Avis n° 27/2010 du 24 novembre 2010

Objet: Projet d'accord bilatéral entre la Belgique et les Etats-Unis sur le renforcement de la coopération dans la prévention et la lutte contre les crimes graves (*draft agreement on enhancing cooperation in Preventing and Combating Serious Crime* – « Accord PCSC ») (CO-A-2010-025).

La Commission de la protection de la vie privée ;

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (ci-après LVP), en particulier l'article 29 ;

Vu la demande d'avis de Monsieur Stefaan de Clerck, Ministre de la Justice, reçue le 20/09/2010;

Vu le rapport de Monsieur Bart de Schutter;

Émet, le 24 novembre 2010, l'avis suivant :

I. Objet et contexte de la demande d'avis

1. Le 20 septembre 2010, M. Stefaan de Clerck, Ministre de la Justice a demandé à la Commission d'émettre un avis concernant un projet d'accord bilatéral entre la Belgique et les Etats-Unis d'Amérique sur le renforcement de la coopération dans la prévention et la lutte contre les crimes graves (*draft agreement on enhancing cooperation in Preventing and Combating Serious Crime* – « Accord PCSC »).

2. Le projet d'Accord PCSC est accompagné d'une annexe : un commentaire sur le droit américain sous la forme de « *Frequently Asked Questions* ». Ces FAQ ont été rédigées par le Département américain de la Sécurité Intérieure (*United States Department of Homeland Security–DHS*) conjointement avec le SPF Justice. Ces FAQ abordent plusieurs points tels que l'indication précise des normes américaines applicables (faq 1), l'exercice du droit d'accès direct ou indirect selon ces législations (faq 2, 3 et 11), l'existence d'autorités de contrôle (faq 4 et 12), la mise en place de mesures de sauvegarde appropriées pour les données dites 'sensibles' (faq 5), et la possibilité d'une saisine judiciaire (faq 2, 7 et 9).

A] Le projet d'Accord PCSC est un « Traité *Prüm-like* »

3. Ce projet d'Accord PCSC est fortement inspiré du Traité de Prüm (et il est autrement connu comme un Traité « *Prüm-like* ») [1] conclu le 27 mai 2005 entre la Belgique, l'Allemagne, l'Espagne, la France, le Luxembourg, les Pays-Bas et l'Autriche et relatif à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme, la criminalité transfrontalière et la migration illégale [2].

4. Ce Traité de Prüm, qui ne lie que certains Etats Membres, a été intégré à l'ensemble de l'Union européenne par la Décision du Conseil européen 2008/615/JAI du 23 juin 2008 relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière [3]. Cette Décision du Conseil règle, entre autres :

— les conditions et procédures applicables au transfert automatisé des profils ADN, des données dactyloscopiques (empreintes digitales) et de certaines données nationales relatives à l'immatriculation des véhicules ;

— les conditions de transmission d'informations en vue de prévenir les infractions terroristes.

---

[1] Le préambule du projet d'Accord PCSC se réfère d'ailleurs explicitement au Traité de Prüm.

[2] La loi d'assentiment à ce Traité a été votée le 28 décembre 2006 (*Mon. bel.*, 30 mars 2007, 3ème édition, page 18359).

[3] Cette Décision 2008/615/JAI a été mise en œuvre par une seconde Décision 2008/616/JAI du 23 juin 2008.

5. Dans la mesure où ces dispositions s'inscrivent dans le cadre intra-européen, l'échange de données policières bénéficie d'un encadrement juridique spécifique : les Etats Membres doivent respecter la Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale.

B] Le projet d'Accord PCSC et le VWP

6. La Belgique participe au Programme d'Exemption des Visas (*US Visa Waiver Program* – VWP) depuis octobre 1991 [4] : moyennant le respect des conditions requises par la législation américaine (*Immigration and Nationality Act, section* 217), la Belgique est inscrite sur une liste des pays participants au VWP, ce qui signifie que les citoyens belges peuvent entrer aux USA sans devoir d'abord obtenir un visa, s'il s'agit d'un voyage de tourisme ou d'affaires ou si ils se trouvent en transit.

