



Audition publique de la Commission des Libertés civiles, de la justice et des affaires intérieures - Parlement Européen - le 07 mai 2007

**« La Décision Prüm : Trouver un équilibre entre la protection des données et une coopération policière efficace »**

**Intervention de M. Georges de La Loyère**

Commissaire de la CNIL pour les Affaires internationales – Groupe article 29

Nous avons effectivement assisté à la montée en puissance de ce Traité de Prüm de droit international, adopté en dehors du cadre de l'Union européenne, entre les 7 pays signataires, et qui instaure un mécanisme d'échanges d'informations et de données d'identification biométriques sans précédents.

Les autorités de protection des données des pays signataires de Prüm se sont saisies de ce Traité analysant l'ensemble des aspects protection des données. Le travail de ce groupe des autorités de protection des données a débouché sur l'adoption de deux documents :

- **un avis en date du 27 juillet 2006 sur le Traité de Prüm** qui sollicite le réexamen d'un certain nombre de dispositions du Traité à préciser dans l'accord d'exécution
- ainsi **qu'une note technique rédigée par les services de l'expertise informatique de la CNIL, en date du 17 août 2006, sur la version avancée de l'accord technique d'application, qui formule des recommandations précises pour garantir la protection et la sécurité des données et des échanges.**

Ces deux documents ont été transmis au groupe de rédaction juridique des gouvernements (Legal drafting team) chargé de rédiger les termes du Traité et de compléter l'accord d'exécution.

Or nous n'avons pas d'éléments probants, à ce jour, nous permettant de constater une prise en compte de nos remarques et recommandations de fond destinées à renforcer le niveau de protection.

Dans le processus de ratification du Traité, notre autorité française de protection des données, la CNIL, a été consultée par le gouvernement Français en Août 2006 sur le projet de loi autorisant la ratification du Traité. La marge de manœuvre pour notre autorité étant fort limitée sur un Traité déjà signé, la CNIL a néanmoins **présenté une délibération en ligne avec celle adoptée avec ses homologues européens, qui souligne les insuffisances, les imprécisions du Traité et le niveau des garanties à renforcer.**

*- La France, à ce jour, n'a pas achevé son processus de ratification ; il a été adopté par le Sénat le 21 février 2007 et attend d'être présenté à l'Assemblée nationale une fois que la nouvelle législature en place-*

C'est au regard de cette première évaluation que nos autorités européennes de protection des données, portent un avis sur les dispositions de **la proposition de décision du Conseil** qui transpose les "parties essentielles" de Prüm et reprend notamment, l'intégralité du chapitre relatif à la protection des données (chapitre 6).

Dans le cadre de cette audition du Parlement Européen qui nous en donne l'opportunité, nous sommes intéressés à reformuler clairement afin d'être bien compris, les termes de l'enjeu de cette législation Prüm :

D'une part, il n'est pas question que l'on nous suspecte, nous autres, autorités de protection des données, d'empêcher les échanges de données entre Etats membres de l'Union Européenne.

**Renforcer la sécurité des citoyens européens, à travers une coopération policière efficace et opérationnelle pour lutter contre la criminalité transfrontière, aussi efficace que possible, tout en maintenant un niveau élevé de protection de leurs droits fondamentaux, en particulier de leurs droits sur leurs données personnelles, constitue aujourd'hui un objectif essentiel.**

**L'ensemble de nos autorités européennes de protections des données considèrent même que, loin d'en être diminuée, l'efficacité de la coopération dans ce domaine sera renforcée par l'existence d'un ensemble de règles garantissant la transparence des traitements de données mis en œuvre, la pertinence et la fiabilité des informations échangées. De telles règles constituent la condition de la confiance entre le citoyen et l'Etat, entre le citoyen et l'Europe, entre les Etats de l'Europe. Un niveau élevé de protection s'appliquant à tous les pays de l'Union européenne ne peut être un frein aux échanges nécessaires et à leur efficacité.**

**En revanche, dans ce processus, on peut souligner et déplorer lors des négociations d'origine du Traité de Prüm, qui fait référence aujourd'hui, l'absence de consultation de nos autorités de protection des données. Même si nos collègues de l'autorité allemande ont été les seuls à être associés dans les débuts à cette négociation, les termes finaux de ce texte qui a subi de fortes évolutions n'a, de toute évidence, pas pris en compte un certain nombre de propositions destinées à renforcer le niveau de protection. Même si le Traité de Prüm comporte effectivement, un certain nombre de garanties importantes sur le plan de la protection des données, contenues essentiellement dans le chapitre spécifique.**

Remarque liminaire : l'adoption de la décision cadre de protection des données dans le troisième pilier devrait être un préalable à l'adoption de la décision Prüm

