LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL AUX ÉTATS-UNIS : CONVERGENCES ET DIVERGENCES AVEC L'APPROCHE EUROPÉENNE

Winston J. MAXWELL*

Aux yeux des autorités européennes, les États-Unis ne disposent pas d'un régime permettant une protection « adéquate » des données à caractère personnel par rapport aux exigences de la directive 95/46/CE. L'utilisation massive de données à caractère personnel par les grandes plateformes américaines de l'Internet, ainsi que les révélations d'Edward Snowden sur les pratiques de la NSA, donnent l'impression que les États-Unis manquent totalement de cadre pour la protection de ces données. La situation est en réalité plus complexe. Même s'il existe des différences non négligeables entre les approches américaine et européenne, les deux régimes reposent sur un socle commun, les « FIPs » (*Fair Information Practices*). De plus, les autorités américaines et européennes arrivent, sur certains sujets, à des solutions proches, privilégiant des méthodes de co-régulation.

La protection de la vie privée – un droit fondamental à l'égard du gouvernement seulement

En Europe, la protection de la vie privée et des données à caractère personnel relèvent d'un droit fondamental[1]. Aux États-Unis, le 4ème Amendement de la Constitution américaine garantit un droit de protection de la vie privée, mais uniquement à l'égard du gouvernement. Le 4ème Amendement reflète la situation particulière qui existait aux États-Unis avant leur indépendance : les soldats britanniques faisaient irruption dans le

* Avocat associé, Hogan Lovells (Paris) LLP.
[1] Art. 8 de la Charte des droits fondamentaux de l'Union européenne.

domicile privé des colons américains. À l'époque, la menace pour la vie privée venait essentiellement des forces de l'État. Au fil des années, la protection du domicile a été étendue à d'autres domaines : la voiture[2], l'extérieur de la maison[3], et les conversations téléphoniques[4]. Cependant, ce droit constitutionnel ne s'applique qu'aux citoyens américains et aux étrangers vivant sur le sol américain. De plus, le droit constitutionnel ne concerne pas les atteintes à la vie privée commises par des acteurs privés.

La « common law *» de chaque État reconnaît un droit à la protection de la vie privée à l'égard d'acteurs privés*

La protection à l'égard d'acteurs privés est reconnue au sein de la *common law* de chaque État, et notamment dans la jurisprudence en matière de responsabilité civile. À la fin du 19ème siècle, la publication de photographies dans la presse a posé un nouveau défi pour la protection de la vie privée en France comme aux États-Unis[5]. En réaction à ce nouveau phénomène technologique, deux éminents juristes américains, Samuel Warren et Louis Brandeis, ont publié un article dans la *Harvard Law Review*, intitulé « *The Right to Privacy* »[6], qui a établi la base des règles de responsabilité civile en matière de vie privée. Appelées « *privacy torts* », ces règles protègent l'individu contre des incursions dans sa « sphère de vie privée », et couvre notamment la publication de faits relevant de la vie privée, ou de photographies sans le consentement des personnes intéressées[7]. Les « *privacy tort*s » ressemblent aux règles posées par l'article 9 du Code civil français.

Des lois fédérales protègent les données à caractère personnel dans plusieurs secteurs de l'industrie

Outre ces règles de la *common law* développées au niveau de chaque État, les États-Unis disposent de lois fédérales visant la protection des données à caractère personnel dans certains secteurs. La première grande loi sur la protection des données à caractère personnel concernait les traitements de données effectués par le gouvernement fédéral. Le *Privacy Act* de 1974 établit des règles sur le traitement des données à caractère personnel collectées par les différentes branches du gouvernement. Cette loi met en

[2] *United States v. Jones*, 132 S.Ct.949 (2012).
[3] *Florida v. Jardines*, 133.S.Ct.1409 (2013).
[4] *Katz v. United States*, 389 U.S. 347 (1967).
[5] J. WHITMAN, « The Two Western Cultures of Privacy: Dignity versus Liberty », 113 *Yale L.J*. 1151, 2003-2004.
[6] S. D. WARREN & L. D. BRANDEIS, « The Right to Privacy », 4 *Harv. L. Rev*. 193 (1890).
[7] W. L. PROSSER, « Privacy », 48 *Calif. L. Rev*. 383, 383 (1960).

œuvre les « FIPs » (*Fair Information Practices*) développées à par le Ministère de la Santé américain en 1973. Les FIPs ont ensuite formé le socle de la Convention 108 du Conseil de l'Europe, des recommandations de l'OCDE de 1980, et de la directive européenne 95/46/CE.

