



Avis n° 25/2012 du 25 juillet 2012

Objet: Avis relatif au projet d'accord de coopération dans le domaine de la sécurité entre la République du Kosovo et le Royaume de Belgique (CO-A-2012-024)

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 la Ministre de l'Intérieur reçue le 25/05/2012;

Vu le rapport de Monsieur Bart De Schutter ;

Émet, le 25 juillet 2012, l'avis suivant :

I. OBJET ET CONTEXTE DE L'AVIS

1. Le 25 mai 2012, le Ministre de l'Intérieur a demandé à la Commission d'émettre un avis concernant le projet d'accord qu'il s'apprête à négocier avec le gouvernement du Kosovo concernant la coopération pénale en matière de sécurité.
2. Cet accord de coopération règlemente la coopération entre les deux États en vue de la lutte contre certaines infractions et contient essentiellement des dispositions portant sur l'échange d'informations entre les deux parties concernant la recherche et la poursuite d'infractions pénales.

II. Les principes applicables en matière de transferts internationaux et de coopération policière et judiciaire

A. Le cadre européen

3. En ce qui concerne la coopération policière et judiciaire en matière pénale, il convient de se référer à la décision-cadre 2008/977/JAI du 27 novembre 2008¹ et à la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (« la LVP »).
4. 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'État tiers concerné assure un niveau de protection adéquat pour le traitement de données envisagé.
5. 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.
6. 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

¹ Décision-cadre 2008/977/JAI du Conseil européen 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*.

décision-cadre – qui énumère les compétences des ACN –, cette compétence ne soit pas dévolue aux Autorités de Contrôle Nationales de protection des données (ACN).

7. Lorsqu'un pays tiers ne bénéficie pas d'une reconnaissance d'adéquation, l'article 13, § 3, d) de cette décision-cadre trouve à s'appliquer : par dérogation au principe de transfert de données vers un État tiers assurant un niveau de protection adéquat, les données à caractère personnel peuvent toutefois être transférées si l'État tiers prévoit des garanties qui sont jugées adéquates par l'État membre concerné conformément à sa législation nationale.
8. Remarquons que le champ d'application de la décision-cadre se limite aux données échangées entre États membres dans le cadre de la coopération policière. Toutefois, les États membres se proposent que le niveau de protection des données atteint pour le traitement de données à l'échelon national corresponde à celui prévu par la décision-cadre.² Dès lors, la Commission recommande que tout traitement de données rentrant dans les finalités de la décision-cadre (prévention, détection des infractions pénales, enquête et poursuite en la matière, exécution des sanctions pénales) adopte au minimum le niveau de protection prévu par la décision-cadre.

B. Le cadre belge

9. 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.
10. Les critères dégagés par l'article 21, § 1, 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.
11. L'effectivité réelle des normes légales (c'est-à-dire le moyen d'assurer leur application efficace, comme par exemple la connaissance des décisions des autorités, le suivi de la jurisprudence, l'existence d'un système de contrôle et de sanctions, ...) fait également partie des critères d'analyse.

² Voir considérants 7 et 8 de la décision-cadre.

12. Par conséquent, si l'analyse des lois nationales est nécessaire pour effectuer une évaluation du caractère adéquat du niveau de protection d'un pays tiers à la Communauté européenne, cet examen n'est, en soi, pas suffisant.
13. L'article 21, § 2 de la loi vie privée permet au Roi, après avis de la Commission, de déterminer pour quelles catégories de traitements de données à caractère personnel et dans quelles circonstances la transmission de données à caractère personnel vers des pays non-membres de la Communauté européenne n'est pas autorisée.
14. Eu égard à l'article 21 de la LVP, et pour ce qui concerne la coopération policière et judiciaire internationale, la Commission souligne qu'elle peut seulement : soit émettre un avis sur les principes fondamentaux de protection des données contenus dans une législation particulière (en sachant que cette analyse n'est pas suffisante à la lumière de l'article 21, § 1^{er} alinéa 2 de la LVP), soit émettre un avis sur un projet d'adéquation (dont l'ensemble des critères ont été analysés par le Roi) en vertu de l'article 21, § 2 de la LVP.
15. Lorsqu'un pays tiers, tel le Kosovo, ne bénéficie pas de la reconnaissance de l'adéquation, il convient d'appliquer les dérogations listées à l'article 22 de la LVP, qui permettent sous certaines conditions le transfert de données vers un pays non membre de la Communauté européenne et dont le niveau de protection adéquat n'a pas été reconnu.
16. En particulier, l'article 22, § 1^{er}, 4^o de la LVP permet le transfert lorsque celui-ci « est rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important ».
17. En application de cet article, La Commission, comprenant la nécessité de flux de données entre le Kosovo et la Belgique, estime que ces données peuvent néanmoins être transférées en vertu de l'accord de coopération – et sa loi d'assentiment à venir – entre la Belgique et le Kosovo.
18. 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 de coopération comporte plusieurs références au droit national et qu'il est difficile pour la Commission

d'appréhender la législation kosovare en matière de protection des données faute de pouvoir contrôler son effectivité réelle.

