Accord de libre-échange transatlantique : pas sans la protection des données personnelles

Les Etats-Unis et l'Europe ont annoncé la négociation d'un nouvel accord transatlantique, dont l'objectif est de réduire les obstacles à l'investissement et au libre-échange de biens et de services entre les deux continents. La protection des données personnelles pèsera sur cette négociation.

Par Winston Maxwell, avocat associé Hogan Lovells LLP

Actuellement, la directive européenne de 1995 sur la protection des données personnelles (1) interdit le transfert de données personnelles vers les Etats-Unis, car les Etats-Unis n'ont pas, selon la Commission européenne, un niveau de protection adéquat. Cette interdiction de principe est contournée en pratique par différents moyens, notamment par l'utilisation de clauses contractuelles types approuvées par la Commission européenne, par la mise en œuvre de codes de conduite internes dits BCRs (Binding Corporate Rules) ou bien si l'entreprise américaine a souscrit aux engagements *Safe Harbor* mis en œuvre par le gouvernement américain.

Intrusions de la police et des entreprises

Néanmoins, le principe de départ est bien l'interdiction pure et simple de tout transfert, ce qui constitue un obstacle considérable au libre-échange de biens et de services entre les deux continents. De plus, l'utilisation par les entreprises américaines de la procédure *Safe Harbor* est contestée par certaines autorités en Europe, lesquelles estiment que la procédure d'auto-certification ne présente pas de garanties suffisantes. L'utilisation du *Safe Harbor* pourrait donc être remise en cause dans le cadre de la future régulation européenne en matière de données personnelles.

Du point de vue américain, inclure les données personnelles dans l'accord de commerce avec l'Europe serait souhaitable afin d'accroître la fluidité des échanges. Du point de vue européen, les avis seront plus mitigés. Les ministères de la Justice et les autorités de protection des données personnelles pourraient dire que les données personnelles ne peuvent pas être incluses dans un accord commercial, car des données personnelles sont un droit fondamental et non un objet de commerce. Les ministères de l'Economie auront peut-être un point de vue différent, estimant que l'ouverture des échanges de données personnelles entre les Etats-Unis et l'Europe contribuera à l'innovation et à la croissance en Europe.

Les Etats-Unis reconnaissent le principe de la protection de la vie privée au sein de leur Constitution, mais cette protection constitutionnelle concerne uniquement les intrusions par l'Etat et non par les entreprises privées. Le quatrième amendement de la Constitution américaine pose le principe d'une protection de la vie privée de l'individu face à l'Etat. Destiné à l'origine à protéger le domicile de chacun contre les intrusions de la police, le quatrième amendement est régulièrement étendu par les tribunaux et s'applique maintenant à différentes formes de surveillance mises en œuvre par la police. En 1974, les Etats-Unis ont adopté une loi générale sur la protection des données personnelles collectées par l'Etat. Dans cette loi, on retrouve les principes de protection adoptés par l'OCDE en 1980 et ensuite par l'Union européenne (UE) dans sa directive de 1995. Le régime de protection des données personnelles à l'égard du gouvernement américain est donc comparable au niveau de protection en Europe.

Pour la protection des données personnelles dans le secteur privé, les Etats-Unis disposent d'un patchwork de lois spécifiques. La loi dite HIPAA (2) protège les données de santé, la loi « Gramm-Leach-Bliley Act » (3) protège des données du secteur financier, la loi COPPA (4) protège l'ensemble des données des enfants collectées sur Internet, la loi « Fair Credit Reporting Act » (5) encadre le traitement des données personnelles pour la création de profils de solvabilité, des lois spécifiques en télécommunication protègent l'utilisation de données de trafic ou des données concernant les programmes audiovisuels. Au niveau de chacun des 50 Etats, il existe des lois protégeant des données personnelles dans le secteur privé, et notamment des lois strictes sur les pertes de données.

FTC : Facebook, Google, Twitter et MySpace

Enfin, il existe une loi fédérale – l'article 5 du « Federal Trade Commission Act » (FTCA) – qui interdit toute pratique déloyale en matière de commerce. Cet article 5 du FTCA donne des pouvoirs très étendus à

Notes

(1) - Directive européenne 95/46/CE du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

(2) - *Health Insurance Portability and Accountability Act* (HIPAA).

(3) - Gramm–Leach–Bliley Act, également appelé *"Financial Services Modernization Act"* de 1999.

(4) - *Children's Online Privacy Protection Act* (COPPA) de 1998.

(5) - *Fair Credit Reporting Act* (FCRA), adopté en 1970 et modifié depuis.

(6) - Commission nationale informatique et libertés (Cnil).

la Federal Trade Commission (FTC) pour sanctionner des pratiques déloyales en matière de données personnelles par des acteurs du secteur privé. La FTC, avec l'appui des tribunaux, a pu étendre le concept de *« pratiques déloyales »* à différentes formes de traitement de données personnelles qui seraient contraires aux attentes légitimes des consommateurs. La FTC dispose de pouvoirs de sanction considérables, de telle sorte que lorsqu'une entreprise est dans le viseur de la FTC, celle-ci est souvent obligée de négocier un accord transactionnel avec cette agence américaine puissante. Ainsi, les plus grandes entreprises de l'Internet, notamment Facebook, Google, Twitter et MySpace ont dû conclure des accords transactionnels de 20 ans avec la FTC, les obligeant à mettre en place un programme de protection de données personnelles au sein de leur groupe, se soumettre à des audits externes réguliers et à un contrôle suivi par la FTC.

