Elaboration d'une méthodologie pour évaluer l'adéquation du niveau de protection des personnes physiques à l'égard du traitement de données à caractère personnel. Rapport final. (Etude réalisée pour la Commission Européenne - DG XV)

Havelange, Benedicte; BURKERT, Herbert; Boulanger, Marie-Helene; Lefebvre, Axel; Poullet, Yves; de Terwangne , Cécile

Publication date:
1996

Document Version
le PDF de l'éditeur

Elaboration d'une méthodologie pour évaluer l'adéquation du niveau de protection des personnes physiques à l'égard du traitement de données à caractère personnel

Executive summary

Yves POULLET
Bénédicte HAVELANGE

avec la collaboration de:
Marie-Hélène BOULANGER
Herbert BURKERT
Axel LEFEBVRE

Décembre 1996
Commission européenne - DG XV
Contrat ETD/95/B5-3000/165

OBJECTIFS, OBJET ET PLAN DE L'ETUDE

1. Objectifs

L'étude confiée au Centre de Recherches Informatique et Droit des Facultés Universitaires Notre-Dame de la Paix de Namur vise à offrir à la Commission européenne un outil permettant d'évaluer l'adéquation de la protection accordée aux données à caractère personnel dans le pays tiers à la Communauté.

Cette méthodologie d'évaluation implique que soient rassemblées toutes les informations pertinentes pour réaliser une évaluation de la protection offerte dans le pays tiers, et cela comme le précise la directive, "au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transferts" donnés.

Dans la mesure où, d'une part, les circonstances entourant le flux ou la catégorie de flux peuvent varier considérablement, et où, d'autre part, la liste des instruments de protection des données peut toujours s'enrichir, l'instrument d'évaluation doit être adaptable à toutes les situations susceptibles de se présenter.

2. Objet de l'étude

La présente étude a pour objet la présentation d'une méthode d'analyse en vue de déterminer l'adéquation de la protection des données dans les flux transfrontières au sens de l'article 25 § 2 de la directive[1]

C'est un instrument très souple qui doit permettre de traiter la diversité des flux transfrontières existants, diversité dont témoignent les exemples suivants:

- Le premier exemple est la création par une multinationale américaine disposant de sièges en Europe d'une banque de données relatives au personnel de cadre, où qu'il soit, et recensant des renseignements de tous ordres: ambitions, formation reçue, hobbies,... Il s'agit, pour cette multinationale, de pouvoir répondre facilement à des besoins internes de la compagnie comme celui de la constitution d'équipes de prospection d'un nouveau marché, de la recherche de formateurs, voire de la création d'une équipe sportive,... Ces données collectées à partir de multiples sources -formulaires ou interviews lors des candidatures, appréciation par des supérieurs hiérarchiques, participation à des cycles de formation- sont en l'occurrence assemblées et envoyées à partir de lieux divers (centres de

---

[1] Dans le cadre de la réflexion menée, les auteurs ont développé nombre de questions corrélées à cet objet précis:

- premièrement, la question des domaines d'application respectifs de l'article 26, de l'article 4.1. (c) et de l'article 25 et de la question de l'application combinée de ces articles;

- deuxièmement, les questions liées aux différents niveaux d'analyse prévus par l'article 25 dans ses différents paragraphes;

- troisièmement, la question du contrat comme technique de protection des données, au sens des articles 25 et 26.

La recherche a également amené les auteurs à analyser de manière plus précise deux systèmes de protections: celui offert par la récente législation taïwanaise, et celui récemment proposé par la Canadian Standard Association.

Ces réflexions complémentaires ou annexes n'ont point été reprises dans la présente étude que les auteurs, à la demande de la Commission européenne, ont strictement limitée à l'objet précis demandé par le cahier des charges. Elles feront l'objet de publications séparées.

formation, directions du personnel des différentes entités locales,...) aux services centraux de direction du personnel de la multinationale. La banque de données localisée au siège central de la multinationale est accessible par les différents sièges locaux.

- La délocalisation d'activités dans des pays du tiers monde suggère un deuxième exemple. Soit une entreprise belge de listes d'adresses, travaillant sur les marchés belges et hollandais et décidant de sous-traiter l'ensemble de ses activités d'encodage, de triage, voire de sélection, dans un pays africain. Les données sont collectées principalement auprès de la personne concernée à partir d'un vaste questionnaire portant sur les habitudes de consommation (voyages, alimentation, culture,...). Elles sont croisées avec d'autres données: numéro de téléphone, importance de la localité, type de quartier (revenu moyen par habitant, etc...) provenant de sources publiques accessibles directement de l'étranger ou transférées par support informatique.

- Le troisième exemple est celui de grands systèmes informatisés de réservation aérienne. L'un des plus importants d'entre eux est localisé pour les cinq continents aux Etats-Unis, et gère quotidiennement 2.000.000 de réservations venant du monde entier. Cela signifie que chaque jour, chaque seconde, des données à caractère personnel sont traitées par cette société. Ces données sont enregistrées sous forme de "Passenger Name Record" (ou PNR). Outre le nom et l'adresse des passagers, ces PNR contiennent leurs destinations aériennes, leur état de fumeur ou non, ainsi parfois que les hôtels qu'ils choisissent, les voitures qu'ils louent ou encore leur numéro de carte de crédit.

Le phénomène "Internet" suggère enfin d'autres exemples: on peut citer la présence sur Internet de nombreux fichiers, annuaires téléphoniques, listes avec photos et curriculum vitae de membres d'institutions universitaires, photos de personnes recherchées par la police,... Ces fichiers et listes contiennent des données collectées à partir de tous points du globe et consultables de la même manière. Ils peuvent être à tout moment transférés d'un endroit à l'autre.

3. Plan de l'étude

L'étude ici résumée présente tout d'abord un bref descriptif du champ d'analyse de notre travail (chapitre I).

Un second chapitre examine la nature des risques existant pour la personne concernée lors d'un transfert de ses données hors de l'Union Européenne. Il s'attache ensuite à déterminer quels facteurs peuvent aggraver ou diminuer ces risques, eu égard à la nature particulière du flux envisagé. La protection est en effet "adéquate" en fonction de ces risques, et tente de couvrir ceux-ci.

Un troisième chapitre vise à déterminer le contenu de la protection adéquate, dont on verra qu'elle se structure autour de quatre principes de fond. Vient alors l'examen des moyens d'effectivité de cette protection, c'est-à-dire, des éléments qui assurent *in concreto* le respect des principes de fond, en les exprimant, en assurant leur mise en oeuvre et permettant un recours (et éventuellement prévoyant des sanctions) en cas de défaillance.

La dernière étape de ce travail (chapitre IV) consiste à appliquer la réflexion conceptuelle qui précède aux cas qui peuvent se présenter dans la pratique. Nous proposons ainsi un outil d'aide à la décision, pour l'évaluation de la protection du pays destinataire de flux en fonction des caractéristiques (risques, facteurs d'aggravation ou de diminution du risque,...) propres à ce flux. Bien sûr, on veille encore à souligner ici qu'il s'agit bien d'un outil d'aide à la décision et non d'un instrument fournissant des réponses

finales. La méthodologie proposée a été "testée" grâce à différents exemples de flux transfrontières inspirés de cas réels[2].

CHAPITRE 1. DESCRIPTIF DU CHAMP DE L'ETUDE

4. Introduction

En vertu de l'article 25.1 de la directive, "les États membres prévoient que le transfert vers un pays tiers de données à caractère personnel faisant l'objet d'un traitement, ou destinées à faire l'objet d'un traitement après leur transfert, ne peut avoir lieu que si, sous réserve des dispositions nationales prises en application des autres dispositions de la présente directive, le pays tiers en question offre un niveau de protection adéquat". Le principe est donc l'interdiction du transfert, sauf à démontrer le caractère adéquat de la protection offerte dans le pays tiers.

La directive précise ensuite en son article 25.2 que l'appréciation du caractère adéquat de la protection du pays tiers doit tenir compte de "toutes les circonstances relatives à un transfert ou à une catégorie de transferts" et en particulier de différents facteurs, dont certains sont fonction du transfert considéré, tels la nature des données, la finalité et la durée des traitements, les pays d'origine et de destination, et certains concernent le niveau de protection en vigueur dans le pays tiers, comme les règles de droit générales ou sectorielles en vigueur, ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées[3]

I. La notion d' "adéquation"

5. Remarques liminaires

Trois remarques liminaires s'imposent d'emblée au sujet de la notion d'"adéquation".

- Tout d'abord, cette notion suppose sans doute un référent (qui permette de répondre à la question: "par rapport à quoi la protection doit-elle être adéquate"?). Or, ce référent n'est pas défini comme tel par la directive. Il n'existe pas de système de référence déterminé par rapport auquel on puisse évaluer, comparer la protection du pays tiers.

- Ensuite, on note que, si les critères énoncés par l'article 25.2 constituent de précieuses indications quant aux éléments à prendre en compte pour évaluer l'adéquation de la protection du pays tiers, ils ne constituent pas une liste exhaustive (l'article 25.2 énonce qu'il faut "en particulier" prendre en considération tel ou tel élément). On peut prendre en compte bien d'autres facteurs pour affiner cette analyse, que ces facteurs soient relatifs au flux considéré ou à la protection existant dans le pays tiers.

- Enfin, le contenu de ces éléments n'est pas défini: si par exemple on sait qu'il faut prendre en compte la durée des traitements, la directive n'indique pas plus avant ce qui serait une durée acceptable ou non. De même, le texte communautaire ne détaille pas ce que devraient être le "contenu minimum" d'une législation ou encore ses conditions d'application, pour considérer qu'elle assure un niveau adéquat de protection. On ajoutera que certains éléments énocés se réfèrent aux caractéristiques du flux et désignent des facteurs de risques (infra n° 10), alors que d'autres désignent la qualité des instruments de protection mis en place dans le pays tiers (infra, n°17 et s.).

---

[2] Nous ne pourrons malheureusement reprendre dans le cadre du présent résumé ces différents cas tests.

[3] Nous soulignons l'importance du mot qui sera explicité ci-après (infra, n°).

6. Caractéristiques de l'approche induite par la notion de protection adéquate

Au-delà de ces réflexions, la notion de "protection adéquate" conduit à une approche - qui, à la lecture du texte de l'article 25, se caractérise comme suit:

- une approche au cas par cas[4], c'est-à-dire que la situation de la protection des données dans un pays tiers est évaluée "par rapport à un transfert déterminé ou une catégorie de transferts". L'instrument méthodologique doit caractériser de manière précise le cas visé;

- une approche souple et ouverte puisque selon le libellé même de l'article 25.2 l'évaluation doit pouvoir tenir compte à la fois des particularités propres et évolutives des divers flux transfrontières mais également des solutions diverses et évolutives que chaque Etat, voire chaque responsable des données, peut apporter, l'article 25 § 2 étant purement indicatif à ce propos. L'instrument méthodologique doit refléter cette ouverture et cette souplesse , et être adaptable aux multiples cas rencontrés ou à rencontrer[5];

- une approche fonctionnelle, c'est-à-dire que la protection s'évalue tant par rapport aux risques d'atteinte à la protection des données, risques générés par le flux en question, que par rapport aux mesures spécifiques ou générales mises en place par le responsable des données dans le pays tiers pour pallier ces risques.

7. La notion de "similarité fonctionnelle"

L'évaluation de ces mesures doit se faire sans a priori; il ne peut être question d'imposer les mécanismes européens mis en place selon la directive (pas d'impéralisme européen) mais bien d'apprécier dans quelle mesure les objectifs de protection poursuivis par la directive sont rencontrés, de façon originale ou non par un pays tiers. En ce sens, la notion de protection adéquate ne représente en aucune manière un affaiblissement de la protection des données des personnes protégées au départ de la directive. Au contraire, elle crée pour l'évaluateur la nécessité, tout en ne perdant pas de vue les exigences qui fondent selon la directive le besoin de protection, de prendre en considération les adaptations originales des modalités de cette protection, adaptations proposées par les pays tiers. L'instrument méthodologique doit laisser la place à cette variabilité de nature et de portée des solutions apportées, à cette recherche de "similarité fonctionnelle"[6].

---

[4] Cela représente une différence fondamentale avec une autre approche possible de la notion d'adéquation, qui serait légistique et abstraite, entièrement fondée sur les textes. L'approche retenue par la directive est résolument pragmatique: c'estconcrètement que doit s'apprécier la protection.

[5] Il est même envisageable de considérer que certaines mesures techniques, du type des PICS (Protocol for Internet Content Selection), par exemple, puissent être considérées comme élément d'un système adéquat de protection.

[6] La "similarité fonctionnelle" implique que l'on recherche non la transposition pure et simple des principes et systèmes de protection européens dans le pays tiers, mais bien la présence de tout élément remplissant les fonctions recherchées, même si les dits éléments doivent être d'une nature différente de ceux que l'on connaît en Europe. Elle permet sans doute un meilleur respect des structures et des caractéristiques juridiques locales qu'un requis de protection équivalente, qui exige une similarité complète, légistique en tout cas.

8. Conséquences de l'approche : deux niveaux d'analyse de l'article 25

L'article 25 al. 1 et al. 2 consacre, nous l'avons dit (supra n° 6), une approche au cas par cas, flux par flux ou catégorie de flux par catégorie de flux. Une telle analyse est évidemment lourde pour les Etats membres et les articles 25.4. et 25.6. mentionnent deux possibilités pour la Commission de leur simplifier le travail. Il s'agit de constater "conformément" à la procédure prévue à l'article 31 § 2 qu'"un pays tiers assure ou n'assure pas un niveau de protection adéquat". En d'autres termes, ces paragraphes permettent la constitution de "white" ou de "black" lists", décision valable pour des catégories de transferts, pour un secteur voire pour l'ensemble des flux vers un pays tiers.

Analyse au cas par cas et analyse globale: les deux types d'analyse ne sont pas contradictoires. L'analyse globale suivra le plus souvent une série d'évaluations au cas par cas, éventuellement pratiquées par différents Etats Membres; elle pourrait également se déduire d'un système de protection générale des données dont le contenu, le contexte et l'application désignent à coup sûr comme adéquate ou inadéquate la protection offerte par les pays tiers.

9. Bénéficiaires de la protection adéquate

Si l'objectif de la directive n'est pas d'exporter son modèle réglementaire hors de ses frontières; son but se limite à protéger les données des personnes bénéficiant au départ de la protection de la directive, y compris lorsque celles-ci sont envoyées à l'étranger.

Par conséquent , ce que la directive impose, ce n'est pas une protection s'appliquant à l'ensemble de la population mondiale mais plutôt de garantir aux personnes bénéficiant au départ de la protection de la directive le maintien d'une protection adéquate pour les traitements même non soumis à la directive. Ainsi, le responsable d'un traitement pourrait, sans modifier les règles de protection qu'il suit habituellement, réserver aux seules personnes originairement bénéficiaires de la protection, la "protection adéquate" de l'article 25[7].

