

SESSION 2 SUR LA PROTECTION DES DONNÉES PERSONNELLES

Yves Poullet

A propos des flux transfrontières : Comment assurer le respect dans les pays étrangers d'une protection adéquate ?

Faut-il des standards internationaux en matière de protection des données personnelles ?

Dans un premier temps il s'agira de décrire la multiplicité des Flux Transfrontières de Données (FTD). Nous les envisagerons uniquement dans le cadre des relations entre personnes privées et non entre administrations et, en particulier, entre autorités de police ou juridictionnelles. Après avoir décrit ces flux, il s'agira de resituer les solutions qui peuvent exister dans ce cadre, celui d'instruments internationaux ou de droit international privé. On s'arrêtera plus particulièrement à la solution européenne, solution qui est loin d'être impérialiste. Enfin, nous plaiderons pour des normes internationales en matière de protection de la vie privée qui apparaissent nécessaires à l'heure où internet est devenu une réalité globale.

1. La réalité multiple des FTD.

On peut imaginer nombre de raisons aux FTD.. Les premiers auxquels on peut penser sont ceux qui accompagnent la mobilité des personnes. Je suis venu à Hanoi et je peux supposer que mon agence de voyage a envoyé toute une série de données à la compagnie vietnamienne, à mon hôtel et autres. Au-delà, entre entreprises, les flux sont légion, ils peuvent se situer à l'intérieur de multinationales (IBM, par exemple, a des filiales un peu partout dans le monde et, en fonction des décisions, elle peut décider de baser les données concernant son personnel dans l'une de ces filiales), les flux dans les multinationales sont quelque chose d'évident. La centralisation des traitements est une

autre réalité : si on prend les cartes de paiement, Europay qui est la société qui gère les cartes de crédits, a centralisé les traitements des opérations relatives à ces cartes aux USA et en Angleterre. Les entreprises peuvent procéder à des FTD dans le cadre de l'outsourcing : 40% des données traitées par les entreprises anglaises sont traitées en Inde. L'outsourcing est quelque chose de très important pour un certain nombre de pays en voie de développement. Enfin, et c'est peut être nouveau, les FTD viennent simplement de notre utilisation d'internet. Lorsque l'on utilise internet on génère des données personnelles qui seront traitées par des pays tiers. Par exemple si je fais des recherches sur Google, mes données seront traitées dans les centres serveurs de Google, souvent situés à des milliers de kilomètres de mon ordinateur ; même remarque quand j'utilise des réseaux sociaux, tels Facebook.

2. L'encadrement des FTD par des instruments internationaux

Les FTD sont devenus habituels. Pour les gérer, il existe des instruments internationaux qui tendent à imposer des standards globaux en matière de vie privée ou du moins à encadrer les FTD.. En matière de protection de la vie privée, le pacte de New York de 1966 consacre le droit à la vie privée et l'article 8 CEDH affirme de même le droit à la vie privée. Si la vie privée est donc un droit universellement reconnu, il n'est cependant pas évident de passer d'un droit à la protection à la vie privée des personnes à un droit plus spécifique à la protection de leurs données à caractère personnel, droit qui soit reconnu de la même manière. D'un point de vue international, les premiers textes intervenus en matière cette fois de protection des données à caractère personnel sont les lignes directrices de l'OCDE qui datent de 1981 et qui ont été complétées par des recommandations de 2006 sur la question de la mise en vigueur (« enforcement ») de ces principes directeurs. Il n'est nulle part affirmé, dans ces principes de l'OCDE, que la protection des données est un droit reconnu par les Etats ; il est simplement recommandé que les Etats encouragent leurs entreprises à protéger les données à caractère personnel. La Convention N°108 du conseil de l'Europe part d'une autre affirmation puisqu'elle propose une approche législative. L'idée est de demander aux Etats de signer et de ratifier la Convention et ainsi de créer des droits reconnus par les Etats et susceptibles, s'ils ne sont pas respectés, d'être portés devant les juridictions. Une résolution 45/95 des Nations Unies, qui n'a pas de force obligatoire affirme en 1990 le droit à la protection des

données et recommande la création d'autorités de protection des données. Sur le plan des instruments internationaux de protection des données, coexistent donc deux approches : la première reconnaît la valeur de la vie privée mais estime que l'autorégulation, le cas échéant encouragée par l'Etat suffit à protéger cet intérêt ; la seconde élève la protection des données à la valeur d'un droit et dès lors protège par la loi ce droit dont le non respect est sanctionnée par els tribunaux y compris pénalement..

