Conseil, JO L 220 du 15.8.2008, p. 32; décision-cadre 2009/315/JAI du Conseil, JO L 93 du 7.4.2009, p. 23; décision 2009/316/JAI du Conseil, JO L 93 du 7.4.2009, p. 33. Voir aussi COM(2005) 10 du 25.1.2005.

48 Décision-cadre 2009/315/JAI du Conseil, JO L 93 du 7.4.2009, p. 23; décision 2005/876/JAI du Conseil, JO L 322 du 9.12.2005, p. 33; décision-cadre 2008/977/JAI du Conseil, JO L 350 du 30.12.2008, p. 60; convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108), Conseil de l'Europe, 28.1.1981 (convention n° 108 du Conseil de l'Europe).

49 Règlement (CE) n° 45/2001, JO L 8 du 12.1.2000, p. 1.

pilote et, parmi ceux-ci, neuf ont commencé à échanger électroniquement des informations extraites des casiers judiciaires. La Commission doit soumettre au Parlement européen et au Conseil deux rapports d'évaluation relatifs au fonctionnement de ce paquet législatif: la décision-cadre 2008/675/JAI doit être réexaminée en 2011; et la décision-cadre 2009/315/JAI doit l'être en 2015. À compter de 2016, la Commission doit aussi publier des rapports réguliers sur le fonctionnement de l'ECRIS.

À la suite d'une initiative finlandaise, le Conseil a adopté, en 2000, un instrument organisant l'échange d'informations entre les **cellules de renseignement financier** (CRF) des États membres aux fins de lutter contre le blanchiment de capitaux et, ultérieurement, le financement du terrorisme[50]. Les CRF sont en général créées au sein des services répressifs, des autorités judiciaires ou des instances administratives faisant rapport aux autorités financières. Elles sont tenues de partager avec leurs homologues de l'UE les données financières ou de nature répressive nécessaires, y compris les détails des transactions financières, sauf dans les cas où leur communication serait disproportionnée par rapport aux intérêts de personnes physiques ou morales. Les données communiquées aux fins de procéder à l'analyse d'informations ou à des enquêtes relatives au blanchiment de capitaux ou au financement du terrorisme peuvent également être utilisées pour des enquêtes ou poursuites en matière pénale, sauf si l'État membre fournisseur interdit leur utilisation à ces fins. Le traitement des données à caractère personnel doit se faire dans le respect des dispositions de la décision-cadre 2008/977/JAI du Conseil, de la convention n° 108 du Conseil de l'Europe et de sa recommandation relative à la police[51]. En 2002, plusieurs États membres ont créé FIU.net, une application de réseau décentralisée permettant l'échange de données entre cellules de renseignement financier et utilisant le réseau s-TESTA de la Commission[52]. Cette initiative rassemble vingt CRF qui ont le statut de membres. Des discussions sont en cours sur l'opportunité d'utiliser l'application sécurisée SIENA d'Europol pour faire fonctionner l'application FIU.net[53]. Après avoir évalué le respect par les États membres de cet instrument, le Conseil a, dans sa troisième directive sur le blanchiment de capitaux, donné compétence aux CRF pour recevoir, analyser et communiquer les déclarations relatives aux transactions suspectes concernant le blanchiment de capitaux *et* le financement du terrorisme[54]. Dans le cadre de son plan d'action pour les services financiers, la Commission réexamine depuis 2009 la mise en œuvre de la troisième directive sur le blanchiment de capitaux[55].

Souscrivant à une initiative proposée par l'Autriche, la Belgique et la Finlande, le Conseil a adopté, en 2007, un instrument dont l'objectif est d'accroître la coopération entre **bureaux de recouvrement des avoirs** (BRA) en matière de dépistage et d'identification des produits du

---

50 Décision 2000/642/JAI du Conseil, JO L 271 du 24.10.2000, p. 4.

51 Décision-cadre 2008/977/JAI du Conseil, JO L 350 du 30.12.2008, p. 60; convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108), Conseil de l'Europe, 28.1.1981 (convention n° 108 du Conseil de l'Europe); recommandation n° R (87) 15 du Comité des ministres aux États membres visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, Conseil de l'Europe, 17.9.1987 (recommandation relative à la police).

52 http://www.fiu.net/

53 SIENA signifie *Secure Information Exchange Network Application* (application de réseau d'échange sécurisé d'informations).

54 Directive 2005/60/CE, JO L 309 du 25.11.2005, p. 15 (troisième directive sur le blanchiment de capitaux).

55 Voir, par exemple, Évaluation de l'impact économique du plan d'action pour les services financiers — Rapport final (pour la Commission européenne, DG MARKT), CRA International, mars 2009.

crime[56]. Comme les CRF, les BRA coopèrent de manière décentralisée, mais sans l'aide d'une plateforme en ligne. Ils sont tenus de faire usage de l'initiative suédoise pour échanger des données, en précisant les informations relatives aux biens visés, comme les comptes bancaires, biens immobiliers et véhicules, et les informations relatives aux personnes physiques ou morales recherchées, comme les noms, adresses, date de naissance et renseignements relatifs aux actionnaires ou aux sociétés. L'utilisation des données échangées grâce à cet instrument est soumise au respect des législations nationales en matière de protection de données, tandis que les États membres ne sont pas autorisés à appliquer un traitement différencié aux données selon qu'elles soient d'origine nationale ou qu'elles proviennent d'autres États membres. Le traitement des données à caractère personnel doit respecter les dispositions de la convention n° 108 du Conseil de l'Europe, de son protocole additionnel n° 181 et de la recommandation relative à la police[57]. À ce jour, plus de vingt États membres ont mis en place des BRA. Compte tenu de la nature sensible des informations échangées, des discussions sont en cours sur l'opportunité d'utiliser l'application sécurisée SIENA d'Europol pour le partage de données entre BRA. Dans le cadre d'un projet pilote lancé en mai 2010, douze BRA ont commencé à utiliser SIENA pour échanger des données présentant un intérêt pour le dépistage d'avoirs. La Commission est tenue de présenter un rapport d'évaluation au Conseil en 2010.

En 2008, la présidence française du Conseil a invité les États membres à mettre en place, au niveau national, des **plateformes de signalement de la cybercriminalité**, et Europol à créer une plateforme européenne de signalement de la cybercriminalité, aux fins de la collecte, de l'échange et de l'analyse d'informations relatives à des infractions perpétrées sur l'internet[58]. Les citoyens peuvent signaler à leur plateforme nationale les cas de contenu ou de comportement illicites détectés sur l'internet. La «plateforme européenne de lutte contre la cybercriminalité» (ECCP pour *European Cybercrime Platform*), gérée par Europol, devrait servir de point central d'information, en analysant et en échangeant avec les services répressifs nationaux des informations liées à la cybercriminalité qui relèvent du mandat d'Europol[59]. À ce jour, presque tous les États membres ont mis en place des plateformes nationales de signalement de la cybercriminalité. Europol travaille actuellement à la mise en œuvre technique de l'ECCP et pourrait bientôt déployer son application SIENA pour accroître l'échange de données avec les plateformes nationales. Dans la mesure où cet échange d'informations implique le traitement de données à caractère personnel par Europol, les règles

---

56 Décision 2007/845/JAI du Conseil, JO L 332 du 18.12.2007, p. 103.

57 Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108), Conseil de l'Europe, 28.1.1981 (convention n° 108 du Conseil de l'Europe); protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel concernant les autorités de contrôle et les flux transfrontières de données (STE n° 181), Conseil de l'Europe, 8.11.2001 (protocole additionnel n° 181); recommandation n° R (87) 15 du Comité des ministres aux États membres visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, Conseil de l'Europe, 17.9.1987 (recommandation relative à la police).

58 Conclusions du Conseil relatives à l'établissement de plateformes nationales et d'une plateforme européenne de signalement des infractions relevées sur Internet, Conseil «Justice et affaires intérieures», 24.10.2008; Conclusions du Conseil concernant un plan d'action visant à mettre en œuvre la stratégie concertée de lutte contre la cybercriminalité, Conseil «Affaires générales», 26.4.2010. Europol a rebaptisé son projet la «plateforme européenne de lutte contre la cybercriminalité» (ECCP pour *European Cybercrime Platform*).

59 L'objectif d'Europol est de prévenir et de combattre la criminalité organisée, le terrorisme et les autres formes graves de criminalité affectant deux États membres ou plus. Voir la décision 2009/371/JAI du Conseil, JO L 121 du 15.5.2009, p. 37.

spécifiques en matière de protection des données figurant dans la décision portant création d'Europol (décision 2009/371/JAI du Conseil), ainsi que le règlement (CE) n° 45/2001, la convention n° 108 du Conseil de l'Europe, son protocole additionnel n° 181 et la recommandation relative à la police s'appliquent[60]. Les dispositions de la décision-cadre 2008/977/JAI du Conseil régissent l'échange de données à caractère personnel entre les États membres et Europol[61]. En l'absence d'instrument juridique, il n'existe aucun mécanisme de réexamen formel pour les plateformes de signalement de la cybercriminalité. Toutefois, Europol couvre déjà ce domaine important et, à l'avenir, rendra compte des activités de l'ECCP dans son rapport annuel présenté au Conseil pour approbation et au Parlement européen pour information.

Agences et organismes de l'UE mandatés pour aider les États membres à prévenir et à combattre les formes graves de criminalité transfrontalière

Créé en 1995, l'**Office européen de police** (Europol) a commencé ses activités en 1999 et est devenu une agence de l'UE en janvier 2010[62]. Son objectif est d'aider les États membres à prévenir et à combattre la criminalité organisée, le terrorisme et les autres formes graves de criminalité affectant deux États membres ou plus. Ses tâches principales consistent à collecter, stocker, traiter, analyser et échanger des informations et des renseignements, à faciliter les enquêtes, et à fournir aux États membres des renseignements et une aide à l'analyse. Les principaux organes de liaison entre Europol et les États membres sont les unités nationales Europol (UNE), qui détachent des officiers de liaison auprès d'Europol. Les chefs des UNE se réunissent périodiquement pour assister Europol sur des questions opérationnelles, tandis que le fonctionnement de l'agence est supervisé par son conseil d'administration et son directeur. Les outils de gestion de l'information utilisés par Europol sont le système d'information Europol (SIE), les fichiers de travail aux fins d'analyse (FTA) et l'application SIENA. Le SIE contient les données à caractère personnel, dont les identifiants biométriques, les condamnations pénales et les liens avec la criminalité organisée, des personnes soupçonnées d'avoir commis une infraction relevant du mandat d'Europol. L'accès est limité aux UNE, aux officiers de liaison, au personnel autorisé d'Europol et à son directeur. Les FTA, ouverts afin de faciliter les enquêtes pénales, comprennent des données relatives à des personnes ainsi que toute autre information que les UNE pourraient décider d'y joindre. Ces fichiers sont accessibles aux officiers de liaison, mais seuls les analystes d'Europol peuvent y saisir des données. Un système d'index permet aux UNE et aux officiers de liaison de vérifier si un FTA contient des informations présentant un intérêt pour leur État membre. L'application SIENA d'Europol est de plus en plus utilisée par les États membres pour partager des données sensibles à des fins répressives. Europol peut traiter des informations et des renseignements, y compris des données à caractère personnel, dans le cadre de ses activités; les États membres

---

60 Décision 2009/371/JAI du Conseil, JO L 121 du 15.5.2009, p. 37; règlement (CE) n° 45/2001, JO L 8 du 12.1.2000, p. 1; convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108), Conseil de l'Europe, 28.1.1981 (convention n° 108 du Conseil de l'Europe); protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel concernant les autorités de contrôle et les flux transfrontières de données (STE n° 181), Conseil de l'Europe, 8.11.2001 (protocole additionnel n° 181); recommandation n° R (87) 15 du Comité des ministres aux États membres visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, Conseil de l'Europe, 17.9.1987 (recommandation relative à la police).

61 Décision-cadre 2008/977/JAI du Conseil, JO L 350 du 30.12.2008, p. 60.

62 Décision 2009/371/JAI du Conseil, JO L 121 du 15.5.2009, p. 37, remplaçant la convention sur la base de l'article K.3 du traité sur l'Union européenne, portant création d'un Office européen de police, JO C 316 du 27.11.1995, p. 2.

ne peuvent utiliser les informations extraites des fichiers de données d'Europol que pour prévenir et combattre les formes graves de criminalité de nature transfrontalière. Toute restriction imposée par un État membre fournisseur à l'utilisation des informations fournies s'applique également aux autres utilisateurs qui extraient ces données des fichiers d'Europol. Europol peut également échanger des informations personnelles avec des pays tiers ayant conclu avec lui des accords de mise en œuvre et garantissant un niveau adéquat de protection des données. Il ne peut conserver des données que le temps nécessaire pour lui permettre de remplir ses fonctions. Les FTA peuvent être conservés pendant une durée de trois ans maximum, pouvant éventuellement être renouvelée une fois. Le traitement des données à caractère personnel par Europol doit être conforme aux règles spécifiques en matière de protection des données contenues dans l'acte régissant son fonctionnement (décision 2009/371/JAI du Conseil), ainsi qu'au règlement (CE) n° 45/2001, à la convention n° 108 du Conseil de l'Europe, à son protocole additionnel n° 181 et à la recommandation relative à la police[63]. Les dispositions de la décision-cadre 2008/977/JAI du Conseil s'appliquent aux échanges de données à caractère personnel entre les États membres et Europol[64]. Une autorité de contrôle commune, composée de membres des autorités de contrôle nationales, surveille les activités d'Europol liées au traitement des données à caractère personnel et à leur transmission à d'autres parties. Elle présente des rapports périodiques au Parlement européen et au Conseil. Europol transmet un rapport annuel sur ses activités au Conseil, pour approbation, et au Parlement européen, pour information.