Une telle différenciation est possible par le biais d'un code de conduite ou par la nomination d'un représentant en Europe, soumis aux dispositions prises en application de la directive et responsable vis-à-vis de tels bénéficiaires.

CHAPITRE II. DOMMAGES - RISQUES ET FACTEURS DE RISQUES

10. Définitions

- Le risque est un événement dont la survenance n'est pas certaine mais entraîne pour la personne fichée un dommage.

Dans le cas des transferts de données personnelles, nous avons distingué quatre catégories de risques: ce sont les risques de perte de contrôle, de réutilisation des données, de manque de proportionnalité et d'inexactitude de ces données.

---

[7] ou d'un contrat à notre opinion. Notre étude excluant l'analyse de la portée des contrats dans les flux transfrontières comme mode de protection, nous n'avons pas développé ce mode de protection.

- Les dommages, quant à eux peuvent être d'ordre immatériel[8], matériel ou encore concerner la sécurité physique des personnes, sans qu'à cet égard, l'on puisse procéder à une "échelle" des dommages suivant leur gravité et réserver la protection des données aux dommages de la seconde et troisième catégorie[9].

- On qualifiera de "facteur de risque", tous les éléments propres à un transfert ou une catégorie de transferts qui, chacune, sont susceptibles d'avoir une influence positive sur la probabilité de réalisation du risque.

Parmi ces facteurs, certains sont particuliers aux flux transfrontières (situation politique ou technologique du pays tiers, fait que les données sont rarement collectées directement auprès de la personne concernée); d'autres sont généraux c-à-d liés à toute forme de transfert de données c'est-à-dire (nature des données, type de transfert, ...).

Enfin, on souligne la nécessité d'appliquer à chaque facteur de risque, un "coefficient pondérateur" élément susceptible de renforcer ou diminuer l'importance des facteurs de risque: il s'agit de ce que l'on appelle la "différence culturelle".

11. D'un tableau d'analyse de risques

Le tableau proposé a pour but de mettre synthétiquement en évidence les facteurs de risques pouvant être relevés dans un flux ou une catégorie de flux[10], ainsi que les risques augmentés ou diminués par ces facteurs.

Une colonne "observations" a pour fonction de permettre l'ajout sous forme synthétique d'éléments difficilement représentables mais nécessaires pour l'analyse.

Risques **Facteurs de risques particuliers aux FTD**	Perte de contrôle	Réutilisation	Manque de proportionnalité	Inexactitude des données	Observations
Situation socio-politique		*[11]			
Retard technologique	*	*			
Technologie avancée		*			
Collecte indirecte des données	*	*			

[8] Le dommage immatériel est une atteinte à la personnalité sans conséquences financières et provenant de la violation d'une liberté ou d'un droit fondamental; ainsi, l'inclusion dans une liste d'adhérents à une société de chasse, d'une personne connue pour ces convictions pacifistes.

[9] L'article 1 de la directive entend en effet protéger les "libertés" et droits fondamentaux des personnes", indépendamment du type de dommage éventuellement subi.

[10] Le tableau proposé est ouvert à la prise en considération d'autres facteurs de risques.

[11] Les signes seront remplacées par un signe + ou - selon que le risque est augmenté ou diminué lors de l'analyse d'un flux concret.

Réexportation des données[12]	*	*			

[12] Le facteur de risque "reexportation de données" est important, en particulier, on peut craindre que la protection offerte par un pays tiers vers lequel le flux originaire de données se situe, soit illsoire dans la mesure où l'entreprise destinatoire réexporte les données vers d'autres pays cette fois sans protection adéquate. La présence de ce facteur de risque peut se déduire d'une variété d'autres facteurs, ainsi si l'entreprise destinataire n'est que la filiale d'une entreprise localisée ailleurs, est un simple service bureau voire des pratiques habituelles de cessions de fichiers propres à une région du globe.

Risques **Facteurs de risques généraux**[13]	Perte de contrôle	Réutilisation	Manque de proportionnalité	Inexactitude des données	Observations
Sensibilité des données			*		
Nombre de renseignements transférés			*		
Nombre de personnes concernées	*				
Fréquence des flux		*		*	
Type de transfert utilisé	*	*			
Localisation du fichier central	*				
Liens entre acteurs	*				
Secteur d'activité du destinataire	*	*			
Cohérence dans les finalités	*	*			
Durée de conservation des données		*	*	*	
Détermination de la finalité	*	*			

CHAPITRE III LE NIVEAU DE PROTECTION ADÉQUAT

12. Principes de fond et règles d'effectivité

Pour constituer une réponse appropriée aux risques ainsi déterminés, la protection doit garantir les principes fondamentaux de la protection des données et ce de manière effective. Cette proposition conduit à distinguer principes de fond et règles d'effectivité.

La protection des données s'ordonne, peu importe l'instrument choisi, autour de quelques principes de fond. Les principes de fond constituent les objectifs de la protection et se présentent comme le résultat à atteindre. Ces principes se déduisent tant de l'analyse des risques que du contenu de tous les instruments existants de protection des données. La recherche et l'énoncé de ces principes, le "noyau dur" de la protection des données sont l'objet de la section I.

Une fois le contenu de ces principes déterminé, il reste à s'assurer qu'ils trouvent une mise en œuvre concrète. Ce sont les règles d'effectivité qui jouent ce rôle. Les règles

[13] c'est-à-dire valable pour tout flux qu'ils soient transfrontières ou non.

d'effectivité mettent en place les moyens de garantir in concreto pour les personnes concernées, le respect des principes de fond[14].

Leur nature, leur qualification et leur nombre importent peu, pourvu que le résultat combiné de leur présence garantisse à suffisance le respect des principes de fond. Il n'est pas possible de décrire toutes les règles d'effectivité; le propos est plutôt d'établir à la fois quelques points de répère pour leur évaluation et d'analyser les conditions dans lesquelles elles peuvent garantir le respect de principes de fond. C'est l'objet de la section II.

Section 1. Les principes de fond

13. Les principes de fond

L'existence des principes de fond se déduit de la volonté essentielle de tout instrument de protection des données d'assurer à l'individu une maîtrise de la circulation de son image informationnelle et de son utilisation (principes de participation individuelle et de finalité) et de leur volonté complémentaire de permettre un contrôle des caractéristiques de cette image informationnelle dans sa qualité (principe de qualité) et son ampleur (principe de proportionnalité).

Le principe de participation individuelle exprime la nécessité de permettre par divers moyens à la personne concernée d'obtenir une information sur "l'image informationnelle" que le responsable du traitement a de lui[15] et, dès lors, d'exercer vis-à-vis de cette image un certain contrôle voire une certaine maîtrise[16].

Le principe de finalité exige la limitation de l'utilisation de données à caractère personnel aux seuls traitements dont les finalités sont compatibles avec les finalités légitimes qui ont été déterminées et rendues explicites de leur collecte initiale.

Le principe de proportionnalité implique de limiter dans la durée, en quantité et en qualité les données traitées aux seules données nécessaires à la poursuite des finalités légitimes.

Le principe de qualité induit la recherche d'exactitude et de mise à jour des données personnelles dans la mesure exigée par la finalité.

14. Des risques aux principes

Ainsi, quatre principes intimement corrélés entendent chacun pallier principalement un des risques identifiés au chapitre II.

---

[14] La distinction de base proposée entre principes de fond et règles d'effectivité nous écarte d'autres typologies qui ne distinguant pas les principes des règles d'effectivité en arrivent à une liste longue et indifférenciée de principes.

[15] Cette première facette du principe renvoie à l'information de la personne concernée sur l'existence de traitements de données le concernant.

[16] Cette seconde facette du principe de participation renvoie à l'exercice de divers moyens d'accès aux données traitées, de rectification de celles-ci, de consentement ou de refus du traitement par la personne concernée.

Risques	Principes de fond
Perte de contrôle	Principe de participation individuelle
Réutilisation	Principe de finalité
Non proportionnalité	Principe de proportionnalité
Inexactitude	Principe de qualité

Certes, il faut se garder de toute simplification: de la même manière que les risques coexistent, et sont parfois des conséquences les uns des autres, les principes de fond interagissent: par exemple, lorsque la légitimité de la finalité du traitement est sujette à caution, le principe de participation individuelle verra son importance renforcée par l'exercice d'un droit de refus voire de consentement. Il est clair également que, dans la pratique, un risque peut être rencontré par différents principes. Le risque de non-proportionnalité renvoie non seulement au principe de proportionnalité, mais encore, aux principes de finalité et de participation individuelle. Enfin, à l'inverse, le principe de participation individuelle joue un rôle dans la prévention du risque de perte de contrôle, mais également des risques de non proportionnalité et d'inexactitude des données.

Le principe de participation individuelle a une place particulière parmi les autres principes de fond car il permet à la personne concernée de contrôler l'application effective des autres principes. C'est en effet à partir de la connaissance de l'existence d'un traitement que les personnes concernées pourront contrôler le respect des autres principes de fond. Cette connaissance pourra être obtenue grâce aux divers moyens découlant de la mise en œuvre du principe de participation individuelle.

La participation individuelle peut être considérée comme découlant directement des Droits de l'homme, étant donné qu'il s'agit de l'expression de la maîtrise par chacun de son image informationnelle. Ce principe relève à la fois du droit de la vie privée et du droit à l'image.

Notons enfin que si l'accès est présenté infra n° 19 et 23 comme un moyen d'assurer l'effectivité de tous les principes de fond, il est en même temps la traduction directe du principe de participation individuelle un principe fondamental.

Le principe de finalité apparait également comme prépondérant dans la mesure où les principes de qualité et de proportionnalité se révèlent comme des corrolaires de ce second principe essentiel. Ces deux principes de participation individuelle et de finalité sont donc à considérer comme essentiels.

15. De la conception de ces principes dans la directive

Les nuances parfois importantes apportées dans l'expression des principes en particulier des deux principes essentiels conduisent à s'interroger sur la façon dont il faut les envisager pour qu'ils constituent le référent d'une protection adéquate.

Par rapport aux divers instruments internationaux[17], la directive se distingue en ce sens:

[17]Ces principes, les principes de fond, sont consacrés dans touts les initiatives de niveai international concernant la protection de la vie privée, notamment la convention 108 du Conseil de l'Europe, la résolution des Nations Unies du 23 décembre 1994, les lignes directrices de l'OCDE et bien sûr la

- qu'en exigeant une finalité "légitime", elle introduit l'idée d'un certain contrôle social de la justification de l'utilisation de cette image informationnelle; en d'autres termes, elle n'abandonne pas à la seule discrétion du responsable du traitement, la définition des finalités. Ce contrôle social peut s'exercer a priori par la négociation individuelle avec la personne concernée (le consentement) ou collective avec les représentants des personnes concernées (les associations de consommateurs, les syndicats). Il s'exerce en toute hypothèse par l'intervention, le cas échéant, a posteriori, d'une autorité indépendante ou juridictionelle (administrative ou judiciaire) susceptible d'être saisie par la personne concernée.

- que par l'exigence de consentement ou par l'ouverture de possibilités d'opposition, elle entend accroître la maîtrise de l'individu sur l'utilisation de son image informationnelle, chaque fois que la légitimation du traitement est délicate en particulier en raison de la nature sensible des données[18] ou en raison de la finalité de prospection commerciale poursuivie par le responsable du traitement[19].

Section II. L'effectivité des principes de fond

I. Les concepts utilisés

16. Réflexions sur l'article 25

L'article 25, nous l'avons dit, prescrit une protection adéquate. La description à la première section des principes de fond permet de définir le référent de cette protection. La seconde section précise le « comment » de cette protection: en d'autres termes, les moyens qui permettront concrètement l'obtention du résultat. A ce propos, l'alinéa 2 de l'article 25 renvoie à une vaste énumération de moyens, énumération par ailleurs non limitative: « les règles de droit, générales ou sectorielles, en vigueur dans le pays tiers en cause ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées ».

Du libellé de cet article, se déduisent les deux considérations fondamentales suivantes:

(i) en ce qui concerne la source de la protection la directive n'entend pas réserver au modèle législatif, le concept de protection adéquate. Ainsi, même si un pays ne dispose pas de loi générale de protection des données, il peut offrir une protection adéquate par d'autres moyens d'expression ... Les règles professionnelles, c'est-à-dire les codes de conduite sectoriels ou même propres à une entreprise pourraient suffire à certaines conditions[20];

---

directive européenne. Ils le sont également dans beacoup de normes de protection des données, prises à un niveau national, sectoriel ou même propres à une organisation: lois, décrets, codes de conduites, privacy policy, ...

[18] Au sens de l'article 8 de la directive européenne, c'est-à-dire les données personnelles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale ainsi que les données relatives à la santé et à la vie sexuelle.

[19] Nous nous référons ici à l'article 14 b) de la directive.

[20] Ces conditions seront développées infra n° 23 et s. à propos du "noyau dur" de l'effectivité. Notons dès à présent que l'existence d'une loi est loin d'être suffisante.

(ii) si les auteurs de la directive témoignent d'une ouverture très large dans l'acceptation des moyens d'expression utilisés pour l'obtention du but, ils exigent cependant que ces moyens soient « *respectés* », en d'autres termes, que les textes, peu importe leur source, soient l'objet d'application effective. On suppose l'existence de mesures de contrôle du respect des principes, et de sanctions en cas de non respect de ces principes, pour que puisse s'exercer, le cas échéant, le principe du "recours" de la personne concernée.

Ainsi l'article 25 invite à distinguer, pour évaluer l'adéquation de la protection, trois aspects de celle-ci :

- le premier consiste à s'interroger sur *l'origine, le mode écrit ou non qui exprime la protection*: la valeur du moyen d'expression dépendra de l'auteur de ce moyen et de son caractère plus ou moins obligatoire et contraignant

- le deuxième envisage les *moyens de contrôle* mis en place pour vérifier le respect des principes ;

- le troisième concerne les *moyens de recours et de contrainte* attachés au défaut de respect des principes.

17. L'effectivité

L'effectivité se conçoit nécessairement comme le résultat d'une combinaison de moyens d'expression, de contrôle et de recours (cf. infra n° 22) et doit tenir compte de deux aspects.

L'effectivité se compose de deux aspects, qui renvoient tous deux aux principes de fond préalablement identifiés. Le premier se situe à un niveau général: il s'agit d'abord de promouvoir la connaissance des principes de fond. Cette promotion de la connaissance se conçoit tant par la large publicité donnée à l'expression des principes[21], que par certains moyens spécifiques mis en œuvre dans le cadre du respect des principes, en particulier par la création d'une autorité indépendante ou d'un détaché à la protection des données.