Dans ce second cas il s'agit de considérer que la vie privée, qui est un droit, engendre nécessairement un droit à la protection des données ; dans ce cadre, le droit à la protection des données découle directement du droit à la vie privée et le droit à la vie privée c'est le droit de se déterminer librement. Or, on ne peut pas se déterminer librement ni on ne peut pas maîtriser la circulation des nos données, on ne peut pas assurer notre liberté d'expression si l'on est constamment sous surveillance et le client d'une banque ne peut pas voir assurer sa liberté de crédit si face à sa banque, il est incapable de savoir de quelles informations la banque dispose et comment elle els traite. C'est la voie suivie par l'Union européenne qui, dans le cadre du Traité de Nice, a reconnu une valeur quasi constitutionnelle du droit à la protection des données.

L'autre approche est celle prônée par les USA qui est de ne pas le consacrer la protection des données comme un droit de l'homme mais considérer qu'elle fait partie des usages loyaux des entreprises. Dans le cadre du fonctionnement d'un marché, il est de bon ton que les entreprises protègent les données à caractère personnel. Aux USA la protection des données est une affaire de marché: la donnée à caractère personnel est une « *commodity* », elle a une valeur économique et c'est à ce titre que l'on pourra, dans une certaine mesure, la protéger.

Ces deux approches posent un problème en matière de FTD. Une solution est possible en se basant sur les principes de Droit International Privé ; un des plus grands spécialistes du droit à la protection de la vie privée et du droit international privé, François Rigaux avait notamment travaillé sur cette question. Mais cette solution de DIP est délicate et contestable. Prenons l'exemple du réseau social Facebook installé aux USA., Dans la mesure où ce site s'adresse à des clients belges, met en place des réseaux sociaux en Belgique le DIP considèrera, si le site viole la vie privée de ses clients par

exemple en vendant leurs données à des entreprises ou à des employeurs potentiels, qu'il y a suffisamment de rattachement à la Belgique pour que les juridictions belges soient compétentes et, dans la mesure où en Belgique la protection des données est un droit de l'homme, il s'agira d'une loi de police applicable directement ; la loi belge sera donc applicable. Mais le problème reste entier quand il s'agit de faire appliquer une décision. On a pu le constater dans l'affaire dite Yahoo de 2000 à propos d'un site aux enchères vendant en France à partir d'un site hébergé sur Yahoo Etats-Unis des produits nazis. Dans cette affaire, même si le tribunal français s'était déclaré avec raison comme compétent, il n'a pu faire valoir sa décision aux USA puisque chez eux la protection contre les messages racistes ne fait pas partie de leur appareil législatif et la protection des données n'est pas un droit de l'homme. Le DIP ici, même s'il offre une solution, n'apparaît pas comme suffisant. Il est donc nécessaire d'avoir des instruments de DIP matériel régissant les flux transfrontières de données. A cet égard, nous nous tournerons vers la solution européenne qui, dans la directive 95/46, contient plusieurs dispositions.