7. Afin d'obtenir leur participation dans le VWP, certains Etats ont été approchés par les USA aux fins de conclure des Accords supplémentaires (*Memorandum Of Understanding concerning US Visa Waiver Program*) [5]. Le DHS indique [6] qu'un tel Accord PCSC s'inscrit dans le cadre du Programme américain d'Exemption de Visa.

C] Les négociations actuelles UE – USA

8. La Commission européenne négocie actuellement avec les USA un Accord général relatif à la protection des données à caractère personnel dans le cadre de leur coopération dans la lutte contre le terrorisme et la criminalité [7].

---

[4] Dans la législation américaine, cette liste se retrouve dans le *Code of Federal Regulation*, section 217.2 (v° *Eligibility*) : www.access.gpo.gov/nara/cfr/waisidx_10/8cfr217_10.html . Voir aussi la liste officielle des 36 pays participants au VWP sur le site des services consulaires du Ministère américain des affaires étrangères : www.travel.state.gov/visa/temp/without/without_1990.html

[5] L'Estonie notamment a été approchée, et en mars 2008 a signé ce MOU [voir le communiqué de presse de l'ambassade de l'Estonie à Washington : www.estemb.org/news/aid-1416], qui indique entre autres que d'autres mesures devraient compléter cet Accord, notamment l'échange d'information (avec des garanties appropriées de protection des données) en ce qui concerne la prévention et la lutte contre le terrorisme et les infractions graves. En septembre 2009, l'Estonie conclu un Accord PCSC similaire [Cet Accord est disponible sur le site du DHS (*United States Department of Homeland Security)* : www.dhs.gov/xlibrary/assets/agreement_usestonia_seriouscrime.pdf] … pour ne pas dire identique à celui qui est soumis ici pour examen à la Commission.

[6] Voir le communiqué de presse : www.dhs.gov/xnews/releases/pr_1222715330518.shtm

[7] Voir le communiqué de presse de la Commission européenne : http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/609&format=HTML&aged=0&language=FR&guiLanguage=en

Poussée par le Parlement européen [8], la Commission européenne peut s'appuyer sur le Rapport du Groupe de contact à haut niveau UE/États-Unis (*EU-US High Level Contact Group* — HLCG) [9]. Ce rapport dégage douze principes communs sur le partage d'informations et la protection de la vie privée et des données à caractère personnel. Le Contrôleur Européen de la Protection des Données (*European Data Protection Supervisor* – EDPS) a également rendu un Avis en la matière [10].

9. Un tel Accord général (« *umbrella agreement* ») entre l'Union européenne et les USA serait considéré comme une lex generalis ne pouvant servir de base légale au partage d'information. Les échanges spécifiques de données devront faire l'objet d'Accords particuliers afin fins de préciser les modalités et conditions de la communication d'informations. Par ailleurs, ce futur Accord-cadre serait sans nul doute complémentaire à l'Accord entre l'Union Européenne et les USA en matière d'entraide judiciaire, signé à Washington le 25 juin 2003 [11].

10. La Présidence belge de l'UE souhaite entériner ces négociations avant la fin de cette année 2010 [12]. Le Parlement Européen est informé de l'avancée des négociations [13] et le Groupe 29 [14] suit également les derniers développements de ce projet d'Accord général.

11. Certains points des négociations suscitent une attention particulière de la part des Autorités de Protection des Données, notamment :

— la rétroactivité de l'accord-cadre : tant la Commission européenne que le Groupe 29 soutiennent le principe de rétroactivité de l'Accord-cadre, ce qui permettrait de réexaminer les accords antérieurs (bi ou multilatéraux) à l'aune des principes contenus dans l'Accord-cadre.

— l'échange de données dans le cadre de procédures judiciaires pouvant aboutir à la peine de mort, ce qui semble une entorse à la Charte des droits fondamentaux adoptée à Nice le 7 décembre 2000 et désormais intégrée dans le Traité sur l'Union européenne (article 6) tel que modifié par le Traité de Lisbonne du 13 décembre 2007.