19. Cette démarche a également été suivie par la Commission européenne lors de l'organisation de divers transferts de données à caractère personnel à destination d'autorités américaines³, ou encore de l'accord de coopération du 6 mai 1999 entre la Belgique et le Maroc relatif à la lutte contre la criminalité organisée.⁴
20. Dans le cas d'espèce, les garanties particulières peuvent être apportées par les services kosovars destinataires des données, et se retrouver dans une législation ou règlement particulier, dans un Protocole d'Implémentation⁵, ou figurer au sein même de l'accord de coopération. Le présent avis en fait l'analyse ci-dessous.
21. 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 listées dans son Annexe A 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 (c'est-à-dire vers un pays non membre de la Communauté européenne et n'assurant pas un niveau de protection adéquat).

III. Le projet d'accord de coopération

A. Champ d'application et objet de la coopération

22. L'article 3 dispose que les parties vont coopérer « to prevent and solve organized and serious crimes and terrorism ». Cette formulation semble indiquer que seuls ces délits pourront donner lieu à la coopération qui fait l'objet de l'accord. Une liste des délits visés est dressée, tout en précisant que la coopération sera particulièrement souhaitable

³ Par exemple dans le cadre du transfert de données de la société Swift : « Traitement par le Département du Trésor des États-Unis (US Treasury – UST), aux fins de la lutte contre le terrorisme, de données à caractère personnel provenant de l'UE » (publié au JOUE du 20 juillet 2007, page C 166/18). Voir aussi pour les données PNR (Passengers Name Records) : lettre des USA (ministère de la sécurité intérieure – Department of Homeland Security – DHS) à l'Union Européenne (publiée au JOUE du 4 août 2007, page L 204/21).

⁴ Avis n°22/2009 du 2 septembre 2009 relatif à la compatibilité de la loi marocaine avec la loi vie privée dans le cadre de la procédure de ratification de l'Accord de coopération du 6 mai 1999 entre le Royaume de Belgique et le Royaume du Maroc relatif à la lutte contre la criminalité organisée.

⁵ Article 7 du projet d'accord.

lorsque les délits impliquent potentiellement ou effectivement les deux parties contractantes. Plusieurs remarques peuvent être formulées à cet égard.

23. Tout d'abord, les termes utilisés pourraient davantage se rapprocher de ceux que contient la décision-cadre 2008/977/JAI, laquelle utilise les termes « prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties » dans son article 1.2. Remarquons que la décision-cadre n'empêche pas l'adoption d'autres accords bilatéraux avec des pays tiers. Toutefois, la Commission recommande une harmonisation des termes employés en matière pénale et judiciaire pour une plus grande cohérence des textes régissant la matière.
24. En deuxième lieu, la liste des délits qui peuvent donner lieu à la coopération n'est pas fermée. En effet, l'article 1 (2) du projet d'accord dresse une liste de délits graves qui donneront lieu à coopération en précisant que cette liste est exemplative. À défaut d'une liste exhaustive, les échanges de données dans le cadre de l'accord de coopération risquent de ne pas être limités à certains délits. La Commission recommande à cet égard de décrire plus clairement les catégories d'infractions pour lesquelles la coopération est autorisée.
25. L'article 1 (3) permet la coopération policière et judiciaire entre les deux parties *en particulier* lorsqu'un délit est commis ou préparé sur le territoire d'une des parties, et qu'il existe des éléments montrant que le délit en question est susceptible d'affecter l'autre partie contractante ou de menacer sa sécurité. La Commission estime qu'il convient de limiter les hypothèses où l'accord de collaboration peut être mis en œuvre. Elle recommande donc de supprimer le terme « in particular », ou de clarifier le champ d'application du projet d'accord sur ce point.⁶

B. Les demandes et transmissions d'information

a) La référence aux règles internes

26. Le projet d'accord prévoit que les demandes d'informations seront transmises par écrit, ou parfois même oralement dans les cas urgents, par l'autorité compétente de l'État

⁶ À cet égard, on peut citer à titre d'exemple le dernier accord PNR entre l'Union Européenne et les États-Unis, qui stipule qu'une infraction est notamment considérée comme de nature transnationale:

i) si elle est commise dans plus d'un pays; ii) si elle est commise dans un seul pays, mais qu'une part importante de sa préparation, de sa planification, de sa conduite ou de son contrôle a lieu dans un autre pays; iii) si elle est commise dans un seul pays, mais implique un groupe criminel organisé qui est engagé dans des activités criminelles dans plusieurs pays; iv) si elle est commise dans un seul pays, mais a des répercussions importantes dans un autre pays; ou v) si elle est commise dans un seul pays et si l'auteur de l'infraction se trouve dans un autre pays ou a l'intention de se rendre dans un autre pays.

requérant à l'autre partie. Cette dernière délivrera l'information par l'intermédiaire de son autorité compétente, conformément au droit interne (voir article 4 du projet d'accord).