Outre l'incidence qu'ils ont eue sur plusieurs des instruments décrits ci-dessus, les attentats terroristes du 11 septembre 2001 ont conduit à la création, en 2002, de l'**unité de coopération judiciaire de l'Union européenne** (Eurojust)[65]. Eurojust est un organe de l'UE dont l'objectif est d'améliorer la coordination des enquêtes et des poursuites dans les États membres et de renforcer la coopération entre les autorités nationales compétentes. Il couvre les mêmes formes de criminalité et infractions pénales qu'Europol. Dans le cadre de ce mandat et aux fins de l'exercice de leurs fonctions, les 27 membres nationaux d'Eurojust, qui composent son collège, ont accès aux données à caractère personnel concernant les suspects et auteurs d'infractions. Ces données comprennent, entre autres: les données biographiques, les coordonnées, les données d'immatriculation des véhicules, les profils ADN, les photographies, les empreintes digitales, ainsi que les données relatives au trafic, les données de localisation, et les données connexes nécessaires pour identifier l'abonné, transmises par les fournisseurs de services de télécommunication. Les États membres sont tenus de partager ces informations avec Eurojust afin de lui permettre d'accomplir sa mission. Toutes les données à caractère personnel liées à une affaire doivent être saisies dans le système automatisé de gestion des affaires, qui utilise le réseau s-TESTA de la Commission. Un système d'index enregistre les données à caractère personnel et non personnel présentant un intérêt pour les enquêtes en

---

63 Décision 2009/371/JAI du Conseil, JO L 121 du 15.5.2009, p. 37; règlement (CE) n° 45/2001, JO L 8 du 12.1.2000, p. 1; convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108), Conseil de l'Europe, 28 janvier 1981 (convention n° 108 du Conseil de l'Europe); protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel concernant les autorités de contrôle et les flux transfrontières de données (STE n° 181), Conseil de l'Europe, 8.11.2001 (protocole additionnel n° 181). Recommandation n° R (87) 15 du Comité des ministres aux États membres visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, Conseil de l'Europe, 17.9.1987 (recommandation relative à la police).

64 Décision-cadre 2008/977/JAI du Conseil, JO L 350 du 30.12.2008, p. 60.

65 Décision 2002/187/JAI du Conseil, JO L 63 du 6.3.2002, p. 1, modifiée par la décision 2009/426/JAI du Conseil, JO L 138 du 4.6.2009, p. 14. Voir également les conclusions de la session extraordinaire du Conseil «Justice et affaires intérieures» du 20.9.2001.

cours. Eurojust peut traiter des données à caractère personnel dans l'accomplissement de sa mission, mais ce traitement doit être conforme aux règles spécifiques contenues dans l'acte régissant son fonctionnement (décision 2009/426/JAI du Conseil), ainsi qu'à la convention n° 108 du Conseil de l'Europe, à son protocole additionnel n° 181 et à la recommandation relative à la police. Les dispositions de la décision-cadre 2008/977/JAI du Conseil s'appliquent aux échanges de données à caractère personnel entre les États membres et Eurojust[66]. Eurojust peut échanger des données avec des autorités nationales et des pays tiers avec lesquels il a conclu un accord, pour autant que le membre national ayant fourni les données ait accepté ce transfert et que le pays tiers assure un niveau adéquat de protection des données à caractère personnel. Les données à caractère personnel peuvent être conservées aussi longtemps que cela est nécessaire pour atteindre les objectifs d'Eurojust, mais doivent être supprimées dès qu'une affaire est classée. Les États membres doivent mettre en œuvre la base juridique modifiée d'Eurojust d'ici à juin 2011. Pour juin 2014 au plus tard, la Commission devra réexaminer l'échange d'informations entre les membres nationaux d'Eurojust et pourra proposer toute modification qu'elle jugera utile. D'ici à 2013, Eurojust fera rapport au Conseil et à la Commission sur l'ouverture au niveau national de l'accès à son système de gestion des affaires. Les États membres pourront revoir les droits d'accès nationaux sur cette base. Un organe de contrôle commun, composé de juges nommés par les États membres, surveille les activités d'Eurojust liées au traitement des données à caractère personnel et fait rapport annuellement au Conseil. Le président du collège présente au Conseil un rapport annuel sur les activités d'Eurojust, que le Conseil transmet au Parlement européen.

Accords internationaux visant à prévenir et à combattre le terrorisme et les autres formes graves de criminalité transnationale

À la suite des attentats terroristes du 11 septembre 2001, les États-Unis ont adopté une législation obligeant les compagnies aériennes assurant des vols à destination ou au départ des États-Unis, ou via ceux-ci, à fournir aux autorités américaines les **données relatives aux passagers aériens** (ou données PNR – *Passenger Name Records*) stockées dans leurs systèmes de réservation automatisés respectifs. Le Canada et l'Australie leur ont rapidement emboîté le pas. La législation de l'UE en la matière exigeant une évaluation préalable du niveau de protection des données assuré par les pays tiers, la Commission est intervenue à cet effet et a négocié des accords PNR avec ces pays[67]. Elle a signé un tel accord avec les États-Unis en juillet 2007 et avec l'Australie en juin 2008, ainsi qu'un accord API/PNR avec le Canada en octobre 2005[68]. Les accords conclus avec les États-Unis et l'Australie sont provisoirement applicables, tandis que l'accord avec le Canada reste en vigueur malgré l'expiration, en septembre 2009, de la décision de la Commission relative à l'adéquation du niveau de protection des données assuré par les normes canadiennes de protection des données[69]. Critique à l'égard du contenu des trois accords, le Parlement européen a invité la

---

66 Décision-cadre 2008/977/JAI du Conseil, JO L 350 du 30.12.2008, p. 60.

67 Directive 95/46/CE (directive relative à la protection des données), JO L 281 du 23.11.1995, p. 31.

68 Le paquet canadien comprend un engagement du Canada concernant le traitement des données API/PNR, la décision de la Commission relative à l'adéquation du niveau de protection assuré par les normes canadiennes de protection des données et un accord international (voir JO L 91 du 29.3.2006, p. 49; JO L 82 du 21.3.2006, p. 14). L'accord conclu avec les États-Unis a été publié au JO L 204 du 4.8.2007, p. 16, et celui conclu avec l'Australie, au JO L 213 du 8.8.2008, p. 47.

69 En 2009, le Canada s'est engagé, vis-à-vis de la Commission, de la présidence du Conseil et des États membres de l'UE, à continuer de respecter son engagement antérieur, de 2005, concernant l'utilisation des données PNR en provenance de l'UE. La décision de la Commission relative à l'adéquation du niveau de protection des données assuré par le Canada était fondée sur cet engagement antérieur.

Commission a les renégocier sur la base d'un ensemble de principes clairs[70]. Grâce à la transmission des données PNR bien avant le départ d'un vol, les services répressifs peuvent déceler plus aisément les liens pouvant exister entre certains passagers et le terrorisme ou d'autres formes graves de criminalité. Chacun de ces accords vise donc à prévenir et à combattre le terrorisme et les autres formes graves de criminalité transfrontalière. En contrepartie des données PNR provenant de l'UE, le ministère américain de la sécurité intérieure (DHS - *Department of Homeland Security*) partage les «indices» tirés de son analyse des données PNR avec les services répressifs de l'UE, Europol et Eurojust; et tant le Canada que les États-Unis se sont engagés, dans leurs accords respectifs, à coopérer avec l'UE aux fins de la mise en place d'un système PNR européen. Les accords avec les États-Unis et l'Australie portent sur 19 types de données, dont les informations biographiques, les informations relatives aux réservations et aux paiements, et les informations supplémentaires; l'accord canadien porte quant à lui sur 25 types de données similaires. Les informations supplémentaires comprennent, entre autres, les données relatives aux allers simples, aux passagers en «stand by» et aux passagers répertoriés comme «défaillants». L'accord avec les États-Unis autorise également, sous certaines conditions, l'utilisation d'informations sensibles. Le DHS peut traiter ces informations si la vie de l'intéressé ou d'autres personnes est en danger, mais doit les supprimer dans les 30 jours. Les données PNR sont envoyées à un ensemble d'unités centrales au sein du DHS, de l'Agence des services frontaliers du Canada et du service des douanes australien, qui ne peuvent les transférer qu'à d'autres services nationaux compétents en matière de répression ou de lutte antiterroriste. Dans l'accord américain, le DHS s'attend à ne pas devoir assurer, lors du traitement de données PNR en provenance de l'UE, une protection des données «plus stricte» que celle assurée par les autorités de l'UE dans leurs systèmes PNR nationaux. Dans le cas contraire, certaines parties de l'accord pourraient être suspendues. L'UE considère que le Canada et l'Australie assurent un niveau de protection «adéquat» pour les données PNR provenant de l'UE s'ils respectent les termes de leurs accords respectifs. Aux États-Unis, les données PNR provenant de l'UE sont conservées pendant sept ans dans une base de données active, et pendant huit années supplémentaires dans une base de données inactive. En Australie, elles sont stockées dans une base de données active pendant 3 ans et demi, puis dans une base de données inactive pendant deux ans. Dans ces deux pays, la base de données inactive n'est accessible que sur autorisation spéciale. Au Canada, les données sont conservées pendant 3 ans et demi, les informations étant rendues anonymes après 72 heures. Chaque accord prévoit des révisions périodiques, et les accords canadien et australien contiennent également une clause de dénonciation. Dans l'UE, seul le Royaume-Uni dispose d'un système PNR. La France, le Danemark, la Belgique, la Suède et les Pays-Bas ont adopté une législation ad hoc ou testent actuellement l'utilisation des données PNR en vue de la mise en place de leur propre système PNR. Plusieurs autres États membres envisagent de mettre en place un système PNR, et l'ensemble des États membres utilisent, au cas par cas, les données PNR à des fins répressives.

À la suite des attentats du 11 septembre 2001, le département du Trésor des États-Unis a élaboré un **programme de surveillance du financement du terrorisme** (TFTP - *Terrorist Finance Tracking Program*) afin d'identifier, de surveiller et de poursuivre les terroristes et leurs appuis financiers. Au titre du TFTP, le département du Trésor des États-Unis a obligé, par injonctions administratives, la filiale américaine d'une entreprise belge à lui transférer certaines données de messagerie financière transitant par son réseau. En janvier 2010, cette entreprise a modifié l'architecture de son réseau, ce qui a réduit de plus de moitié le volume des données relevant de la compétence des juridictions américaines qui font normalement

[70] Résolution P7_TA(2010)0144 du Parlement européen du 5.5.2010.

l'objet des injonctions ministérielles. En novembre 2009, la présidence du Conseil de l'Union européenne et le gouvernement des États-Unis ont signé un accord intermédiaire relatif au traitement et au transfert de l'UE vers les États-Unis de données de messagerie financière aux fins du TFTP, accord que le Parlement européen n'a pas approuvé[71]. Sur la base d'un nouveau mandat, la Commission européenne a négocié un nouveau projet d'accord avec les États-Unis et a présenté au Conseil, le 18 juin 2010, une proposition de décision du Conseil relative à la conclusion de l'accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données de messagerie financière de l'Union européenne aux États-Unis aux fins du programme de surveillance du financement du terrorisme (l'accord TFTP UE-États-Unis)[72]. Le Parlement européen a approuvé la conclusion de cet accord le 8 juillet 2010[73]. Le Conseil devrait à présent adopter une décision du Conseil relative à la conclusion de cet accord, après quoi l'accord entrera en vigueur par l'intermédiaire d'un échange de lettres entre les deux parties. L'accord TFTP UE-États-Unis a pour objet la prévention et la détection du terrorisme ou de son financement, ainsi que les enquêtes et les poursuites dans ce domaine. Il oblige les fournisseurs désignés de services de messagerie financière à transférer au Trésor américain, sur la base d'évaluations spécifiques des menaces géographiques et de demandes adaptées aux besoins, des séries de données de messagerie financière contenant, entre autres, le nom, le numéro de compte, l'adresse et le numéro d'identification du donneur d'ordre et du ou des bénéficiaires de certaines opérations. Le Trésor ne peut interroger ces données qu'aux fins du TFTP et seulement s'il a des raisons de croire à l'existence d'un lien entre une personne identifiée et le terrorisme ou son financement. L'extraction et le transfert de données relatives aux transactions effectuées à l'intérieur de l'espace unique de paiement en euros sont interdits. Les États-Unis fournissent aux États membres de l'UE, à Europol et à Eurojust tout «indice» relatif à l'existence de complots terroristes dans l'UE et aideront l'UE à mettre en place un système analogue au système TFTP. Si l'UE élaborait un tel programme, les deux parties pourraient revoir les termes de cet accord. Avant tout transfert de données, chaque demande d'informations émanant des États-Unis doit être vérifiée par Europol afin de s'assurer qu'elle respecte bien les conditions de l'accord. Les informations extraites des messages financiers ne peuvent être conservées plus longtemps que cela n'est nécessaire aux fins d'enquêtes ou de poursuites spécifiques; les données non extraites peuvent être conservées pendant 5 ans maximum. Si nécessaires aux fins de la prévention du terrorisme ou de son financement, ainsi que des enquêtes ou des poursuites en la matière, le Trésor américain peut transférer aux services répressifs, aux organismes chargés de la sécurité publique ou aux autorités chargées de la lutte contre le terrorisme aux États-Unis, aux États membres de l'UE, à Europol ou à Eurojust toutes les données à caractère personnel extraites des messages financiers. Il peut aussi partager avec des pays tiers tout indice relatif à des citoyens et des résidents de l'UE, sous réserve de l'autorisation de l'État membre concerné. Le respect par les parties de la limitation stricte de la finalité de l'accord à la lutte antiterroriste ainsi que des autres garanties prévues fait l'objet d'un contrôle par des superviseurs indépendants, dont une personne désignée par la Commission. L'accord a une durée de cinq ans et peut être dénoncé ou suspendu par chacune des parties. Une équipe de réexamen de l'UE, dirigée par la Commission et composée de représentants de deux autorités chargées de la protection des données et d'une personnalité issue du monde judiciaire, réexaminera l'accord six mois après son entrée en vigueur, et évaluera en particulier la mise en œuvre par les parties des dispositions relatives à la limitation des finalités et à la proportionnalité, ainsi que le respect des obligations qui leur incombent en matière de

[71] Résolution P7_TA(2010)0029 du Parlement européen du 11.2.2010.
[72] COM(2010) 316 final/2 du 18.6.2010.
[73] Résolution P7_TA-PROV(2010)0279 du Parlement européen du 8.7.2010.

protection des données. Le rapport de la Commission sera présenté au Parlement européen et au Conseil.

2.2. Initiatives au titre du plan d'action mettant en œuvre le programme de Stockholm

Propositions législatives devant être présentées par la Commission

Dans le programme de Stockholm, le Conseil européen a invité la Commission à soumettre trois propositions présentant un intérêt direct pour la présente communication: un système PNR européen aux fins de la prévention et de la détection du terrorisme et des formes graves de criminalité, ainsi que des poursuites en la matière; un système d'entrée/de sortie; et un programme d'enregistrement des voyageurs. Le Conseil européen a souligné que les deux dernières propositions devaient être présentées «le plus rapidement possible». La Commission a intégré chacune de ces trois demandes dans son plan d'action mettant en œuvre le programme de Stockholm[74]. Elle s'attachera dans l'immédiat à donner suite à ces demandes et, plus tard, à évaluer ces instruments sur la base des principes d'élaboration des politiques énoncés à la section 4.