Le second aspect se situe à un niveau particulier: on vise ici la résolution des problèmes divers que peuvent connaître les personnes concernées au regard du traitement de leurs données personnelles.

A première analyse, les moyens d'expression ont plutôt pour objet d'assurer le versant "général" de l'effectivité (affirmation et mise en oeuvre des principes), tandis que les moyens de contrainte et de recours visent évidemment la résolution des problèmes individuels (quoique les sanctions puissent avoir un effet dissuasif qui les renvoie au premier objectif. Enfin, les moyens de contrôle présentent souvent les deux facettes: ils tendent à assurer la mise en oeuvre des principes, et à permettre certains recours.

---

[21] Il est à noter que cette publicité est nécessaire peu importe le mode d'expression choisi. La publicité d'une législation exige plus que la seule publication au Journal Officiel national et une privacy policy doit faire l'objet d'une véritable information des destinataires du traitement et des personnes concernées par le ou les traitements du responsable.

II. La diversité des moyens d'expression , de contrôle, de recours et de contrainte

18. Les moyens d'expression

Parmi les moyens d'expression, l'étude a retenu[22] outre les règles normatives issues de l'autorité publique la certification, la *privacy policy*, le code de conduite sectoriel ou les règles professionnelles et finalement les règles . La non exhaustivité de l'article 25 invite à ne rejeter a priori aucun de ces modes mais à en évaluer soigneusement l'effectivité en tenant compte de traditions culturelles et juridiques peut-être différentes de celles européennes.

On distinguera les moyens d'expression suivant l'autorité qui en est l'auteur. Cette classification en apparence simple cache mal quelques difficultés. Ainsi un code de conduite sectoriel émane bien d'un secteur, mais sa valeur, voire l'obligation de le produire et pour chaque membre du secteur de le suivre, peut émaner d'une norme légale. On ajoutera qu'un moyen d'expression peut se subdiviser en de multiples sous catégories.

Ainsi la règle normative issue de l'autorité publique peut être globale ou sectorielle, émaner de l'autorité législative suprême ou de simples décisions administratives.

Source d'expression	**Qui exprime?**	**Renvoi possible à d'autres moyens d'expression**
Privacy Policy	Entreprise	Certifications, codes de conduite
Certification	Organe de standardisation	Règles normatives prises par l'autorité publique
Codes de conduite	Organe sectoriel	Règles normatives issues de l'autorité publique
Règles normatives issues de l'autorité publique	¬ constitution ¬ pouvoir législatif ¬ gouvernement ¬ Board	Tous les autres hormis le contrat

19. Les moyens de contrôle

Par moyens de contrôle, on vise les diverses méthodes (qu'il s'agisse de techniques, de nominations de personnes ou d'institution d'organes), qui ont pour fonction directe ou indirecte, exclusive ou non, de garantir le respect des principes.

Le tableau suivant résume les différents moyens de contrôle qui bien souvent se combineront.

---

[22] Les auteurs de cette étude considèrent qu'un contrat conclu entre l'exportateur et le destinataire des données, et reprenant les principes de fond peut être considéré comme un moyen d'expression, et, en d'autres termes, comme un des moyens envisagés par l'article 25 pour assurer l'adéquation de la protection. Le fait que les mesures contractuelles soient envisagées de manière distincte à l'article 26.2 de la directive n'altère pas cette possibilité. En effet, dans un cas, on considère le contrat comme un moyen de rendre une protection adéquate, et dans l'autre, on le voit comme un palliatif au cas où la protection du pays tiers n'est pas considérée comme adéquate. Cette réflexion ne fera toutefois pas l'objet de plus de développements dans le cadre du présent rapport.

Moyen de contrôle	Mis en place par	Exercé par
Mesures de sécurité	Responsable du traitement	Responsable du traitement le cas échéant, contrôle en outre par: - entreprise tierce spécialisée - organe sectoriel - autorité de contrôle
Autorité indépendante de contrôle	Autorités publiques	Autorité indépendante de contrôle
Accès	Responsable du traitement	Personne concernée (exceptionnellement par une autorité de contrôle)
Détaché à la protection des données	Responsable du traitement	Détaché à la protection des données
Représentant	Responsable du traitement	Entreprise soit représentante, soit tierce
Audit	Responsable du traitement	Entreprise tierce spécialisée Autorité indépendante de contrôle
Notification	Autorité de contrôle Organisme privé	Autorité de contrôle Organisme privé + contrôle collectif diffus

20 Les moyens de recours et de contrainte

Par moyens de sanction des principes de fond, on entend, au sens large, les divers modes et procédures de dissuasion, de réparation ou de répression mis en place pour combattre les déviances par rapport aux comportements attendus pour assurer le respect des principes de fond.

Nous proposons de distinguer les sanctions selon leurs auteurs.

Auteurs	Sanctions	Dimension
Organe de standardisation ou de certification	Refus ou retrait d'un certificat	Nature commerciale
Secteur	Recommandations Blâme, amendes, retrait de l'association	Nature commerciale Effets sectoriels si publication Effets vers le public
Autorité de contrôle	Recommandations Destruction de données Interdiction de traitements Avis préalable	Nature commerciale avec effets sectoriels Si publication, effets vers le public
Juridictions administratives	Destruction de données Interdiction de traitements Amendes	Nature administrative Effets vers le public
Juridictions civiles	Réparation du dommage Mesures de réparation en nature Publication du jugement	Nature judiciaire Effets vers le public
Juridictions pénales	Amendes, emprisonnement Réparation du dommage Saisie et destruction Publication du jugement	Nature judiciaire Effets vers le public

21. Conclusions à propos des divers moyens

L'analyse des moyens d'expression, de contrôle et de sanctions atteste d'une diversité très grande des solutions susceptibles d'être retenues pour arriver au résultat, à savoir le respect des principes essentiels.

Quelques conclusions peuvent cependant être tirées de ce qui précède:

1) chaque moyen doit être analysé dans sa logique propre et en en fonction du contexte du système juridique dans lequel il apparaît. A nouveau apparaît ici l'importance du coefficient pondérateur dit de "différence culturelle"[23].

2) Chaque moyen renvoie à ses propres conditions d'effectivité dont le respect devra être établie[24].

3) Le résultat à atteindre dépend non d'un seul moyen mais toujours d'une combinaison de moyens d'expression, de contrôle, de recours et de sanction.

4) La combinaison de moyens proposés doit nécessairement garantir le respect non d'un seul principe mais en particulier des deux principes essentiels: ceux de la participation individuelle et de la finalité[25].

5) Ces deux principes peuvent in concreto être consacrés par des moyens différents: ainsi, on peut imaginer vis-à-vis de traitements de l'Administration que le principe de participation individuelle fasse l'objet d'une consécration légale dans le cadre par exemple d'une loi d'accès aux documents administratifs, alors que le principe de finalité ne soit exprimé que par une charte, sorte de privacy policy, des administrations.

6) De manière générale, on peut considérer que plus faible est le moyen d'expression, plus il faudra être attentif à l'effectivité des moyens de contrôle et de sanctions. On peut également affirmer que, sans exclure les autres, seront privilégiés des moyens qui permettent directement ou indirectement une action à partir de l'Union européenne. Ainsi, notamment parmi les moyens de contrôle, le représentant ou l'autorité de contrôle, et parmi les moyens de sanctions, la sanction pénale qui permet la coopération policière.

---

[23] Sur cette notion, cf. déjà nos réflexions n° 10 in fine à propos de l'analyse des risques. Ainsi, l'énoncé d'une "privacy policy" peut, dans certains ordres juridiques, être doté d'une force contraignante importante. La sensibilité d'une population ou des responsables du traitement vis-à-vis d'un mode d'expression peut varier d'un pays à l'autre. La force contraignante d'une loi peut être liée à la volonté du gouvernement de la voir sanctionnée.

[24] Nous renvoyons le lecteur à l'analyse proposée par l'étude des conditions d'effectivité propres à chaque moyen d'expression, de contrôle, de recours et de sanctions. La check list proposée en annexe détaille ces conditions.

Prenons le cas du "détaché à la protection des données", un tel moyen de contrôle n'aura d'efficacité que si ce détaché jouit statutairement d'une certaine indépendance par rapport à l'entreprise qui le nomme, a en charge certaines fonctions, etc.

[25] ...les deux autres principes de fond (proportionnalité et qualité des données) découlant du second.

III. Conditions minimales de l'effectivité

22. Position du problème

L'effectivité se conçoit, avons-nous dit, de la combinaison, de moyens d'expression, de contrôle, de recours et de contrainte. De multiples combinaisons sont possibles, catégorie par catégorie et entre catégories. Il est cependant possible de définir et de justifier certaines conditions minimales d'effectivité dont la présence doit être vérifiée absolument.

Aucune moyen d'expression ne peut être a priori privilégié même si on insiste sur la nécessité de large "publicité" que le moyen d'expression doit donner aux principes qu'il consacre, publicité tant auprès des responsables de traitement que des personnes concernées. Outre cette première condition relative au moyen d'expression, trois conditions relatives aux moyens de contrôle, de recours et de contrainte s'avèrent en outre indispensables:

- l'existence d'un droit et non d'une simple possibilité d'accès et de contestation (n° 23);

- l'existence d'une autorité indépendante de contrôle (n° 24);

- l'existence de mesures de sécurité appropriées (n° 25).

23. Le droit d'accès et de correction

L'effectivité des moyens de contrôle et de sanctions pour la personne européenne concernée[26] suppose, en tout cas, la reconnaissance directe ou indirecte[27] de droits d'accès et de contestation faciles à exercer[28] devant une juridiction[29] et ce peu importe la technique d'expression choisie[30]. Cette reconnaissance est nécessaire si on souhaite que l'effectivité des principes ne soit pas laissée à la discrétion des responsables de traitement et/ou à la seule action de l'autorité publique. En outre, l'accès et la contestation

---

[26] et en tout cas aux personnes protégées par la directive, ce qui peut poser quelques difficultés pour des législations dont le bénéfice est réservé aux seuls nationaux.

[27] La reconnaissance des droits peut être directe ou indirecte: ainsi, en matière de codes de conduite, le droit d'accès et de contestation pourrait être reconnu indirectement par le biais soit du contrat d'adhésion de l'entreprise responsable du traitement à ce code de conduite, ou par la reconnaissance judiciaire de ce code comme "règles de l'art".

[28] La facilité de contestation suppose que les procédures mises en place pour assurer cette contestation soient transparentes, puissent être portées à la connaissance de la personne concernée et que le coût de leur mise en œuvre soit abordable.

[29] La contestation doit pouvoir être tranchée par un organe "juridictionnel" disposant de la possibilité pour des autorités reconnues par l'Etat ou par engagement du responsable du traitement de faire exécuter ces décisions par le responsable du traitement. Ce peut être une juridiction civile ordinaire, une juridiction spécifique chargée par exemple de traiter les problèmes des consommateur, une juridiction administrative voire une autorité de contrôle dotée des prérogatives d'exécution forcée.

[30] En d'autres termes, le mode d'expression ne peut être simplement pour le responsable du traitement créateur d'une simple obligation morale ou d'un devoir de conscience. Notons que cette assertion n'exclut a priori aucun moyen d'expression. En effet, une privacy policy précise et publique peut dans certains ordres juridiques être par elle-même source d'obligations juridiquement sanctionnables, a fortiori, si elle est reprise dans les contrats conclus avec les personnes concernées.

apparaissent non seulement comme le moyen le plus évident de réalisation du principe de participation individuelle dont on a souligné l'importance (supra n° 14) mais également comme la meilleure technique de contrôle du respect des autres principes.

Le droit de contestation doit s'entendre au sens large c'est-à-dire au sens des différents principes de fond. Par "contestation", on entend, non seulement, la possibilité de mettre en cause l'exactitude d'une donnée (principe de qualité) mais, également, celle d'en contester la pertinence (principe de proportionnalité) voire plus fondamentalement la légitimité du traitement (principe de finalité).

Cette dernière facette doit pouvoir être excercée directement auprès du responsable du traitement (droit d'opposition) lorsque la finalité est a priori contestable soit à raison de la nature des données, soit à raison de la finalité de prospection commerciale poursuivie par le responsable du traitement[31]

24. Les mesures de sécurité appropriées

L'exigence de mesures de sécurité appropriées tant internes que le cas échéant externes (réseaux de télécommunication) s'impose dans la mesure où, sans ces mesures, les garanties offertes par les autres moyens risquent de rester lettre morte[32].

25. Une autorité indépendante de contrôle

Une condition minimale supplémentaire est l'existence d'une autorité de contrôle accessible agissant de manière indépendante et caractérisée par l'exercice de certaines fonctions.

Chaque caractéristique mérite quelques développements

- l'accessibilité de l'autorité se conçoit tant par l'annonce auprès des personnes concernées de son existence, que par sa saisine aisée.

- l'action indépendante de l'autorité suppose une liberté d'action par rapport aux intérêts du ou des responsables de traitement. Elle se déduit de divers facteurs (composition de l'organe, transparence du fonctionnement, moyens d'investigation, caractère public du rapport d'activités).

- quant aux fonctions de cette autorité, elles consistent non seulement en la promotion des principes auprès des responsables, l'assistance des personnes concernées dans l'accès et la contestation, le contrôle du respect des principes auprès des responsables du traitement[33].

---

[31] Cfr. à ce propos, n° 15 in fine.

[32] Ainsi, la nécessité de limiter l'accès est une condition essentielle au respect du principe de finalité. En outre, la sécurité joue un rôle également vis-à-vis de l'exactitude des données soit proportionnel aux besoins légitimes de chaque utilisateur. Par ailleurs, c'est dans la mesure où il y a sécurité, c'est-à-dire garantie par le responsable du traitement d'un certain contrôle de l'utilisation des données; que la personne concernée peut avoir confiance dans les dires de ce responsable lorsqu'elle exerce son droit d'accès. En ce sens, la sécurité garantit l'effectivité minimale du principe de participation individuelle.

[33] Cette conception fonctionnelle large de l'autorité de contrôle se distingue de celle institutionnelle (conception présente dans la directive). Elle permet de considérer comme autorité indépendante de contrôle, un organe de médiation créé au sein d'une fédération professionnelle à condition qu'il remplisse les 3 conditions détaillées ci-dessus (accessibilité, indépendance, fonctions).

