

26^e Conférence internationale sur la vie privée et la protection des données personnelles
Wroclaw, 14-16 septembre 2004

Session : « Les flux transfrontières de données
et les défis de l'économie mondiale »

Présentation de la session par

M. Alex TÜRK, Président de la Commission Nationale de l'Informatique et des Libertés

I – L'émergence de la problématique en matière de flux transfrontières et les réponses apportées par les instruments internationaux et les autorités de protection de données

La problématique des flux transfrontières de données personnelles a été concomitante à l'apparition des préoccupations nationales en matière de protection des données personnelles dans le courant des années 1970.

Ainsi, la Convention 108 et les lignes directrices de l'OCDE ont été élaboré au moment même de l'apparition des premières législations nationales et adoptées dès le début des années 1980 pour répondre à cette préoccupation : la protection assurée dans les Etats parties à ces instruments permet d'assurer la libre circulation des données. Dès lors ces instruments ne régulent que les transferts de données entre pays parties à la Convention ou adhérant aux lignes directrices.

Ce sont les autorités indépendantes de protection des données qui ont élaboré de manière pragmatique des solutions au cas par cas, quand les transferts envisagés avaient lieu vers des pays tiers : elles ont ainsi élaboré une première solution contractuelle (cas « FIAT » de 1986) puis celle des règles internes des entreprises multinationales (cas « IBM » de 1990).

La directive européenne a été le premier instrument juridique international comportant des règles claires sur les questions de transferts de données vers des pays tiers. Sa philosophie en la matière, reprise par des législateurs de pays non-européens (Hong Kong, Canada, etc.), mais aussi par le Conseil de l'Europe (Protocole additionnel), est la suivante :

- des données personnelles ne peuvent circuler librement qu'entre pays accordant une protection adéquate aux personnes dont les données sont transférées, que ce soit par des législations générales ou sectorielles ;
- différentes exceptions à ce principe peuvent être mises en œuvre, qui permettent que des données soient transférées vers un pays n'accordant pas une telle protection quand le transfert a lieu, malgré tout, dans des conditions garantissant sa sécurité, notamment par contrat.

M. Ulrich Dammann, de l'autorité fédérale allemande de protection des données personnelles retracera cette perspective historique, qui lui permettra d'apporter des éléments de réponse aux questions suivantes : comment le système fonctionne-t-il ? Où en sommes-nous ?

M. Ken Anderson, Commissaire adjoint de la Province canadienne de l'Ontario, nous rappellera quant à lui que les transferts de données personnelles ne peuvent être envisagés que dans une logique de « chaîne de sécurité », et qu'un transfert ne peut être dissocié de son traitement d'origine ; il nous présentera sans doute les activités pédagogiques de son autorité sur ces questions.

II – Complexité et simplification des outils d'encadrement des flux transfrontières de données

Dans nos débats, nous ne pourrions pas éviter d'aborder le thème, récurrent de nos jours, de la complexité des outils juridiques mis au point pour encadrer les flux transfrontières de données vers des pays tiers, et du besoin de simplification qui en découlerait.

La complexité de la matière provient non pas des règles de protection des données personnelles, mais de la complexité de la réalité des flux transfrontières et de celle des réalités juridiques des Etats dans différents continents. En effet, pour offrir à chaque organisme la possibilité de transférer des données selon les modalités qui lui conviennent le mieux en fonction des cas de figure dans lesquels il se trouve, il a fallu complexifier le modèle de mise en œuvre des règles relatives aux transferts de données (ainsi : le régime particulier de l'adéquation de la protection assurée aux USA par le « Safe harbor », les contrats, les « règles internes contraignante des entreprises multinationales », etc.). **Ainsi, paradoxalement, c'est en grande partie pour simplifier la vie des entreprises dans un monde globalisé que le modèle est devenu complexe.**

En tout état de cause, il est important de rappeler que toute entreprise de simplification en la matière ne peut être envisagée que dans la mesure où elle préserve les droits des personnes dont les données sont transférées.

C'est ainsi qu'il revient aux autorités de protection des données de s'assurer entre elles que ces différents outils sont mis en œuvre de manière adéquate et cohérente et de veiller, ce faisant, à ce que ces droits et leur effectivité soient toujours préservés.

Il revient aussi aux législateurs d'adopter des législations de protection des données qui accorderaient une protection adéquate et pourrait dès lors être reconnue comme telle par la Commission européenne ; et il revient aux entreprises, notamment dans l'élaboration de règles internes, d'accepter de s'aligner sur le plus haut niveau de protection, plutôt que de rechercher des solutions globales autour du plus petit dénominateur commun, qui impliquent donc qu'elles aient ensuite à gérer la complexité d'exigences particulières supérieures.

D'autres domaines ou d'autres voies de simplification sont peut-être encore à explorer, notamment en matière de commerce électronique. **Mme Lilian Edwards**, gagnante du Prix Barbara Wellberry, nous exposera ses propositions sur ce point, dont il faut reconnaître qu'elles sont assez iconoclastes...

