ALAIN BENSOUSSAN
Juristendances Informatique et Libertés
n° 38 – Mars – Avr. 2011

# ISRAËL DÉSIGNÉ PAYS ADÉQUAT POUR LE TRANSFERT DE DONNÉES !

## L'encadrement légal des flux transfrontières de données personnelles

▪ Par **décision du 31 janvier 2011** (1), la Commission européenne a reconnu à l'Etat d'Israël un niveau de protection adéquat des données à caractère personnel transférées à partir de l'Union européenne en ce qui concerne les **transferts internationaux automatisés de données à caractère personnel au départ de l'Union européenne** ou, s'ils ne sont pas automatisés, les transferts soumis à un traitement automatisé complémentaire sur le territoire de l'État d'Israël.

▪ Rappelons qu'aucune restriction ne peut être émise sur des flux transfrontières de données à caractère personnel effectués au sein de l'Union européenne. En revanche, l'**article 68 de la loi Informatique et libertés** interdit, en principe, un tel transfert de données vers un Etat destinataire situé en dehors de l'Union européenne qui n'assurerait pas un **niveau de protection suffisant de la vie privée et des libertés et droits fondamentaux des personnes** à l'égard du traitement dont ces données font l'objet ou sont susceptibles de faire l'objet.

▪ Pour mémoire, le **caractère suffisant** du niveau de protection assuré par un État s'apprécie en fonction notamment de la réglementation en vigueur dans cet Etat, des mesures de sécurité qui y sont appliquées, des caractéristiques propres au traitement, telles que ses fins et sa durée, ainsi que la nature, l'origine et la destination des données traitées.

▪ A ce jour, les **Etats reconnus par la Commission européenne** comme ayant le statut de pays adéquat sont l'Argentine, le Canada, Guernesey, l'Ile de Man, l'Islande, Jersey, le Liechtenstein, la Norvège, la Suisse et les Etats-Unis (3).

## Les fondements juridiques de la décision de la Commission européenne

▪ Pour fonder sa décision, la Commission européenne observe, tout d'abord, que les **normes juridiques** pour la protection des données à caractère personnel dans l'État d'Israël se fondent, dans une large mesure, sur les normes énoncées dans la **directive 95/46/CE du 24 octobre 1985** dite « *données personnelles* », et que, par ailleurs, elles figurent dans la **loi 5741-1981 du 1er avril 1981** de protection de la vie privée, modifiée en dernier lieu en 2007, afin d'instaurer de nouvelles exigences en matière de traitement des données à caractère personnel.

▪ A ce titre, la Commission européenne retient qu'aux fins de l'**article 25**, paragraphe 2, de la directive 95/46/CE, l'Etat d'Israël est réputé assurer un niveau de protection adéquat des données à caractère personnel transférées à partir de l'Union européenne en ce qui concerne les transferts internationaux automatisés de données à caractère personnel au départ de l'Union européenne (Article 1er).

▪ L'autorité de contrôle compétente de l'Etat d'Israël en matière de protection des données est l'**Autorité israélienne chargée du droit, de l'information et des technologies**. Organisme de régulation indépendant créé par le Ministère israélien de la Justice en septembre 2006, l'**ILITA** est dotée de pouvoirs d'investigation et d'intervention s'appliquant tant au secteur privé qu'au secteur public (2).

▪ Si les flux transfrontières de données n'ont plus à faire l'objet d'une demande autorisation, la Cnil en est informée par le biais de l'annexe "Flux transfrontières" de la formalité correspondante.

## L'enjeu

Inciter au développement des échanges commerciaux bilatéraux entre l'Etat d'Israël et les Etats membres de l'Union européenne.

(1) Décision 2011/61/UE du 31-1-2011

(2) Tech ILITA - The Israeli Law, Information and Technology Authority

(3) Dans le cadre du Safe Harbor.

## Les conséquences

Le responsable de traitement situé sur le territoire de l'Union européenne n' a plus besoin de conclure de convention de flux transfrontières de données pour les traitements effectués sur le sol de l'Etat d'Israël.

En revanche, le traitement concerné par les flux transrontières doit faire l'objet de formalités préalables auprès de la Cnil.

STEPHANIE LE BRIS

# FICHIERS DE POLICE À GRANDE ÉCHELLE : CRÉATION D'UNE AGENCE EUROPÉENNE

## Une agence de régulation indépendante des Etats membres

▪ La **proposition de règlement** du Parlement européen et du Conseil portant 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 devrait être examinée le **11 avril 2011** par le Conseil de l'Union européenne. Un accord politique pourrait donc intervenir pour le mois de juin 2011.

▪ A l'**Assemblée nationale**, la Commission des affaires européennes a approuvé la proposition de règlement au cours de sa réunion du **6 avril 2010**. Celle-ci en a profité pour signaler qu'étant donné que la proposition ne préjuge en rien du futur siège de l'Agence, la France se porte candidate.