En novembre 2007, la Commission a présenté une proposition de décision-cadre du Conseil relative à l'utilisation des données PNR à des fins répressives[75]. Cette initiative a reçu le soutien du Conseil et a ensuite été modifiée pour tenir compte des modifications proposées par le Parlement européen et des observations du contrôleur européen de la protection des données. Toutefois, elle est devenue caduque à l'entrée en vigueur du traité de Lisbonne. Comme elle l'a indiqué dans son plan d'action mettant en œuvre le programme de Stockholm, la Commission prépare actuellement, en vue d'une présentation début 2011, un **paquet PNR** composé: d'une communication relative à une stratégie PNR extérieure de l'UE énonçant les principes fondamentaux régissant la négociation d'accords avec les pays tiers; de directives de négociation pour la renégociation d'accords PNR avec les États-Unis et l'Australie; et de directives de négociation pour la conclusion d'un nouvel accord avec le Canada. La Commission élabore également une nouvelle proposition PNR de l'UE.

En 2008, la Commission a présenté plusieurs propositions visant à développer la gestion intégrée des frontières de l'UE en facilitant les déplacements des ressortissants de pays tiers tout en renforçant la sécurité intérieure[76]. La communication consacrée à cette question précisait que les personnes qui dépassent la durée de séjour autorisée constituaient la catégorie la plus nombreuse d'immigrés en séjour irrégulier dans l'UE, et proposait l'introduction éventuelle d'un **système d'entrée/de sortie** (SES) pour les ressortissants de pays tiers entrant dans l'UE pour de courts séjours de trois mois maximum. Ce système enregistrerait l'heure et le lieu d'entrée et la durée de séjour autorisée, et transmettrait des signalements automatiques aux autorités compétentes en cas de dépassement de la durée de séjour autorisée. Fondé sur la vérification des données biométriques, il exploiterait le même le système de correspondance biométrique et le même équipement opérationnel que ceux utilisés par le SIS II et le VIS. La Commission réalise actuellement une analyse d'impact et, comme indiqué dans le plan

---

74 Le programme de Stockholm – Une Europe ouverte et sûre qui sert et protège les citoyens, document 5731/10 du Conseil du 3.3.2010; COM(2010) 171 du 20.4.2010 (plan d'action mettant en œuvre le programme de Stockholm).

75 COM(2007) 654 du 6.11.2007.

76 COM(2008) 69 du 13.2.2008.

d'action mettant en œuvre le programme de Stockholm, s'appliquera à présenter une proposition législative en 2011.

L'établissement d'un **programme d'enregistrement des voyageurs** (PEV) constituait la troisième proposition à examiner[77]. Ce programme permettrait de simplifier les contrôles aux frontières pour certaines catégories de voyageurs réguliers en provenance de pays tiers qui pourraient, après avoir fait l'objet d'une procédure adéquate d'examen préalable, entrer dans l'UE en franchissant des barrières automatiques. Le PEV prévoirait également une vérification d'identité sur la base des données biométriques et permettrait d'abandonner progressivement l'approche actuelle du contrôle général aux frontières au profit d'une nouvelle approche fondée sur le risque individuel. La Commission a effectué une analyse d'impact et, conformément au plan d'action mettant en œuvre le programme de Stockholm, prévoit de présenter une proposition législative en 2011.

Initiatives devant être examinées par la Commission

Dans le programme de Stockholm, le Conseil européen a invité la Commission à examiner trois initiatives présentant un intérêt pour la présente communication et portant sur: les moyens permettant de pister le financement du terrorisme au sein de l'UE; la possibilité et l'utilité de développer un système européen d'autorisation de voyage; et la nécessité et la valeur ajoutée de la mise en place d'un système européen d'information sur les registres de la police. La Commission a également intégré ces initiatives dans son plan d'action mettant en œuvre le programme de Stockholm. Elle doit à présent en apprécier la faisabilité et l'opportunité et déterminer, le cas échéant, la manière de les mettre en œuvre sur la base des principes d'élaboration des politiques énoncés à la section 4.

L'accord TFTP UE-États-Unis invite la Commission européenne à réaliser une étude sur l'opportunité de mettre en place un **système européen de surveillance du financement du terrorisme** équivalent au TFTP américain et permettant un transfert «plus ciblé» de données entre l'UE et les États-Unis. Le projet de décision de Conseil relative à la conclusion de cet accord invite également la Commission à présenter au Parlement européen et au Conseil, au plus tard un an après l'entrée en vigueur de l'accord TFTP UE-États-Unis, un cadre juridique et technique pour l'extraction de données sur le territoire de l'UE[78]. Dans les trois ans à compter de l'entrée en vigueur de cet accord, la Commission présentera un état d'avancement de l'élaboration d'un tel système équivalent propre à l'UE. Si ce système n'est pas mis en place dans les cinq ans à compter de l'entrée en vigueur de l'accord, l'UE peut décider de dénoncer l'accord. De plus, en vertu de l'accord TFTP UE-États-Unis, les États-Unis s'engagent à coopérer avec l'UE et à lui fournir conseils et assistance dans le cas où elle déciderait de mettre en place un tel système. Sans préjudice de la décision qui sera finalement prise, la Commission a commencé à étudier les conséquences d'une telle initiative pour la protection des données et les ressources, ainsi que sur le plan pratique. Comme indiqué dans le plan d'action mettant en œuvre le programme de Stockholm, la Commission présentera, en 2011, une communication sur la faisabilité de la création d'un programme européen de surveillance du financement du terrorisme (TFTP de l'UE).

---

77 COM(2008) 69 du 13.2.2008.

78 Document 11222/1/10 REV 1 du Conseil du 24.6.2010; document 11222/1/10 REV 1 COR 1 du Conseil du 24.6.2010.

Dans sa communication de 2008 sur la gestion intégrée des frontières, la Commission a proposé la création éventuelle d'un **système électronique d'autorisation de voyage** (ESTA) pour les ressortissants de pays tiers exemptés de l'obligation de visa[79]. Au titre de ce programme, les ressortissants de pays tiers éligibles seraient invités, avant leur départ, à s'inscrire par voie électronique en fournissant leurs informations biographiques, les données figurant sur leur passeport et les informations relatives à leur voyage. Par rapport à la procédure de demande de visa, l'ESTA offrirait un moyen plus rapide et plus simple de vérifier si une personne remplit les conditions d'entrée nécessaires. La Commission étudie actuellement les avantages, les inconvénients et les conséquences pratiques qu'entraînerait la mise en place de l'ESTA. Comme indiqué dans le plan d'action mettant en œuvre le programme de Stockholm, elle vise à présenter, en 2011, une communication sur la faisabilité de l'élaboration d'un tel programme.

Durant sa présidence du Conseil en 2007, l'Allemagne a lancé une discussion sur la possibilité de mettre en place un **système européen d'information sur les registres de la police** (EPRIS)[80]. L'EPRIS aiderait les agents des services répressifs à trouver des informations dans toute l'UE, notamment en ce qui concerne les relations entre les personnes soupçonnées de participer à la criminalité organisée. En 2010, la Commission présentera au Conseil un projet de cahier des charges pour son étude de faisabilité relative à l'EPRIS. Comme indiqué dans le plan d'action mettant en œuvre le programme de Stockholm, elle s'attachera à présenter, en 2012, une communication sur la faisabilité de la mise en place d'un tel système.

3. ANALYSE DES INSTRUMENTS ACTUELLEMENT UTILISÉS OU EN COURS DE MISE EN ŒUVRE OU D'EXAMEN

À la lumière de la présentation générale ci-dessus, les observations préliminaires suivantes peuvent être formulées.

Structure décentralisée

Parmi les divers instruments actuellement utilisés ou en cours de mise en œuvre ou d'examen, seuls six prévoient la collecte ou le stockage de données à caractère personnel au niveau de l'UE, à savoir le SIS (et le SIS II), le VIS, EURODAC, le SID, Europol et Eurojust. Toutes les autres mesures régissent l'échange décentralisé et transfrontalier d'informations personnelles collectées au niveau national par les pouvoirs publics ou des entreprises privées ainsi que leur transfert vers des pays tiers. La majorité des données à caractère personnel sont collectées et stockées au niveau national; l'UE cherche à apporter une valeur ajoutée en permettant, sous certaines conditions, l'échange de ces informations avec des partenaires de l'UE et des pays tiers. La Commission a récemment présenté au Parlement européen et au Conseil une proposition modifiée relative à la création d'une agence pour la gestion opérationnelle des systèmes d'information à grande échelle dans le domaine de la liberté, de la sécurité et de la justice[81]. La future agence IT aura pour mission d'assurer la gestion opérationnelle du SIS II, du VIS et d'EURODAC, ainsi que de tout autre futur système informatique dans le domaine de la liberté, de la sécurité et de la justice, de manière à ce que ces systèmes fonctionnent en permanence, en garantissant ainsi la continuité du flux d'information.

---

79 COM(2008) 69 du 13.2.2008.

80 Voir document 15526/1/09 du Conseil du 2.12.2009.

81 COM(2010) 93 du 19.3.2010.

Finalité limitée

La plupart des instruments analysés ci-dessus poursuivent chacun un objectif spécifique: EURODAC vise à améliorer le fonctionnement du système de Dublin; le système API, à améliorer les contrôles aux frontières; l'initiative suédoise, à renforcer les enquêtes pénales et les opérations de renseignement; la convention Naples II, à contribuer à la prévention et à la détection de la fraude douanière, ainsi qu'aux poursuites et à la répression en la matière; le SID, à contribuer à la prévention des infractions graves aux lois nationales, ainsi qu'aux enquêtes et aux poursuites en la matière, en renforçant l'efficacité de la coopération entre les administrations douanières nationales; l'ECRIS, les CRF et les BRA, à rationaliser le partage transfrontalier de données dans des domaines particuliers; et la décision de Prüm, la directive sur la conservation des données, le TFTP et le système PNR, à lutter contre le terrorisme et les formes graves de criminalité. Le SIS, le SIS II et le VIS semblent être les seules exceptions à cette règle: l'objectif initial du VIS était de faciliter les échanges transfrontaliers de données sur les visas, mais il a ensuite été étendu à la prévention du terrorisme et des formes graves de criminalité et à la lutte contre ces phénomènes. Le SIS et le SIS II visent à assurer un niveau élevé de sécurité dans le domaine de la liberté, de la sécurité et de la justice, ainsi qu'à faciliter la circulation des personnes au moyen des informations qu'ils permettent de transmettre. Exception faite de ces systèmes d'information centralisés, la limitation des finalités semble constituer un critère essentiel dans la conception des mesures de gestion de l'information au niveau de l'UE.

Chevauchements potentiels entre les fonctions des différents instruments

Les mêmes informations personnelles peuvent être collectées au moyen de différents instruments, mais ces informations ne peuvent être utilisées que pour une finalité limitée au titre d'un instrument particulier (à l'exception du VIS, du SIS et du SIS II). Par exemple, les données biographiques d'une personne, y compris son nom, sa date et son lieu de naissance et sa nationalité, peuvent être traitées dans le cadre du SIS, du SIS II, du VIS, du système API, du SID, de l'initiative suédoise, de la décision de Prüm, de l'ECRIS, des CRF, des BRA, d'Europol, d'Eurojust et des accords PNR et TFTP. En revanche, ces données peuvent uniquement être traitées aux fins du contrôle aux frontières dans le cas du système API; de la prévention de la fraude douanière et des enquêtes et poursuites en la matière dans le cas du SID; des enquêtes pénales et des opérations de renseignement dans le cas de l'initiative suédoise; de la prévention du terrorisme et de la criminalité transfrontalière dans le cas de la décision de Prüm; de l'examen du casier judiciaire d'une personne dans le cas de l'ECRIS; des enquêtes sur les liens qu'entretient une personne avec la criminalité organisée et les réseaux terroristes dans le cas des CRF; du dépistage d'avoirs dans le cas des BRA; des enquêtes et des poursuites relatives aux formes graves de criminalité transfrontalière dans le cas d'Europol et d'Eurojust; de la prévention du terrorisme et des autres formes graves de criminalité transfrontalière et de la lutte contre ces phénomènes dans le cas des systèmes PNR; et de l'identification et de la poursuite des terroristes et de leurs appuis financiers dans le cas du TFTP. Les données biométriques, telles que les empreintes digitales et les photographies, peuvent être traitées dans le cadre du SIS II, du VIS, d'EURODAC, de l'initiative suédoise, de la décision de Prüm, de l'ECRIS, d'Europol et d'Eurojust – également en fonction de leurs finalités respectives. La décision de Prüm est l'unique instrument permettant l'échange transfrontalier de profils ADN anonymes (bien que ce type de données puisse également être transmis à Europol et à Eurojust). D'autres mesures prévoient le traitement d'informations personnelles hautement spécialisées présentant un intérêt pour la réalisation de leur objectif unique: les systèmes PNR traitent les informations relatives aux réservations d'avion des passagers; le FIDE, les données présentant un intérêt pour les enquêtes en matière de fraude

douanière; la directive sur la conservation des données, les adresses IP et les identifiants des équipements mobiles; l'ECRIS, les casiers judiciaires; les BRA, les avoirs privés et les informations relatives aux sociétés; les plateformes de lutte contre la cybercriminalité, les infractions sur l'internet; Europol, les liens avec les filières criminelles; et le TFTP, les données de messagerie financière. Seul l'échange transfrontalier d'informations et de renseignements aux fins des enquêtes pénales présente d'importants chevauchements entre les fonctions des différents instruments. Du point de vue juridique, l'initiative suédoise serait suffisante pour échanger *tout* type d'informations présentant un intérêt pour ces enquêtes (pour autant que l'échange de ces données à caractère personnel soit autorisé par le droit national). Toutefois, sous l'angle opérationnel, la décision de Prüm pourrait se révéler préférable pour le partage de profils ADN et d'empreintes digitales, son système de concordance/non-concordance (*hit/no hit*) garantissant des réponses instantanées, et sa méthode de partage automatisé des données offrant un niveau élevé de sécurité des données[82]. De même, il pourrait s'avérer plus efficace pour les CRF, les BRA et les plateformes de lutte contre la cybercriminalité de traiter directement avec leurs homologues de l'UE, sans avoir à remplir les formulaires requis par l'initiative suédoise pour toute demande d'information.