---

[8] Dans une résolution du 26 mars 2009 (publiée au Journal Officiel, C 117, du 6 mai 2010), le Parlement européen a appelé à la conclusion d'un accord UE-États-Unis qui assure la protection adéquate des libertés civiles et des données à caractère personnel : « *Le Parlement européen met en avant que l'échange de données et d'informations est un outil précieux dans la lutte internationale contre le terrorisme et le crime transnational, mais souligne qu'il doit s'inscrire dans un cadre juridique approprié, assurant la protection adéquate des libertés civiles, y compris le droit à la vie privée, et se fonder sur un accord international contraignant, tel que cela a été convenu lors du sommet UE/États-Unis de 2008* » (point 43)

[9] Ce HLCG a été institué en novembre 2006, et est composé de représentants européens de la Commission et du Conseil, ainsi que de représentants américains des Département de la Justice et de l'Intérieur. Le rapport du HLCG (28 mai 2008) est disponible via : http://ec.europa.eu/justice/policies/privacy/news/2008_en.htm#

[10] Voir l'Avis de l'EDPS du 11 novembre 2008 concernant le rapport final du Groupe de contact à haut niveau UE/États-Unis sur le partage d'informations et la protection de la vie privée et des données à caractère personnel (publié au Journal Officiel, C 128, 6 juin 2009)

[11] Cet Accord est publié au Journal Officiel L 181, du 19 juillet 2003.

[12] Voir le communiqué de presse du Parlement européen : www.europarl.europa.eu/news/public/story_page/019-89976-298-10-44-902-20101025STO89954-2010-25-10-2010/default_en.htm

[13] Un débat est intervenu au sein de la Commission des Libertés civiles, justice et affaires intérieures (Commission LIBE du Parlement européen) ce 25 octobre 2010 : www.europarl.europa.eu/news/public/story_page/019-89976-298-10-44-902-20101025STO89954-2010-25-10-2010/default_en.htm

[14] Le Groupe 29 est un organe consultatif européen indépendant sur la protection des données et de la vie privée, établi en vertu de l'article 29 de la Directive 95/46/CE, regroupant toutes les Autorités de Protection des données des Etats membres, en ce compris la Commission Vie Privée belge.

— la nécessité de prévoir explicitement la possibilité d'un recours effectif devant les autorités judiciaires : en effet, la législation américaine sur la protection des données étant sectorielle [15], les recours des personnes concernées sont organisés de manière différente selon le cas, et il peut s'agir d'un recours seulement administratif, seulement judiciaire, ou l'un consécutif à l'autre, ou ne portant que sur l'exercice partiel des droits de la personne concernée.
— l'inclusion dans le champ d'application de l'Accord-cadre des informations échangées en provenance du secteur privé [16].
— l'évaluation de l'Accord-cadre par un Comité dont la composition devrait aussi comprendre des membres des Autorités de Protection des Données européennes.

II. Les dispositions légales applicables

A] Le cadre européen

12. En ce qui concerne la coopération policière et judiciaire en matière pénale, il faudra – dès sa transposition en droit belge (le délai de transposition court jusqu'au 27 novembre 2010) – se référer à la Décision-cadre 2008/977/JAI du 27 novembre 2008 précitée. Néanmoins, il peut déjà être tenu compte des principes adoptés par cette Décision-cadre.

13. « *Il convient que les futurs accords [avec des Etats tiers] respectent les règles relatives aux échanges avec des États tiers* » (considérant 38 de la Décision-cadre).

14. L'article 13 de cette Décision-cadre stipule notamment que les transferts de données vers des pays non membres de la Communauté Européenne ne pourront être réalisés que si l'Etat tiers concerné assure un niveau de protection adéquat pour le traitement de données envisagé.

15. Selon l'article 13 §4, le caractère adéquat du niveau de protection s'apprécie au regard de toutes les circonstances relatives à une opération de transfert ou à un ensemble d'opérations de transfert de données. En particulier, sont pris en considération la nature des données, la finalité et la durée du ou des traitements envisagés, l'État d'origine et l'État ou l'instance internationale de destination finale, les règles de droit, générales ou sectorielles, en vigueur dans l'État tiers ou l'instance internationale en question, ainsi que les règles professionnelles et les mesures de sécurité qui s'y appliquent.