L'existence de cet organe se justifie par la volonté de rendre effectifs les deux principes majeurs de la protection des données. A propos de la "participation individuelle", les considérants de la directive estiment "essentielle" la création d'une autorité indépendante, créant ainsi le "droit" de la personne concernée de ne pas être laissée seule face au responsable du traitement. A fortiori en cas de flux transfrontières, cette exigence se trouve renforcée lorsque la personne concernée se trouve face à un responsable située en terre lointaine dans la mesure où la personne concernée voire l'autorité indépendante européenne de protection des données trouvera dans cet organes, le relais nécessaire pour procéder aux investigations nécessaires, le cas échéant, appuyer une demande d'accès voire intervenir ! A propos du second principe celui de la finalité, l'exigence d'un contrôle "social" des finalités d'utilisation (supra n° 15) suppose la possibilité de débats publics initiés par ou débattus devant des instances neutres.

26. Conditions minimales et risques de "retransfert"

L'étude des risques (supra n° 11, note 11) a révélé que certains transferts vers un pays tiers ne peuvent être jugée du seul point de vue de la protection offerte par ce pays tiers dans la mesure où les données pourraient être, en raison des caractéristiques du destinataire ou du flux, retransférées vers un autre pays. Un tel retransfert, s'il n'y a pas dans ce second pays de protection adéquate, est bien évidemment potentiellement dangereux. La présence d'un tel risque de retransfert amène à exiger du premier pays une condition supplémentaire d'effectivité pour qu'il y ait protection adéquate. Il importe de vérifier que des dispositions interdisent les transferts de ce pays vers d'autres pays tiers ne disposant pas de protection adéquate ou soumettent de tels transferts à des conditions (par ex. l'existence d'un contrat)[34].

CHAPITRE 4. METHODOLOGIE

27. Questions à se poser!

La méthode d'analyse des flux et de la protection adéquate au regard de ces flux se déduit des caractéristiques de la notion de protection "adéquate", des distinctions proposées et des éléments du "noyau dur" retenus.

Trois questions constituent les trois étapes de l'analyse proposée

- La première est préjudicielle: quelles informations collecter?

- La deuxième est cruciale: qui analyse les informations ainsi collectées?

- La troisième a trait à l'objet de la décision ou plutôt des décisions.

Section 1 La collecte d'informations

28. Sur quoi collecte-t-on?

Pour ce faire, on suggère de réaliser une analyse en deux temps: il s'agit tout d'abord de déterminer les caractéristiques d'un flux ou d'une catégorie de flux en termes de risques et de facteurs de risque (i), et ensuite de procéder à l'examen de l'adéquation de la protection offerte par le pays tiers (ii).

---

[34] Ainsi le projet de loi australien prévoit des dispositions à propos des flux transfrontières similaires à celles européennes. Il va de soi que des interdictions et ces limites peuvent venir d'autres sources dont on vérifiera l'effectivité: codes de conduite, etc.

(i) Nous avons vu que certains facteurs avaient une influence sur certains risques, et nous proposons donc un tableau d'analyse permettant de recenser aisément les facteurs de risque présents dans un flux particulier, et de déterminer à quel(s) risque(s) il faudra être particulièrement attentif.

(ii) Une fois que l'on a déterminé le(s) type(s) de risques spécifiquement entraîné(s) par le transfert, il s'agit de rechercher comment le pays tiers couvre adéquatement ce(s) risque(s).

En d'autres termes, il importe de vérifier les techniques de protection (moyen d'expression de contrôle, de recours et de sanctions) offertes par le destinataire ou imposées aux destinataires et leur effectivité.

Deux questionnaires sont présentés en annexe: l'un précise les facteurs de risques présents dans le flux en considération; l'autre identifie les moyens mis en œuvre et vérifie leurs conditions d'effectivité propres[35].

29. Qui collecte?

L'émetteur du transfert est à même de répondre aux questions concernant le flux lui-même (destinataire, données contenues, réseau utilisé, etc...). En outre, si l'émetteur du transfert est lié au destinataire (société-mère et filiales, sociétés du même groupe, membre d'une même organisation caritative, médicale, politique,...), il disposera également sans doute de connaissances relatives à la protection offerte au flux, si cette protection est, fût-ce seulement en partie, mise en place par l'organisation ou la société en question[36]. Il appartiendra alors à la société émettrice de collecter auprès du destinataire tous les éléments qui lui seront nécessaires pour fournir une réponse complète.

Si l'émetteur et le destinataire ne sont point liés ou que la collecte a lieu directement auprès de la personne concernée (via Internet, par exemple), la collecte d'informations à propos de la protection offerte dans le pays tiers par le destinataire est plus délicate. Certes, on peut confier cette tâche au destinataire lui-même, on la confiera plus volontiers à des spécialistes, experts de la protection des données, qu'il s'agisse d'autorités de contrôle agissant dans ce pays tiers ou spécialistes experts dont le rôle est décisif, nous semble-t-il, pour la seconde étape: la phase d'analyse.

Section 2 L'analyse des informations collectées

30. Le coefficient "différence culturelle" et le rating

Si la décision finale est du ressort des autorités nationales ou communautaires, on peut imaginer que cette décision s'appuie sur l'analyse préalable d'experts voire que cette expertise soit construite sur le modèle du "rating" déjà existant dans le domaine des

---

[35] Deux exemples:

- la privacy policy est-elle complète (expression des différents principes de fonds), précise et publique. Renvoie-t-elle à des moyens de contrôle de son application?;

- le détaché à la protection des données jouit-il de quelques prérogatives? Peut-il être considéré comme disposant d'une certaine indépendance.

[36] On pense ici aux instruments tels les codes de conduite, privacy policy,... dont la société émettrice connaît l'existence et le contenu s'ils sont communs aux différentes sociétés du groupe ou de l'association à travers le monde.

risques financiers à l'exportation[37]. Cela permettrait en particulier une meilleure prise en considération du coefficient "différence culturelle". Ce coefficient joue tant dans l'appréciation des facteurs de risques (ex. habitude des sociétés de marketing de s'échanger les fichiers; conception différente de la sensibilité des données, ...) que dans l'évaluation de l'effectivité des techniques de protection (ex: valeur juridique d'une privacy policy, neutralité d'une autorité sectorielle de contrôle, ...)[38]. La prise en considération de ce "coefficient" répond à la volonté des auteurs de la directive de ne pas imposer leur modèle et à la nécessité d'une expertise du système sociétaire et réglementaire étranger.

Section 3. La décision[39]

31. ... et les facteurs de risque

Deux étapes s'imposent:

La première se déduit de l'analyse des facteurs de risques. Premièrement, il est sans doute possible de jouer sur l'un ou l'autre facteur afin de réduire le risque. Ainsi, s'il ressort de la grille d'analyse des risques que le transfert considéré n'entraîne un risque (par exemple, manque de proportionnalité) qu'à cause de la présence d'un seul facteur de risque (par exemple, durée illimitée du traitement envisagé), alors que tous les autres paramètres conduisent à une évaluation positive, il peut être souhaitable de proposer à l'émetteur du flux de prendre une mesure diminuant ou supprimant l'impact de ce facteur (dans l'exemple cité, introduire une limitation de durée). De la sorte, la "dangerosité" du flux est fort réduite.

Suivant les facteurs relevés, l'attention sera portée sur la mise en cause de tel ou tel principe de fond[40] dont la vérification du respect devra alors faire l'objet d'une attention particulière. Ainsi, si le tableau d'analyse des risques fait ressortir que les risques d'inexactitude ou de manque de proportionnalité des données sont particulièrement élevés, on devra attacher une grande importance à la présence des principes protecteurs correspondants dans les moyens d'expression du pays tiers. On rappelle que le même raisonnement ne vaut pas pour les risques de perte de contrôle et de

---

[37] Le système de rating auquel sont soumis les sociétés ou les Etats membres lors d'une émission obligataire présente avec le système d'évaluation proposé dans le contexte des flux transfrontières certaines ressemblances intéressantes. L'évaluation faite par l'agence de rating vise en effet des éléments propres à un contexte d'opérations financières (tels par exemple que les comptes de la société, sa politique d'investissement, le soutien dont elle jouit de la part de l'Etat, le "risque-devise" existant dans le pays en question), mais également des facteurs non-financiers tels que la prise de mesures de sécurité adéquates, ou encore, le "risque-pays" (corruption, stabilité politique, ...) qui est à peu de choses près l'équivalent de ce que nous avons appelé la "différence culturelle", transposée dans le domaine financier.

Le classement obtenu pour les pays à devise forte (risque en principe nul) est A.A., qui est en général la cote des Etats membres de l'OCDE à devise forte ; il peut être D ("défaut, lorsque le risque est très élevé). La société ou l'Etat émetteur peut malgré une mauvaise évaluation parvenir à trouver preneur pour ses obligations, à condition de fournir des garanties supplémentaires appropriées aux risques qui ont entraîné une mauvaise évaluation, ce qui n'est pas sans rappeler l'article 26.2 de la directive (mesures contractuelles appropriées dans le cas où la protection du pays tiers est jugée inadéquate).

[38] Cf. à propos, supra n° 10 et n° 21

[39] Cf. supra n° 11 le tableau présentant la corrélation entre les facteurs de risques et les risques et supra n° 14, le tableau présentant la corrélation entre risques et principes de fond.

[40] Dans le cadre de l'étude, nous avons testé la présente méthodologie à deux flux tests. Lors de la réunion des commissaires à la protection des données, d'autres flux ests ont été également présentés.

réutilisation, car les principes qui leurs correspondent sont jugés si fondamentaux qu'ils doivent être exprimés dans tous les cas. Mais on peut imaginer d'être moins exigeant au sujet des principes d'exactitude et de proportionnalité si le risque ne paraît pas significatif.

32.... et les moyens de protection

La seconde analyse l'adéquation des combinaisons de moyens de protection aux facteurs de risques retenus par la première étape. Elle se décompose comme suit:

Il convient tout d'abord de déterminer quels principes de fond doivent être affirmés par le moyen d'expression proposé par le pays tiers. Les principes de participation individuelle et de légitimité, sont fondamentaux et leur protection doit en tous les cas être assurée par les pays tiers. Par contre, la nécessité de trouver dans le pays tiers la protection des principes d'exactitude et de proportionnalité est fonction des caractéristiques d'un transfert et de facteurs de risque qu'il génère.

Ensuite, il s'agira d'analyser l'adéquation des moyens d'effectivité proposés pour garantir le respect des principes de fond ainsi déterminés.

33.... Proposition quant à la demarche

La démarche pourrait se résumer comme suit:

a) Moyens d'expression

Il faut, pour chaque principe retenu, déterminer par quel moyen il est exprimé: code de conduite, norme établie par l'autorité publique, etc,...

Pour être retenu, chacun de ces moyens d'expression doit:

- être créateur de droits pour les personnes concernées (voir supra, chapitre III);

- quant à son contenu, faire l'objet d'une information large auprès des responsables de traitement et des personnes concernées;

- s'appliquer aux étrangers non résidents sur le territoire du pays tiers (et en particulier, aux ressortissants de l'Union européenne);

b) Moyens de contrôle

Chaque principe de fond retenu doit voir son effectivité assurée également par des moyens de contrôle. Les moyens de contrôle à rechercher sont, dans tous les cas, ceux qui font partie du "noyau dur de l'effectivité". Il s'agit de mesures de sécurité, de l'existence d'une autorité indépendante de contrôle et de mesures garantissant l'accès des personnes concernées à leurs données.

L'analyse du flux permet de déterminer de façon plus précise quel niveau d'exigence est souhaitable pour admettre ces moyens; elle permet également de déterminer si d'autres moyens de contrôle doivent être exigés. Ainsi, si le flux analysé est un flux "marketing", l'accès des personnes concernées devra leur permettre non seulement de vérifier les données les concernant, mais encore de s'opposer (opt out) au traitement. Si le pays tiers est affecté d'un retard technologique important, il importe que les mesures de sécurité prises par le responsable du traitement tiennent compte de ce facteur. Si le risque de perte de contrôle est accentué par de nombreux facteurs tenant essentiellement à l'éloignement et la difficulté d'atteindre le maître du fichier, la nomination d'un "représentant" sera sans doute nécessaire.

On le voit, il est difficile de dresser un tableau de toutes les combinaisons de moyens possibles: elles sont fonctions d'éléments propres au flux considéré, et sont également influencées par la "différence culturelle". Cependant, il est vraisemblable que la pratique permette de dégager plus systématiquement des moyens ou combinaisons de moyens particulièrement adaptés pour tel ou tel type de flux.

c) Moyens de recours et de sanctions

Il faut ensuite voir à quels moyens de recours et de sanction le moyen d'expression renvoie: s'agit-il d'un moyen de recours particulier à ce moyen d'expression, ou renvoie-t-il plus généralement aux recours judiciaires? Ici aussi, il faudra pour chaque cas analyser l'effectivité des moyens de recours et de sanction. Peu importe leur nature, les moyens de recours doivent d'une part, assurer le droit des personnes concernées à une procédure contradictoire d'accès aisé devant un organe juridictionnel disposant d'une compétence d'exécution de ses décisions. Quant aux moyens de sanction, ils doivent être suffisants pour faire craindre au responsable du traitement un dommage supérieur au bénéfice qu'il tire du non respect des principes. Chaque principe de fond doit être assorti de moyens de recours et de sanction. Cela implique que l'autorité en charge du contrôle pourrait considérer la protection du pays tiers comme inadéquate si aucune sanction appropriée n'est prévue pour l'un ou l'autre principe.

A cette présentation quelque peu sommaire de la démarche proposée, nous joignons en annexe 2, l'analyse de l'application de cette démarche à trois cas présentés dans l'introduction de l'étude.

ANNEXE I

QUESTIONNAIRE

Ndl'A: Au-delà de la synthèse proposée par le rapport, nous avons cru nécessaire de reprendre ci-après les questionnaires ci-joints. Le premier s'attarde à la description du flux et permet un repérage des facteurs de risque selon le tableau proposé au n° 11 du rapport et dès lors des risques pour lesquels une protection adéqaute devra être offerte. Le second caractérise les éléments de la protection offerte par le destinataire tant en ce qui concerne le référent de cette protection (les principes protégés) que les moyens offerts pour assurer cette protection.

I. Description générale du flux

1. Responsable du traitement dans le pays d'origine

Coordonnées complètes du responsable du traitement dans le pays d'origine: nom et prénoms, ou dénomination de la société ou l'association, adresse, secteur d'activité, n° TVA le cas échéant,...

2. Destinataire du fichier dans le pays tiers

A. Coordonnées complètes du destinataire du fichier: pays et région, nom et prénoms ou dénomination de la société ou l'association, adresse, secteur d'activité, ...

B. Le fichier central est-il situé sur le territoire de l'Union Européenne ou dans le pays tiers?

C. Le destinataire est-il un individu ou une organisation directement liés à l'émetteur (autre société du même groupe, filiales, employé ou agent, fournisseurs de biens ou de services,...). Détailler.