Néanmoins, je tiens à souligner que dans le secteur très actif de la coopération policière transfrontière organisée dans le troisième pilier, nous sommes confrontés aujourd'hui encore, à la création d'une nouvelle législation spécifique d'envergure **marquée par l'absence d'une norme spécifique de protection des données harmonisée et à haut niveau.**

Compte tenu des enjeux de protection des données dans le cadre de tels partages de données à caractère personnel qui sont stockées dans des fichiers nationaux, échangés, soumis à traitements voire à transferts ultérieurs, là justement où les mécanismes diffèrent d'un pays à l'autre, nous estimons que la référence à *la Convention du Conseil de l'Europe du 28 janvier 1981, au protocole additionnel du 8 novembre 2001, et à la Recommandation n° R (87) 15 du Comité des ministres du Conseil de l'Europe aux Etats membres relative à l'utilisation de données à caractère personnel dans le domaine policier du 17 septembre 1987, est nettement insuffisante.* **Il apparaît que seule l'adoption de l'instrument de décision-cadre dans le troisième pilier, pourrait créer un niveau suffisamment élevé et uniforme de garanties en Europe.**

Sur les finalités : les définir strictement

- Au regard des modalités d'échange et de consultation des données génétiques ou dactyloscopiques mises en place, nos autorités tiennent à rappeler que l'accès aux données biométriques doit être suffisamment encadré afin de ne pas excéder les finalités de prévention et lutte contre les infractions pénales.

- Sur les échanges de données réalisées à des fins de maintien de l'ordre et de sécurité publics (articles 12, 14 et 16), le texte est trop imprécis sur ces aspects.

En effet, s'agissant de la consultation automatisée de données dans les registres d'immatriculation de véhicules, (visée à l'article 12), il apparaît impératif **de clarifier les finalités pour lesquelles l'accès aux données du registre des véhicules et la recherche automatisée peuvent être autorisée,** compte tenu de la portée très large de l'objectif de maintien de l'ordre et de la sécurité publique.

## Sur la typologie des données à caractère personnel : bien trop d'imprécisions

- Il nous apparaît tout d'abord indispensable de préciser que **toutes les données traitées dans le cadre de ce texte**, à l'exception éventuellement, des données visées à l'art 13, supposées traiter les informations non personnelles relatives aux événements de grande envergure, **constituent des données personnelles**, y compris les bases de données qui ne contiennent que les profils ADN et les données d'index.

- de même, il serait utile de rappeler ce que l'on entend par « une donnée à caractère personnel ». A cet égard, il pourrait être fait référence à la définition des données à caractère personnel qui figure dans la Directive 95/45/CE du 24 octobre 1995<sup>1</sup>.

- il conviendrait également de **définir les catégories de données visées** respectivement aux articles 5, (la transmission d'autres données à caractère personnel), 10 (d'autres données à caractère personnel), ainsi que « **les données à caractère non personnel** » visées à l'article 13, afin de vérifier le caractère non personnel de ces données.

- il serait utile de définir la notion « *de manifestation de grande envergure à dimension transfrontalière* », en particulier dans le domaine sportif ou en rapport avec des réunions du Conseil européen » (visée à l'art 14) car toute manifestation internationale d'envergure ne justifie pas le transfert de données et il est essentiel de pouvoir porter une appréciation au regard du principe de proportionnalité.

- Par ailleurs, il est question à l'article 27 de transmission des données à caractère à « d'Autorités compétentes » selon une procédure d'accord préalable, il nous paraît essentiel de clarifier et encadrer cette notion ouverte d'autres autorités.

## Sur les garanties complémentaires à prévoir

- En matière de consultation automatisée de profils ADN (article 3 ) et pour la transmission d'autres données à caractère personnel et d'autres informations en complément des données d'ADN (art 5), il y aurait lieu de **préciser que toute transmission de données à la partie nationale requérante, devrait être précédée d'une motivation de sa demande. Il s'agit d'une condition essentielle afin de pouvoir vérifier, dans le cadre des contrôles de nos autorités, le bien fondé de la demande.**

- En ce qui concerne la transmission de données lors de manifestations d'envergure (article 14), la définition de **catégories de personnes considérées comme suspectes dont les données pourraient être transmises** est très large ou à tout le moins insuffisamment précise : « *lorsque des condamnations définitives ou d'autres circonstances font présumer que les personnes concernées vont commettre des infractions pénales dans le cadre de ces manifestations ou qu'elles présentent un danger pour l'ordre et la sécurité publique* ».

- Cette même demande de précision doit s'appliquer **s'agissant des personnes suspectes** (visées à l'article 16) dont les données sont susceptibles d'être transmises dans le cadre de la lutte anti-terroriste.