---

[15] Il s'agit notamment du Privacy Act de 1974, du Freedom of Information Act (FOIA) de 1966, et de l'Administrative Procedure Act (APA). Les différents mécanismes de recours sont développés dans la FAQ n°2 annexé au projet d'Accord PCSC.

[16] telles que par exemple les données bancaire dans l'affaire Swift, ou les données des compagnies aériennes dans l'affaire PNR – Passengers Name Record.

16. La Décision-cadre ne précise toutefois pas clairement quelle autorité sera en charge de procéder à une telle évaluation. Il semblerait toutefois qu'en vertu de l'article 25 de la Décision-cadre – qui énumère les compétences des ACN –, cette compétence ne soit pas dévolue aux Autorités de Contrôle Nationales de protection des données (ACN).

17. Lorsqu'un pays tiers ne bénéficie pas d'une reconnaissance d'adéquation, l'article 13 §3, b) de cette Décision-cadre trouve à s'appliquer : par dérogation au principe de transfert de données vers un Etat tiers assurant un niveau de protection adéquat, les données à caractère personnel peuvent toutefois être transférées notamment si l'État tiers prévoit des garanties qui sont jugées adéquates par l'État membre concerné conformément à sa législation nationale.

B] <u>Le cadre belge</u>

18. En vertu de l'article 21 de la LVP, le transfert de données à caractère personnel vers un pays non membre de la Communauté européenne, ne peut avoir lieu que si le pays en question assure un niveau de protection adéquat.

19. Les critères dégagés par l'article 21 §1er alinéa 2 de la LVP pour l'appréciation du caractère adéquat du niveau de protection sont identiques à ceux décrits dans la Décision-cadre 2008/977/JAI du 27 novembre 2008 précitée.

20. La Commission, comprenant la nécessité du flux de ces données entre la Belgique et les USA, estime que ces données peuvent être transférées en vertu de l'Accord PCSC (« transfert rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important » – article 22 §1er, 4° de la LVP).

21. Toutefois, la Commission souligne qu'il est essentiel que les personnes concernées puissent continuer à bénéficier des droits et garanties fondamentaux reconnus à l'égard des traitements de leurs données en Belgique, une fois celles-ci transférées dans des pays tiers. Il est par conséquent indispensable que des garanties soient apportées afin de protéger les données une fois transmises, d'autant plus que l'Accord PCSC comporte plusieurs références au droit national.

22. La Commission estime que de telles garanties doivent réellement engager l'Etat tiers, ce qui, dans le cas d'espèce, est rencontré lorsque ces garanties se retrouvent dans une législation particulière (en vertu de la loi américaine), ou dans un *Memorandum Of Understanding* (MOU) accompagnant l'Accord PCSC, ou, de préférence, au sein même de l'Accord PCSC. Une simple déclaration générale accompagnant l'Accord PCSC n'est pas suffisante aux yeux de la Commission, étant donné son absence de valeur contraignante.

23. La Commission rappelle également la teneur de la Circulaire COL 2/2000 du Collège des Procureurs Généraux du 14 février 2000 concernant la coopération policière internationale à finalité judiciaire :

— seules les données listée dans son Annexe A [17] peuvent être traitées de manière indépendante (c'est-à-dire faire l'objet d'un transfert international) par les services de police.

— pour toutes les autres données, l'accord d'un magistrat est nécessaire avant tout transfert vers l'étranger : soit pour autoriser le transfert, soit pour indiquer qu'une demande d'entraide judiciaire (commission rogatoire internationale émanant d'une autorité judiciaire) est nécessaire.

24. Si la COL 2/2000 semble se limiter aux transferts d'information en vertu des Conventions Schengen et Europol [18], la Commission rappelle l'application des articles 21 et 22 de la LVP en cas de transfert vers des pays non-membres de l'Union européenne (principe du niveau de protection adéquat et dérogations à ce principe).

III. Le projet d'Accord PCSC

25. Le projet d'Accord PCSC permet, moyennant le respect de certaines conditions et procédures, l'échange de données entre la Belgique et les USA à des fins de prévention et de lutte contre les infractions graves.