D. Dans quelle catégorie d'activité se situe le destinataire:

1. Sociétés privées (Marketing, courtier en données, organisations politiques, associations ou organisations bénévoles, caritatives ou religieuses,...). Détaillez.

2. Services de santé (Mutuelles, hôpitaux, médecins, autres agents du secteur soins de santé,...). Détaillez.

3. Banques et compagnies d'assurances (Banques, compagnies d'assurances, agences d'évaluation de la solvabilité, agences de recouvrement de créances, autres organisations financières,...). Détaillez.

4. Autre catégorie de destinataires de données. Détaillez.

3. Données transférées

A. Quel est le nombre de personnes fichées concernées par le transfert?

B. Quel est le nombre de renseignements transférés?

C. Quel est le contenu des données transférées?

1. Données d'identification (nom, adresse, tél., n° de carte d'identité, de permis de conduire,...). Détaillez.

2. Caractéristiques personnelles (âge, sexe, état-civil, données physiques, nationalité, statut d'immigration, situation militaire, composition du ménage, loisirs et intérêts, habitudes de consommation, éducation et formation,...). Détaillez.

3. Données financières (identifiants financiers, revenus, possessions, investissements, crédits, emprunts, solvabilité, transactions financières, détails, relatifs à la pension ou aux assurances,...). Détaillez.

4. Données relatives à la profession et l'emploi (emploi actuel, détails sur la terminaison d'emploi, historique de carrière, historique de présence et disciplinaire, salaire, évaluation,...). Détaillez.

5. Données judiciaires (suspicions ou mises en accusation, condamnations et peines, mesures judiciaires,...). Détaillez.

6. Données médicales (Relatives à l'état de santé physique ou psychique, aux situations et comportements à risques, aux antécédents médicaux de la personnefichée,...). Détaillez.

7. Données relatives au comportement sexuel de la personne fichée. Détaillez.

8. Données relatives à l'origine raciale ou ethnique de la personne fichée. Détaillez.

9. Données relatives aux convictions religieuses, philosophiques ou politiques de la personne fichée. Détaillez.

10. Données relatives à l'affiliation syndicale de la personne fichée. Détaillez.

11. Autres catégories de données. Détaillez.

4. Finalité du traitement dans le pays tiers

A. Quelle est la finalité du traitement envisagé dans le pays tiers?

1. Gestion des entreprises (administration du personnel, planification des activités, gestion de la clientèle, gestion du contentieux, relations publiques, renseignements technico-commerciaux,...). Détaillez.

2. Justice et police (sécurité publique, enregistrement des condamnations,...). Détaillez.

3. Secteurs bancaire, du crédit et des assurances (gestion des comptes, octroi et gestion des crédits, services liés aux cartes de crédit, services de courtage, vision globale d'un client, gestion des assurances,...). Détaillez.

4. Commerce (vente par correspondance, profilage de la clientèle, marketing direct,...). Détaillez.

5. Enseignement et culture (administration des élèves, gestion de bibliothèque,...). Détaillez.

6. Soins de santé (soins des patients, administration des hôpitaux, enregistrements de groupes à risques, enregistrement de donneurs,...)

7. Recherche scientifique (recherches épidémiologiques, recherches bio-médicales,...). Détaillez.

8. Autres buts (à définir par le maître du fichier)

B. La finalité du traitement dans le pays tiers est-elle identique à celle poursuivie par l'émetteur des données

5. Périodicité du flux

Quelle est la fréquence des transferts pour lesquels l'autorisation est demandée?

- Permanent
- Régulier
- Exceptionnel

6. Durée de traitement prévue par le destinataire

A. Quelle durée de conservation est-elle envisagée pour les données après leur enregistrement par le destinataire?

1. Pas de conservation (destruction immédiate)`

2. Durée de conservation limitée (préciser dans ce cas la durée de conservation en mois et en années, et le but de la conservation- par exemple, à fin de preuve)

3. Durée de conservation illimitée (Préciser les raisons)

7. Moyens de transfert

A. Quel est le moyen de transfert choisi (réseau, transfert physique,...)?

B. S'il s'agit d'un réseau, s'agit-il d'un réseau fermé (ex: Galileo) ou ouvert (Internet)? Détailler.

II. Niveau de protection du pays tiers

1. Les principes de fond

Les questions qui suivent visent à déterminer si, dans l'un ou l'autre des moyens d'expression mentionnés par après (normes issues de l'autorité publique, standards, privacy policy, etc,...), les principes suivants sont exprimés, et selon quelles modalités.

8. Principe de participation individuelle

Le(s) moyen(s) d'expression existant(s) envisagent-ils les points suivants:

A. Les personnes concernées ont-elles la possibilité d'obtenir les informations qu'elles souhaitent sur le traitement des données les concernant?

B. Peuvent-elles prendre connaissance des données détenues par le responsable du traitement?

C. Peuvent-elles faire rectifier ou effacer les données incomplètes ou inexactes?

D. Le responsable du traitement a-t-il l'obligation de prendre l'initiative d'informer les personnes concernées sur le traitement qu'il effectue?

E. Le traitement peut-il se faire sans le consentement de la personne concernée?

F. Les personnes concernées ont-elles la possibilité de s'opposer au traitement des données les concernant? Pour quel motif? Cette possibilité existe-t-elle dans tous les secteurs?

9. Principe de finalité

A. Les moyens d'expression prévoient-ils que la ou les finalités du traitement des données collectées doivent être légitimes?

B. Quels critères permettent d'apprécier la légitimité?

C. Existe-il une liste des traitements toujours considérés comme illégitimes?

D. Cette exigence de légitimité peut-elle être supprimée (dans le cas où la personne concernée a donné son consentement au traitement de ses données, par exemple? Détaillez)

E. Les normes prévoient-elles des limites à la réutilisation des données?

F. Plus spécifiquement, prévoient-elles que les données peuvent être communiquées à un tiers ou utilisées à des fins autres que celles pour lesquelles elles ont été transférées par l'émetteur:

1. en aucun cas?

2. dans des cas précis (consentement de la personne, protection d'un intérêt public du pays tiers,...)? Détaillez.

G. Si ces réutilisations sont permises, existe-t-il des dispositions telles que:

1. l''information de la personne concernée. Par quel moyen? Quel est le contenu de cette information?

2. La possibilité pour la personne fichée de s'opposer à cette réutilisation?

3. Autres? Détaillez.

H. Les moyens d'expression prévoient-ils que la ou les finalités du traitement des données collectées doivent être déterminées (à quel moment doivent-elles être déterminées?)

I. Existe-t-il des mesures spécifiques de protection concernant les transferts transfrontières de données au départ du pays tiers? Lesquelles?

10. Principe de proportionnalité

A. Les données traitées doivent-elles être impérativement en rapport avec la finalité du traitement?

B. Ce rapport est-il défini strictement?

C. Des données peuvent-elles être conservées au-delà de la durée nécessaire à la réalisation du traitement correspondant à la finalité initiale?

11. Principe de qualité des données

A. Le(s) moyen(s) d'expression prévoient-ils des conditions de qualité des données?

B. Plus spécifiquement, est-il prévu que les données doivent être:

1. Tenues à jour? (Des mécanisme-s précis sont-ils exigés pour assurer la mise à jour?)

2. Exactes?

3. Complètes?

4. Autres exigences? Détaillez.

C. L'obligation mise à charge de l'utilisateur des données en matière de qualité des données est-elle une obligation de moyens ou de résultat?

2. Effectivité des principes de fond

Moyens d'expression

Quelle est la nature des moyens d'expression des principes de fond dans le pays destinataire? (Répondez le cas échéant de manière distincte pour chaque principe)

12. Privacy Policy

A. L'entreprise destinataire a-t-elle une privacy policy?

B. Si oui, ce texte fait-il l'objet de publication ?

C. Ces publications sont-elles accessibles au public en général? Comment?

D. Quels sont les moyens internes mis en place au sein de l'entreprise destinataire pour contrôler le respect de la *privacy policy* ?

E. L'adoption d'une privacy policy est-elle une condition d'obtention d'un certificat ? du respect d'un code de conduite ?

F. A votre connaissance un tribunal peut-il sur base de sa *privacy policy* condamner l'entreprise destinataire en cas de non respect ?

13. Standardisation

A. L'entreprise ou organisme destinataire des données a-t-il obtenu un certificat de respect d'une norme fixée par un organisme de normalisation? Si oui, quel est cet organisme?

B. Cette norme implique-t-elle le respect de principes de fond de la protection des données? Enoncez le contenu des mesures concernant la protection de la vie privée.

C. Y a-t-il eu une participation à la conception du standard des différents acteurs intéressés à la protection des données? Par quel moyen?

D. Le standard en question, ainsi que ses conditions d'obtention, sont-ils publiés?

E. L'organisme certificateur ou d'autres sociétés effectuent-ils des missions d'audit afin de vérifier le respect de la norme? Si oui:

- quelles sont les conditions d'agréation de la société auditrice?

- à quelle fréquence l'audit se fait-il?

- quels sont les pouvoirs de sanction éventuels de la société auditrice?

14. Code de conduite sectoriel

A. L'entreprise ou organisme destinataire des données respectent-ils un code de conduite contenant des dispositions en matière de principes de fond de la protection des données?

B. Ce code a-t-il été négocié avec des instances extérieures au secteur professionnel concerné? En particulier, les personnes concernées autres que les responsables du traitement ont-elles pu participer à sa conception?

C. De quelle représentativité au sein du secteur jouissent les associations qui ont promulgué ce code?

D. Ce code a-t-il été publié ou mis à disposition du public d'une autre façon?

E. Existe-t-il un mécanisme de contrôle du respect de ce code? Le code prévoit-il lui-même ce mécanisme, ou renvoie-t-il à un contrôle externe?

F. Le code prévoit-il des sanctions pour le non-respect des règles qu'il édicte? Si non, renvoie-t-il à des sanctions externes?

15. Normes issues de l'autorité publique

A. Existe-t-il dans le pays (ou Etat, ou région) destinataire des normes issues de l'autorité publique ayant pour objet, direct ou indirect la protection des principes fondamentaux de protection des données? Dans l'affirmative, fournissez-en le texte.

B. La norme étend-elle la protection qu'elle institue aux étrangers non-résidents dans le pays tiers?

C. Quelle est la place, dans la hiérarchie du pays tiers, de l'autorité qui a édicté la norme?

D. S'agit-il d'une norme générale, sectorielle, ou spécifique à certaines activités ou opérations?

E. La norme prévoit-elle des sanctions?

- Si oui, de quelle nature sont-elles?

- De quelle instance émanent-elles

- Existe-t-il à votre connaissance, une jurisprudence en cette matière?

Moyens de contrôle

16. Mesures de sécurité

A. Existe-t-il dans l'entreprise ou organisme destinataire des données:

- des protections logiques, contrôlant les accès au réseau et aux fichiers? Lesquelles?

Les données transférées sont-elles cryptées? Si oui, quel est le système utilisé?

- des systèmes de sécurité physique protégeant les sites d'exploitation? Lesquels?

- des dispositifs de back-up, concernant aussi bien les réseaux que les fichiers (permettant de redémarrer rapidement après un incident)? Détailler.

- des mesures organisationnelles ayant pour objet d'assurer la sécurité interne des données?

B. Des mesures de sécurité sont-elles spécifiquement imposées par un des moyens d'expression cités ci-dessus (certification, code de conduite, norme issue de l'autorité publique,...)?

17. Autorité indépendante de contrôle

A. Existe-t-il une instance de contrôle du respect des principes de fond cités ci-dessus?

B. Est-ce une instance spécifique à la protection des données?

C. Par qui a-t-elle été instituée?

D. Quelle est sa composition?

- A-t-elle un personnel spécifique?

- A-t-elle un personnel permanent?

- Travaille-t-elle en relation avec des "relais" (organes de certification,...) dans certains secteurs?

E. Quels sont les missions et les compétences de cette instance?

F. Des mesures de publicité sont-elles prévues pour les décisions prises par cette instance? Lesquelles? Publie-t-elle un rapport d'activité?

G. A-t-elle des pouvoirs d'investigation:

- propres?

- avec le concours de l'autorité publique?

H. Les particuliers peuvent-ils introduire une plainte à propos d'un traitement de données les concernant auprès de cette instance?Si oui, selon quelles modalités (coût, délais,...)?

I. Cette instance dispose-t-elle de moyens de contrainte suffisants pour contraindre les responsables de traitements à suivre ses avis ou recommandations?

J. A-t-elle des pouvoirs de sanction propres?

- Si oui, lesquels,

- Le pouvoir judiciaire a-t-il l'obligation de sanctionner les infractions constatées par cette instance?

18. Accès des personnes concernées

A. Les personnes concernées reçoivent-elles une information au sujet du traitement opéré dans le pays tiers?

- A quel moment?

- L'information est-elle donnée spontanément par le maître du fichier, ou sur demande?

- Sur quels éléments porte l'information?

- Que peut exiger la personne concernée sur base de cette information (rectification, opposition au traitement, effacement des données,...)?

B. La personne concernée bénéficie-t-elle d'une aide pour lui faciliter l'accès à ses données (intervention d'une autorité indépendante de contrôle, d'un représentant en Europe, d'un détaché à la protection des données,...)?

C. L'exercice de l'accès est-il payant?

19. Détaché à la protection des données

A. Existe-t-il au sein de l'entreprise ou organisme destinataire des données une personne ou un service compétent pour vérifier à l'intérieur de l'organisation le respect des principes de protection des données et pour accueillir les plaintes et demandes des personnes concernées?

B. Le détaché a-t-il fait l'objet d'une désignation publique?

C. Quelle place occupe-t-il dans l'organigramme de l'entreprise ou organisme destinataire?

D. Le détaché rend-il public un rapport de ses missions?

E. Le détaché dispose-t-il de pouvoirs d'invetigation au sein de l'&?

20. Représentant

A. L'& a-t-elle chargé une organisation située sur le territoire de l'Union Européenne de veiller au respect des prescrits de la directive européenne à propos du traitement opéré dans le pays tiers?

B. La nomination du représentant a-t-elle été portée à la connaissance des personnes concernées? Par quel moyen?

C. Les missions du représentant sont-elles définies par un contrat?

- Quelles sont-elles?

- Le contenu de ce contrat est-il accessible aux personnes concernées ou aux autorités de protection des données?

D. Des sanctions sont-elles prévues pour le cas où le responsable du traitement à l'étranger ne respecte pas ses engagements (prévus éventuellement par le contrat)?

21. Audits

A. L'entreprise ou organisation destinataire des données est-elle soumise à un audit visant à vérifier le respect par elle:

- de mesures de sécurité?

- de l'ensemble des principes de fond de la protection des données?

B. Par qui cet audit est-il effectué?

C. La firme auditrice doit-elle:

- être agréée?