3. La solution européenne – une relative ouverture

L'article 4.1.c) contient toutefois une dérogation au principe de la territorialité. La directive est applicable si le responsable du traitement établi en dehors du territoire utilise (*makes use*), à des fins de traitements, un équipement situé sur le territoire d'un Etat membre : « *chaque Etat Membre applique son droit de la protection des données, lorsque le responsable du traitement n'est pas établi sur le territoire mais recourt, à des fins de traitement des données à caractère personnel, à des moyens de traitement situés sur le territoire de cet Etat européen* ». En d'autres termes, l'article 4-c prévoit qu'une entreprise telle que facebook devra appliquer le droit européen si elle recourt à des moyens situés sur le territoire européen. Le problème est ici de savoir ce que signifie le terme « recourir à des moyens ». Le Groupe de travail dit de l'article 29, groupe constitué d'un représentant de chaque autorité nationale de protection des données et agissant comme organe consultatif auprès de la Commission, a donné une interprétation assez audacieuse du texte : l'article 4-c est applicable chaque fois qu'une entreprise a, grâce à la technologie, une maîtrise même partielle (voir le cas des cookies) du fonctionnement de l'ordinateur d'un utilisateur et ce par le biais, par exemple, de l'introduction dans l'ordinateur personnel d'un « cookie » (comme le font Facebook ou Google) grâce auquel

cette entreprise reçoit automatiquement des informations sans même que l'utilisateur y consente, lorsqu'il reste passif derrière son ordinateur.

L'adoption de cette disposition, dont même les auteurs de la directive ont quelque difficulté à saisir le sens est, pour moi, prémonitoire, appliqué au contexte de nos infrastructures globales et interactives. Elle signifie que si, à partir d'un territoire hors de l'Union européenne, un responsable de traitement dispose de la pleine maîtrise du fonctionnement total ou partiel d'un terminal situé dans l'Union européenne et on songe aux « *spywares* », aux « *cookies* » et à certains programmes d'extraction à distance de données dans des bases de données européennes, il est entièrement soumis à la directive. Cet article s'applique donc aux transferts passifs dans la mesure où le transfert en cause est entièrement soumis technologiquement au bon vouloir du responsable du traitement situé à l'extérieur de l'Europe.

A l'inverse, les articles 25 et 26 s'appliquent aux transferts actifs de données, c'est-à-dire ceux où le responsable du traitement décide de l'envoi des données ou du moins en autorise le transfert. La règle d'or en la matière est qu'il doit s'assurer qu'une protection adéquate soit assurée par les destinataires, sous peine de quoi le transfert est interdit. L'utilisation des mots « protection adéquate » en lieu et place des termes « protection équivalence » ou « protection suffisante » constitue une originalité de l'approche européenne. Elle implique le rejet de toute attitude a priori qui s'attacherait à la seule nature et au contenu du mode de protection offert par le destinataire.

La question n'est pas de savoir s'il existe dans le pays du destinataire, un instrument de protection de même nature qu'en Europe, en l'occurrence une loi et dont le contenu serait quasi similaire à celui de la directive, ce qui eût constitué un acte d'impérialisme européen. Il s'agit de se poser la question : « Au vu du flux en question et des risques liés aux caractéristiques de ce flux, le moyen de protection offert par le destinataire, garantit-il le respect des exigences de protection des données telles que voulues par l'Union européenne ? La garantie du respect doit s'examiner, rappelle le fameux « *Methodology Paper* » du Groupe de l'article 29, tant à propos du contenu de la protection offerte, qu'à propos des moyens mis en place pour s'assurer du respect de ce contenu. La constatation de la conformité de contenu n'évacue pas la nécessité de

s'assurer de l'effectivité du respect de celui-ci, peu importe la nature de la réglementation choisie et les institutions ou sanctions formellement mises en place par le pays étrangers. Ainsi, l'article 25 accepte que la protection adéquate se fasse par le biais d'un système de code de conduite, d'autorégulation. C'est par exemple ce qu'ont proposé les USA en 2000. Ce qui est important est non pas la nature législative ou la réglementation des règles mais que, tout d'abord, certains principes soient reconnus et également, qu'il y ait des garanties quand à la mise en vigueur des principes. Ces principes sont les principes de finalité, de pertinence, d'accès, de sécurité. J'insiste sur ce point au moment où les évaluations du caractère adéquat me semblent parfois basculer vers une analyse tatillonne du seul contenu et délaisse la vérification de l'effectivité.