III – Les autres défis contemporains posés par les flux transfrontières de données pour les autorités de protection des données

Mais des défis autres que ceux consistant à développer des méthodes ou des outils d'encadrement des flux transfrontières de données se posent, à l'heure actuelle, aux autorités de protection des données, qui résultent du phénomène bien connu de la « mondialisation ».

M. Alfred Büllsbach, Data Protection Officer du groupe Daimler Chrysler, a ainsi centré sa présentation sur les conséquences de la mondialisation sur la protection des personnes l'égard du traitement de leurs données personnelles.

Dans ce contexte, deux défis particuliers se posent avec acuité aux autorités de protection :

1. Dynamiser les actions de coopération pour tenir compte du développement sans précédent des flux transfrontières de données vers des destinations nouvelles

Notre monde actuel est marqué dans les pays développés et au Nord par une forte tendance à l'externalisation, et dans les pays en développement par une nouvelle capacité à mieux s'insérer dans le marché mondial grâce au système mondial de communication, notamment internet. En conséquence les flux transfrontières de données s'opèrent non seulement, comme hier, entre pays du Nord, mais également, et c'est beaucoup plus récent, entre pays développés (Europe, OCDE) et pays du Sud, et plus généralement y compris avec des pays en développement dont la main d'œuvre est très qualifiée (maintenance informatique à distance ; délocalisation de centre d'appels en Inde, au Maroc, en Tunisie, au Sénégal, etc.).

Cette tendance induit une priorité majeure pour les autorités de protection des données : prendre, avec l'appui de leurs gouvernements et des institutions régionalement compétentes, des initiatives pour inciter ces pays à adopter des règles de protection des données personnelles, comme il y a 25 ans entre pays du Nord, en promouvant la coopération et en mettant à leur disposition l'expérience et l'expertise dont ils ont besoin.

De telles actions de coopération ont d'ores et déjà été initiées au plus haut niveau par nos collègues espagnols dans les différents pays d'Amérique latine ; des initiatives similaires sont également en cours entre les pays de la francophonie et dans les pays de la zone Asie-Pacifique. Ces actions de coopération sont fondamentales, car elles seules permettront que la protection des personnes se développe en parallèle avec l'accroissement des échanges économiques et commerciaux.

2. Prendre en compte les risques liés aux lois de sécurité publique et de lutte contre le terrorisme du pays destinataire

Après une longue période très positive au cours de laquelle des instruments de protection diversifiés et adaptés ont été recherchés et mis en œuvre avec succès pour favoriser les échanges tout en assurant la protection une nouvelle période plus difficile paraît s'ouvrir. Dans le contexte d'insécurité actuelle, les autorités doivent également faire face à une tendance très préoccupante qui consiste, pour les autorités publiques de certains pays, à opérer une véritable « OPA » sur les fichiers du secteur privé.

L'on pense bien sûr à la loi dite « Patriot Act » votée aux Etats-Unis en octobre 2001. En vertu de la Section 215 de cette loi, le FBI peut en effet exiger que lui soient produites des données dont disposeraient des sociétés américaines et leurs filiales, quand bien même celles-ci proviendraient de l'extérieur des Etats-Unis, et ce sans que les personnes concernées en

aient été informées.¹ Cette situation préoccupe à juste titre nos homologues canadiens dans la mesure où différents services de l'Etat externalisent des activités auprès de sociétés de service américaines.

Ne faudrait-il pas, en s'appuyant sur les clauses de sauvegarde prévues dans tous les instruments de protection destinés justement à faire face aux situations exceptionnelles, intervenir si l'on apprenait que des données de personnes ne résidant pas aux Etats-Unis et ne relevant donc pas de la juridiction américaine sont susceptibles malgré tout de faire l'objet d'une communication au FBI en vertu de cette loi ? Ne faudrait-il pas entrer en négociation avec les pays concernés pour obtenir que les personnes en question ne soient pas soumises à cette législation et que l'Etat de résidence en soit informé ? Faudrait-il aller jusqu'à suspendre certains flux autorisés antérieurement ?

Par ailleurs, en tant qu'entreprise, que peut-on envisager dans de telles situations ? Faut-il renoncer à délocaliser certains fichiers aux Etats-Unis ? Comment peuvent alors réagir des sociétés devant respecter la volonté de la maison-mère de centraliser toutes ses données du personnel à son siège américain ?

Je vous livre en ce début de session ces différentes questions et espère que quelques pistes de solution émergeront de nos discussions, d'abord de la part des intervenants, puis de la salle.

¹ La section 215 prévoit en effet qu'une juridiction puisse émettre une injonction tenue secrète de produire « toutes choses tangibles » (« any tangible thing ») au FBI, y compris des données à caractère personnel, dès lors que le FBI aura spécifié qu'il agit dans le cadre d'une enquête liée au terrorisme international ou à des activités d'espionnage (« clandestine intelligence »). Toute personne se voyant enjoindre de produire de telles données a l'interdiction d'en informer les tiers, y compris les personnes dont les données ont été communiquées.