▪ Cette proposition consiste en la création d'une **structure de gestion unique, dotée de la personnalité juridique**, en charge de la gestion opérationnelle à long terme du système d'information sur les visas (VIS), du système d'information Schengen (SIS II), d'Eurodac et d'autres systèmes d'information à grande échelle au sein de l'Union européenne dans le domaine de la liberté, de la sécurité et de la justice.

▪ Cette entité s'apparenterait à un « *centre d'excellence* » auquel serait rattaché un personnel d'exécution spécialisé.

## L'étendue des compétences du nouvel organisme communautaire

▪ Le **Système d'information sur les visas (VIS)** vise à permettre aux consulats et autres autorités compétentes des États membres d'échanger des informations sur les visas dans le but, notamment, de simplifier les procédures de demande, d'éviter le « visa shopping », de lutter contre la fraude, d'identifier les ressortissants de pays tiers et de contribuer à la prévention des menaces pesant sur la sécurité intérieure des Etats membres.

▪ Le **Système d'information Schengen de deuxième génération (SIS II)** a pour objet d'assurer un niveau élevé de sécurité dans l'espace de liberté, de sécurité et de justice de l'Union européenne, et d'appliquer les dispositions relatives à la libre circulation des personnes sur le territoire des États membres.

▪ **Eurodac**, le système informatique servant à comparer les empreintes digitales des demandeurs d'asile et des immigrants clandestins, a été créé pour faciliter l'application de la Convention de Dublin, destinée à établir un mécanisme de détermination de la responsabilité de l'examen des demandes d'asile présentées dans l'un des États membres de l'Union.

▪ L'agence sera chargée de toutes les tâches liées à l'**infrastructure de communication** concernant le système Eurodac pour la comparaison des empreintes digitales.

▪ Elle s'acquittera en outre des tâches liées à la **formation d'experts** du VIS et du SIS II, y compris la formation relative à l'échange d'informations supplémentaires, ainsi que le suivi des recherches et la mise en oeuvre de projets pilotes à la demande expresse de la Commission.

▪ Le **principal organe de gestion** de l'Agence sera le Conseil d'administration, au sein duquel les États membres et la Commission seront représentés d'une manière adéquate.

▪ La **représentation des États membres** devrait refléter les droits et obligations de chacun prévus par le traité. Les pays associés à la mise en oeuvre, à l'application et au développement de l'acquis de Schengen et aux mesures relatives à Eurodac participeront également aux activités de l'Agence.

## Les objectifs

- confier à un organisme spécialisé la gestion globale et le fonctionnement des systèmes d'information ;

- atteindre un niveau d'efficacité et de réactivité élevé, dans la perspective du développement et de la gestion opérationnelle d'autres systèmes informatiques potentiels.

## Les perspectives

L'Agence devrait être chargée des aspects opérationnels de tout autre système informatique à grande échelle qui sera développé dans le domaine de la liberté, de la sécurité et de la justice.

Cela dépendrait de l'adoption d'instruments législatifs portant création de ces systèmes qui conféreraient à leur tour à l'Agence les compétences correspondantes.

Proposition de règlement du Parlement européen et du Conseil (COM (2009) 293 final du 26–6-2009

EMMANUEL WALLE

## L'utilisation à des fins de marketing de fichiers d'adresses électroniques est-elle licite ?

▪ **Oui si la collecte est loyale,** la constitution de fichiers d'adresses mél en vue de leur commercialisation est licite à la condition que les coordonnées du destinataire aient été recueillies directement auprès de lui et qu'il ait explicitement accepté d'être démarché (1).

▪ Le consentement s'entend de toute manifestation de volonté libre, spécifique et informée par laquelle une personne accepte que des données à caractère personnel la concernant soient utilisées en vue de promouvoir, directement ou indirectement, des biens, des services ou l'image d'une personne vendant des biens ou fournissant des services.

▪ L'information concernant l'utilisation potentielle d'une adresse électronique à des fins de prospection commerciale doit être délivrée lors de la collecte des données.

▪ Si la prospection concerne des produits ou services analogues à ceux déjà fournis par l'entreprise dont la personne est cliente ou si la prospection n'est pas de nature commerciale (par exemple, prospection caritative), l'accord de la personne intéressée n'est pas requis préalablement au lancement d'une campagne d'emailing.

▪ La CNIL a reconnu conformes à la loi du 6 janvier 1978 deux projets de codes de déontologie des professionnels du marketing direct relatifs à l'e-mailing (2).

## L'internaute peut-il s'opposer à l'utilisation de ses coordonnées ?

▪ **Oui**, toute personne doit pouvoir être en mesure de s'opposer, de manière simple et sans frais, hormis ceux liés à la transmission du refus, à l'utilisation de ses coordonnées lorsque celles-ci sont recueillies et chaque fois qu'un courrier électronique de prospection lui est adressé.