La directive prévoit donc un principe et trois cas d'exceptions. Le principe est l'interdiction de transférer des données en dehors de l'Europe si l'entreprise est dans un pays étranger qui n'offre pas une protection adéquate. Mais la protection adéquate peut être offerte de différentes manières : soit par le fait que l'entreprise est située dans un pays qui, au regard du flux, offre un système de régulation de la vie privée qui est adéquat par rapport au risque que comporte le transfert, soit par le fait que dans le cadre du FTD, entre les partenaires, il y a une protection adéquate offerte par le contrat ou, enfin, que les deux entreprises participent à une multinationale qui s'est engagée à protéger les données à caractère personnel. Ainsi, a priori, l'Europe s'interdit tout préjugé – et nous revenons à la question initiale qui constitue l'objet de ce propos – sur la nature de la méthode de protection choisie. Des solutions d'autorégulation (les « *Safe Harbour Principles* », les solutions contractuelles ou les Binding Corporate Rules (B.C.R.) en sont), de corégulation (le cas japonais s'appuyant sur la combinaison d'une loi, la loi de 2003, des codes de conduite et d'un système de label l'illustre) sont toutes acceptables à condition que ces solutions soient conformes et effectives.

Progressivement, avec l'aide du Groupe de l'article 29, s'est ainsi construit un véritable système des différents modes de protection qui peuvent être offerts en matière de protection des données. Ainsi, la protection offerte par le destinataire peut trouver sa source dans l'environnement « régulateur » au sens le plus large dans lequel se meut son activité (qu'il s'agisse d'un secteur précis ou non, qu'il s'agisse de systèmes d'autorégulation, codes de conduite, label, ...). En ce qui concerne cette première

hypothèse de l'article 25 et l'exigence de protection adéquate. L'idée est que l'on peut transférer des données lorsque le système proposé par le pays Tiers vers lequel les données sont transférées est un système de protection adéquat. L'Europe s'est très vite rendue compte que si elle laissait faire chaque Etat Membre, il allait y avoir très rapidement un phénomène de concurrence. Il est donc prévu que la Commission puisse elle-même décider si un pays offre une protection adéquate ou non et les Etats Membres sont tenus d'informer la Commission si jamais ils souhaitent considérer un pays comme adéquat de façon à ce qu'elle puisse intervenir et prendre une décision qui soit la même pour l'ensemble des pays européens. L'article 25-4 permet à la commission de déclarer un pays adéquat. C'est dans ce cadre que la plupart des décisions d'adéquation ont été prises, ainsi la Suisse, le Canada, les Etats-Unis dans le cadre du Safe Harbour et nombre d'autres pays ont pu être déclarés par la Commission comme offrant une protection adéquate. .

La solution peut également trouver sa source dans le contrat spécifique que noue l'émetteur et son destinataire à propos précisément du flux qui les concerne. Elle peut s'appuyer enfin – c'est l'innovation prometteuse des B.C.R. – sur la structure hiérarchique qui caractérise les multinationales et les modes internes de contrôle, d'audit et de sanction que ces multinationales peuvent aisément imposer.

Revenons un moment à la solution contractuelle. Selon l'article 26, il est possible – et la Commission propose trois contrats modèles à cet égard - d'offrir une protection dans le cadre d'un contrat à condition qu'il reprenne les principes et à condition que ce contrat passé entre une entreprise européenne et une entreprise étrangère permette aux personnes concernées de pouvoir aller devant le tribunal afin de faire respecter les engagements contractuels. Le droit européen doit pouvoir être applicable. En ce qui concerne la dernière solution, celle retenue pour les flux à l'intérieur des multinationales, elle est encore plus imaginative : il s'agit d'exiger de la maison mère un engagement d'autorégulation c'est-à-dire d'avoir une « privacy policy » et de mettre en œuvre les moyens propres aux multinationales de façon à la faire respecter. Ces moyens propres sont : l'information aux employés de l'existence de cette « privacy policy », le tenue d'audit de façon régulière, l'information des personnes concernées et la possibilité d'avoir un recours devant les tribunaux en cas de non respect de cette « privacy policy ».