Droits d'accès contrôlés

Les droits d'accès aux instruments créés dans la logique de la lutte contre le terrorisme et les formes graves de criminalité ne sont généralement accordés qu'à une partie restreinte des services répressifs, c'est-à-dire aux services de police, aux autorités de contrôle aux frontières et aux autorités douanières. Les droits d'accès aux mesures répondant à la logique «Schengen» sont en principe octroyés aux services de l'immigration et, sous certaines conditions, aux services de police, aux autorités de contrôle aux frontières et aux autorités douanières. Le flux d'information est contrôlé par les interfaces nationales dans le cas du SIS et du VIS centralisés et par les points de contact nationaux ou les unités centrales de coordination dans le cas des instruments décentralisés, tels que la décision de Prüm, l'initiative suédoise, la convention Naples II, l'ECRIS, le TFTP, les accords PNR, les CRF, les BRA et les plateformes de lutte contre la cybercriminalité.

Disparité des règles en matière de conservation des données

Les durées de conservation des données varient fortement en fonction des objectifs des divers instruments. L'accord PNR avec les États-Unis prévoit la plus longue durée de conservation, soit 15 ans, tandis que le système API prévoit la plus courte, à savoir 24 heures. Les accords PNR établissent une distinction intéressante entre les données utilisées activement et celles qui sont utilisées passivement: après un certain temps, les informations doivent être archivées et ne peuvent être «déverrouillées» que sur autorisation spéciale. L'utilisation que fait le Canada des données PNR provenant de l'UE illustre bien cette approche: les informations doivent être rendues anonymes après 72 heures, mais restent disponibles pour les agents autorisés pendant 3 ans et demi.

---

82 La décision de Prüm (décision 2008/615/JAI du Conseil, JO L 210 du 6.8.2008, p. 1) est assortie d'une décision d'application (décision 2008/616/JAI du Conseil, JO L 210 du 6.8.2008, p. 12) visant à garantir l'utilisation de mesures répondant aux techniques les plus récentes pour assurer la protection et la sécurité des données, ainsi que des procédures d'encryptage et d'autorisation pour l'accès aux données, et comprend des règles spécifiques régissant l'admissibilité des consultations.

Gestion efficace de l'identité

Plusieurs mesures analysées ci-dessus, dont le futur SIS II et le VIS, visent à permettre la vérification de l'identité au moyen des données biométriques. La mise en place du SIS II devrait renforcer la sécurité dans le domaine de la liberté, de la sécurité et de la justice, notamment en contribuant, par exemple, à identifier les personnes faisant l'objet d'un mandat d'arrêt européen, celles auxquelles l'entrée dans l'espace Schengen doit être refusée et celles qui sont recherchées pour d'autres motifs spécifiques liés à des enquêtes en cours (telles que des personnes disparues ou des témoins dans le cadre d'affaires judiciaires), indépendamment de la disponibilité ou de l'authenticité des documents d'identification. La mise en œuvre du VIS devrait faciliter la procédure de délivrance des visas ainsi que la gestion des visas.

Des solutions européennes pour garantir la sécurité des données

Pour les échanges d'informations sensibles par-delà les frontières de l'Union, les États membres privilégient les solutions européennes. Plusieurs instruments de tailles, de structures et de finalités différentes exploitent, pour le partage d'informations sensibles, le réseau de communication de données s-TESTA, financé par la Commission. Il s'agit notamment des systèmes d'information centralisés SIS II, VIS, et EURODAC, des instruments décentralisés que constituent la décision de Prüm, l'ECRIS et les CRF, ainsi que d'Europol et d'Eurojust. Le SID et le FIDE utilisent le réseau commun de communication, l'interface commune des systèmes ou l'accès internet sécurisé que fournit la Commission. Entre-temps, SIENA, l'application de réseau d'échange d'informations d'Europol semble être devenue l'application de prédilection pour plusieurs initiatives récentes fondées sur le transfert sécurisé de données: des discussions sont en cours sur l'opportunité de faire fonctionner le réseau FIU.net, les BRA et les plateformes de lutte contre la cybercriminalité sur la base de cette application.

Disparité des mécanismes de réexamen

Les instruments analysés ci-dessus prévoient une série de mécanismes de réexamen différents. Dans le cas de systèmes d'information complexes tels que le SIS II, le VIS et EURODAC, la Commission doit présenter au Parlement européen et au Conseil des rapports annuels et semestriels sur le fonctionnement de ces systèmes ou leur degré de mise en œuvre. En ce qui concerne les instruments d'échange d'informations décentralisés, la Commission est tenue de soumettre aux autres institutions un rapport d'évaluation unique quelques années après la mise en œuvre: la directive sur la conservation des données, l'initiative suédoise et les mesures BRA doivent être évaluées en 2010; la décision de Prüm en 2012; et l'ECRIS en 2016. Les trois accords PNR prévoient des réexamens périodiques et ad hoc, et deux d'entre eux comprennent également des clauses de caducité. Europol et Eurojust présentent des rapports annuels au Conseil, qui les transmet pour information au Parlement européen. Ces considérations portent à croire que 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.

4. PRINCIPES D'ÉLABORATION DES POLITIQUES

La section 2 décrit plusieurs initiatives que la Commission européenne a mises en œuvre, présentées ou envisagées au cours de ces dernières années. En raison du foisonnement d'idées nouvelles et d'une législation de plus en plus abondante dans le domaine de la sécurité intérieure et de la gestion des flux migratoires, il convient de définir un socle de principes appelé à guider le lancement et l'évaluation des propositions d'actions au cours des prochaines années. Ces principes se fondent sur les principes généraux, qu'ils sont destinés à compléter, consacrés par les traités de l'UE, la jurisprudence de la Cour européenne de justice et de la Cour européenne des droits de l'homme, et les accords interinstitutionnels pertinents conclus entre le Parlement européen, le Conseil et la Commission européenne. La Commission propose d'élaborer et de mettre en œuvre de nouvelles initiatives et d'évaluer les instruments existants sur la base des deux catégories de principes suivants:

Principes matériels

Protéger les droits fondamentaux, notamment le droit au respect de la vie privée et à la protection des données

La protection des droits fondamentaux des personnes telle que prévue par la charte des droits fondamentaux de l'Union européenne, et en particulier le droit au respect de la vie privée et à la protection des données à caractère personnel, constituera une priorité pour la Commission lors de l'élaboration de nouvelles propositions impliquant le traitement de données à caractère personnel dans le domaine de la sécurité intérieure et de la gestion des flux migratoires. Les articles 7 et 8 de la charte consacrent le droit de toute personne «au respect de sa vie privée et familiale» et «à la protection des données à caractère personnel la concernant»[83]. L'article 16 du traité sur le fonctionnement de l'Union européenne (TFUE), qui revêt un caractère contraignant pour les activités des États membres et des institutions, agences, organes et organismes de l'Union, réaffirme le droit de toute personne «à la protection des données à caractère personnel la concernant»[84]. Lorsqu'elle élaborera de nouveaux instruments reposant sur l'utilisation des technologies de l'information, la Commission s'attachera à suivre une approche fondée sur la prise en compte du respect de la vie privée dès la conception («*privacy by design*»). Pour ce faire, elle intégrera la protection des données à caractère personnel dans la base technologique des instruments proposés, en limitant le traitement des données au strict nécessaire compte tenu de la finalité envisagée et en n'accordant l'accès aux données qu'aux entités ayant «besoin d'en connaître»[85].

Nécessité

L'ingérence d'une autorité publique dans l'exercice par les personnes de leur droit au respect de leur vie privée peut être nécessaire dans l'intérêt de la sécurité nationale, de la sûreté publique ou de la prévention de la criminalité[86]. La jurisprudence de la Cour européenne des droits de l'homme établit trois conditions auxquelles ces restrictions peuvent être justifiées: si

---

83 Charte des droits fondamentaux de l'Union européenne, JO C 83 du 30.3.2010, p. 389.

84 Versions consolidées du traité sur l'Union européenne et du traité sur le fonctionnement de l'Union européenne, JO C 83 du 30.3.2010, p. 1.

85 Pour une description complète du principe de «*privacy by design*», voir l'avis du contrôleur européen de la protection des données du 18.3.2010 sur la promotion de la confiance dans la société de l'information grâce au renforcement de la protection des données et de la vie privée (*Opinion of 18 March 2010 on promoting trust in the Information Society by fostering data protection and privacy* – disponible uniquement en anglais).

86 Voir l'article 8 de la convention de sauvegarde des droits de l'homme et des libertés fondamentales (STCE n° 5), Conseil de l'Europe, 4.11.1950.

elles sont prévues par la loi, si elles poursuivent un but légitime et si elles sont nécessaires dans une société démocratique. L'ingérence dans le droit au respect de la vie privée est considérée comme nécessaire si elle répond à un besoin social impérieux, si elle est proportionnée au but poursuivi et si les motifs invoqués par les autorités publiques pour la justifier apparaissent pertinents et suffisants[87]. Dans toutes ses futures propositions, la Commission évaluera l'incidence attendue de l'initiative en question sur le droit des personnes au respect de la vie privée et à la protection des données à caractère personnel et précisera en quoi cette incidence est nécessaire et en quoi la solution proposée est proportionnée au but légitime que constituent le maintien de la sécurité intérieure dans l'Union européenne, la prévention de la criminalité ou la gestion des flux migratoires. Le respect des règles relatives à la protection des données à caractère personnel fera dans tous les cas l'objet d'un contrôle par une autorité indépendante au niveau national ou de l'UE.

Subsidiarité

La Commission s'attachera à justifier ses nouvelles propositions au regard des principes de subsidiarité et de proportionnalité, conformément à l'article 5 du protocole (n° 2) annexé au traité sur l'Union européenne. Toute nouvelle proposition législative comprendra une fiche contenant des éléments permettant d'apprécier le respect du principe de subsidiarité, tel qu'énoncé à l'article 5 du traité sur l'Union européenne. Cette fiche comportera des éléments permettant d'évaluer l'impact financier et socio-économique de la proposition et, lorsqu'il s'agira d'une directive, ses implications sur la réglementation à mettre en œuvre par les États membres[88]. Les raisons permettant de conclure qu'un objectif de l'UE peut être mieux atteint au niveau de l'UE s'appuieront sur des indicateurs qualitatifs. Les propositions législatives devront veiller à ce que toute charge incombant à l'UE, aux gouvernements nationaux, aux autorités régionales, aux opérateurs économiques et aux citoyens soit réduite au minimum et proportionnée à l'objectif à atteindre. Dans le cas de propositions visant la conclusion de nouveaux accords internationaux, cette fiche mentionnera les effets escomptés de la proposition sur les relations avec les pays tiers concernés.

Gestion rigoureuse des risques

Les échanges d'informations dans le domaine de la liberté, de la sécurité et de la justice visent généralement à analyser les menaces qui pèsent sur la sécurité, à mettre en évidence des tendances dans les activités criminelles ou à évaluer les risques liés à certains domaines d'action[89]. Les risques sont souvent, mais pas nécessairement, liés à des personnes dont le comportement passé ou le mode comportemental indique la persistance d'un risque à l'avenir. Toutefois, les risques doivent être évalués sur la base de preuves et non d'hypothèses. Il est essentiel pour toute mesure de gestion de l'information de prévoir une vérification de la nécessité et de respecter le principe de limitation des finalités. L'élaboration de profils de risque – à ne pas confondre avec les profils raciaux ou autre profils discriminatoires, qui ne sont pas compatibles avec les droits fondamentaux – présente un intérêt certain. En effet, ces

---

87 Voir l'arrêt de la Cour européenne des droits de l'homme (Strasbourg) du 4.12.2008 dans l'affaire Marper contre Royaume-Uni.

88 Les principes de base des analyses d'impact sont énoncés dans les lignes directrices de la Commission européenne concernant l'analyse d'impact (SEC(2009) 92 du 15.1.2009).

89 Entre autres exemples pratiques de gestion efficace des risques, citons le fait d'empêcher une personne expulsée après avoir commis une infraction pénale grave dans un État membre de rentrer dans l'espace Schengen via un autre État membre (SIS), ou encore le fait d'empêcher une personne de demander l'asile dans plusieurs États membres (EURODAC).

profils peuvent contribuer à concentrer les ressources sur certaines personnes aux fins du recensement des menaces pour la sécurité et de la protection des victimes de la criminalité.

Principes axés sur les processus[90]

Un bon rapport coût-efficacité

Des services publics fondés sur les technologies de l'information devraient permettre d'offrir aux contribuables de meilleurs services et un meilleur rapport qualité-prix. Compte tenu de la situation économique actuelle, toutes les nouvelles propositions, et en particulier celles qui porteront sur la création ou la mise à niveau de systèmes d'information, devront présenter le rapport coût-efficacité le plus intéressant possible. Cette approche se fondera sur les solutions préexistantes afin de réduire les chevauchements au minimum et de maximiser les synergies éventuelles. La Commission établira si un meilleur usage des instruments existants permettrait d'atteindre les objectifs des propositions. Elle envisagera également, avant de proposer la création de nouveaux systèmes, de doter les systèmes d'information existants de fonctions auxiliaires supplémentaires.

Élaborer les politiques en partant de la base

Il est essentiel que les contributions de toutes les parties prenantes, dont celles des autorités nationales responsables de la mise en œuvre, des acteurs économiques et de la société civile, soient prises en considération le plus tôt possible dans le cadre des nouvelles initiatives. L'élaboration de politiques qui tiennent compte des intérêts des utilisateurs finals requiert que soient menées une réflexion horizontale et une large consultation[91]. C'est pourquoi la Commission s'attachera à nouer des liens permanents avec les fonctionnaires et praticiens nationaux par l'intermédiaire des structures du Conseil, de comités de gestion et de formations ad hoc.

Une répartition claire des responsabilités

Compte tenu de la complexité technique des projets de collecte et d'échange d'informations dans le domaine de la liberté, de la sécurité et de la justice, une attention particulière doit être accordée à la conception initiale des structures de gouvernance. L'expérience du projet SIS II a démontré que si des objectifs, rôles et responsabilités globaux clairs et stables ne sont pas définis d'entrée de jeu, des dépassements de budget considérables et d'importants retards dans la mise en œuvre peuvent survenir. Selon une première évaluation de la mise en œuvre de la décision de Prüm, une structure de gouvernance décentralisée ne serait pas non plus la panacée, les États membres n'ayant aucun «chef de projet» vers qui se tourner pour obtenir des conseils concernant les aspects financiers ou techniques de la mise en œuvre. Peut-être la future agence IT pourrait-elle prodiguer ce genre de conseils techniques aux responsables des systèmes d'information dans le domaine de la liberté, de la sécurité et de la justice. Elle pourrait également offrir une plateforme en vue d'une large participation des parties prenantes à la gestion opérationnelle et au développement des systèmes informatiques. Afin d'éviter autant que possible les dépassements de budget et les retards dus à une modification des exigences, tout nouveau système d'information dans le domaine de la liberté, de la sécurité et

---

90 Ces principes s'inspirent des conclusions du Conseil concernant une stratégie de gestion de l'information pour la sécurité intérieure de l'UE, Conseil «Justice et affaires intérieures», 30.11.2009.