---

[17] Il s'agit plus précisément de :

1. Informations relatives à des personnes physiques: Nom, noms de baptême, prénoms, prénoms usuels, surnoms, alias, Lieu de naissance et date de naissance, Sexe, Etat civil, Nationalité / statut de résident, Profession, Numéros de téléphone, et GSM publiés (mais pas les non publiés), adresse et domicile / lieu de résidence, PAS le numéro de registre national, données personnelles concernant des suspects ou des personnes connues (à l'exception des données d'ordre public, de la sûreté d'état et du service des affaires étrangères), relation entre des personnes connues, des faits, des endroits et des objets suspects (mais limité aux données reprises dans les fichiers policiers manuels ou automatisés), données pénitentiaires, antécédents (pour autant qu'il s'agisse de données disponibles dans les fichiers policiers manuels ou automatisés), PAS les condamnations, personnes disparues, cadavres non-identifiés.

2. Informations relatives à des personnes morales : Dénomination / noms commerciaux, forme légale, siège, adresse d'exploitation, adresses d'établissement, date d'établissement, administrateurs, directeurs, associés, nombre de travailleurs inscrits, objet social / activités de l'entreprise / description de l'entreprise, bilans (pour autant que les données aient été publiées)

3. Objets, à l'exception des véhicules : Objets signalés, objets liés à des personnes, à des faits ou à des endroits suspects (pour autant qu'il s'agisse de données disponibles dans les fichiers policiers manuels ou automatisés), objets perdus, données du registre des armes

4. Faits : lieu, date et heure, *modus operandi*, relation entre des faits, des personnes, des lieux, des traces, des objets (pour autant qu'il s'agisse de données disponibles dans les fichiers policiers manuels ou automatisés),

5. Véhicules : catégorie, marque, type, numéro d'immatriculation, numéro de châssis, relations avec des personnes (à moins qu'il ne s'agisse d'un numéro d'immatriculation protégé), relations avec des faits, relations avec des lieux

6. Lieux : nature des faits / des incidents, description du lieu, personnes pertinentes, véhicules pertinents

7. Missions émanant des autorités judiciaires : missions résultant des signalements effectués par les autorités belges au moyen d'Interpol et du SIS, données fournies en appui des opérations transfrontalières (poursuites, observations, alerte de police …)

[18] Convention d'application du 19 juin 1990 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 – Décision 2009/371/JAI du Conseil du 6 avril 2009 portant création de l'Office européen de police (Europol).

26. Chaque Etat désigne également des Points de Contacts Nationaux (PCN) qui sont seuls habilités à effectuer des demandes d'information ; ces demandes des PCN ne pouvant avoir pour objectif que des finalités de justice pénale, ce qui comprend « *la réalisation d'une des activités suivantes : recherche, arrestation, incarcération, libération avant procès, libération après procès, poursuites judiciaires, décision judiciaire, contrôle judiciaire ou activités de réinsertion de prévenus ou d'auteurs d'infractions pénales. Ceci inclut également les activités d'identification judiciaire* » [19] (article 1er, §1er). **Il n'apparait pas clairement aux yeux de la Commission quel serait l'objet de l'échange de données pour le cas de « *rehabilitation activities of accused person or criminal offenders* » : la Commission recommande dès lors une clarification quant à ce point.**

27. Une liste des infractions graves (à savoir celles qui sont punissables d'au moins un an d'emprisonnement) est d'ailleurs annexée à l'Accord PCSC (article 2 §3).

A] <u>les empreintes digitales et les profils ADN (articles 3 à 10)</u>

28. Tant la Belgique que les Etats-Unis doivent mettre en place des bases de données reprenant les empreintes digitales/les profils ADN et les données de référence y afférents (c'est-à-dire les numéros d'identification et de profils) [20]. Les données de référence dont il est question ne peuvent en aucun cas permettre l'identification directe de la personne concernée.

29. L'interrogation ponctuelle des bases de données par les PCN engendre une réponse sous forme de « hit/no hit ». En cas de correspondance entre les empreintes/profils comparées, le PCN devra communiquer ensuite au PCN de l'autre Etat, en conformité avec sa législation nationale, les données à caractère personnel de la personne à qui appartient l'empreinte digitale/le profil ADN.