Cette diversité des modes acceptables traduit la large ouverture de l'Union européenne à accepter les solutions originales mises en place dans des pays de culture différentes. Je le répète, il ne peut être question d'impérialisme européen.

4. Vers une solution globale ?

Certes la solution européenne est intéressante, elle permet d'assurer la protection des données même au-delà de l'Europe, ce qui est le devoir de l'Union Européenne, celui d'assurer les libertés de ses citoyens mais il apparaît être plus qu'urgent d'aller plus loin. Si les FTD sont devenus le « pain quotidien », il apparaît nécessaire que l'on aille vers une protection globale des données à caractère personnel. Cela répondrait à l'appel des sommets mondiaux de la société de l'information de Genève et de Tunis qui affirment sans ambages qu'il est utile et nécessaire de trouver des garanties appropriées en matière de protection des données. Au sein de l'espace francophone dont le Vietnam est partie prenante, 54 chefs d'Etat et de gouvernements de la Francophonie pris à Bucarest en septembre 2006 en vue d'intensifier, sur la plan national, les travaux législatifs et réglementaires nécessaires à l'établissement du droit des personnes à la protection des données et à oeuvrer, sur le plan mondial, en faveur de l'élaboration d'une convention internationale garantissant l'effectivité du droit à la protection des données. Les deux réseaux Nord / Sud (le réseau ibéro – américain de protection des données, L'association francophone des autorités de protection des données (AFAPDP) issue de l'initiative de ce sommet francophone a adopté de même une résolution dans laquelle elle exprime sa volonté de contribuer activement au renforcement de la coopération internationale dans le domaine de la protection des données et exprime son soutien au développement des instruments internationaux permettant la réduction des divergences existantes parmi les différentes structures légales nationales et régionales sur la protection des données personnelles et de la vie privée, garantissant au niveau mondial un haut niveau de protection et contribuant à éliminer tous les obstacles à des échanges d'informations fluides et sûrs au niveau international.

De même, la Conférence internationale des commissaires à la protection des données et à la vie privée répète (Venise 2000, Montreux 2005, Strasbourg 2008) la nécessité d'un instrument global du droit à la protection des données et à la vie privée. La

déclaration de cette même conférence internationale tenue à Madrid en 2009 marque une étape importante et décisive pour la protection des droits et des libertés fondamentaux des citoyens et citoyennes du monde entier lors du traitement de données à caractère personnel. En effet non seulement les commissaires à la protection des données sont convaincus de la nécessité d'une réglementation universelle, mais également la société civile et le secteur privé adhèrent à cette démarche. Il reste à convaincre les Etats et les gouvernements. La déclaration de Madrid relative à des standards mondiaux relatives à la protection des données et à la vie privée a adopté un « Projet de normes internationales en matière de protection des données et de la vie privée », qui renforce par la coopération entre autorités de protection des données l'effectivité de la protection des données dans le monde et se prononce clairement en faveur du caractère universel du droit à la protection des données et à la vie privée.

Par l'adoption de cet instrument international, nous rejoindrions ici la Déclaration faite par l'ensemble des représentants des sociétés civiles, des associations de consommateurs et du monde académique présents à Madrid au cours de la réunion dite « Public Voice », qui instamment réclament la mise en place d'un instrument international en matière de protection des données tout en désignant la Convention N° 108 du conseil de l'Europe comme étant la base de cet instrument. Cette Convention est certes un instrument européen mais on sait qu'elle est ouverte à la signature de n'importe quel pays dans le monde.

Que cet appel puisse être entendu dans votre beau pays est mon vœu le plus cher.

© Yves Poullet

Professeur aux facultés de droit de Namur et de Liège (Belgique)

Directeur du CRID

Yves.poullet@fundp.ac.be