91 Les principes généraux et les normes minimales de consultation publique sont définis dans le document COM(2002) 704 du 11.12.2002.

de la justice, en particulier s'il s'agit d'un système informatique à grande échelle, ne sera pas développé avant que les instruments juridiques de base définissant son objet, sa portée, ses fonctions et ses caractéristiques techniques aient été définitivement adoptés.

Clauses de réexamen et de caducité

La Commission évaluera chaque instrument décrit dans la présente communication. Cette évaluation portera sur l'ensemble des instruments qui existent dans le domaine de la gestion de l'information, et devrait permettre de se faire une idée précise de la manière dont les différents instruments s'insèrent dans le cadre plus large de la sécurité intérieure et de la gestion des flux migratoires. Les propositions qui seront présentées à l'avenir prévoiront, le cas échéant, des rapports annuels obligatoires, des réexamens périodiques et ad hoc, ainsi qu'une clause de caducité. Les instruments existants ne seront maintenus que s'ils continuent à servir l'objectif légitime pour lequel ils ont été conçus. L'annexe II fixe la date et le mécanisme de réexamen pour chaque instrument faisant l'objet de la présente communication.

5. PERSPECTIVES D'AVENIR

La présente communication présente, pour la première fois, un panorama clair et complet des mesures en place, en cours de mise en œuvre ou d'examen qui régissent, au niveau de l'UE, la collecte, le stockage ou l'échange transfrontalier d'informations à caractère personnel à des fins répressives ou de gestion des flux migratoires.

Elle explique aux citoyens quels types d'informations sont collectés, stockés ou échangés à leur sujet, et à quelles fins et par qui ces opérations sont effectuées. Il s'agit d'un outil de référence transparent pour les parties prenantes qui souhaitent réfléchir à la direction que doit prendre la politique de l'UE dans ce domaine à l'avenir. Parallèlement, elle fournit une première réponse à la demande du Conseil européen, qui a invité la Commission européenne à élaborer des instruments de gestion de l'information au niveau de l'UE conformément à la stratégie de gestion de l'information de l'UE[92] et à étudier la nécessité d'un modèle européen d'échange d'informations[93].

La Commission a l'intention de donner suite à la présente communication en présentant une communication sur le modèle européen d'échange d'informations en 2012[94]. À cette fin, la Commission a lancé, en janvier 2010, un exercice de «cartographie de l'information» en se fondant sur les bases juridiques et le fonctionnement pratique des échanges entre États membres de renseignements et d'informations en matière pénale, exercice dont elle rendra compte au Conseil et au Parlement européen en 2011[95].

---

92 Conclusions du Conseil concernant une stratégie de gestion de l'information pour la sécurité intérieure de l'UE, Conseil «Justice et affaires intérieures», 30.11.2009 (stratégie de gestion de l'information de l'UE).

93 Le programme de Stockholm – Une Europe ouverte et sûre qui sert et protège les citoyens, document 5731/10 du Conseil du 3.3.2010, section 4.2.2.

94 Comme le précise le plan d'action de la Commission mettant en œuvre le programme de Stockholm (COM(2010) 171 du 20.4.2010).

95 Cet exercice de cartographie de l'information est réalisé en étroite collaboration avec une équipe ad hoc composée de représentants des États membres de l'UE et de l'AELE, d'Europol, d'Eurojust, de Frontex et du contrôleur européen de la protection des données.

Enfin, la présente communication expose, pour la première fois, l'optique de la Commission à l'égard des principes généraux qu'elle entend suivre à l'avenir dans le cadre de l'élaboration d'instruments de collecte, de stockage ou d'échange de données. Ces principes seront également appliqués pour évaluer les instruments existants. L'adoption d'une approche de l'élaboration et de l'évaluation des politiques fondée sur une série de principes aussi clairement définis devrait renforcer la cohérence et l'efficacité des instruments actuels et futurs, tout en respectant pleinement les droits fondamentaux des citoyens.

ANNEXE I

Les données et exemples suivants visent à illustrer la mise en œuvre pratique des mesures de gestion de l'information qui sont actuellement utilisées.

Système d'information Schengen (SIS)

Nombre total des signalements SIS enregistrés dans la base de données SIS centrale (C.SIS)[96]

Catégories de signalements	**2007**	**2008**	**2009**
Billets de banque	177 327	168 982	134 255
Documents vierges	390 306	360 349	341 675
Armes à feu	314 897	332 028	348 353
Documents délivrés	17 876 227	22 216 158	25 685 572
Véhicules	3 012 856	3 618 199	3 889 098
Personnes recherchées (nom d'emprunt)	299 473	296 815	290 452
Personnes recherchées (nom principal)	859 300	927 318	929 546
Dont:			
Personnes recherchées pour arrestation à des fins d'extradition	19 119	24 560	28 666
Ressortissants de pays tiers figurant sur la liste des personnes non admissibles	696 419	746 994	736 868
Personnes disparues adultes	24 594	23 931	26 707
Personnes disparues mineures	22 907	24 628	25 612
Témoins ou personnes faisant l'objet d'une citation en justice	64 684	72 958	78 869
Personnes faisant l'objet d'une surveillance exceptionnelle visant à prévenir des menaces pour la sécurité publique	31 568	34 149	32 571
Personnes faisant l'objet d'une surveillance exceptionnelle visant à prévenir des menaces pour la sécurité nationale	9	98	253

[96] Document 6162/10 du Conseil du 5.2.2010; document 5764/09 du Conseil du 28.1.2009; document 5441/08 du Conseil du 30.1.2008.

Total	**22 933 370**	**27 919 849**	**31 618 951**

EURODAC – Mouvements de demandeurs d'asile ayant introduit de nouvelles demandes dans le même État membre ou dans d'autres (2008)

		État membre dans lequel la première demande d'asile a été introduite[97]																													**Total des 2es demandes**	
		AT	BE	BG	CH	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IS	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SE	SI	SK	UK	**Résultats positifs nationaux**	**Total résultats positifs**
Envois par les États membres d'empreintes digitales à des fins de comparaison et d'obtention de «résultats positifs» auprès des États membres (colonnes) dans lesquels une personne a précédem	AT	1 725	74	2	0	1	87	274	5	2	31	12	25	115	212	5	0	134	3	14	0	9	52	49	1 371	1	42	111	17	260	61	**1 725**	**4 694**
	BE	180	5 450	4	0	3	38	408	17	0	41	17	28	378	67	28	0	69	3	37	0	2	180	73	625	6	3	192	17	58	205	**5 450**	**8 129**
	BG	5	2	116	0	1	1	5	1	0	7	0	0	0	1	0	0	1	0	2	0	0	1	3	0	0	6	8	0	0	4	**116**	**164**
	CH	32	52	1	4	3	5	35	0	0	17	17	8	39	19	1	0	355	0	1	0	13	15	37	3	1	0	41	4	4	25	**4**	**732**
	CY	1	0	0	0	68	0	1	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	**68**	**73**
	CZ	55	12	0	0	0	637	48	4	0	0	3	4	13	0	1	0	8	2	1	0	0	7	6	17	1	0	13	0	1	6	**637**	**839**
	DE	260	268	12	0	4	79	1 852	42	0	174	39	56	256	106	9	2	200	5	26	2	5	174	137	149	4	43	567	30	89	128	**1 852**	**4 718**
	DK	44	43	3	0	0	13	126	119	0	27	13	44	36	13	4	0	47	0	7	0	0	30	225	55	2	4	436	2	7	41	**119**	**1 341**
	EE	0	0	0	0	0	0	1	1	0	0	0	8	0	0	0	0	0	0	0	0	0	0	1	0	0	0	3	0	0	9	**0**	**23**
	EL	66	88	27	0	12	9	131	10	0	766	8	8	35	3	9	0	48	0	1	0	0	33	24	3	0	13	141	0	8	316	**766**	**1 759**
	ES	16	18	2	0	1	3	37	1	0	11	108	0	29	4	5	0	35	0	0	0	0	9	9	4	6	0	21	5	1	16	**108**	**341**
	FI	37	44	1	0	1	10	115	25	0	48	5	229	14	30	10	1	194	0	3	0	90	49	107	44	2	4	362	3	3	81	**229**	**1 512**
	FR	365	339	0	0	8	97	502	29	0	92	78	31	860	161	8	0	336	11	26	1	29	106	74	1 739	8	9	286	37	75	190	**860**	**5 497**
	HU	297	53	4	0	1	3	169	4	0	2	3	19	70	791	1	0	27	1	10	0	0	28	32	0	0	76	79	19	14	14	**791**	**1 717**
	IE	20	21	0	0	4	2	24	1	0	9	8	0	23	4	309	0	35	0	4	0	4	16	7	0	0	0	22	2	2	187	**309**	**704**
	IS	4	3	0	0	0	0	3	0	0	3	1	1	6	2	1	0	3	0	1	0	1	3	10	1	0	0	11	1	0	3	**0**	**58**
	IT	390	111	5	0	6	33	349	11	0	270	47	27	192	60	23	5	3 290	0	11	0	58	78	116	9	2	6	201	59	224	680	**3 290**	**6 263**
	LT	3	1	0	0	1	3	0	0	0	0	1	0	1	0	0	0	0	5	0	0	0	0	4	14	0	0	5	0	2	0	**5**	**40**
	LU	7	21	4	0	0	0	12	2	0	0	0	1	9	6	0	1	8	0	2	0	1	6	4	0	0	0	10	3	1	3	**2**	**101**
	LV	3	1	0	0	0	0	1	0	1	0	0	0	1	0	0	0	0	5	0	0	0	0	0	0	0	0	1	0	2	0	**0**	**15**
	MT	1	0	0	0	0	0	0	0	0	0	0	5	1	0	0	0	6	0	0	0	16	0	1	0	0	0	1	1	0	0	**16**	**32**
	NL	109	223	16	0	1	27	198	21	0	113	16	29	109	33	7	1	226	0	14	0	58	1 240	95	16	8	9	289	8	22	129	**1 240**	**3 017**
	NO	84	103	6	0	2	13	256	76	0	199	55	57	78	23	8	0	524	8	13	1	83	86	276	164	1	9	826	10	21	96	**276**	**3 078**
	PL	188	65	0	0	0	30	68	15	0	0	2	4	75	1	1	0	0	3	3	0	0	7	27	1 208	1	1	43	1	13	4	**1 208**	**1 760**
	PT	1	10	0	0	0	0	4	1	0	0	11	0	9	0	0	0	2	0	2	0	0	2	2	0	3	0	2	0	1	2	**3**	**52**
	RO	43	2	5	0	1	9	33	0	0	3	0	5	14	11	0	0	0	0	1	0	0	9	1	1	0	64	17	0	4	4	**64**	**227**
	SE	243	133	30	0	4	36	516	173	0	143	29	143	145	80	16	3	276	0	16	0	130	98	430	147	5	13	1 914	11	26	122	**1 914**	**4 882**
	SI	14	4	0	0	0	1	10	1	0	1	1	2	15	6	0	0	5	0	1	0	0	2	3	0	0	0	5	45	3	2	**45**	**121**
	SK	105	4	0	0	0	7	33	0	1	0	0	1	2	12	0	0	3	0	0	1	0	4	4	4	0	0	9	2	195	6	**195**	**393**
	UK	109	153	7	0	3	12	276	30	0	108	6	38	209	25	217	2	768	0	8	0	43	128	76	7	4	11	174	6	46	3 141	**3 141**	**5 607**

97 COM(2009) 494 du 25.9.2009. Par «résultat positif national», on entend l'introduction d'une nouvelle demande d'asile dans l'État membre dans lequel la demande précédente a été introduite.

ment introduit une demande d'asile																																	
Total des 1res demandes	**4 407**	**7 298**	**245**	**4**	**125**	**1 155**	**5 487**	**589**	**4**	**2 067**	**480**	**773**	**2 734**	**1 670**	**663**	**15**	**6 600**	**46**	**204**	**5**	**542**	**2 363**	**1 833**	**5 581**	**55**	**313**	**5 791**	**283**	**1 082**	**5 475**	**24 433**	**57 889**

Système d'informations anticipées sur les passagers (API)

Utilisation par le Royaume-Uni des informations préalables sur les passagers à des fins d'amélioration du contrôle aux frontières et de lutte contre l'immigration clandestine[98]	
Nombre d'actions entreprises en 2009	
Antécédents défavorables (entrée refusée à la personne)	379
Passeports perdus/volés/annulés (document saisi)	56

[98] La UK Border Agency (l'agence britannique pour la gestion des frontières) a fourni ces informations à la Commission aux fins de la présente communication.

Système d'information douanier (SID)

Nombre total de dossiers enregistrés dans la base de données SID (2009)[99]	
Action	**SID (sur la base de la convention SID)**
Dossiers créés	2 007
Dossiers en cours	274
Dossiers consultés	11 920
Dossiers supprimés	1 355

[99] Ces informations ont été fournies par la Commission.

Initiative suédoise

Exemples d'utilisation de l'initiative suédoise pour enquêter sur des infractions pénales[100]	
Homicide	En 2009, une tentative d'homicide a eu lieu dans la capitale d'un État membre. La police a recueilli un échantillon biologique sur un verre dans lequel le suspect avait bu. Les agents de la police scientifique ont extrait l'ADN de cet échantillon et ont établi un profil ADN. Une comparaison de ce profil avec d'autres profils de référence stockés dans la base de données ADN nationale n'a donné aucun résultat positif. Les forces de police chargées de l'enquête ont alors envoyé, par l'intermédiaire de leur point de contact Prüm, une demande de comparaison avec les profils ADN de référence détenus par d'autres États membres ayant été autorisés à échanger ces données sur la base de la décision de Prüm ou de l'accord de Prüm. Cette comparaison transfrontalière a permis d'obtenir un «résultat positif». Sur la base de l'initiative suédoise, les forces de police ont demandé des informations complémentaires sur le suspect. Leur point de contact national a reçu une réponse de plusieurs autres États membres dans les 36 heures, ce qui a permis à la police d'identifier le suspect.
Viol	En 2003, un suspect non identifié a violé une femme. La police a recueilli des échantillons sur la victime, mais le profil ADN obtenu au départ de ces échantillons ne correspondait à aucun des profils de référence stockés dans la base de données ADN nationale. Une demande de comparaison d'ADN, envoyée par le point de contact Prüm aux autres États membres qui avaient été autorisés à échanger les profils ADN de référence sur la base de la décision de Prüm ou de l'accord de Prüm, a produit un «résultat positif». Les forces de police ont alors demandé des informations complémentaires sur le suspect dans le cadre de l'initiative suédoise. Leur point de contact national a reçu une réponse dans les huit heures, ce qui a permis à la police d'identifier le suspect.