▪ Dans l'éventualité où son droit d'opposition n'est pas respecté, il revient à la personne sollicitée de saisir la Cnil, qui lutte activement contre l'envoi massif de courriers électroniques non sollicités (spam).

## Quelles sont les sanctions ?

▪ Une contravention de la 4e classe (amende de 750 €) peut être infligée par message expédié en dehors du cadre de l'article L. 34-5 du CPCE (3).

▪ Par ailleurs, le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 € d'amende (4).

▪ Une proposition de loi déposée au Sénat le 7 janvier 2011 (5) vise à interdire purement et simplement, la vente, cession, location ou prêt de fichiers d'adresses mail sans l'accord explicite des personnes concernées.

▪ En cas d'infraction, des sanctions seraient appliquées sur la base des atteintes à la vie privée (jusqu'à un an de prison et 45 000 € d'amende)

### L'essentiel

(1) CPCE, art. L. 34-5

(2) SNCD, Code de déontologie ; UFMD, Charte de l'emailing

Il est interdit :

- d'émettre un courrier électronique à des fins de prospection sans indiquer de coordonnées valables auxquelles le destinataire puisse valablement transmettre une demande tendant à faire cesser ces communications intempestives.

- de dissimuler l'identité de la personne pour le compte de laquelle la communication est émise et de mentionner un objet sans rapport avec la prestation ou le service proposé.

- de récupérer des adresses mails à l'insu des personnes concernées et de constituer des fichiers qui seront par la suite vendus. Ce procédé de collectes de données à caractère personnel est illicite car contraire à la loi et au respect de la vie privée.

(3) CPCE, art. R.10-1

(4) C. pén. art. 226-18.

(5) Doc. Sénat n° 205 du 7-1-2011

## Cession et location de fichiers d'adresses mail : une proposition de loi

▪ Le **1er février 2011**, le député Marie-Jo Zimmermann a présenté une proposition de loi visant à interdire la commercialisation de fichiers d'adresses mail sans l'accord explicite des personnes concernées.

## Empreintes digitales : élargissement de l'accès au FNAEG

▪ Un décret (2), publié au Journal officiel du **9 février 2011**, vient modifier le décret n° 87-249 du 8 avril 1987 relatif au fichier automatisé des empreintes digitales (FAED), géré par le ministère de l'intérieur.
▪ Le nouveau dispositif, pris après avis de la Cnil du 20 mai 2010 (3), intervient dans le cadre du traité relatif à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme, la criminalité transfrontalière et la migration illégale, signé à Prüm le 27 mai 2005.
▪ La consultation des données enregistrées dans le fichier est désormais autorisée pour les douaniers, les agents d'organismes de coopération internationale en matière de police judiciaire, ainsi que les agents des services de police ou de justice d'Etats étrangers, dans le respect des conditions édictées au présent décret.

## Halte à la vente de fichiers d'adresses électroniques !

▪ Une proposition de loi, déposée au Sénat le **7 janvier 2011**, tend à subordonner la commercialisation de fichiers d'adresses électroniques à l'accord des personnes concernées (4).
▪ Le texte, renvoyé pour examen à la Commission des affaires économiques, prévoit de compléter l'article L. 34-5 du Code des postes et des communications électroniques par l'insertion d'un cinquième alinéa prohibant la commercialisation de fichiers d'adresses constitués sans l'accord explicite et matérialisé des intéressés.

## Scanners de sûreté dans les aéroports européens : l'avis du CESE

▪ Consulté par la Commission européenne au sujet de l'utilisation de scanners de sûreté dans les aéroports de l'Union, le Comité économique et social de l'Union européenne (CESE) a publié un avis, adopté en séance du **16 février 2011** (5).
▪ Considérant que « l'utilisation de ce type de scanner pourrait porter particulièrement atteinte à la protection des droits fondamentaux s'agissant de la dignité humaine, de la vie privée et de la protection des données », le Comité estime que le passager devrait avoir le droit de choisir de se soumettre à ce type de contrôle ou non (opt out) et, quel que soit son choix, devrait conserver le droit de voler. Le Comité est d'avis qu'il convient d'étudier sérieusement d'autres possibilités que l'utilisation des scanners de sûreté ou des scanners corporels.

### Sources

(1) Doc. Sénat n° 205 du 7-1-2011

(2) Décr. 2011-157 du 7-2-2011

(3) Cnil, délib. 2010-194 du 20-5-2010

(4) Doc. Sénat n° 205 du 7-1-2011

(5) CESE, Avis TEN/429 du16-2-2011

Directeur de la publication : Alain Bensoussan
Rédigée par les avocats et juristes de ALAIN BENSOUSSAN SELAS
Animée par Chloé Torres et Isabelle Pottier, avocats
Diffusée uniquement par voie électronique
ISSN 1634-071X
Abonnement à : paris@alain-bensoussan.com