Après le *Privacy Act* de 1974, le législateur fédéral a développé une série de lois visant la protection des données à caractère personnel dans le secteur privé :

- HIPAA (*Health Insurance Portability and Accountability Act*) – visant la protection des données de santé ;
- GLBA (*Gramm-Leach-Bliley Act*) – visant la protection des données financières ;
- COPPA (*Children's Online Privacy Protection Act*) – visant la protection des données concernant les enfants ;
- FCRA (*Fair Credit Reporting Act*)[8] – visant à réguler les profils de solvabilité des individus ;
- ECPA (*Electronic Communications Privacy Act*) – visant la protection des données de télécommunications ;
- VPPA (*Video Privacy Protection Act*) – visant la protection des données sur les locations vidéos ;
- *Cable TV Privacy Act* – visant la protection des données sur les choix des individus en matière de programmes de télévision ;
- *« Can-SPAM » Act* – visant l'interdiction des messages publicitaires.

Certaines de ces lois sont aussi protectrices que les lois européennes, même si leur champ d'application est plus restreint. En plus de ces lois fédérales, chacun des États américains a adopté des lois visant la protection de certains aspects de la vie privée de leurs citoyens. L'État de Californie a notamment adopté une loi protégeant les données à caractère personnel dans le cadre de sites Internet, ainsi qu'une loi accordant un droit à l'effacement à des utilisateurs mineurs de réseaux sociaux. Presque tous les États aux États-Unis ont adopté des lois définissant les conditions dans lesquelles les violations de sécurité de données à caractère personnel doivent être déclarées aux autorités et aux victimes.

L'interdiction des « pratiques déloyales » dans le commerce

En plus de ces lois ciblées, le législateur fédéral a adopté une loi générale sur la protection du consommateur, qui interdit toute pratique déloyale dans le commerce[9]. Cette loi est utilisée par l'agence fédérale pour

[8] La loi FCRA inclut une forme de droit à l'oubli.
[9] Section 5, *Federal Trade Commission Act.*

la protection des consommateurs, la FTC, pour protéger les données à caractère personnel. Au fil des années, la FTC a étendu le concept de « pratique déloyale » pour inclure tout traitement de données à caractère personnel incompatible avec les attentes légitimes du consommateur. Le concept de « pratique déloyale » est vague, mais la FTC utilise ses outils de régulation (sanctions, recommandations) pour définir le concept de manière précise. Le professeur Daniel Solove appelle cette politique de la FTC la nouvelle « *common law* » des données à caractère personnel[10]. La plupart des États des États-Unis ont leur propre loi sur les pratiques déloyales, et leur propre autorité de régulation. L'autorité de chaque État est généralement le ministre de la Justice (*attorney general*) de l'État. Ces autorités ont en charge l'application des lois de chaque État en matière de protection des données à caractère personnel. Ces autorités émettent des recommandations qui complètent celles de la FTC.

L'affaire Snowden

Les États-Unis disposent de règles pour les enquêtes judiciaires classiques et des règles pour les activités de renseignements. Les enquêtes judiciaires classiques sont régulées par le Code de procédure pénale[11] ; les activités de renseignements sont régulées par les textes applicables à l'espionnage et à la guerre[12]. Cette architecture binaire est similaire à celle qui existe en France : le Code de procédure pénale s'applique aux enquêtes judiciaires, et le Code de la sécurité intérieure s'applique aux activités de renseignements. Les règles concernant les activités de renseignement contiennent moins de protections de droits individuels et de transparence que celles applicables aux enquêtes judiciaires classiques. Pour les enquêtes judiciaires classiques, la police doit généralement obtenir l'approbation d'un juge avant d'entreprendre une mesure de surveillance intrusive. En matière d'activité de renseignements, des autorisations peuvent être accordées par un tribunal spécial (c'est le cas des États-Unis), ou par une personne spécialement désignée par le premier ministre (c'est le cas de la France). La transparence et l'encadrement de ces mesures sont faibles, voire inexistants dans certains cas, que ce soit aux États-Unis ou en France.

L'affaire Snowden a soulevé des questions sérieuses concernant le niveau de protection accordée aux individus dans le cadre des activités de renseignements. Les rapports publiés récemment à la demande du Président Obama démontrent que le régime américain est défaillant sur certains points

[10] D. SOLOVE and W. HARTZOG, « The FTC's New Common Law of Privacy », août 2013, www.ssrn.com

[11] Title 18, U.S. Code, « Crime and Criminal Procedure ».