[100] Les forces de police d'un État membre ont fourni ces exemples à la Commission aux fins de la présente communication.

Obtention par l'Allemagne de «résultats positifs» dans le cadre de la comparaison transfrontalière de profils ADN, en fonction du type d'infraction (2009)[101]

Résultats positifs par type d'infraction	**Autriche**	**Espagne**	**Luxembourg**	**Pays-Bas**	**Slovénie**
Infractions portant atteinte aux intérêts publics	32	4	0	5	2
Infractions portant atteinte à la liberté des personnes	9	3	5	2	0
Infractions à caractère sexuel	40	22	0	31	4
Atteintes à la personne humaine	49	24	0	15	2
Autres infractions	3 005	712	18	1 105	71

[101] Réponse du gouvernement allemand à une question parlementaire de Ulla Jelpke, Inge Höger et Jan Korte (référence n° 16/14120), Bundestag, 16e session, référence n° 16/14150, 22.10.2009. Ces chiffres concernent la période commençant à la date à laquelle un État membre a commencé à échanger des données avec l'Allemagne et se terminant le 30 septembre 2009.

Directive sur la conservation des données

Exemples d'États membres ayant détecté des cas d'infractions graves à partir de données conservées[102]	
Assassinat	Les services de police d'un État membre sont parvenus à retrouver un groupe de meurtriers ayant assassiné, pour des considérations raciales, six personnes. Les auteurs ont tenté d'échapper à la police en changeant de cartes SIM, mais les listes de leurs appels téléphoniques et les identifiants de leurs téléphones portables les ont trahis.
Homicide	Un service de police a été à même de prouver l'implication de deux suspects dans une affaire d'homicide, en analysant les données relatives au trafic du téléphone portable de la victime. Cette analyse a permis aux enquêteurs de reconstituer l'itinéraire parcouru, ensemble, par la victime et les deux suspects.
Vol avec effraction	Les autorités ont retrouvé la trace d'un cambrioleur ayant commis 17 vols avec effraction, en étudiant les données relatives au trafic de sa carte SIM anonyme prépayée. En identifiant son amie, elles ont pu également localiser l'auteur des vols.
Fraude	Les enquêteurs ont élucidé une affaire d'escroquerie dans le cadre de laquelle une bande qui proposait des voitures de luxe «contre espèces» sur internet détroussait systématiquement les acheteurs venus prendre possession de leur véhicule. Une adresse IP a permis à la police de retrouver l'abonné et d'arrêter les escrocs.

[102] Ces exemples anonymes se fondent sur les réponses des États membres à un questionnaire de 2009 de la Commission concernant la transposition de la directive 2006/24/CE (directive sur la conservation des données).

Coopération entre les cellules de renseignement financier (CRF)

Nombre total de demandes d'informations introduites par les CRF nationales via FIU.net[103]		
Année	**Demandes d'informations**	**Utilisateurs actifs**
2007	3 133	12 États membres
2008	3 084	13 États membres
2009	3 520	18 États membres

[103] Le bureau FIU.net a fourni ces informations à la Commission aux fins de la présente communication.

Coopération entre les bureaux de recouvrement des avoirs (BRA)

Demandes de dépistage d'avoirs introduites par les États membres et traitées par Europol[104]

Année	**2004**	**2005**	**2006**	**2007**
Demandes	5	57	53	133
Dont:				
Affaires de fraude				29
Affaires de blanchiment d'argent				26
Affaires de drogue				25
Affaires liées à d'autres infractions				18
Affaires de drogue et de blanchiment d'argent				19
Affaires de fraude et de blanchiment d'argent				7
Affaires liées à plusieurs infractions				9

Affaires de confiscation d'avoirs traitées par Eurojust (2006-2007)[105]

Types d'affaire		**Dossiers ouverts par**	
Affaires liées à la criminalité environnementale	1	Allemagne	27 %
Affaires liées à une participation à une organisation criminelle	5	Pays-Bas	21 %
Affaires liées au trafic de drogue	15	Royaume-Uni	15 %
Affaires de fraude fiscale	8	Finlande	13 %
Affaires de fraude	8	France	8 %
Affaires de fraude à la TVA	1	Espagne	6 %
Affaires de blanchiment d'argent	9	Portugal	4 %
Affaires de corruption	1	Suède	2 %
Affaires d'atteinte au patrimoine	2	Danemark	2 %
Affaires de trafic d'armes	1	Lettonie	2 %
Affaires de contrefaçon et de piratage de produits	2		
Affaires liées à la fraude sur les paiements d'avance	2		
Affaires de falsification de documents administratifs	1		
Affaires de criminalité liée aux véhicules	1		
Affaires liées au terrorisme	1		
Affaires de falsification	2		
Affaires liées à la traite des êtres humains	1		

104 Évaluation de l'efficacité des pratiques des États membres de l'UE en matière d'identification, de dépistage, de gel et de confiscation d'avoirs d'origine criminelle – Rapport final (pour la Commission européenne, DG JLS), Matrix Insight, juin 2009.

105 Ibidem.

Plateformes de signalement de la cybercriminalité

Exemples de la plateforme française de signalement de la cybercriminalité, Pharos, qui enquête sur des affaires de cybercriminalité[106]	
Pédopornographie	Un internaute a informé Pharos de l'existence d'un blog contenant des photographies et des images de type dessin animé d'exploitation sexuelle d'enfants. L'auteur du blog, qui apparaissait nu sur une photo, tentait également de séduire les enfants via son blog. Les enquêteurs ont identifié un professeur de mathématiques comme principal suspect. Une perquisition à son domicile a permis de découvrir 49 vidéos comportant des images de pédopornographie. L'enquête a également révélé qu'il préparait l'organisation de leçons particulières à domicile. Le défendeur a par conséquent été reconnu coupable et a été condamné à une peine de prison avec sursis.
Exploitation sexuelle des enfants	La police française a eu connaissance du fait qu'un individu offrait de l'argent sur internet en échange de relations sexuelles avec des enfants. Un enquêteur de Pharos se faisant passer pour un mineur a alors pris contact avec le suspect, qui lui a proposé de l'argent en échange de relations sexuelles. La discussion sur internet qui s'en est suivie a permis à Pharos d'identifier l'adresse du protocole internet du suspect et de le retrouver dans une ville connue pour son nombre élevé de cas d'exploitation sexuelle des enfants. Le défendeur a ensuite été reconnu coupable et a été condamné à une peine d'emprisonnement avec sursis.

[106] Pharos est l'abréviation de «plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements».

Exemples de contribution d'Europol à la lutte contre les formes graves de criminalité transfrontalière[107]	
Opération Andromède	En décembre 2009, Europol a participé à la mise en œuvre d'une vaste opération de police transfrontalière contre un réseau de trafic de drogue ayant des contacts dans 42 pays. Le réseau était établi en Belgique et en Norvège, et organisait un trafic de drogue au départ du Pérou, via les Pays-Bas, jusqu'en Belgique, au Royaume-Uni, en Italie et d'autres États membres. La coopération policière a été coordonnée par Europol; la coopération judiciaire par Eurojust. Les autorités participantes ont mis en place un bureau mobile à Pise, et Europol, un centre opérationnel à La Haye. Europol a procédé à une comparaison croisée des informations entre les suspects et a établi un rapport décrivant le réseau criminel.
Participants	Italie, Pays-Bas, Allemagne, Belgique, Royaume-Uni, Lituanie, Norvège et Eurojust.
Résultats	Les forces de police participantes ont saisi 49 kg de cocaïne, 10 kg d'héroïne, 6 000 pilules d'ecstasy, deux armes à feu, cinq faux documents d'identité et 43 000 EUR en espèces. Elles ont arrêté 15 personnes.
Opération Typhon	Entre avril 2008 et février 2010, Europol a fourni un support analytique aux forces de police de 20 pays participant à l'Opération Typhon. À l'occasion de cette vaste opération contre un réseau pédophile distribuant des images de pédopornographie via un site Web autrichien, Europol s'est chargé du support technique et de l'analyse des renseignements de nature pénale, sur la base des images transmises par l'Autriche. Il a ensuite évalué la fiabilité des données et les a restructurées avant de préparer ses propres renseignements. En procédant à une comparaison croisée des données avec les informations contenues dans son fichier de travail à des fins d'analyse, elle a produit 30 rapports de renseignement sur la base desquels des enquêtes ont été ouvertes dans plusieurs pays.
Participants	Autriche, Belgique, Bulgarie, Canada, Danemark, France, Allemagne, Hongrie, Italie, Lituanie, Luxembourg, Malte, Pays-Bas, Pologne, Roumanie, Slovaquie, Slovénie, Espagne,

[107] Europol a fourni ces informations à la Commission aux fins de la présente communication. Des informations complémentaires sur l'opération Andromède sont disponibles à l'adresse http://www.eurojust.europa.eu/.

	Suisse et Royaume-Uni.
Résultats	Les forces de police participantes ont identifié 286 suspects, en ont arrêté 118 et ont sauvé cinq victimes d'abus dans quatre pays.

Exemples de coordination par Eurojust de vastes opérations judiciaires transfrontalières de lutte contre les formes graves de criminalité[108]

Traite des êtres humains et financement du terrorisme	En mai 2010, Eurojust a coordonné une opération transfrontalière qui a permis d'arrêter cinq membres d'un réseau criminel organisé actif en Afghanistan, au Pakistan, en Roumanie, en Albanie et en Italie. Le groupe fournissait des documents falsifiés à des Afghans et des Pakistanais qu'ils faisaient frauduleusement passer en Italie, via l'Iran, la Turquie et la Grèce. À leur arrivée en Italie, les migrants étaient envoyés en Allemagne, en Suède, en Belgique, au Royaume-Uni et en Norvège. Les bénéfices de ce trafic étaient destinés à financer le terrorisme.
Fraude à la carte bancaire	En coordonnant la coopération policière et judiciaire transfrontalière, Europol et Eurojust ont aidé à démanteler un réseau de fraude à la carte bancaire actif en Irlande, en Italie, aux Pays-Bas, en Belgique et en Roumanie. Ce réseau avait volé les données d'identification de quelque 15 000 cartes de paiement, et causé une perte de 6,5 millions EUR. En prévision de cette opération, qui a entraîné 24 arrestations en juillet 2009, des magistrats belges, irlandais, italiens, néerlandais et roumains ont facilité l'émission de mandats d'arrêt européens et l'autorisation de mises sur écoute des suspects.
Traite des êtres humains et trafic de drogue	À la suite d'une réunion de coordination organisée par Eurojust en mars 2009, les autorités italiennes, néerlandaises et colombiennes ont arrêté 62 individus soupçonnés de traite d'êtres humains et de trafic de drogue. Ce réseau était spécialisé dans la traite de femmes vulnérables originaires du Nigeria à destination des Pays-Bas. Celles-ci étaient ensuite contraintes à se prostituer en Italie, en France et en Espagne. Les bénéfices de la prostitution finançaient les achats de cocaïne du réseau en Colombie, la drogue étant ensuite acheminée dans l'UE, à des fins de consommation.

[108] Ces exemples proviennent du site http://www.eurojust.europa.eu/.

Exemples d'analyse PNR permettant de collecter des informations dans le cadre d'enquêtes sur des formes graves de criminalité transfrontalière[109]	
Traite des enfants	L'analyse PNR a révélé que trois enfants non accompagnés voyageaient d'un État membre de l'UE vers un pays tiers, sans que l'on sache qui allait les accueillir à leur arrivée. Alertées par la police de l'État membre après le départ, les autorités du pays tiers ont arrêté la personne qui était venue chercher les enfants, qui s'est révélée être un délinquant sexuel enregistré dans l'État membre.
Traite des êtres humains	L'analyse PNR a permis de démasquer un groupe de trafiquants d'êtres humains qui empruntaient toujours le même itinéraire. Ceux-ci utilisaient des documents falsifiés pour procéder aux formalités d'enregistrement sur un vol intra-UE et utilisaient des documents authentiques pour procéder, simultanément, aux formalités d'enregistrement sur un autre vol à destination d'un pays tiers. Une fois dans la salle d'attente de l'aéroport, ils embarquaient sur le vol intra-UE.
Fraude à la carte de crédit	Plusieurs familles voyageaient à destination d'un État membre avec des billets achetés à l'aide de cartes de crédit volées. L'enquête a démontré qu'un groupement criminel utilisait ces cartes pour acheter les billets qu'il revendait ensuite librement, dans des centres de téléphonie longue distance. Ce sont les données PNR qui ont permis de faire le rapprochement entre les voyageurs, d'une part, et les cartes de crédit et les vendeurs, d'autre part.
Trafic de drogue	Les services de police d'un État membre disposaient d'informations suggérant qu'un homme était impliqué dans un trafic de drogue au départ d'un pays tiers, mais les gardes-frontières n'ont jamais rien trouvé sur lui à son arrivée dans l'UE. L'analyse PNR a révélé qu'il voyageait toujours avec un associé. La fouille de cet associé a permis de trouver d'importantes quantités de drogue.

[109] Ces exemples ont été rendus anonymes pour protéger les sources d'information.

Programme de surveillance du financement du terrorisme (TFTP)

Exemples d'informations recueillies dans le cadre du TFTP aux fins d'enquêtes relatives à des complots terroristes[110]	
Complot terroriste à Barcelone 2008	En janvier 2008, dix suspects ont été arrêtés à Barcelone dans le cadre d'une tentative déjouée d'attentat dans les transports publics de la ville. Les données TFTP ont été utilisées pour identifier les liens des suspects avec l'Asie, l'Afrique et l'Amérique du Nord.
Tentative d'attentat aux explosifs liquides sur un vol transatlantique 2006	Les informations TFTP ont été utilisées pour mener l'enquête sur des individus et condamner ceux-ci dans le cadre d'une tentative déjouée d'attentat qui visait, en août 2006, à faire exploser dix vols transatlantiques à destination des USA et du Canada, au départ du Royaume-Uni.
Attentats à la bombe de Londres 2005	Les données TFTP ont été utilisées pour fournir de nouvelles pistes aux enquêteurs, confirmer l'identité des suspects et faire apparaître les liens entre les individus responsables de ces attentats.
Attentats à la bombe de Madrid 2004	Les données TFTP ont été fournies à plusieurs États membres de l'UE afin de les aider dans leurs enquêtes lancées à la suite de ces attentats.

