



COMMUNIQUÉ DE PRESSE

EDPS/2013/08

Bruxelles, vendredi 19 juillet 2013

‘Frontières intelligentes’: la proposition clé est coûteuse, insuffisamment justifiée et intrusive

Selon l'annonce faite aujourd'hui par le Contrôleur Européen de la Protection des Données (CEPD), il n'y a **pas d'indications claires** selon lesquelles les Propositions de la Commission visant à créer un système de **frontières intelligentes** pour les frontières extérieures de l'UE atteindront l'objectif poursuivi. Suite à la publication de son avis qui met en particulier l'accent sur le **système Entrée/Sortie**, le CEPD note que l'un des objectifs annoncés dans les Propositions est de remplacer le système existant, 'lent et non fiable', alors que les estimations de la Commission elle-même ne permettent pas d'affirmer que l'alternative sera suffisamment efficace pour **justifier la dépense** et les **intrusions dans la vie privée**.

Peter Hustinx, CEPD, ajoute: "*Améliorer la gestion des contrôles aux frontières est un exercice légitime. Mais il serait **plus efficace** de le faire lorsqu'une politique européenne claire de gestion des 'over stayers' (individus qui dépassent la durée du droit de séjour) aura été établie. En l'absence d'une telle politique, la création d'une nouvelle base de données IT à grande échelle pour stocker des quantités massives de données personnelles est une réponse **disproportionnée** à un problème que d'autres systèmes créés récemment pourraient être à même de résoudre. Il serait **prudent**, d'un point de vue à la fois économique et pratique, d'évaluer les systèmes **existants** afin, au minimum, de garantir **cohérence** et **bonnes pratiques**.*"

Le système "Entrée/Sortie" proposé se fonde sur l'utilisation de données **biométriques**, à savoir les dix empreintes digitales, pour vérifier l'identité des individus au passage de la frontière et calculer ainsi la durée du séjour des résidents des pays tiers. Le CEPD questionne la **nécessité**, dans une **société démocratique**, de collecter et stocker une telle quantité de données personnelles, en particulier quand deux ou quatre empreintes digitales seraient suffisantes dans un but de vérification.

Alors que les autorités répressives pourraient éventuellement se voir accorder l'accès à la base de données après une période d'évaluation qui courrait à compter de l'entrée en vigueur du système, il apparaît que les propositions **anticipent** un tel accès, avant que la nécessité de **l'intrusion** dans la vie privée des individus soit effectivement démontrée. La **tendance générale** qui est de donner accès aux autorités répressives aux données d'individus qui ne sont a priori coupables d'aucun crime est **dangereuse**. Le CEPD recommande fermement que la **valeur ajoutée** précise d'un tel accès, comparé à l'accès aux bases de données biométriques existantes, soit **identifiée**.

Le CEPD insiste également pour qu'une attention particulière soit portée aux **conséquences juridiques** des procédures qui seront **automatiquement** mises en œuvre aux frontières. Par exemple, le système calculera automatiquement la durée de séjour d'un visiteur, mais il n'y a pas de prise en compte satisfaisante du traitement des erreurs dues à l'automatisation, à savoir, par exemple, l'impossibilité d'enregistrer correctement la sortie d'un individu parce qu'il suit un traitement médical ou en raison de problèmes techniques du système. De plus, les personnes doivent être informées de façon complète et en temps utile de toute décision défavorable les concernant, afin qu'elles soient à même d'exercer leurs droits. Ceci est

d'autant plus **important** que la multiplication des bases de données dans le secteur de la gestion des frontières (telles que VIS, SIS, CIS, EURODAC) **complique** de plus en plus l'exercice de leurs **droits** par les individus.

Enfin, le fonctionnement habituel du système impliquera un besoin d'**échanger** des données personnelles avec des pays tiers, dans le cadre du retour des personnes concernées dans leur pays d'origine. Le CEPD recommande par conséquent que les conditions et objectifs **spécifiques** en vertu desquels ces pays pourraient obtenir confirmation de leur identité soient étayés, d'autant plus que de nombreux pays tiers n'offrent pas le même **niveau** de protection des données personnelles que celui offert par **l'UE**.