30. Mais en attendant la mise en place d'un tel système en Belgique, les PCN pourront formuler leurs demandes sur base d' « *autres données d'identification afin d'obtenir une correspondance reliant l'individu à ces données supplémentaires* » (article 5 *in fine*).

31. D'après le projet d'Accord PCSC, les demandes pour ce qui concerne tant les empreintes digitales que les profils ADN ne peuvent être effectuées par les PCN que dans le cadre de la finalité de prévention et de poursuite des infractions graves.

---

[19] Traduction libre effectuée par le secrétariat de la Commission en l'absence de traduction officielle

[20] La base de données belge relative aux empreintes digitales devrait également être reliée au casier judiciaire central (article 5 du projet d'Accord PCSC).

32. Dans une optique de clarification, la Commission recommande de préciser dans les articles 3 et 4 (empreintes digitales) et l'article 8 (profils ADN) que les infractions graves sont celles énumérées dans l'annexe visée à l'article 2 §3 de l'Accord.

B] <u>les autres données à caractère personnel (article 11)</u>

33. D'autres données à caractère personnel peuvent être échangées, ponctuellement et en conformité avec la législation nationale, lorsqu'en raison de circonstances particulières, il y lieu de croire que la personne concernée a commis, commettra, a participé ou participera à certaines infractions graves ou à certaines infractions liées au terrorisme, ou que la personne concernée fait partie d'une organisation criminelle.

34. Ces données comprennent les nom et prénoms (anciens et actuels), alias, surnoms, orthographe alternative des noms, sexe, lieu et date de naissance, nationalité (actuelle et ancienne), numéro de passeport, numéro d'autres documents d'identité, empreintes digitales, ainsi que les circonstances particulières qui permettent cette communication de données.

35. L'Etat qui communique ces données peut les assortir de conditions d'utilisation ponctuelles, auxquelles l'Etat receveur est tenu. Toutefois le simple respect de la législation relative à la protection des données ne peut constituer une de ces conditions d'utilisation. En d'autres termes, la législation relative à la protection des données d'un Etat ne peut s'appliquer *de jure* à l'autre Etat.

36. D'après le projet d'Accord PCSC, les demandes pour ce qui concerne ces données peuvent être effectuées par les PCN dans le cadre de la finalité de prévention et de poursuite des infractions graves, mais aussi dans en vue de la prévention du terrorisme. Une liste des infractions relevant du terrorisme est également dressée par chaque partie et notifiée à l'autre (article 11 §3).

37. Dans une optique de clarification, la Commission recommande de préciser dans cet article 11 que les infractions graves sont celles énumérées dans l'annexe visée à l'article 2 §3 de l'Accord.

38. S'inspirant du principe de double incrimination, l'Accord PCSC prévoit que la Belgique ne pourra transférer des données relatives à des faits de terrorisme que s'ils constituent également une infraction en droit belge (article 11, §1er, a)), ce que la Commission considère comme une garantie pour la personne concernée.

C] <u>les autres finalités (article 14)</u>

39. L'article 14 du projet d'Accord PCSC est intitulé « *limitations de traitement aux fins de protéger les données à caractère personnel et les autres données* », et prévoit que chaque Etat peut disposer des données qu'il a reçues à plusieurs fins :

a) pour les finalités de poursuite pénale, ou

b) pour la prévention d'une menace sérieuse de sécurité publique, ou

c) pour des procédures administratives ou non pénale mais en lien direct avec les poursuites visées au point a), ou

d) pour toute autre finalité, moyennant l'accord préalable de l'autre Etat.

40. La Commission note que si les demandes effectuées par les PCN sont strictement limitées au cadre des poursuites pénales en lien avec deux listes d'infractions (article 2§3 et 11 §3), l'Etat peut ensuite largement utiliser les données reçues (dont les empreintes digitales et les profils ADN), moyennant néanmoins l'accord de l'autre Etat.