[110] Deuxième rapport sur le traitement des données à caractère personnel en provenance de l'UE par le Trésor américain aux fins de la lutte antiterroriste, juge Jean-Louis Bruguière, janvier 2010.

ANNEXE II

Tableau récapitulatif des instruments actuellement utilisés ou en cours de mise en œuvre ou d'examen

Instrument	Contexte	Finalité(s)	Structure	Types des données à caractère personnel	Accès aux données	Protection des données	Conservation des données	Degré de mise en œuvre	Réexamen
Système d'information Schengen (SIS)	Initiative des États membres	Maintenir la sécurité publique, y compris la sécurité nationale, à l'intérieur de l'espace Schengen et faciliter la circulation des personnes au moyen des informations que ce système permet de transférer	Centralisée: N.SIS (parties nationales) connectées par interface au C.SIS (partie centrale)	Noms et pseudonymes («alias»), caractéristiques physiques, date et lieu de naissance, nationalité et indication que l'intéressé est ou non armé ou violent. Les signalements SIS portent sur plusieurs groupes de personnes différents.	Les autorités policières, douanières et judiciaires et celles chargées des contrôles aux frontières ont accès à toutes les données; les services d'immigration et les autorités consulaires, à la liste des personnes non admissibles et aux documents perdus et volés. Europol et Eurojust ont accès à certaines données.	Convention n° 108 du Conseil de l'Europe (CdE) et recommandation R (87) 15 du CdE relative à la police	Les données à caractère personnel saisies dans le SIS à des fins de recherche de personnes ne peuvent être conservées que pendant la durée nécessaire pour atteindre les finalités pour lesquelles elles ont été fournies et pendant trois ans maximum. Les données relatives aux personnes faisant l'objet d'une surveillance exceptionnelle en raison de la menace qu'elles constituent pour la sécurité publique ou nationale doivent être supprimées après un an.	Le SIS est applicable dans son intégralité dans 22 États membres, ainsi qu'en Suisse, en Norvège et en Islande. Le Royaume-Uni et l'Irlande participent au SIS sauf pour ce qui est des signalements concernant les ressortissants de pays tiers figurant sur la liste des personnes non admissibles. La Bulgarie, la Roumanie et le Liechtenstein devraient le mettre en œuvre prochainement.	Les signataires peuvent proposer des modifications à la convention de Schengen. Le texte modifié doit être adopté à l'unanimité et ratifié par les parlements.

Tableau récapitulatif des instruments actuellement utilisés ou en cours de mise en œuvre ou d'examen

Instrument	Contexte	Finalité(s)	Structure	Types des données à caractère personnel	Accès aux données	Protection des données	Conservation des données	Degré de mise en œuvre	Réexamen
Système d'information Schengen II (SIS II)	Initiative de la Commission	Assurer un niveau élevé de sécurité dans le domaine de la liberté, de la sécurité et de la justice, et faciliter la circulation des personnes au moyen des informations que ce système permet de transférer	Centralisée: N.SIS (parties nationales) connectées par interface au CS-SIS (partie centrale). Le SIS II utilisera le réseau sécurisé s-TESTA.	Les types de données du SIS, plus les empreintes digitales, les photographies, les copies du mandat d'arrêt européen, les signalements relatifs aux usurpations d'identité et les liens entre les signalements. Les signalements SIS II portent sur plusieurs groupes de personnes différents.	Les autorités policières, douanières et judiciaires et celles chargées des contrôles aux frontières auront accès à toutes les données; les services d'immigration et les autorités consulaires, à la liste des personnes non admissibles et aux documents perdus et volés. Europol et Eurojust pourront accéder à certaines données.	Dispositions spécifiques figurant dans les actes législatifs de base régissant le SIS II et directive 95/46/CE, règlement (CE) n° 45/2001, décision-cadre 2008/977/JAI du Conseil, règlement (CE) n° 45/2011, convention n° 108 du CdE et recommandation R (87) 15 du CdE relative à la police	Les données à caractère personnel saisies dans le SIS à des fins de recherche de personnes ne peuvent être conservées que pendant la durée nécessaire pour atteindre les finalités pour lesquelles elles ont été fournies et pendant trois ans maximum. Les données relatives aux personnes faisant l'objet d'une surveillance exceptionnelle en raison de la menace qu'elles constituent pour la sécurité publique ou nationale doivent être supprimées après un an.	Le SIS II est en cours de mise en œuvre. Dès qu'il sera opérationnel, il sera applicable dans l'UE-27, en Suisse, au Liechtenstein, en Norvège et en Islande. Le Royaume-Uni et l'Irlande participeront au SIS II sauf pour ce qui est des signalements concernant les ressortissants de pays tiers figurant sur la liste des personnes non admissibles.	La Commission doit transmettre des rapports d'avancement semestriels au Parlement européen (PE) et au Conseil sur le développement du SIS II et la migration éventuelle du SIS vers le SIS II.

Tableau récapitulatif des instruments actuellement utilisés ou en cours de mise en œuvre ou d'examen

Instrument	Contexte	Finalité(s)	Structure	Types des données à caractère personnel	Accès aux données	Protection des données	Conservation des données	Degré de mise en œuvre	Réexamen
EURODAC	Initiative de la Commission	Contribuer à déterminer l'État membre responsable de l'examen d'une demande d'asile	Centralisée, composée de points d'accès nationaux connectés par une interface a l'unité centrale d'EURODAC. EURODAC utilise le réseau s-TESTA.	Données dactyloscopiques, sexe, lieu et date de la demande d'asile, numéro de référence utilisé par l'État membre d'origine et date à laquelle les empreintes digitales ont été relevées, transmises et introduites dans le système	Les États membres doivent préciser la liste des autorités ayant accès aux données, parmi lesquelles, le plus souvent, les services de l'immigration et de l'asile, les gardes-frontières et les services de police.	Directive 95/46/CE	10 ans pour les empreintes digitales des demandeurs d'asile; 2 ans pour les ressortissants de pays tiers appréhendés lors du franchissement irrégulier d'une frontière extérieure	Le règlement EURODAC est en vigueur dans tous les États membres, en Norvège, en Islande et en Suisse. Un accord permettant la connexion du Liechtenstein devrait être conclu sous peu.	La Commission doit transmettre un rapport annuel au PE et au Conseil sur le fonctionnement de l'unité centrale d'EURODAC.
Système d'information sur les visas (VIS)	Initiative de la Commission	Contribuer à mettre en œuvre une politique commune des visas et à prévenir les menaces dirigées contre la sécurité intérieure	Centralisée, composée de parties nationales qui seront connectées par une interface à la partie centrale. Le VIS utilisera le réseau s-TESTA.	Demandes de visa, empreintes digitales, photographies, décisions connexes relatives aux visas et liens entre demandes connexes	Les services chargés des visas, de l'asile, de l'immigration et des contrôles aux frontières auront accès à toutes les données. Les services de police et Europol peuvent consulter le VIS aux fins de la prévention et de la détection des formes graves de criminalité, ainsi que des enquêtes en la matière.	Dispositions spécifiques figurant dans les actes législatifs de base régissant le VIS et directive 95/46/CE, règlement (CE) n° 45/2001, décision-cadre 2008/977/JAI du Conseil, convention n° 108 du CdE et recommandation R (87) 15 du CdE relative à la police	5 ans	Le VIS est en cours de mise en œuvre et sera applicable dans tous les États membres (à l'exception du Royaume-Uni et de l'Irlande) ainsi qu'en Norvège, en Islande et en Suisse.	La Commission doit faire rapport au PE et au Conseil sur le fonctionnement du VIS trois ans après son lancement et tous les quatre ans par la suite.

Tableau récapitulatif des instruments actuellement utilisés ou en cours de mise en œuvre ou d'examen

Instrument	Contexte	Finalité(s)	Structure	Types des données à caractère personnel	Accès aux données	Protection des données	Conservation des données	Degré de mise en œuvre	Réexamen
Système d'informations anticipées sur les passagers (API)	Initiative de l'Espagne	Améliorer les contrôles aux frontières et lutter contre l'immigration clandestine	Décentralisée	Données à caractère personnel extraites des passeports, point d'embarquement et point d'entrée dans l'UE	Autorités chargées du contrôle aux frontières et, sur demande, services répressifs	Directive 95/46/CE	Les données doivent être supprimées dans les 24 heures après l'arrivée d'un vol dans l'UE.	Le système API est en vigueur dans tous les États membres, mais n'est utilisé que par quelques-uns d'entre eux.	La Commission évaluera le système API en 2011.
Convention Naples II	Initiative des États membres	Aider les administrations douanières nationales à prévenir et à détecter les infractions aux réglementations douanières nationales et à poursuivre et réprimer les infractions aux réglementations douanières communautaires et nationales	Décentralisée, fonctionne sur la base d'une série d'unités centrales de coordination	Toutes les informations relatives à une personne identifiée ou identifiable	Les unités centrales de coordination transmettent les informations aux administrations douanières, instances judiciaires et autorités de poursuite nationales et, moyennant le consentement préalable de l'État membre fournissant les informations, à d'autres autorités.	Directive 95/46/CE et convention n° 108 du CdE. Les données doivent, dans l'État membre qui les reçoit, bénéficier d'un niveau de protection au moins équivalent à celui garanti dans l'État membre qui les fournit.	Les données ne peuvent être conservées plus longtemps que cela est nécessaire pour atteindre les finalités pour lesquelles elles ont été fournies.	La convention Naples II a été ratifiée par tous les États membres.	Les signataires peuvent proposer des modifications à la convention Naples II. Le texte modifié doit être adopté par le Conseil et ratifié par les États membres.

Tableau récapitulatif des instruments actuellement utilisés ou en cours de mise en œuvre ou d'examen

Instrument	Contexte	Finalité(s)	Structure	Types des données à caractère personnel	Accès aux données	Protection des données	Conservation des données	Degré de mise en œuvre	Réexamen
Système d'information douanier (SID)	Initiative des États membres	Aider les autorités compétentes à prévenir, instruire et poursuivre les infractions graves aux réglementations douanières nationales.	Centralisée, accessible via des terminaux dans chaque État membre et à la Commission. Le SID et le FIDE utilisent l'AFIS, qui utilise le réseau commun de communication, l'interface commune des systèmes ou l'accès web sécurisé que fournit la Commission.	Noms et noms d'emprunt, date et lieu de naissance, nationalité, sexe, signes particuliers, documents d'identité, adresse, tout antécédent de faits de violence, motif de saisie des données dans le SID, action suggérée et numéro d'immatriculation du moyen de transport	Les autorités douanières nationales, Europol et Eurojust peuvent accéder aux données du SID.	Dispositions spécifiques figurant dans la convention SID et directive 95/46/CE, règlement (CE) n° 45/2001, convention n° 108 du CdE et recommandation R (87) 15 du CdE relative à la police	Les données à caractère personnel copiées du SID dans d'autres systèmes à des fins de gestion des risques ou d'analyse opérationnelle ne peuvent être conservées que pendant la durée nécessaire pour atteindre les finalités pour lesquelles elles ont été copiées et doivent être effacées au plus tard après 10 ans.	En vigueur dans tous les États membres	La Commission, en collaboration avec les États membres, présente un rapport annuel au PE et au Conseil sur le fonctionnement du SID.

Tableau récapitulatif des instruments actuellement utilisés ou en cours de mise en œuvre ou d'examen

Instrument	Contexte	Finalité(s)	Structure	Types des données à caractère personnel	Accès aux données	Protection des données	Conservation des données	Degré de mise en œuvre	Réexamen
Initiative suédoise	Initiative de la Suède	Rationaliser les échanges d'informations aux fins d'enquêtes pénales et d'opérations de renseignement en matière pénale	Décentralisée, les États membres doivent désigner des points de contact nationaux chargés de répondre aux demandes urgentes d'informations.	Toute information ou tout renseignement de nature pénale existants dont disposent les autorités répressives	Les autorités policières et douanières et toute autre autorité ayant le pouvoir d'enquêter sur des infractions pénales (à l'exception des services de renseignement)	Règles nationales en matière de protection des données, et convention n° 108 du CdE, protocole additionnel n° 181 du CdE et recommandation R (87) 15 du CdE relative à la police	Les informations et renseignements fournis au titre de cet instrument ne peuvent être utilisés qu'aux fins pour lesquelles ils ont été fournis et sous certaines conditions définies par l'État membre fournisseur.	12 des 31 signataires (États membres de l'UE et de l'AELE) ont adopté des lois nationales mettant en œuvre cet instrument; 5 remplissent le formulaire pour demander des informations; et 2 l'utilisent fréquemment pour échanger des informations.	La Commission doit présenter son rapport d'évaluation au Conseil en 2010.

Tableau récapitulatif des instruments actuellement utilisés ou en cours de mise en œuvre ou d'examen

Instrument	Contexte	Finalité(s)	Structure	Types des données à caractère personnel	Accès aux données	Protection des données	Conservation des données	Degré de mise en œuvre	Réexamen
Décision de Prüm	Initiative des États membres	Renforcer la prévention des infractions pénales, notamment le terrorisme, et maintenir l'ordre public	Décentralisée, interconnexion via le réseau s-TESTA. Des points de contact nationaux traitent les demandes sortantes et entrantes de comparaison de données.	Profils ADN anonymes et empreintes digitales, données d'immatriculation de véhicules et informations relatives aux personnes soupçonnées d'entretenir des liens avec le terrorisme	Les points de contact transmettent les demandes; l'accès national est régi par le droit interne.	Règles spécifiques établies par la décision de Prüm et convention n° 108 du CdE, protocole additionnel n° 181 du CdE et recommandation R (87) 15 du CdE relative à la police. Les personnes peuvent s'adresser à leur contrôleur national de la protection des données pour faire valoir leurs droits en matière de traitement de leurs données à caractère personnel.	Les données à caractère personnel doivent être supprimées dès lors qu'elles ne sont plus nécessaires aux fins pour lesquelles elles ont été fournies. La période maximale de conservation des données au niveau national dans l'État qui fournit les données est contraignante pour l'État qui les reçoit.	La décision de Prüm est en cours de mise en œuvre. 10 États membres ont été autorisés à échanger des données ADN, 5 à échanger des empreintes digitales, 7 à échanger des données d'immatriculation de véhicules. La Norvège et l'Islande sont sur le point d'avoir accès à cet instrument.	La Commission doit présenter son rapport d'évaluation au Conseil en 2012.