- répondre à des conditions d'indépendance par rapport à l'entreprise ou organisation faisant l'objet de l'audit?

D. Que comporte le mandat de l'auditeur en terme de pouvoirs d'investigation?

E. L'entreprise ou organisation faisant l'objet de l'audit est-elle tenue de suivre les recommandations de l'auditeur?

F. Les résultats de l'audit sont-ils rendus publics?

c. Autres types de protection

Existe-t-il d'autres instruments applicables à ce flux:

1. Statuts de l'entreprise ou institution destinataire

2. Jurisprudence (vérifier alors sa force contraignante)

3. Principes généraux du droit

4. Présence d'un médiateur ou ombudsman au sein de l'entreprise (ayant éventuellement développé une jurisprudence interne)

5. Autres:...

d. Mesures de protection et normes ayant d'autres objets

Il est possible que l'on ne trouve aucune norme ayant pour objet spécifique la protection de la vie privée: il convient alors de voir si d'autres normes peuvent être applicables. On cite, par exemple (liste non exhaustive, bien entendu):

1. Secret médical (quelle est sa force juridique, qui est lié, quelle est sa portée sur l'accès aux données ou leur transfert)

2. Secret bancaire

3. Responsabilité du fait de l'information

4. Réglementation en matière de télécommunications

5. Normes en matières d'écoutes téléphoniques

6. Autres

Les mécanismes et normes de protection s'appliquent-ils

Les mécanismes et normes de protection s'appliquent-ils à toutes les données contenues dans le flux ou à une partie de celles-ci?

2.e. Cas particuliers

Les questions suivantes ne seront posées que si la réponse aux questions correspondantes dans la première partie de la check-list l'exige.

(i) Données jugées "sensibles"

Existe-t-il une protection particulière pour les données sensibles (du type de celles contenues dans le flux) dans le pays tiers? Comment opère-t-elle?

Si non, le niveau de protection offert en général est-il suffisant pour autoriser malgré tout le transfert?

(ii) Durée du traitement

Le pays tiers prévoit-il des durées d'utilisation maximales?

3. Respect de ces principes: effectivité du contrôle et recours de la personne fichée

8. Mesures de sécurité

3.a. Mesures garantissant le respect des mécanismes et normes de protection des données personnelles

Comment le responsable est-il informé de ses obligations en matière de protection des données personnelles?

Comment s'assure-t-il de la connaissance et du respect de ces principes protecteurs par les personnes qui prestent des services en sa faveur?

Le respect par le responsable du traitement des données de ces principes protecteurs a-t-il été vérifié par une instance extérieure ?

Dans l'affirmative, quelle est cette instance? (Description)

Quel est son degré d'indépendance par rapport à la société contrôlée? (Expliquer)

Par quels moyens procède-t-elle aux vérifications nécessaires?

Un système d'audit est-il mis en place sur une place régulière?

S'agit-il d'un audit interne ou externe?

Quelle est la force contraignante des résultats de l'audit?

Quelles sanctions frappent-elles le responsable du traitement s'il ne respecte pas ses obligations en matière de protection des données?

Les sanctions sont-elles de nature:

1. pénale

2. civile

3. déontologique (exclusion, amende, suspension, autres...)

De qui émanent-elles : instance indépendante, ombudsman ...?

3.a. Information et recours de la personne fichée

1. Comment les personnes concernées peuvent-elles connaître leurs droits dans cette matière?

2. Les personnes fichées disposent-elles d'un droit de recours? Comment peut-il être exercé, le cas échéant?

3. En-dehors des procédures judiciaires, existe-t-il d'autres voies de recours ouvertes aux personnes concernées? Détaillez.

4.

ANNEXE II

ANALYSE DE 3 FLUX-TEST

L'introduction du rapport décrivait quelques cas de flux transfrontières. L'annexe applique à trois des cas mentionnés, l'examen méthodologique proposé. Sans doute, outre une démonstration de la démarche, les lecteurs y trouveront des enseignements utiles sur la variété des situations rencontrées.

Le premier cas analyse, à travers deux variantes, un transfert de données relatives à la gestion du personnel, transfert opéré au sein d'une multinationale ayant son siège central hors Europe;

Le deuxième cas concerne le transfert de données "marketing", opéré par une société européenne vers un sous traitant d'Europe de l'Est; sous traitance expliquée par les coûts réduits de personnel dans ce pays.

Le troisième cas s'intéresse au transfert opéré vers un site www Internet, localisé en Colombie Britannique et dont le responsable s'engage à respecter le "Canadian Standard Association Model Code".

Les 3 cas seront analysés selon la méthodologie présentée dans le rapport

A. Présentation du cas

B. Collecte des informations nécessaires à l'évaluation

C. Analyse des flux

D. Analyse de la protection offerte par le pays tiers in casu

E. Apport de l'analyse de ce flux test

Premier cas : Transfert de données relatives à la gestion du personnel à l'intérieur d'un groupe

A. Présentation du cas

On se base ici (en le modifiant légèrement) sur l'exemple donné dans l'introduction de la présente étude, relatif à la création par une société étrangère disposant de sièges en Europe, d'une banque de données relatives au personnel de cadre, où qu'il soit et recensant des renseignements de tous ordres. Il s'agit, pour cette société, de pouvoir répondre facilement à des besoins internes de la compagnie comme celui de la constitution d'équipes de prospection d'un nouveau marché, de la recherche de formateurs, voire de la création d'une équipe sportive,... Ces données collectées à partir de multiples sources -formulaires ou interviews lors des candidatures, appréciation par des supérieurs hiérarchiques, participation à des cycles de formation- sont en l'occurrence assemblées et envoyées à partir de lieux divers (centres de formation, directions du personnel des différentes entités locales,...) aux services centraux de direction du personnel de la multinationale.

B. Collecte des informations nécessaires à l'évaluation

Ici, l'émetteur et le destinataire sont liés, puisqu'il s'agit d'une part de filiales, et d'autre part, de la société-mère. On demandera donc à l'émetteur des renseignements à la fois sur le flux considéré et dans le chef de l'entreprise destinataire sur l'existence éventuelle et le contenu d'un code de conduite ou d'une *privacy policy*. Les autres questions seront posées à des spécialistes du pays tiers.

C. Analyse du flux :

Variante 1

a) La société-mère est une société de pétrochimie implantée dans un pays du Sud-Est Le tableau des risques[1] pour ce flux se présente comme suit (il sera commenté ci-dessous):

[1] ... établi conformément à la grille d'identification des risques présentée dans le rapport.

Risques **Facteurs d'influence**	Perte de contrôle	Réutilisation	Manque de proportionnalité	Inexactitude des données	Observations
Situation socio-politique					
Retard technologique					
Technologie avancée					
Collecte indirecte des données	+[2]	+			
Sensibilité des données					
Nombre de renseignements transférés					
Nombre de personnes concernées					
Fréquence des flux		-		-	
Type de réseau utilisé	-	-			
Localisation du fichier central	+				
Liens entre acteurs	-				
Secteur d'activité du destinataire	-	-			
Cohérence dans les finalités	-	-			
Durée de conservation des données			+	+	
Détermination de la finalité	-	-			
Risques de retransfert	-	-			

On le voit, peu de risques se posent à cause du pays de destination lui-même: la situation socio-politique y est stable, l'état de la technologie y est assez avancé (mais les croisements de fichiers n'y sont pas une habitude répandue. Cette information ressort de l'analyse de la "différence culturelle".

Le flux lui-même présente quelques facteurs aggravant le risque: le fait que les données n'ont pas toutes été collectées auprès des personnes concernées elle-même, la fréquence des transferts, la localisation de la société-mère, et donc du fichier central et de l'archivage des données hors de l'Union Européenne, ainsi que l'indétermination de la durée d'utilisation et de conservation des données.

Par contre, d'autres éléments diminuent le risque: le réseau utilisé est un Intranet totalement sécurisé, il existe un lien organique entre les acteurs, le secteur d'activité du destinataire n'est pas "dangereux" (sa raison sociale n'est pas le commerce de données, et, par hypothèse, la société n'est active que dans le secteur de la pétrochimie, et n'a donc

[2] pour rappel, le signe + désigne une augmentation du risque, le signe - une diminution du risque.

pas d'intérêt à faire profiter d'autres sociétés du groupe ayant d'autres activités des informations obtenues), la cohérence des finalités (gestion du personnel), et la détermination des finalités. Enfin, ce transfert ne comprend pas de données sensibles (aucune donnée médicale concernant le personnel, par exemple).

Les facteurs propres à ces transferts et aggravant les risques sont donc relativement peu nombreux. Néanmoins, certains risques sont présents: perte de contrôle, car les données provenant de différentes sources sont utilisées, et il peut être difficile pour la personne concernée de garder une maîtrise sur l'image d'elle que peuvent donner toutes ces informations rassemblées et recoupées. Le risque de réutilisation est également présent: si aucune norme ne l'empêche, la société mère peut tirer un bénéfice certain de la vente des informations sur ses employés, car, par hypothèse, ces informations peuvent donner un profil assez précis des personnes concernées. Enfin, l'indétermination de la durée de conservation des données crée un risque de manque de proportionnalité et d'inexactitude des données (ce dernier risque étant encore aggravé par la fréquence des flux).

b) Mesures envisageables au niveau des facteurs de risque

Il est possible de proposer à la société émettrice de prendre des mesures de manière à diminuer un risque propre au flux, ce qui permet de ne pas considérer la présence du principe correspondant dans le pays tiers comme fondamentale. Le risque considéré est, en l'occurrence, celui de manque de proportionnalité des données, qui ne nous semble provoqué que par l'indétermination de la durée de conservation des données par la société. Dès lors, en proposant à la société émettrice de ne transmettre les données personnelles à la société mère qu'à condition de définir la durée de conservation de ces données, le risque de manque de proportionnalité est sérieusement limité.

Variante 2

La société-mère est une société minière implantée dans un pays d'Afrique centrale en proie à des troubles économiques et politiques importants, ayant entre autres pour conséquence une désorganisation du système judiciaire, une insécurité importante, et une corruption présente à tous les niveaux de la société.

Il paraît clair que, dans ce cas, la simple accumulation de facteurs propres au pays tiers et aggravant le risque peut mener à un refus de transfert des données sans qu'il faille prendre en considération d'autres informations relatives au flux, voire à l'existence d'instruments de protection de ce pays, car on ne voit pas comment ils pourraient être effectifs.

D) Analyse de la protection par le pays tiers in casu

Variante 1

L'hypothèse reprise ici est celle qui a été développée ci-dessous comme "variante 1": la société-mère est une société de pétrochimie implantée dans un pays d'Asie du Sud-Est, que nous appellerons "pays A".

a) Principes de fond

Il ressort de l'analyse des risques que les principes dont il faut rechercher l'effectivité dans le pays A sont, outre ceux de participation individuelle et de finalité (qui font de toute manière partie du noyau dur), celui de qualité des données. Nous retenons ici

l'hypothèse ou la société a accepté de limiter la durée de conservation des données (le principe de proportionnalité ne doit pas être recherché).

b) Effectivité des principes de fond

1. Moyens d'expression et de sanction

La collecte des informations a permis de trouver dans le pays A deux moyens d'expression qui peuvent être pertinents:

- un décret d'exécution d'une loi portant sur les relations de travail (ce décret d'exécution porte spécifiquement sur le traitement des données, qu'elles soient à caractère personnel ou qu'il s'agisse de données de recherche scientifique,...);

- un code de conduite édicté par le secteur des industries chimiques du pays.

Le décret a été pris par le Ministère de l'Industrie et est applicable à toutes les données traitées par les entreprises du pays, quel que soit leur contenu: le critère de rattachement est le lieu du traitement. Il protège donc bien les données personnelles concernant les Européens. Il prévoit des sanctions pénales en cas de défaillance du maître du fichier, et renvoie à une procédure simplifiée pour l'obtention éventuelle de dommages et intérêts. Ce décret correspond donc aux conditions définies dans le chapitre III pour être pris en compte comme moyen d'expression.

Toutefois, on ne peut en rester là pour la recherche de moyens d'expression, car ce décret n'édicte de règles qu'en matière d'information des personnes concernées, de qualité et de proportionnalité des données (ces derniers principes ne doivent, par hypothèse, pas être retenus ici). Par contre, ce décret ne contient pas de disposition en matière de légitimité des finalités de traitement des données, ni d'ailleurs en matière de flux transfrontières au départ du pays A.

Il convient alors d'examiner si le code de conduite, appliqué dans le secteur des industries chimiques du pays règle ces questions.

Hypothèse 1: le code de conduite ne traite pas de ces questions. Dans ce cas, si l'on ne peut pas trouver d'autre moyen d'expression qui contienne ces principes, la protection nous paraît inadéquate. En effet, le principe de légitimité est fondamental et fait partie du noyau dur; en outre, la question des flux transfrontières au départ du pays tiers n'est pas réglée, ce qui fait perdre son effectivité à l'ensemble du système de protection des données personnelles, y compris celle assurée par le décret.

On peut imaginer alors que les sociétés émettrice et réceptrices choisissent de régler cette question par contrat.

Hypothèse 2: le code de conduite reprend ces questions. Il convient alors d'examiner si le code de conduite peut être pris en compte comme moyen d'expression. Il est créateur de droits pour les personnes concernées car, dans le pays A, les codes de conduite doivent être approuvés officiellement par le ministère dont dépend l'entreprise ou le secteur qui l'édicte. Le code que nous examinons engage le responsable du traitement et peut être invoqué devant les tribunaux. Il protège également les données personnelles concernant des ressortissants de l'Union européenne, car il vise, comme le décret, toutes les données traitées par l'entreprise, indépendamment de leur provenance et de leur type.

Le mode d'élaboration de ce code de conduite répond par hypothèse aux conditions d'effectivité définies pour ce moyen d'expression dans le chapitre III de la présente étude. Il n'a pas fait l'objet d'une décision unilatérale par les responsables de traitement, mais a impliqué des représentants des travailleurs, ainsi que des membres de l'administration, qui ont entre autres eu pour mission de vérifier la réelle participation de toutes les parties

concernées à l'élaboration du code. Cette condition (participation des différentes parties concernées) est particulièrement importante dans ce cas-ci, puisque l'on recherche une expression correcte du principe de finalité. Il faut en outre que la définition des conditions de légitimité des finalités ne soit pas conçue unilatéralement par les seuls responsables de traitements. Depuis, dans la mesure où ce code est appliqué dans l'ensemble des industries chimiques du pays, il ne représente pas un point de vue minoritaire. Enfin, l'existence de ce code est connue, et l'entreprise a pour pratique d'en donner une copie à tous ses employés lors de leur engagement.