Absence de loi « chapeau » aux Etats-Unis

Ces accords, qui prévoient notamment la mise en place de programmes de formation interne pour les salariés du groupe, ressemblent aux « Binding Corporate Rules » (BCR) que la Cnil (6) en France et certaines de ses homologues en Europe (7) souhaitent généraliser pour les groupes internationaux. Les sanctions de la FTC en matière de données personnelles sont bien plus sévères que les sanctions en Europe.

Avec autant de dispositifs en place au niveau fédéral et au niveau de chaque Etat, pourquoi les Etats-Unis ne peuvent-ils pas être « adéquats » aux yeux des autorités européennes ? Selon les européens, les Etats-Unis ne pourront pas accéder au statut de pays « adéquat » tant qu'ils n'auront pas une loi « chapeau » énonçant le principe de la protection des données personnelles dans tous les secteurs aux Etats-Unis. Une telle loi chapeau existe depuis 1974, pour le traitement des données personnelles par l'Etat américain. En revanche, il n'existe pas de loi chapeau au niveau fédéral pour le traitement des données personnelles dans le secteur privé. Il existe des lois spécifiques pour certaines données et secteurs sensibles, et il existe une loi très générale sur les pratiques déloyales qui est utilisée avec beaucoup d'efficacité et de zèle par la FTC pour couvrir les données personnelles. Mais pour l'Europe, cela ne suffit pas. L'administration Obama a suggéré l'adoption d'une loi reconnaissant les grands principes de la protection des données personnelles. Mais le parti républicain souhaite minimiser l'intervention du pouvoir fédéral dans des affaires qui relèvent selon eux du pouvoir de chaque Etat fédéré (8).

Certains Européens critiquent également les Etats-Unis pour leur loi en matière d'espionnage et de police. Le « Patriot Act » (9), adopté après le 11 septembre 2001, et FISA (10) de 1978 permettent aux autorités américaines d'accéder à des données en matière de terrorisme et d'espionnage. Mais ils constituent, selon certains, un obstacle à ce que les Etats-Unis deviennent un jour « adéquats » aux yeux des Européens.

Cette critique n'est pas entièrement fondée. Les Etats européens disposent eux-mêmes de moyens exceptionnels de surveillance en matière d'espionnage. Or, les critiques du système américain ont tendance à comparer les dispositions américaines en matière d'espionnage aux dispositions judiciaires normales en Europe, alors que la comparaison plus juste serait de comparer les dispositions exceptionnelles américaines en matière d'espionnage et les dispositions exceptionnelles européennes en matière d'espionnage.

En résumé, la négociation d'un accord commercial entre l'Europe et les Etats-Unis ne permettra pas d'effacer le problème de fond, qui est l'absence aux Etats-Unis d'une loi chapeau en matière de protection des données personnelles dans le secteur privé. Par conséquent, il semble peu probable que la Commission européenne accorde un statut de « protection adéquate » aux Etats-Unis tant qu'une telle loi chapeau n'est pas adoptée. En revanche, l'existence de lois très fortes dans certains secteurs de l'industrie (11) pourrait permettre à la Commission de reconnaître que les Etats-Unis disposent d'une protection adéquate dans ces secteurs. De plus, les agences américaines, avec l'appui de la Maison Blanche, poussent maintenant pour la négociation d'accords sectoriels pour la protection des données personnelles.

Promu sous le nom de *« multistakeholder process »*, la négociation de ces accords sectoriels pourrait ouvrir la voie à une « interopérabilité » entre les régimes européens et américains. Les accords sectoriels engageraient leurs signataires, et la FTC aurait compétence pour appliquer des sanctions sévères en cas de violation.

Vers une co-régulation US-UE des données

Cette approche de co-régulation est également promue en Europe, notamment par certains Etats membres tels que l'Allemagne, pour la protection des données personnelles. On pourrait imaginer une concertation entre régulateurs américains et européens, afin que les accords sectoriels qui émergent du « multistakeholder process » soient reconnus des deux côtés de l'Atlantique. @

Notes

(7) - *Via* le G29, le groupement européen des "Cnil" dans l'Europe des Vingt-sept.

(8) - Comme en matière de protection de la santé, les républicains voient l'intervention du pouvoir central dans la protection des données personnelles comme une incursion injustifiée par rapport aux compétences de chaque Etat. Ainsi, même s'il y avait un accord sur le fond sur la nécessité de protéger les données personnelles, les différences philosophiques entre les républicains, hostiles à l'intervention du pouvoir fédéral, et les démocrates, favorables à une telle intervention, rendraient toute adoption d'une loi fédérale difficile.

(9) - *USA Patriot Act (acronyme de "Uniting (and) Strengthening America (by) Providing Appropriate Tools Required (to) Intercept (and) Obstruct Terrorism Act of 2001").*

(10) - *Foreign Intelligence Surveillance Act* (FISA).

(11) - Par exemple dans le domaine de la santé et dans le domaine des services financiers.