27. En Belgique, la circulaire 2/2000 des procureurs généraux près les Cours d'appel concernant la coopération policière internationale à finalité judiciaire règle la manière dont les autorités policières envoient les informations aux autorités compétentes d'un autre État. Toutefois, la Commission n'a pas connaissance de règles similaires en matière de communication d'informations par un service public fédéral tel que le SPF Finances ou le SPF Affaires étrangères.
28. Or, l'établissement de règles et principes clairs et transparents encadrant la manière dont les autorités compétentes en Belgique communiquent des informations à d'autres autorités étrangères est primordial pour assurer un niveau de protection maximal des données transmises, la sécurité de cette communication et la transparence à l'égard des citoyens et des individus. Dès lors, la Commission recommande l'établissement, au sein des services publics concernés, de règles similaires à celles en vigueur au sein des autorités de police pour la coopération internationale. Toutefois, dans la mesure où les données et renseignements de Services publics fédéraux tels que le SPF Finances ou le SPF Affaires étrangères sont repris dans une information ou une instruction, la Circulaire COL 2/2000 est quoi qu'il en soit d'application.
29. La Commission constate également que le projet d'accord prévoit que les requêtes seront transmises en anglais ou en suédois, ou dans toute autre langue convenue par les parties (article 4 (2) du projet d'accord). Il semble que le choix du suédois ne soit pas le plus approprié dans ce cas, dès lors que cette langue n'est une langue officielle dans aucun des deux États parties à l'accord. L'usage de l'anglais semble donc la langue la plus indiquée pour s'assurer que les demandes d'informations soient bien comprises et traitées par l'État recevant la requête.

b) Les transferts ultérieurs à des tiers

30. L'article 4 (4) du projet d'accord prévoit que toute information transmise par une autorité compétente ne pourra être communiquée à des tiers sans le consentement de la partie qui a transmis l'information.
31. Cette disposition appelle plusieurs commentaires. Dans un premier temps, la Commission constate que la définition de tiers est peu claire. Il est difficile de savoir si le

texte vise par là un autre État, ou d'autres entités ou personnes que les autorités compétentes désignées par l'article 6 du projet d'accord, ou d'autres autorités compétentes désignées par le projet d'accord que celles initialement désignées dans la demande d'informations. Pour ces raisons, la Commission demande que le projet d'accord décrive clairement ce qu'il y a lieu d'entendre par « tiers ».

32. En outre, l'article 5 (3) précise que les informations échangées ne pourront pas être utilisées dans le cadre d'une assistance mutuelle en matière pénale sans le consentement de l'État ayant communiqué les informations. La Commission comprend que ce mécanisme empêche les transferts ultérieurs de données obtenues par une des parties vers un autre État avec qui existerait un accord d'assistance mutuelle en matière pénale. Cette interdiction est conforme à l'interdiction de détournement de finalité et interdit les transferts ultérieurs des informations à d'autres entités non mentionnées dans le projet d'accord.
33. La Commission recommande néanmoins que le projet d'accord rende compte de manière plus générale du principe d'interdiction de détournement de finalité et de transferts ultérieurs. Ainsi, il devrait être précisé que seront interdits toute utilisation non prévue par l'accord et tout transfert à une autorité ou instance autre que celle qui a reçu l'information, sauf consentement de l'État ayant fourni l'information.
34. À ce titre, il conviendrait de rappeler les termes de l'article 26 de la décision-cadre 2008/977/JAI, qui stipule que le transfert à un État tiers de données collectées auprès d'un autre État membre est réalisé dans le respect de l'article 13, 1, c) ou 13, 2 selon le cas. Les deux hypothèses auxquelles renvoie cette disposition sont les suivantes :
 - L'État membre ayant communiqué ses données a donné son accord préalable ;
 - Le transfert de données est réalisé pour prévenir un danger immédiat et sérieux pour la sécurité publique d'un État membre ou d'un État tiers ou pour les intérêts essentiels d'un État membre et que l'accord préalable ne peut pas être obtenu en temps utile.
35. La première hypothèse recouvre celle déjà mentionnée dans le projet d'accord. Cependant, ce dernier se limite au transfert d'informations dans le cadre d'assistance mutuelle en matière pénale. Il conviendrait donc de supprimer cette limitation, qui n'existe en effet pas dans la décision-cadre 2008/977/JAI. Les transferts ultérieurs de données vers d'autres États ou entités devraient être interdits sauf accord de l'État ayant fourni l'information.