Tableau récapitulatif des instruments actuellement utilisés ou en cours de mise en œuvre ou d'examen

Instrument	Contexte	Finalité(s)	Structure	Types des données à caractère personnel	Accès aux données	Protection des données	Conservation des données	Degré de mise en œuvre	Réexamen
Directive sur la conservation des données	Initiative des États membres	Renforcer l'instruction, la détection et la poursuite des formes graves de criminalité en conservant les données relatives au trafic de télécommunications et les données de localisation	Décentralisée, cet instrument impose des obligations aux fournisseurs de services de télécommunication en matière de conservation des données	Numéros de téléphone, adresses IP et identifiants d'équipements mobiles	Les autorités jouissant de droits d'accès sont définies au niveau national.	Directive 95/46/CE et directive 2002/58/CE	De 6 à 24 mois	6 États membres n'ont pas encore transposé cette directive, et les Cours constitutionnelles allemande et roumaine ont déclaré les lois d'exécution anticonstitutionnelles	La Commission doit présenter son rapport d'évaluation au PE et au Conseil en 2010.
Système européen d'information sur les casiers judiciaires (ECRIS)	Initiative de la Belgique et proposition de la Commission	Améliorer le partage transfrontalier de données relatives aux casiers judiciaires des citoyens de l'UE	Décentralisée, interconnexion via un ensemble d'autorités centrales qui échangeront les informations extraites des casiers judiciaires au moyen du réseau s-TESTA	Données biographiques; condamnations, peines et infractions; informations complémentaires, y compris empreintes digitales (si disponibles).	Autorités judiciaires et autorités administratives compétentes	Règles spécifiques établies par la décision-cadre 2009/315/JAI du Conseil, qui intègre les règles de la décision 2005/876/JAI du Conseil, et décision-cadre 2008/977/JAI du Conseil, convention n° 108 du CdE et règlement (CE) n° 45/2001	Les règles nationales en matière de conservation des données s'appliquent, cet instrument ne régissant que les échanges de données.	L'ECRIS est en cours de mise en œuvre. 9 États membres ont commencé à échanger des données par voie électronique.	La Commission doit présenter deux rapports d'évaluation au PE et au Consei: l'un sur la décision-cadre 2008/675/JAI du Conseil; l'autre sur la décision-cadre 2009/315/JAI du Conseil, en 2015. À partir de 2016, la Commission devra publier des rapports réguliers sur l'application de la décision 2009/316/JAI du Conseil (ECRIS).

Tableau récapitulatif des instruments actuellement utilisés ou en cours de mise en œuvre ou d'examen

Instrument	Contexte	Finalité(s)	Structure	Types des données à caractère personnel	Accès aux données	Protection des données	Conservation des données	Degré de mise en œuvre	Réexamen
Coopération entre cellules de renseignement financier (FIU.net)	Initiative des Pays-Bas	Échanger les informations nécessaires à l'analyse des activités de blanchiment d'argent et de financement du terrorisme, ainsi qu'aux enquêtes en la matière	Décentralisée, les CRF s'échangent des données via le réseau FIU.net, qui utilise le réseau s-TESTA. L'application SIENA d'Europol pourrait bientôt venir renforcer le réseau FIU.net.	Toutes les données présentant un intérêt pour l'analyse des activités de blanchiment d'argent et de financement du terrorisme, ainsi que pour les enquêtes en la matière	Cellules de renseignement financier (au sein des services de police, des autorités judiciaires ou des autorités administratives rendant compte aux autorités financières)	Décision-cadre 2008/977/JAI du Conseil, convention n° 108 du CdE et recommandation R (87) 15 du CdE relative à la police	Les règles nationales en matière de conservation des données s'appliquent, cet instrument ne régissant que les échanges de données.	20 États membres participent au FIU.net, une application de partage de données en ligne utilisant s-TESTA	Dans le cadre de son plan d'action pour les services financiers, la Commission réexamine la mise en œuvre de la directive 2005/60/CE depuis 2009.
Coopération entre bureaux de recouvrement des avoirs (BRA)	Initiative des États membres	Échanger les informations nécessaires au dépistage et à l'identification des produits du crime	Décentralisée, les BRA sont tenus d'échanger les informations via l'initiative suédoise. L'application SIENA d'Europol pourrait bientôt venir renforcer la coopération entre les BRA.	Informations relatives aux avoirs et biens visés, telles que comptes bancaires, biens immobiliers et véhicules, et informations relatives aux personnes recherchées, telles que noms, adresses et informations relatives aux actionnaires et aux sociétés	Bureaux de recouvrement des avoirs	Convention n° 108 du CdE, protocole additionnel n° 181 du CdE et recommandation R (87) 15 du CdE relative à la police	Les règles nationales en matière de conservation des données s'appliquent, cet instrument ne régissant que les échanges de données.	Plus de 20 États membres ont mis sur pied des BRA; 12 participent à un projet pilote ayant déployé l'application SIENA d'Europol pour échanger des données présentant un intérêt pour le dépistage d'avoirs.	La Commission doit présenter son rapport d'évaluation au Conseil en 2010.

Tableau récapitulatif des instruments actuellement utilisés ou en cours de mise en œuvre ou d'examen

Instrument	Contexte	Finalité(s)	Structure	Types des données à caractère personnel	Accès aux données	Protection des données	Conservation des données	Degré de mise en œuvre	Réexamen
Plateformes nationales et européenne de lutte contre la cybercriminalité	Initiative de la France	Collecter, échanger et analyser des informations relatives aux infractions commises sur l'internet	Décentralisée, elle rassemble les plateformes nationales de signalement et la plateforme européenne de lutte contre la cybercriminalité d'Europol. L'application SIENA d'Europol pourrait bientôt venir renforcer les échanges de données entre les plateformes de signalement.	Contenu ou comportement illégal détecté sur l'internet	Les plateformes nationales reçoivent les signalements des citoyens; la plateforme européenne de lutte contre la cybercriminalité d'Europol reçoit les signalements relatifs aux formes graves de cybercriminalité transfrontalière des services répressifs.	Règles spécifiques établies par la décision Europol et la décision-cadre 2008/977/JAI du Conseil, convention n° 108 du CdE, protocole additionnel n° 181 du CdE, recommandation R (87) 15 du CdE relative à la police et règlement (CE) n° 45/2001	Les règles nationales en matière de conservation des données s'appliquent, cette mesure ne régissant que les échanges d'informations.	Presque tous les États membres ont mis en place des plateformes nationales de signalement; Europol travaille à sa plateforme européenne de lutte contre la cybercriminalité	Europol couvre la cybercriminalité et rendra compte, à l'avenir, des activités de la plateforme européenne de lutte contre la cybercriminalité dans son rapport annuel présenté au Conseil pour approbation et au Parlement européen pour information.

Tableau récapitulatif des instruments actuellement utilisés ou en cours de mise en œuvre ou d'examen

Instrument	Contexte	Finalité(s)	Structure	Types des données à caractère personnel	Accès aux données	Protection des données	Conservation des données	Degré de mise en œuvre	Réexamen
Europol	Initiative des États membres	Aider les États membres à prévenir et à combattre la criminalité organisée, le terrorisme et les autres formes graves de criminalité affectant deux États membres ou plus	Europol est une agence de l'UE basée à La Haye. Il développe SIENA, sa propre application réseau d'échange sécurisé d'informations.	Le système d'information Europol (SIE) contient les données à caractère personnel, dont les identifiants biométriques, les condamnations et les liens avec la criminalité organisée, des personnes soupçonnées d'avoir commis une infraction relevant du mandat d'Europol. Les fichiers de travail aux fins d'analyse (FTA) contiennent toutes les données à caractère personnel pertinentes.	Le SIE est accessible aux unités nationales d'Europol, aux officiers de liaison, au personnel d'Europol et à son directeur. L'accès aux FTA est accordé aux officiers de liaison. Les données à caractère personnel peuvent être échangées avec les pays tiers ayant conclu un accord avec Europol.	Règles spécifiques établies par la décision Europol et la décision-cadre 2008/977/JAI du Conseil, convention n° 108 du CdE, protocole additionnel n° 181 du CdE, recommandation R (87) 15 du CdE relative à la police et règlement (CE) n° 45/2001	Les FTA peuvent être conservés pour une durée de trois ans maximum, qui peut éventuellement être prolongée de trois années supplémentaires.	Europol est activement utilisé par tous les États membres, ainsi que par les pays tiers avec lesquels l'office a conclu un accord opérationnel. La nouvelle base juridique d'Europol a été mise en œuvre dans tous les États membres.	Une autorité de contrôle commune surveille les activités d'Europol en matière de traitement des données à caractère personnel et de transmission de ces données à d'autres parties. Elle présente des rapports périodiques au PE et au Conseil. Europol transmet également un rapport annuel sur ses activités au Conseil pour approbation et au PE pour information.

Tableau récapitulatif des instruments actuellement utilisés ou en cours de mise en œuvre ou d'examen

Instrument	Contexte	Finalité(s)	Structure	Types des données à caractère personnel	Accès aux données	Protection des données	Conservation des données	Degré de mise en œuvre	Réexamen
Eurojust	Initiative des États membres	Améliorer la coordination des enquêtes et des poursuites dans les États membres et renforcer la coopération entre les autorités compétentes	Eurojust est un organe de l'UE basé à La Haye, qui utilise le réseau s-TESTA pour les échanges de données.	Données à caractère personnel des suspects et auteurs d'infraction grave affectant deux États membres ou plus, y compris les données biographiques, les coordonnées, les profils ADN, les photographies, les empreintes digitales, ainsi que les données relatives au trafic de télécommunications et les données de localisation	Les 27 membres nationaux d'Europol, qui peuvent partager des données avec des autorités nationales et des pays tiers moyennant l'accord de la source des informations	Règles spécifiques établies par la décision Eurojust et décision-cadre 2008/977/JAI du Conseil, convention n° 108 du CdE, protocole additionnel n° 181 du CdE et recommandation R (87) 15 du CdE relative à la police	Les informations doivent être supprimées dès qu'elles ont rempli la fonction pour laquelle elles ont été fournies, et dès qu'une affaire est classée.	La base juridique d'Eurojust est actuellement mise en œuvre par les États membres.	La Commission doit réexaminer les échanges de données entre les membres nationaux d'Eurojust d'ici à juin 2014. Pour juin 2013 au plus tard, Eurojust fera rapport au Conseil et à la Commission au sujet de l'ouverture au niveau national de l'accès à son système de gestion des affaires. Un organe de contrôle commun surveille les activités d'Eurojust en matière de traitement des données à caractère personnel et fait rapport chaque année au Conseil. Le président du collège d'Eurojust présente au Conseil un rapport annuel sur les activités d'Eurojust, que le Conseil transmet au PE.

Tableau récapitulatif des instruments actuellement utilisés ou en cours de mise en œuvre ou d'examen

Instrument	Contexte	Finalité(s)	Structure	Types des données à caractère personnel	Accès aux données	Protection des données	Conservation des données	Degré de mise en œuvre	Réexamen
Accords PNR avec les États-Unis et l'Australie; accord API/PNR avec le Canada	Initiative de la Commission	Prévenir et combattre le terrorisme et les autres formes graves de criminalité transnationale	Accords internationaux	Les accords avec les États-Unis et l'Australie portent sur 19 types de données PNR, dont les informations biographiques, les informations relatives aux réservations et aux paiements, et des informations supplémentaires; l'accord canadien prévoit 25 types de données similaires.	Le ministère américain de la sécurité intérieure, l'Agence des services frontaliers du Canada et le service douanier australien, qui peuvent partager des données avec les services nationaux chargés de la répression et de la lutte antiterroriste	Les règles en matière de protection des données sont définies dans les accords internationaux spécifiques.	États-Unis: 7 ans d'utilisation active, 8 ans d'utilisation passive; Australie: 3 ans et demi d'utilisation active, 2 ans d'utilisation passive; Canada: 72 heures d'utilisation active, 3 ans et demi d'utilisation passive	Les accords conclus avec les États-Unis et l'Australie sont provisoirement applicables; l'accord canadien est entré en vigueur. La Commission renégociera ces accords. 6 États membres de l'UE ont adopté des lois permettant l'utilisation des données PNR à des fins répressives.	Chaque accord prévoit un réexamen périodique, et les accords canadien et australien comprennent également une clause de dénonciation.

Tableau récapitulatif des instruments actuellement utilisés ou en cours de mise en œuvre ou d'examen

Instrument	Contexte	Finalité(s)	Structure	Types des données à caractère personnel	Accès aux données	Protection des données	Conservation des données	Degré de mise en œuvre	Réexamen
Accord TFTP UE-États-Unis	Initiative de la Commission	Favoriser la prévention et la détection du terrorisme ou de son financement, ainsi que les enquêtes et les poursuites en la matière	Accord international	Données de messagerie financière comprenant, entre autres, le nom, le numéro de compte, l'adresse et le numéro d'identification du donneur d'ordre et des bénéficiaires de certaines transactions financières	Le Trésor américain peut partager les données à caractère personnel extraites des messages financiers avec les services répressifs, les organismes chargés de la sécurité publique ou les autorités chargées de la lutte contre le terrorisme aux États-Unis, les États membres de l'UE, Europol ou Eurojust. Le transfert vers des pays tiers est subordonné à l'approbation des États membres.	L'accord prévoit des clauses strictes de limitation des finalités et de proportionnalité.	Les données à caractère personnel extraites des messages financiers ne peuvent être conservées plus longtemps que cela est nécessaire aux fins d'enquêtes ou de poursuites spécifiques; les données non extraites ne peuvent être conservées que pendant 5 ans.	Le PE a approuvé la conclusion de l'accord TFTP UE-États-Unis le 8 juillet 2010 . Le Conseil devrait à présent adopter une décision du Conseil relative à la conclusion de cet accord, après quoi l'accord entrera en vigueur par l'intermédiaire d'un échange de lettres entre les parties	La Commission doit réexaminer cet accord six mois après son entrée en vigueur. Son rapport d'évaluation doit être transmis au PE et au Conseil.