41. Le fait de pouvoir utiliser ces données « *pour toute autre finalité, moyennant l'accord préalable de l'autre Etat* » (article 14, §1er d)) n'est pas, en l'état actuel du libellé, de nature à rassurer la Commission [21]. **Ce traitement ultérieur pour toute autre finalité devrait être assorti de garanties, telles qu'au minimum :**

— cette faculté ne s'applique qu'au cas par cas,

— pour une autre finalité spécifiée et motivée au moment de la demande,

— moyennant l'accord préalable, spécifique et au cas par cas de l'Etat (un accord de principe général ne serait pas admissible), **et**

— avec une journalisation non seulement des transferts internationaux de données, mais aussi des transferts au sein même de l'Etat (entre autorités nationales habilitées), de sorte qu'un contrôle effectif, notamment par la Commission, soit rendu possible (voir *infra* point 45).

— l'accord préalable de l'Etat et la décision de transmission doivent pouvoir faire l'objet d'un contrôle juridictionnel,

— si les cinq conditions ci-dessus ne sont pas rencontrées dans le corps même du texte de l'Accord PCSC, la Commission émet un avis défavorable sur cette transmission « pour toute autre finalité » et recommande la suppression pure et simple d'une telle possibilité dans l'Accord PCSC.

---

[21] Le Contrôleur Européen de la Protection des Données (EDPS) demeure aussi très critique quant à ce type de clause : voir ses Avis du 27 avril 2007 (point 23) et du 16 octobre 2007 (point 2) relatif à la Décision-cadre du Conseil sur la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale (avis disponibles sur le site de l'EDPS).

D] <u>les règles de protection des données</u>

42. L'article 12 dispose que les deux Etats signataires de l'Accord PCSC doivent respecter leur législation nationale en matière de protection des données, et en particulier en ce qui concerne l'exactitude et la pertinence des données, le principe de finalité, les délais de conservation, la correction des données inexactes, et les droits des personnes concernées.

43. L'article 13 requiert que les parties adoptent des mesures de sauvegarde appropriées pour le traitement des données dites sensibles, à savoir celles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que celles relatives à la santé et à la vie sexuelle**. La Commission sera particulièrement attentive au respect de cette disposition et veillera à sa conformité avec l'article 6 de la LVP.**

44. L'article 16 oblige les parties à tenir une journalisation des accès aux bases de données (fichiers logs), ces fichiers étant conservés pendant un délai de deux ans. La Commission note avec satisfaction que cette mesure permet la traçabilité des accès dans le but notamment, comme le précise d'ailleurs le projet d'Accord PCSC, d'assurer un contrôle effectif de protection des données.

45. Toutefois, la Commission estime que la journalisation des accès aux bases de données serait utilement complétée par une journalisation de chaque communication des données, en ce compris une fois qu'elles ont quitté le PCN. **En d'autres termes, la traçabilité doit aussi pouvoir être effectuée pour les communications entre les autorités nationales. A cette fin, la Commission recommande le libellé suivant [22] :**

> « *All transmissions and receptions of personal data are to be logged or documented. The Contracting Parties shall communicate the list of authorities or services authorized to access the data transferred. The log files must be kept at disposal of the supervisory authority and/or the competent contact body in charge of ensuring data processing as well as data integrity and security*".

46. La Commission recommande l'ajout de deux dispositions supplémentaires dans le corps même de l'Accord PCSC :

— d'une part, une disposition sur les mécanismes de contrôle : ce contrôle doit porter sur l'exploitation *de facto* par une quelconque autorité ou organisme des données transmises, et doit être effectué par des autorités publiques indépendantes.

---

[22] Il s'agit d'une clause (légèrement adaptée *in casu*), tirée des Clauses contractuelles types adoptées en 2009 par le *Working Party on Police and Justice*. Le WPPJ est un Groupe de travail, au sein de la Conférence européenne des Autorités de Protection des Données, dont la mission est de surveiller les développements en matière de coopération policière et judiciaire.