[12] Title 50, U.S. Code, « War and National Defense ».

et doit être amélioré, en particulier pour mieux protéger la vie privée des citoyens non-américains[13]. La Commission européenne[14] et le Parlement européen ont également critiqué le système américain. Le Parlement européen a demandé l'arrêt immédiat du système « *Safe Harbor* »[15]. L'affaire Snowden a également révélé que les agences de renseignements de certains pays européens, dont la France, conduisent des pratiques similaires. Le débat sur ce point concerne autant la France que les États-Unis : dans un environnement de données massives, quel est le bon l'équilibre entre le droit à la sécurité et le droit à la protection de la vie privée ? La sécurité, comme la protection de la vie privée, est un droit fondamental. La sécurité permet aux autres droits d'exister[16]. En même temps, le droit à la sécurité ne peut pas envahir de manière disproportionnée la vie privée. La plupart des décisions judiciaires et des textes de loi sur ce sujet datent des années 1990, et visent les écoutes téléphoniques. Ces textes n'ont pas encore évolué pour appréhender toutes les difficultés posées par la surveillance des données massives.

Une différence de philosophie sur la nature d'une donnée à caractère personnel

Nous avons vu de nombreuses similitudes entre l'Europe et les États-Unis. Quelles sont les différences[17] ? L'une des plus grandes différences entre l'approche européenne et l'approche américaine concerne le caractère commercial ou non des données à caractère personnel. Aux États-Unis, certaines données – par exemple des données collectées par les hôpitaux ou par les banques – bénéficient d'une protection élevée. Mais en dehors de ces zones protégées, les entreprises sont libres d'exploiter des données pour autant que les entreprises ne commettent pas de « pratique déloyale ». En Europe, les données à caractère personnel sont rattachées à un droit fondamental. Toute exploitation de données constitue une violation potentielle d'un droit fondamental, et devra être justifiée par un intérêt légitime, un consentement, l'exécution d'un contrat, etc. En pratique, les

[13] « Liberty and Security in a Changing World », *Report and Recommendations of the President's Review Group on Intelligence and Communications Technology*, 12 déc. 2013.

[14] European Commission Press Release : « European Commission calls on the U.S. to restore trust in EU-U.S. data flows », 27 nov. 2013, IP/13/1166

[15] Résolution du Parlement européen du 12 mars 2014 sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures (2013/2188/(INI)).

[16] Conseil constitutionnel, déc. N° 94-352 DC du 18 janv. 1995.

[17] Ch. WOLF and W. MAXWELL, « So Close, Yet so far Apart: The EU and U.S. Visions of a New Privacy Framework », *Antitrust*, vol. 26, n° 3, 2012.

approches américaines et européennes conduisent souvent au même résultat pratique. Mais le point de départ est différent.

Les États-Unis et l'Europe convergent sur la co-régulation

La co-régulation est un système par lequel une institution de l'État, par exemple une autorité de régulation indépendante, établit un cadre à l'intérieur duquel des acteurs du secteur privé essaient de définir des mesures de régulation destinées à remédier à une défaillance du marché. La co-régulation est similaire à l'auto-régulation, sauf que dans le cadre de la co-régulation, l'État exerce une influence sur le développement des règles. De plus, l'État peut dans certains cas donner aux mesures de co-régulation une force contraignante. En principe, la co-régulation est destinée à rendre le processus d'élaboration des règles plus légitime, puisque l'État, à travers une autorité de régulation, est présent pour garantir que les règles développées par les acteurs privés contribuent à l'intérêt général. De plus, la co-régulation est censée rendre les règles plus efficaces, puisque leur application peut être garantie par l'État.

Binding corporate rules (BCRs) *: une forme de co-régulation*

Les autorités de protection des données personnelles en Europe restent méfiantes à l'égard des mesures d'auto-régulation pures. Elles préfèrent des mesures de co-régulation, puisque l'État reste impliqué dans l'élaboration des règles et dans leur mise en application effective. L'importance accordée aux BCRs en Europe témoigne de cette préférence pour les mesures de co-régulation.

La Commission européenne n'a pas encore reconnu les États-Unis comme offrant un niveau de protection adéquate des données personnelles. Ainsi, l'envoi de données personnelles vers les États-Unis est interdit, sauf si l'une des exceptions prévues par la directive s'applique. La directive prévoit notamment que l'envoi peut être effectué à l'intérieur d'un groupe de sociétés si le groupe a adopté des BCRs. Les BCRs sont des procédures internes qui garantissent un niveau élevé de protection des données à caractère personnel partout dans le groupe, y compris dans des filiales établies dans des pays sans protection « adéquate » des données à caractère personnel. Les BCRs doivent être développées en coopération étroite avec les autorités en Europe chargées de la protection des données à caractère personnel. Les BCRs sont négociées point par point avec l'autorité chef de file, et lorsque l'autorité chef de file est satisfaite du contenu des BCRs, le dossier est ensuite envoyé à deux autres autorités de régulation qui examinent le contenu du dossier. Les BCRs sont une forme de co-régulation parce qu'elles sont élaborées par des acteurs privés à l'intérieur d'un cadre

établi par des autorités de régulation. De plus, une fois adoptées, les BCRs deviennent opposables, leur violation pouvant donner lieu à la fois à des actions privées par des victimes, ainsi qu'à des mesures de sanction appliquées par les autorités de régulation.