Le code de conduite envisagé renvoie à des sanctions de type civil: les personnes concernées peuvent s'en prévaloir de la même façon que si ses dispositions étaient incorporées à leur contrat de travail.

Enfin, il prévoit que les données traitées par l'entreprise ne peuvent être transférées à l'étranger qu'à la condition d'y bénéficier d'une protection identique à celles dont elles bénéficient dans le pays A.

2. *Moyens de contrôle*

Il faudra rechercher ici les moyens d'effectivité de chaque principe de fond retenu: il faut que, pour chacun, les conditions minimales d'effectivité (voir *supra*) soit présentes (mais il est possible que certains éléments de ces conditions minimales soient communes aux deux principes).

Chaque moyen d'effectivité doit être examiné en fonction de ce que l'on en dit dans le chapitre III de la présente étude.

2.1. Effectivité des principes de participation individuelle et de qualité

- Mesures de sécurité

Outre les données personnelles des employés, la société A traite des données scientifiques et commerciales d'une importance économique vitale pour elle. Son système informatique est extrêmement sécurisé, et les données sont protégées contre la destruction, l'altération et la divulgation à des tiers non autorisés par des moyens physiques (accès aux locaux uniquement grâce à des cartes magnétiques, ...) et techniques (accès aux données limité à une partie du personnel selon ses fonctions, système de back-ups centraux fréquents,...) très complets. Notons qu'une partie des mesures de sécurité (en partie les questions d'accès du personnel aux données) est réglée par le code de conduite que l'on a examiné ci-dessus; le reste des mesures est pris volontairement par l'entreprise.

- Autorité indépendante de contrôle

Dans le pays A, les entreprises sont soumises à des contrôles fréquents par les ministères dont elles dépendent. Ces contrôles ont pour objet non seulement des vérifications financières ou comptables, mais encore le respect de toutes les réglementations en vigueur dans le pays et concernant les dites entreprises (entre autres, donc, le décret sur le traitement des données personnelles). Pourrait-on dès lors considérer les ministères comme autorités indépendantes de contrôle pour les entreprises qui en dépendent? Il faut, pour répondre à cette question, vérifier différents éléments:

- Fonctions remplies par ces organes: les ministères ont dans le système du pays A, des fonctions de promotion et de respect des principes de fond énoncés par la loi. Ils vérifient en outre que l'accès aux données soit aisé, et interviennent en cas de difficulté; les personnes concernées peuvent s'adresser à eux en cas de refus d'accès, de correction, ou

d'effacement de la part du responsable du traitement. Les ministères ont alors un pouvoir d'injonction vis-à-vis des entreprises concernées. Ceci n'exclut d'ailleurs pas des recours judiciaires.

- Indépendance de ces organes: du point de vue de leur composition, les ministères peuvent être considérés comme indépendants des entreprises privées, à condition toutefois que l'Etat n'ait pas une participation importante dans les dites entreprises. Dans ce cas, l'entreprise et l'Etat seraient trop liés pour que les ministères satisfassent au requis d'indépendance. Dans le flux-test que nous examinons ici, ce n'est par hypothèse pas le cas.

Le fonctionnement des ministères n'est pas totalement transparent (pas de publication d'un rapport d'activités, par exemple), mais les décisions prises sont accessibles au public, et, après leur signification à la personne concernée, peuvent faire l'objet d'un recours soit devant les tribunaux administratifs, soit devant une autorité supervisant le travail des ministères. Dès lors, il nous semble que le fonctionnement est suffisamment transparent; en outre, les ministères jouissent de considérables pouvoirs d'investigation, sur plainte ou d'initiative, ce qui leur assure un certain degré d'indépendance par rapport aux responsables de traitement qu'ils contrôlent.

- accessibilité: les ministères sont facilement accessibles, et leur existence est forcément connue. Le seul problème pour les personnes concernées, peut être de savoir de quel ministère dépend l'entreprise qui traite leurs données, mais il existe un système de renvoi entre ministères.

La saisine est gratuite et les ministères sont tenus de répondre aux demandes dans un délai déterminé.

- Effectivité des mesures prises par ces ministères: tant les moyens d'investigation des ministères que leurs moyens de contrainte vis-à-vis des entreprises, sont importants. Les sanctions qui peuvent être prises à l'égard de responsables de traitements défaillants sont assez lourdes (amendes, retrait de licence,...).

Il nous semble donc que, dans le cas analysé, le ministère titulaire peut jouer le rôle d'autorité indépendante de contrôle (sans être du tout créé sur le modèle occidental). Notons que le coefficient "différence culturelle" intervient également: dans le pays A, l'administration a un rôle très actif, et respecté. Une entreprise qui aurait fait l'objet d'une sanction de la part de son ministère de contrôle souffrirait d'une très mauvaise publicité, que ce soit auprès du public ou dans son secteur d'activité. Ceci renforce l'effectivité de ce moyen de contrôle.

- Accès de la personne concernée

En matière d'accès et d'information de la personne concernée, on note deux types de mesures; les unes sont imposées par le décret, et les autres sont prises sur initiative de la société-mère.

Le décret fait peser sur le responsable du traitement une série d'obligations en matière d'information de la personne concernée; en outre, nous avons déjà vu que les ministères devaient vérifier le respect de ces obligations, et pouvaient intervenir pour en exiger l'application de mesures appropriées.

Une information très complète doit être donnée à la personne concernée lors de la collecte (ce qui ne nous concerne pas ici, puisque, par hypothès, la collecte a été effectuée en Europe), ou lors d'un changement de finalité de traitement, ou, de toute manière, une fois par an. Cette information porte aussi bien sur les données détenues par le responsable que

sur les finalités du traitement, ainsi que les modalités d'accès, ou les possibilités de rectification ou de radiation de certaines données.

L'entreprise que nous examinons a mis en place ce système d'information; pour les membres de son personnel localisés à l'étranger (sur le territoire de l'Union européenne, par exemple), elle a prévu que l'information puisse se faire sur demande, en faisant transiter cette demande par un service responsable établi dans sa plus importante filiale européenne, située à Manchester. Notons qu'il ne s'agit pas de la formule du "représentant" dont il est question dans le chapitre III de la présente étude, car le service en question n'a pas pour fonction de veiller au respect du prescrit de la directive; il doit jouer un rôle d'intermédiaire entre la maison-mère et les filiales pour tout ce qui concerne la gestion du personnel. Toutefois, son existence facilite considérablement l'accès des personnes concernées aux données et renforce l'impact de ce moyen de contrôle.

A ce stade, on le voit, les conditions normales d'effectivité sont présentes pour les principes de participation individuelle et de qualité des données. On pourrait, nous semble-t-il, s'arrêter ici dans l'analyse des moyens d'effectivité, et considérer la protection du pays A comme adéquate pour ces principes: le flux présentant un nombre peu élevé de facteurs de risque, et l'efficacité présumée des trois moyens de contrôle précités sont des facteurs positifs. En outre, la présence officielle d'un relai européen, même s'il ne peut être considéré comme un "représentant" est également un point important.

Toutefois, on note qu'il existe un dernier moyen de contrôle: un système de notification préventive auprès des ministères responsables. La notification doit être réitérée à chaque changement d'éléments importants du traitement: finalité, données concernées,... Sur base de ces notifications, les autorités de contrôle peuvent prendre diverses mesures préventives, comme par exemple, la négociation avec l'entreprise concernée d'une meilleure spécification de la finalité du traitement, ou la prise de mesures de sécurité adéquates.

2.2. **Effectivité du principe de finalité**

Il s'agit du principe qui était exprimé dans le code de conduite. Notons que certains moyens de contrôle peuvent être communs avec ceux que nous venons de mentionner pour les principes énoncés dans le décret. Ainsi, les mesures de sécurité prises par l'entreprise assurent l'effectivité du principe de légitimité des finalités aussi bien que des autres principes cités plus haut. En ce qui concerne les autres moyens de contrôle, il convient également de voir s'ils assurent l'effectivité du principe de finalité. Ainsi, par exemple, l'autorité indépendante de contrôle peut être identique, mais il faut vérifier si ses pouvoirs d'investigation, de sanction, etc,... portent également sur le principe de finalité.

- Autorité indépendante de contrôle

Dans le pays A, on l'a dit, l'application des codes de conduite est supervisée par les ministères. On renvoie à l'examen qui en a été fait ci-dessus et tendait à montrer que ces ministères répondent aux conditions fonctionnelles pour être considérés comme des autorités indépendantes de contrôle. Dans la mesure où leurs tâches de contrôle portent également sur le contenu des codes de conduite, on peut considérer que ce moyen de contrôle est rempli ici aussi.

Notons qu'on aurait pu concevoir qu'il existe une autre autorité indépendante de contrôle pour ce principe, comme par exemple, une commission sectorielle mise en place par le code de conduite. Il aurait fallu dans ce cas analyser cette commission de façon à voir si elle pouvait être considérée comme autorité indépendante.

- Accès

On a déjà détaillé précédemment les mesures prises par le responsable du traitement pour assurer l'accès des personnes concernées aux données. Il convient donc d'examiner ici si cet accès permet aux personnes concernées une vérification, voire une contestation de la légitimité du traitement, et, en outre, si l'autorité indépendante de contrôle peut les aider dans ces démarches, en cas de problème ou de contestation. Dans ce cas-ci, le code de conduite renvoie à l'action de ces ministères qui peuvent assurer le respect du code de conduite comme s'il s'agissait d'une norme issue de l'autorité publique.

E) Conclusion de l'analyse de ce flux-test

Le noyau dur est présent dans le pays tiers, tant au niveau des principes de fond que de leur effectivité (expression, contrôle et sanction). Des recours sont accessibles aux personnes concernées en cas de défaillance, que ce soir à un niveau interne à l'entreprise (par le relai installé en Europe), à un niveau administratif (autorité indépendante de contrôle) ou à un niveau judiciaire (procédure devant les tribunaux). A cet égard, on relève l'existence de sanctions pénales, ce qui permet éventuellement à la personne concernée de s'appuyer sur la coopération entre polices en cas d'infraction au décret.

Il nous semble donc que le transfert effectué dans ces conditions peut être autorisé.

Deuxième cas : Transfert massif de données pour la constitution de fichiers marketing vers un pays d'Europe de l'Est

A) Présentation du cas

Une entreprise belge de sondages marketing collecte les données principalement auprès de la personne concernée à partir d'un vaste questionnaire portant sur les habitudes de consommation (voyages, alimentation, culture,...). Elle vend les données obtenues à une société sise dans un pays tiers qui exécute les tâches d'encodage, de triage, voire de sélection. Les données sont transférées sur un support papier. Une fois encodées dans le pays tiers, ces données sont croisées avec d'autres données: numéro de téléphone, importance de la localité, type de quartier (revenu moyen par habitant, etc...) provenant de sources publiques accessibles directement de l'étranger ou transférées par support informatique. Une fois triées, ces listes sont revendues à différents clients désireux de commercialiser certains produits sur le marché belge auprès d'un public ciblé.

B. Collecte des informations nécessaires à l'évaluation

Les informations concernant le flux seront demandées à l'émetteur (la société belge). Dans la mesure où les sociétés émettrice et réceptrice ne sont pas organiquement liées, toutes les informations concernant le pays tiers devront être demandées à des experts en la matière.

C. Analyse du flux et de la protection du pays tiers

Le pays tiers est un pays d'Europe de l'Est à l'industrie très peu développée.

a) Analyse des risques

Le tableau des risques se présente comme suit:

Risques **Facteurs d'influence**	Perte de contrôle	Réutilisa-tion	Manque de propor-tionnalité	Inexacti-tude des données	Observa-tions
Situation socio-politique					
Retard technologique	+	+			
Technologie avancée					
Collecte indirecte des données					(1)
Sensibilité des données					(2)
Nombre de renseignements transférés			+		
Nombre de personnes concernées					
Fréquence des flux					
Type de transfert	+	+			
Localisation du fichier central	+				
Liens entre acteurs	+				
Secteur d'activité du destinataire	+	+			
Cohérence dans les finalités					
Durée de conservation des données					
Détermination de la finalité					
Risques de retranfert	+	+	+		

Observations:

- Observation (1): la collecte d'une partie des données a été faite directement auprès des personnes concernées, mais cet élément ne nous paraît pas être de nature à diminuer le risque car les données sont destinées à être croisées avec des données provenant d'autres sources.
- Observation (2): le transfert ne comporte pas de données sensibles comme telles. Cependant, le recoupement d'informations relatives au nom, au domicile, et à certaines habitudes de consommation peut permettre l'obtention de données relatives à la race ou à la religion. Lors de l'analyse de la différence culturelle, il conviendra d'être attentif à cet élément, et de voir en particulier si le pays tiers risque d'en faire.

- Observation (3) : il sera absolument nécessaire de vérifier quelle mesure existe pour la prévention de flux transfrontières vers des pays tiers.

2. Analyse du tableau

Le tableau fait apparaître un nombre important de facteurs aggravant les risques. Le pays tiers est par hypothèse affecté d'un important retard technologique, ce qui rend difficile la prise de mesures de sécurité adéquates. Le nombre de renseignements transférés est considérable et porte sur une grande variété d'éléments. Le type de transfert (support papier) nous paraît aggraver les risques dans la mesure où un document imprimé nous paraît relativement facile à reproduire et détourner même dans un pays où la technologie informatique n'est pas moderne. Le fichier central est localisé dans le pays tiers de façon permanente; il n'y a pas de lien organique entre les acteurs; en outre, le secteur d'activité du destinataire (courtage en données) aggrave aussi considérablement les risques, puisque cette activité consiste à croiser et vendre des données. Notons que, dans notre hypothèse, la conservation des données est limitée dans le temps (cela correspond à l'intérêt économique du responsable du traitement, car ces données se périment très vite).

Les risques de perte de contrôle et de réutilisation sont donc importants, et les conséquences de la réalisation de ces risques pourraient être alourdies par la déduction possible d'éléments tels la race ou la religion du croisement de données du flux avec d'autres données. Le risque de manque de proportionnalité existe également: il est induit à la fois par le nombre de renseignements transférés et par le croisement de ces renseignements avec d'autres.

D) Analyse de la protection offerte par le pays tiers in casu

a) Principes de fond

Il ressort de l'analyse du flux que les principes de participation individuelle, de finalité, et de proportionnalité doivent être présents dans le pays tiers.

b) Effectivité des principes de fond

1. Moyens d'expression et de sanction

Dans le pays B, il existe une législation générale de protection des données à caractère personnel, adoptée très récemment, et inspirée entre autres de la Convention 108 du Conseil de l'Europe. Cette législation reprend les trois principes mentionnées ci-dessus. Elle a été prise au niveau fédéral, et s'impose à tous les traitements qui ont lieu dans le pays. Il est difficile de savoir si elle s'applique ou non aux étrangers non réseidents dans le pays B; il n'existe aucune jurisprudence sur le sujet, mais la Constitution ne dit rien de contraire. On peut donc considérer avec un degré raisonnable de certitude que des étrangers pourraient l'invoquer, d'autant qu'elle vise les traitements, sans mentionner la provenance des données qui en font l'objet.