## Dans le chapitre spécifique consacré à la protection des données (chapitre 6)

- je voudrai souligner une situation qui mérite d'être explicitée car sa formulation paraît ambiguë : A l'article 28 consacré à « l'exactitude, l'actualité et la durée de stockage des données », le paragraphe (3) prévoit, en son premier alinéa que « *si des données à caractère personnel ont été*

---

<sup>1</sup> «données à caractère personnel»: toute information concernant une personne physique identifiée ou identifiable (personne concernée); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale ».

*transmises sans qu'il y ait eu de demandes l'autorité destinataire est tenue d'examiner sans délai si celles-ci sont nécessaires au regard des finalités pour lesquelles elles ont été transmises* ». **Les situations visées par cette disposition mériteraient d'être explicitées.**

- A l'article 30 « Documentation et journalisation, dispositions particulières relatives à la transmission automatisée et non-automatisée », il est prévu que « *les autorités indépendantes compétentes en matière de contrôle des données* » assurent le contrôle juridique de la transmission et de la réception des données à caractère personnel. **Les modalités d'information de ces autorités sur la journalisation, leur transmission, leur réception nécessiteraient d'être clarifiées, afin de permettre aux autorités de protection des données d'assurer leurs contrôles de façon efficaces.**

Il apparaît également nécessaire de préciser ce que sont ces « contrôles aléatoires », prévus dans le même article.

- De plus, cette obligation ne devrait pas seulement lier les autorités de protection des données mais également les responsables de traitement ; ces contrôles n'ayant de sens que si les résultats sont communiqués au responsable de traitement.

- Enfin, dans la mesure où l'exercice par les autorités de protection des données de leur contrôle sur ces échanges de données, nécessitera la mise en place d'une coopération institutionnalisée, un soutien matériel devrait leur être apporté par leurs gouvernements respectifs.

- Sur la question du droit des personnes concernées d'être informées et indemnisées (article 31) : cette disposition de la décision reconnaît à toute personne le droit d'accéder au traitement pour obtenir, le cas échéant, une mise à jour des données les concernant lorsque les données sont erronées. Néanmoins, le dispositif prévoit de renseigner la personne **dès lors que celle-ci a prouvé son identité et sans que cela entraîne de frais déraisonnables ni de retard déraisonnable.**

Sur ce point, nous estimons que le droit d'information des personnes constitue un droit fondamental des personnes qui doit être réaffirmé sans ambiguïté ni conditions suspensives. Ce principe devrait même être rappelé dans l'exposé des motifs de la décision.

- Par ailleurs, dans la mesure où les données d'une personne effectuant une requête, peuvent figurer dans les fichiers de plusieurs ou de toutes les parties contractantes, le requérant ne doit pas avoir à établir lui-même le lien avec toutes les autorités compétentes des pays contractants : il appartient à l'organisme contacté par la personne concernée d'assurer la coordination en coopération avec les autres autorités des parties contractantes. **Ce point pourrait utilement être précisé dans le texte de la décision Prüm.**

**En conclusion, je suis conscient du risque que la plupart de ces préconisations, très précises, peuvent donner l'impression à l'auditeur d'être excessivement précautionneuses. Ne parlons-nous pas de points de détail? Ne sommes-nous pas excessifs dans nos remarques? Au fond, les autorités de protection des données ne sont-elles irréalistes?**

La réponse à ces questions doit bien évidemment être négative. Il ne s'agit pas, encore une fois, d'empêcher les services police et de justice pénale de travailler correctement. Les autorités de protection des données sont composées de citoyens qui comprennent, tout autant que les autres, l'importance de l'échange et du partage d'informations entre les autorités de police et de justice, en particulier pour des crimes graves ou des événements de grande ampleur. Mais ne nous y trompons pas: une disposition imprécise ou floue peut avoir des conséquences graves pour les personnes concernées, comme pour les autorités qui appliquent le texte. Dans des domaines aussi sensibles, la concision du langage, la délimitation précise du périmètre des dispositions sont des exigences fondamentales, qui ne peuvent être traitées à la légère.

La défense des libertés se joue aussi dans le traitement du détail. Comme le disent nos amis anglais : "the devil is in the detail".

C'est pourquoi les autorités de Protection des données DP invitent avec insistance la Présidence du Conseil, les Etats membres et la Commission à prendre en compte les avis et positions qu'elles ont exprimées. Il semble aujourd'hui indispensable, non pas d'accélérer la prise de décision, mais au contraire de renforcer les échanges et les consultations sur ce texte, afin que ce texte gagne en légitimité, dans un domaine fondamental pour la défense de la sécurité, de la liberté et de la justice des citoyens dans l'Union Européenne.