Contexte

Le 28 février 2013, la Commission a adopté:

- Une Proposition de règlement du Parlement Européen et du Conseil portant création d'un système d'entrée/sortie pour l'enregistrement des entrées et sorties des ressortissants de pays tiers franchissant les frontières extérieures des États membres de l'Union européenne.
- Une Proposition de règlement du Parlement Européen et du Conseil portant création d'un programme d'enregistrement des voyageurs.
- Une Proposition de règlement du Parlement Européen et du Conseil modifiant le règlement (CE) no 562/2006 en ce qui concerne l'utilisation du système d'entrée/sortie (EES) et le programme d'enregistrement des voyageurs (RTP).

Le même jour, les propositions ont été envoyées au CEPD pour consultation. Le CEPD avait préalablement communiqué ses commentaires informels à la Commission avant l'adoption des propositions.

Le respect de la vie privée et la protection des données sont des droits fondamentaux dans l'UE. Dans le cadre du règlement sur la protection des données (CE) n° 45/2001, l'une des fonctions du CEPD est de conseiller la Commission européenne, le Parlement européen et le Conseil sur les propositions de nouvelle législation et un large éventail d'autres questions qui ont un impact sur la protection des données. En outre, les institutions et organes de l'UE traitant des données personnelles qui présentent des risques particuliers pour les droits et les libertés des individus sont soumis à un contrôle préalable par le CEPD. Si, de l'avis du CEPD, le traitement notifié risque d'entraîner une violation d'une disposition du règlement, il doit faire des propositions afin d'éviter une telle violation.

Données personnelles: toute information concernant une personne physique identifiée ou identifiable. Les exemples sont le nom, la date de naissance, les photographies, les adresses e-mail et les numéros de téléphone. D'autres informations telles que les données de santé, les données utilisées à des fins d'évaluation et les données d'utilisation du téléphone, de l'e-mail ou de l'Internet sont également considérées comme des données personnelles.

Respect de la vie privée: droit d'un individu à être laissé seul et à contrôler l'information le concernant. Le droit à la vie privée est consacré par la Déclaration universelle des Droits de l'Homme (article 12), la Convention européenne des Droits de l'Homme (article 8) et la Charte européenne des Droits fondamentaux (article 7). La Charte contient également un droit explicite à la protection des données à caractère personnel (article 8).

Privacy by design: concept qui promeut l'intégration de la protection des données dès la conception et la définition de l'architecture des systèmes et technologies de l'information et de la communication, afin de se conformer aux principes de respect de la vie privée et de la protection des données.

Limitation de la finalité: les données personnelles ne peuvent être collectées qu'à des fins déterminées, explicites et légitimes. Une fois collectées, elles ne peuvent être traitées de manière incompatible avec ces finalités. Le principe est conçu pour protéger les individus en limitant l'utilisation de leurs données à des fins prédéfinies, sauf dans des conditions strictes et avec des garanties appropriées.

Le Contrôleur européen de la protection des données (CEPD) est une autorité de contrôle indépendante dont l'objectif est de protéger les données à caractère personnel et la vie privée et de promouvoir les bonnes pratiques dans les institutions et organes de l'UE. À cet effet, il remplit les tâches suivantes:

- contrôler les traitements de données à caractère personnel effectués par l'administration de l'UE;
- donner des conseils sur les politiques et les textes législatifs qui touchent à la vie privée;
- coopérer avec les autorités de même nature afin de garantir une protection des données qui soit cohérente.

[L'avis du CEPD](#) (EN) est disponible sur le site Internet. Pour plus d'informations: press@edps.europa.eu

CEPD - Le gardien européen de la protection des données

www.edps.europa.eu



Suivez-nous sur Twitter: [@EU_EDPS](https://twitter.com/EU_EDPS)