— **d'autre part, une disposition sur le mécanisme d'évaluation de l'Accord PCSC [23] : une telle évaluation devra être effectuée par un comité *ad hoc* dans lequel la Commission souhaite être partie.**

47. Dans la mesure où un Accord général entre l'Union européenne et les Etats-Unis est actuellement en cours de négociation, et que ce futur accord contiendra des principes de protection de données**, la Commission recommande de limiter cet Accord PCSC dans le temps : au moment de l'adoption de l'Accord général, une révision de l'Accord PCSC pourra intervenir s'il s'avère que certaines dispositions de l'Accord PCSC sont en porte-à-faux par rapport à l'Accord général.**

E] les droits des personnes concernées

48. L'article 18 du projet d'Accord PCSC est trop général et doit être développé. **La Commission estime qu'une référence aux droits des personnes concernées tels que consacrés dans le droit national n'est pas suffisante et que l'Accord PCSC doit comprendre dans le corps même du texte, une disposition explicite garantissant le droit d'accès aux personnes concernées.**

49. L'on peut s'inspirer du libellé suivant [24] :

> « *The rights to access the transferred data, to have them rectified and/or erased shall be granted to the individual the data refer to. To this end the Contracting Party before which the said individual invokes this right must have in place specific and accessible procedures enabling him/her to exercise his/her rights*".

50. Le recours judiciaire, qui constitue également un droit pour la personne concernée, ne se retrouve pas dans l'énumération de l'article 18. Pourtant, il fait l'objet d'un commentaire en annexe (faq 2, 7 et 9).

51. La faq 2 précise que, bien que le *Privacy Act* américain ne s'applique pas *de jure* aux citoyens européens, le DHS a adopté cependant une politique donnant *de facto* les mêmes droits d'accès et de correction aux personnes étrangères à la nationalité américaine et dont les données sont traitées dans un système contenant également des données de citoyens américains. La Commission note

---

[23] L'on peut s'inspirer de l'article 13 (réexamen conjoint) de l'Accord du 28 juin 2010 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 (Terrorist Finance Tracking Program – TFTP) (Accord TFTP II, publié au Journal Officiel *L 195 du 27 juillet 2010).*

[24] Il s'agit d'une clause tirée des Clauses contractuelles types adoptées en 2009 par le *Working Party on Police and Justice*. Le WPPJ est un Groupe de travail, au sein de la Conférence européenne des Autorités de Protection des Données, dont la mission est de surveiller les développements en matière de coopération policière et judiciaire.

d'une part que cette souplesse dans l'interprétation de la législation américaine est le résultat d'une décision administrative susceptible de revirement (administratif, judiciaire ou législatif) à tout moment. D'autre part, cette possibilité de recours judiciaire pour les citoyens européens est inexistante lorsque les données de ces citoyens européens sont traitées dans un système spécifique, c'est-à-dire séparé du système dédié aux citoyens américains.

52. La Commission recommande d'inclure explicitement dans le corps du texte de l'Accord PCSC – en se référant le cas échéant au commentaire (faq) annexé – la possibilité pour toute personne concernée de saisir l'autorité judiciaire aux fins de faire respecter ses droits d'accès, de correction et de suppression en matière de protection des données.

PAR CES MOTIFS,

La Commission estime que :

— le projet d'Accord PCSC, s'inspirant du Traité de Prüm du 27 mai 2005, permet le partage d'information (empreintes digitales, profil ADN, autres données) avec les USA moyennant le respect de procédures adéquates (PCN, demande casuistique, correspondance 'hit-no hit') ;

— le projet d'Accord PCSC contient certes certaines dispositions de protection des données, qu'il est toutefois nécessaire de compléter sur plusieurs points : le renvoi explicite à une liste d'infractions, des garanties supplémentaires pour le transfert pour toute autre finalité, la journalisation de tous les transferts de données (internationaux et intranationaux), un mécanisme de contrôle par des autorités indépendantes, un mécanisme de révision et la limitation temporelle d'un tel Accord (vu les négociations européennes actuelles pour un cadre général de ce genre de partage d'information) ;

— les dispositions relatives aux droits des personnes concernées doivent être davantage développées et doivent notamment explicitement prévoir la possibilité de recours aux autorités judiciaires dans le corps même de l'Accord, et non dans un commentaire général et non contraignant annexé à l'Accord PCSC.

Vu les remarques formulées dans le présent avis, la Commission de la Protection de la Vie Privée émet un **avis favorable**, quant au contenu actuel du projet d'Accord PCSC, moyennant le strict respect de ses observations formulées aux **points 26, 32, 37, 41, 43, 45 à 49 et 52** du présent avis.

Pour l'Administrateur e.c., Le Président,

(sé) Patrick Van Wouwe (sé) Willem Debeuckelaere