Cette législation prévoit des sanctions civiles, mais l'organisation judiciaire du pays B présente certaines déficiences graves (essentiellement complexité de la saisine des tribunaux et longueur des procédures). Ceci représente un facteur négatif, qui doit attirer l'attention sur l'existence éventuelle de recours extra-judiciaires, éventuellement auprès d'une autorité de contrôle.

2. Moyens de contrôle

2.1. **Mesures de sécurité**:

Considérant l'existence de facteurs de risque dans ce flux, il convient d'être particulièrement exigeant au sujet des mesures de sécurité prises dans le pays tiers. Vu le retard technlogique qui y existe, et les risques inhérents à un transfert sur support papier (impossibilité de cryptage des données,...), il faut que la société destinataire compense cela par la prise de mesures de sécurité très complètes. Or, par hypothèse, les mesures de sécurité prises par l'entreprise destinataire sont très insuffisantes. L'accès aux locaux n'est pas contrôlé; il n'existe pas de système de back-up régulier, le local où se trouvent les imprimantes utilisées pour la publication des listes est partagé par une autre société totalement indépendante,...

2.2. **Autorité indépendante de contrôle**

Le pays en question a créee un organisme public de protection des données, agissant de manière consultative lors de projets de création de banques de données du secteur public. Elle n'exerce aucun contrôle vis-à-vis des entreprises du secteur privé et ne peut aider les particuliers qui souhaiteraient exercer le droit d'accès conféré par la loi, nonobstant les réticences du responsable du fichier. En d'autres termes, les citoyens européens se trouvent démunis et ne peuvent bénéficier d'organes relais de leurs propres autorités nationales de contrôle.

E. Apport de l'analyse de ce flux à la méthodologie proposée

Il nous semble dès lors que, vu la gravité de ces manquements au regard des risques entraînés par le flux en question, ce dernier ne peut être autorisé. Même si la législation énonce de manière précise et détaillée l'ensemble des principes de fond, leur effectivité ne peut être assurée dans les conditions décrites ci-dessus.

Notons que, si l'on avait pu poursuivre cette analyse, il aurait fallu vérifier la possibilité de recours extra-judiciaires (vu la déficience du système judiciaire), ainsi que la possibilité pour les personnes concernées de s'opposer au traitement (car il s'agit d'un traitement "marketing").

3ème cas: Transfert par un individu vers un site www[3]

A. Présentation du cas

Une entreprise gère un site Web localisé en Colombie britannique, province canadienne. Ce site scientifique s'adresse de manière mondiale à des universitaires, spécialistes en sciences nucléaires et outre un forum de discussion en la matière, offre des services variés d'annonces d'événements scientifiques, d'informations scientifique.

Elle offre également à des tiers, en particulier à des sociétés d'organisation de voyage, la possibilité, lorsqu'un événement scientifique est organisé, de transmettre des offres via courrier électronique aux personnes ayant souscrit au site. La transmission de données peut également avoir lieu vers des librairies, etc.

Pour offrir de tels services, elle demande aux personnes qui souscrivent au site de répondre à un questionnaire, reprenant outre des informations concernant un curriculum vitae détaillé, des informations relatives aux préférences en matière de voyage.Ces informations peuvent parfois présenter un caractère sensible, ainsi les questions de santé voire les opinions philosophiques ou religieuses.

Rien n'oblige les abonnés au site à répondre à l'ensemble des questions ceux-ci peuvent s'opposer au transfert des données à des tiers.

B. Collecte des informations nécessaires à l'évaluation

L'information est transmise directement par la personne concernée. Il est donc difficile de lui demander de procéder elle-même à l'évaluation des risques. Sans doute, sera-t-il requis de passer par un expert local chargé de procéder à l'évaluation, en particulier de la qualité de la protection offerte par le site.

---

[3] Ce cas soulève un problème délicat d'interprétation de la directive. A priori, deux types de dispositions pourraient s'appliquer à un tel cas. En effet, on pourrait considérer comme applicable l'article 4.1. c) en estimant que par la collecte des données auprès de la personne concernée, l'organisme responsable situé à l'étranger "recourt, selon les termes même de l'article, à des moyens..., situés sur le territoire dudit Etat membre". Dans un tel cas, on dira que la loi de l'Etat membre (ou plutôt les divers lois des Etats membres) est (sont) applicable(s) et donc par là que les principes de la directive devront être intégralement respectés. En outre, un représentant du responsable doit être nommé localisé sur l'Etat membre (ou les Etats membres) concerné(s). A l'inverse, il serait envisageable d'affirmer qu'il y a simplement au sens de l'article 25, transfert vers un pays tiers, et alors exigera-t-on protection adéquate.
Une analyse de la directive nous a conduit a considérer que cette seconde disposition était seule applicable (sur ce point, différents articles: M-H. Boulanger, C. de Terwangne, Internet et le respect de la vie privée Internet face au Droit, E. Montero (éd.), Cahier du CRID n° 12, p. 195; C. de Terwangne, S. Louveaux, Data Protection and on-line networks, Computer Law and Security Report, 1997, à paraître.

C. Analyse des flux

a)Tableau des risques

Risques **Facteurs d'influence**	Perte de contrôle	Réutilisation	Manque de proportionnalité	Inexactitude des données	Observations
Situation socio-politique					
Retard technologique					
Technologie avancée		—			(1)
Collecte indirecte des données	—	—	—		vu
Sensibilité des données					(2)
Nombre de renseignements transférés					
Nombre de personnes concernées					
Fréquence des flux		-		-	
Type de réseau utilisé	-	-			(3)
Localisation du fichier central					
Liens entre acteurs					
Secteur d'activité du destinataire					
Cohérence dans les finalités	-	-			
Durée de conservation des données					
Détermination de la finalité	-	-			
Risque de retransfert	-	-			

Observ. (1) A noter que la technique avancée utilisée présente ici un haut facteur élevé de risque du aux larges possibilités de réutilisation des données que permet Internet et ce à partir de n'importe quel point du globe.

Observ. (2) L'interactivité de la technologie d'Internet peut faire craindre la création par les utilisations du site de nombreuses données et ce parfois à l'insu même de l'utilisateur.

Observ. (3) On connaît le manque de confidentialité qui affecte le transfert de messages via Internet, sauf à adopter des techniques de cryptage.

b) Mesures envisageables au niveau des facteurs de risque

Le premier risque - et il n'est pas des moindres - est la difficulté que l'on pourrait avoir à identifier le responsable du site, plus précisément, le responsable des données. Le nom de domaine du serveur n'indique ni sa localisation du site, ni sa personnalité. Sans doute, une page écran peut répondre à cette absolue exigence, faute de quoi, aucun contrôle du site ne sera possible.

La sécurité d'un réseau tel Internet est sujette à caution. On conçoit qu'il soit aisé de remédier à cette lacune, en exigeant l'utilisation de techniques de cryptographie lors de l'envoi des réponses au questionnaire.

On ajoutera qu'au risque lié au transfert à des tiers, en particulier aux agences de voyages un tel risque peut facilement être évité en évitant le transfert *a priori* mais en offrant à l'intéressé la possibilité d'avoir quelques informations sur les sites de telles agences et de s'y rendre via un lien Html, ne permettant alors seulement que le transfert des données *ad hoc*.

La structure du questionnaire pourrait également distinguer suivant les services souhaités les informations demandées en rapport avec ceux-ci et parmi elles, déterminer celles à laquelle il est nécessaire de répondre et les autres.

D. Analyse de la protection du pays tiers

Aucune législation ne régit le secteur privé au Canada. Par hypothèse, le responsable du traitement a souscrit au code de conduite "Privacy" modèle, développé par le "Canadian Standards Association". On ajoute que le responsable a fait l'objet de la certification suivant la procédure mise en place par ce code de conduite.

a) Principes de fond

1. La finalité

L'analyse du code de conduite laisse apparaître une lacune importante à propos du principe de finalité, dont le respect apparait particulièrement important, vu le nombre d'utilisations secondaires possibles. Il ne s'agit pas seulement ici de dénoncer les risques liés au transfert vers les tiers déjà identifiés (libraires, agences de voyages) mais, également, ceux nés notamment de l'analyse des comportements de tel ou tel participant au forum de discussions, pour en définir les domaines de spécialisation, les affinités réciproques et, le cas échéant, fournir le résultat de telles investigations à l'employeur, à une société concurrente.

On ajoutera que des utilisations secondaires peuvent être le fait non seulement du responsable du traitement mais également de personnes ayant accès au site, en particulier au forum de discussions et que dès lors des garanties doivent être prises vis-à-vis de telles utilisations, par le biais de clauses appropriées figurant dans l'Acceptable Use Policies et faisant l'objet de sanctions (exclusion du site, etc.).

Enfin, étant donné le caractère ouvert et international du réseau mais également du site de telles utilisations peuvent être vu, la réutilisation peut être le fait de personnes se connectant à partir de pays tiers ne disposant pas de protection adéquate. A cet égard, on notera qu'aucune disposition du CSA Model Code ne limite les transferts vers les pays tiers. Cette absence de disposition pose de sérieux problèmes. Des mesures techniques permettraient peut être de bloquer l'accès au site depuis certains pays. Faute de quoi, il sera absolument nécessaire de limiter très sévèrement les données figurant sur le site et ainsi rendues accessibles.

Pour lutter contre des utilisations secondaires illégitimes, le C.S.A. Model Code prévoit que les fins pour lesquels des renseignements personnels sont reccueillies doivent être déterminées par l'organisme avant ou au moment de la collecte (ou après la collecte mais avant de s'en servir) et précisés c'est-à-dire expliqués. Ceci s'applique indéniablement au site Web analysé qui devra décrire les diverses finalités de manière précise. On retrouve le principe de la directive selon lequel les données doivent être collectées ou traitées pour des finalités déterminées... la directive ajoute que ces finalités doivent être légitimes et prévoit des mécanismes de contrôle externe de cette légitimité. Il n'est pas évident que nonobstant l'emploi du terme "légitime" par le principe 4.3.3. du CSA Model Code, ce terme soit l'indication d'une possibilité de contrôle externe des finalités. A noter que le consentement apparait en toute hypothèse comme un fondement suffisant de légitimité même pour des données sensibles, ce qui est contestable selon la directive.

2. La proportionnalité et l'exactitude des données

Le CSA Model Code canadien ...

3. La participation individuelle

Sur certains points, le principe de participation individuelle apparaît bien assuré par le CSA Model Code.

- Obligation du responsable de mettre à disposition des renseignements précis sur sa politique, ses pratiques et sa stratégie concernant la gestion des renseignements personnels. Cette obligation est idéalement assurée par la création d'une page écran appelable par l'utilisateur.

- Obligation d'informer toute personne de l'existence de renseignements personnels qui la concernent, de l'usage qui en est fait et du fait qu'ils ont été communiqués à des tiers; obligation de permettre la consultations de telles données et d'autoriser contestations ou corrections.

- "Invitation" à indiquer la source des renseignements et les tiers auxquels communication a été faite.

Sans doute est-ce à propos de la possibilité d'opposition à l'utilisation pour des opérations de prospection commerciale que le CSA Model Code se montre plus défavorable à l'utilisateur que la directive. Au regard des possibilités importantes d'utilisation des données à des fins de prospection commerciale, sans doute, faudra-t-il être attentif à ce point.

b) Effectivité

1. moyen d'expression

Le premier moyen d'expression identifié est un code de bonne conduite multisectoriel. Il importe d'évaluer le degré de publicité de ce code auprès des utilisateurs. Il est à noter que la création d'un hyperlien en direction d'un site présentant ce code permettrait à l'utilisateur d'en connaître facilement le contenu.

On note qu'à ce premier moyen d'expression, s'ajoute celui de la certification opérée dans le cadre de ce code de conduite et auquel, par hypothèse, le responsable du site Web s'est soumis. Sans doute, un logo mentionnant cette certification pourrait apparaître à l'écran et ouvrirait un lien avec le site du certificateur où seraient décrites les procédures de certification et les dispositions du C.S.A. Model Code.

Il est à noter que ces moyens d'expression s'ils sont applicables au site Web qui collecte les données ne sont peut être pas suivis par le tiers auxquels le site Web communique des données ou les rend accessibles.

2. Moyen de contrôle

Le principe 1 du code canadien prévoit la nomination d'un "responsable", ou, pour suivre la terminologie européenne, d'un détaché à la protection des données.

L'audit annuel de l'organe de certification permet en outre d'être sûr de la continuité des pratiques "privacy" du responsable du site et de leur respect des principes du code.

La possibilité d'exiger l'accès dans un délai raisonnable aux données, de les contester est consacrée par le même code.

Enfin, l'obligation de prendre des mesures de sécurité appropriées est consacrée par le code canadien.

3. Moyen de recours et de contrainte

La possibilité de recours devant les juridictions ordinaires (non pénales!) devrait être évaluée. Le non respect d'un code auquel on a souscrit constitue peut être un *false statement*. En toute hypothèse, la preuve et le coût d'un tel procès (sauf si une action collective est possible) dissuaderont la personne victime de dommage d'un recours. Sans doute, est-ce sur ce point que le CSA Model Code s'avère le plus déficient: le recours fondé sur un tel code est donc peu aisé et les sanctions peu dissuasives.

E. Aspect de l'analyse de ce flux à la méthodologie proposée

La question de la protection adéquate trouve des solutions difficiles en matière d'utilisation de services "on line" comme Internet.

Un premier point est certes la multiplication possible de réutilisation des données, peu contrôlables par le responsable du traitement et susceptibles d'être opérés à partir de pays n'offrant pas de protection.

Un second point est l'amélioration possible, grâce à l'interactivité du réseau et à l'activation d'hyperliens, du principe de participation individuelle.

En ce qui concerne la protection offerte par le C.S.A. Model Code, on regrettera, même si ce point doit faire l'objet d'évaluation par un expert, l'absence du principe de légitimité en matière de finalité, au sens que lui a donné la jurisprudence du Conseil de l'Europe. L'absence de restrictions à propos des données sensibles et la toute puissance du consentement comme cause de légitimité sont d'autres motifs de doute quant à l'existence d'une protection adéquate.

L'effectivité de la protection offerte par le C.S.A. Model Code montre bien les limites de l'autorégulation: existence d'une autorité indépendante, recours aisé des utilisateurs, sanctions efficaces, ... autant de points sujets à caution et qui inciteront à une évaluation attentive.