Les accords transactionnels de la FTC

Aux États-Unis, la FTC applique une forme de co-régulation à travers les accords transactionnels qu'elle conclut avec des entreprises accusées d'avoir violé les règles américaines sur les pratiques déloyales. La FTC commence une enquête pour violation de la loi américaine interdisant des pratiques déloyales. Lorsque les preuves d'une violation sont suffisamment étayées, la FTC donne le choix à l'entreprise soit de conclure un accord transactionnel avec la FTC, soit de faire l'objet d'une poursuite judiciaire. Conclu pour une durée de 20 ans, l'accord transactionnel oblige la société à mettre fin aux pratiques déloyales, et à mettre en place des procédures internes d'*accountability* similaires à celles prévues par les BCRs : audits de conformité, programmes de formation et l'obligation de rendre compte à la FTC régulièrement. Compte tenu de la durée très longue de ces accords (20 ans), la FTC dispose d'un moyen puissant pour réguler des entreprises et notamment les grands acteurs de l'Internet. Si l'accord transactionnel concerne une plateforme majeure de l'Internet telle que Facebook[18], l'accord transactionnel aura un effet direct sur une grande partie de l'écosystème de l'Internet à travers cette plateforme. Un accord transactionnel aura également des effets indirects sur les autres acteurs du secteur, montrant aux acteurs de l'industrie les meilleures pratiques et les attentes de l'agence de régulation américaine. Ces accords ont une fonction pédagogique importante, similaire à celle d'une recommandation du groupe Article 29 en Europe.

Le multi-stakeholder process

Le gouvernement américain essaie d'encourager d'autres formes de co-régulation, utilisant le terme « *multi-stakeholder process* » pour désigner ces initiatives. Au titre du « *multi-stakeholder process* », l'agence américaine de télécommunications et d'information, la NTIA, invite les acteurs du secteur privé à développer des codes de conduite relatifs à certains secteurs de l'Internet. La NTIA organise des réunions entre acteurs, facilite l'échange d'informations et brandit la menace d'une mesure de régulation contraignante si les acteurs n'arrivent pas à trouver un accord. L'agence

[18] Une copie de l'accord transactionnel entre la FTC et Facebook est disponible sur le site de la FTC.

américaine agit en tant que régulateur maïeutique[19] en essayant de pousser les acteurs privés vers un consensus. La présence de l'État dans la discussion aide à garantir que les mesures qui émergent de la discussion seront en conformité avec l'intérêt général et que le point de vue des consommateurs est défendu. Ce processus de « *multi-stakeholder process* » mené par la NTIA a récemment donné lieu à un projet de recommandation en matière de transparence pour les applications mobiles.[20]

*L'*accountability *: une nouvelle norme globale*

L'importance accordée par les autorités de régulation aux mesures de co-régulation n'est guère surprenante. Les nouvelles recommandations de l'OCDE de 2013, la proposition de règlement européen pour la protection des données personnelles, le cadre APEC pour la protection des données personnelles et la politique de protection des données personnelles de la Maison Blanche[21] accordent une importance particulière au concept de « *accountability* ». L'*accountability* consiste en la mise en place de programmes de conformité à l'intérieur d'entreprises, et de la supervision de ces mesures par les autorités de l'État. L'*accountability* est une forme de co-régulation, pas très éloigné des BCRs et des accords de transaction de la FTC.

La convergence entre les approches « d'*accountability* » sera mise à l'épreuve dans le cadre des efforts en cours pour créer un système d'interopérabilité entre les BCRs européens et les *Cross Border Privacy Rules* (CBPR) développées au sein de l'APEC[22]. Comme les BCRs, les CBPRs sont des procédures internes mises en œuvre dans un groupe multinational pour assurer le respect des principes de l'APEC en matière de données à caractère personnel. L'application de ces procédures est vérifiée par un agent d'*accountability*, et la violation des règles peut donner lieu à des sanctions. Un groupe international qui met en œuvre à la fois les BCRs et les CBPRs aura satisfait aux obligations d'*accountability* à la fois en Europe et dans les pays de l'APEC. Le concept d'*accountability* est susceptible de devenir ainsi une norme mondiale en matière de protection des données à caractère personnel.

---

[19] N. CURIEN, « Innovation and Regulation serving the digital Revolution », *The Journal of Regulation*, 2011, I-1.32, pp. 572-578.

[20] http://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency

[21] United States White House, « Consumer data privacy in a networked world: a framework for protecting privacy and promoting innovation in the global digital economy », fév. 2012.

[22] http://www.apec.org/Press/News-Releases/2013/0306_data.aspx