36. La seconde hypothèse, qui permet un transfert dans des circonstances où cela est nécessaire par un intérêt impérieux, n'est pas inscrite dans le projet d'accord. La Commission invite les négociateurs à inclure cette hypothèse, non seulement parce qu'il y a de bonnes raisons opérationnelles de le faire mais aussi pour des raisons de cohérence avec les dispositions de la décision-cadre précitée.

C. Les principes relatifs au traitement de données

37. La Commission constate que plusieurs principes de la LVP mais également la décision-cadre 2008/977/JAI sont repris dans le projet d'accord de coopération examiné.
38. Sans préjudice de la recommandation de la Commission au point 33 ci-dessus, le principe de finalité est repris dans l'article 8, aux points 1 et 2, lesquels prévoient que les finalités doivent être annoncées au préalable par les autorités compétentes qui reçoivent l'information, et que celle-ci ne peut être utilisée que pour les finalités annoncées à l'avance.
39. En outre, le principe de qualité des données, est confirmé par l'article 8.3, lequel commande que les données communiquées soient correctes, et que leur communication soit nécessaire à la finalité poursuivie. Leur conservation ne peut dépasser la durée nécessaire à la finalité de la communication (article 8.6). L'État ayant communiqué les données doit également informer l'État recevant ces dernières d'une éventuelle durée de conservation maximum prévue dans sa législation nationale.
40. Le principe de dédommagement des individus pour usage illicite de leurs données est également prévu dans le projet d'accord. La Commission recommande de vérifier auprès de l'autorité Kosovare ou des instances publiques l'existence d'une possibilité d'obtenir un tel dédommagement. Un tel recours juridictionnel existe en Belgique en application de l'article 20 de la décision-cadre 2008/977/JAI.
41. L'article 8.4 prévoit que les personnes concernées auront un droit d'accès, qu'elles pourront exercer en vertu du droit national. Un tel accès indirect est déjà prévu par l'article 13 de la LVP, et s'effectue auprès de la Commission, qui interroge les services de police sur l'existence d'informations sur la personne concernée, sans préjudice des compétences des autorités judiciaires.

42. L'accord ne prévoit cependant pas de droit et d'obligation de rectification, de suppression ou de verrouillage des données. Ces droits sont prévus par la décision-cadre 2008/977/JAI⁷ et permettent aux personnes concernées de s'adresser soit au responsable du traitement soit à une autorité de contrôle nationale (ACN) pour s'assurer de l'effectivité de ces droits. La Commission recommande qu'un mécanisme de vérification soit inséré dans le projet d'accord de coopération permettant à une autorité nationale (par exemple, la Commission) de vérifier, sans préjudice des compétences des autorités judiciaires, que les droits de rectification, de suppression et de verrouillage des personnes concernées soient respectés.
43. L'article 8.7 prévoit qu'une journalisation des envois et réceptions des données devra être effectuée. Conformément à l'article 10 de la décision-cadre 2008/977/JAI, cette journalisation est effectuée à des fins de vérification de la licéité des informations communiquées, d'autocontrôle et de garantie de l'intégrité et de la sécurité des données. La Commission demande que le projet d'accord prévoie que cette documentation de journalisation soit mise à disposition de la Commission ou d'une autre autorité de contrôle compétente à des fins de contrôle.
44. Une obligation de sécuriser les données est également prévue par l'article 8.8, qui oblige les États à adopter des mesures de sécurité contre l'accès, la modification ou la divulgation non autorisés des données. Cette obligation pourrait être précisée, par exemple dans un protocole d'implémentation tel que prévu à l'article 7, en s'inspirant des principes décrits dans la décision-cadre 2008/977/JAI et plus particulièrement son article 22. La Commission recommande également, outre cette précision, que soit décrite la manière donc la sécurité de la communication des informations sera assurée. En effet, aucune disposition ne précise selon quelles modalités techniques les informations seront communiquées d'une autorité compétente à une autre.

PAR CES MOTIFS,

La Commission estime qu'en vertu d'un accord tel que celui qui lui a été demandé d'examiner, le transfert de données à caractère personnel peut s'effectuer vers le Kosovo du fait qu'il est « rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important » (article 22, § 1, 4° de la LVP).

⁷ Articles 4, 5 et 18.

Par conséquent, la Commission émet un **avis favorable** quant à l'accord de coopération policière entre la Belgique et le Kosovo, pour autant que les recommandations développées aux points 23, 24, 25, 28, 29, 31, 33, 35, 36, 40, 42, 43, 44, et 45 soient prises en considération pour la négociation de la version finale de l'accord de coopération.

L'Administrateur f.f.,

Le Président,

(sé) Patrick Van Wouwe

(sé) Willem Debeuckelaere