Protection de la vie privée et l'interdépendance du droit, de la technologie et de l'autorégulation

Joel R.Reidenberg[1]

Introduction

Un nouveau paradigme a émergé pour la protection efficace des données personnelles dans l'environnement en ligne de l'Internet et de la société de l'information. Alors que les lois sur la protection des données se sont étendues à un grand nombre de pays dans le monde au cours des vingt dernières années, les divergences dans les lois nationales et la prolifération du traitement transfrontalier des données rendent difficile l'exécution des normes légales existantes. En même temps, il y a eu un développement des possibilités techniques qui permet et entrave tout à la fois la capacité de la loi à garantir le traitement équitable des données personnelles. En effet, la réglementation juridique partage le pouvoir régulateur avec les normes et protocoles technologiques. Pour le traitement des informations personnelles, la réglementation la plus directe du traitement de l'information vient plutôt des règles technologiques incorporées dans les infrastructures des réseaux par les acteurs économiques que de la loi elle-même. En effet, l'architecture des réseaux d'information établit les règles implicites du traitement de l'information.

Cet article étudie donc l'interdépendance complexe existant entre la loi, la technologie et les usages d'entreprise. En se basant sur les expériences américaines et européennes en matière de protection de l'informatique et de la liberté, cet article propose que pour l'Internet la loi fournisse une incitation aux avancées technologiques qui développent des technologies de protection de la vie privée. L'article soutient que la loi doit en outre créer les conditions de promotion de l'extension des technologies de protection de la vie privée et de la création de systèmes par les entreprises. Dans une société démocratique, la régulation par la technologie doit être modelée par les objectifs d'intérêt public et le débat public. La loi est donc nécessaire pour établir les objectifs d'intérêt public, mais insuffisante pour garantir l'application des bons usages en informatique.

---

1 Professeur de droit, Faculté de droit de l'université de Fordham. Une première version de cet article a été élaborée pour la conférence " Vers de nouvelles évolutions dans le droit de l'informatique" pour le 20e anniversaire du C.R.I.D. à Namur, Belgique, avec une grande reconnaissance au Doyen Yves Poullet qui a inspiré tant de spécialistes dans ce domaine. Cet article va paraître dans les Cahiers du C.R.I.D. (prochain numéro).

I. Différents modèles de réglementation de la protection des données

Les règles pour la protection des données proviennent de trois perspectives différentes: politique, économique et technologique. En Europe, la protection des données est un droit fondamentalement politique et s'appuie sur des mécanismes légaux pour garantir le respect d'un droit de l'homme fondamental à la protection de la vie privée.[2] Au contraire, aux Etats-Unis, la protection des informations est laissée au marché et à la préférence de trouver des protections des consommateus dans les résultats des marchés. [3] Dans ces deux modèles de protection des données , les règles technologiques et implicites définissent les usages de l'informatique pour les activités sur réseaux.[4]

En Europe, la perspective politique sur la protection des données insiste sur le fait que les citoyens ont un droit de l'homme fondamental au traitement équitable de leurs données nominatives. Ce droit à "l'autodétermination en matière d'information" fait nécessairement partie de la société démocratique. L'autodétermination en matière d'information met l'accent sur la liberté des citoyens et définit un droit de l'ordre public du citoyen à contrôler la collecte et l'usage des informations personnelles. Le modèle des droits politiques demande des règles juridiques dans une législation générale de protection des données. En conséquence, les lois européennes modernes de protection des données imposent un ensemble complet de normes pour le traitement équitable des informations personnelles allant de la finalité à l'accès et à l'exécution. Bien que les termes spécifiques et l'interprétation de ces lois puissent varier, les principes sous-jacents partent de la même idée que la protection des données est un droit de l'homme qui doit être garanti par l'état.

Aux Etats-Unis une approche opposée adopte un calcul économique à la place de la base politique pour la protection des informations se rapportant à la vie privée. L'approche américaine considère l'état avec plus de scepticisme et préfère laisser les citoyens se débrouiller tout seuls. Dans l'approche économique, l'autorégulation détermine les termes de la protection des données personnelles. Les codes de conduite des acteurs économiques et les usages des entreprises l'emportent sur la loi. La protection des données devient plus une question de pouvoir économique que de droit politique. En fait, le débat se définit plus typiquement en termes de "consommateurs" que de "citoyens". Dans cette approche, la loi n'intervient que sur une base très ciblée pour résoudre des problèmes spécifiques là où le marché a échoué. Les lois sectorielles ad hoc, par conséquent, ne concernent qu'un ensemble éclectique de problèmes. Les consommateurs de stupéfiants, par exemple, ont plus de protection que les utilisateurs du web, et les titres des films vidéos loués sont confidentiels , alors que les dossiers médicaux peuvent être divulgués.[5]

Indépendamment de ces deux modèles de confidentialité des données, la *Lex informatica* ou approche de "code" régule par les règles techniques incorporées dans l'architecture des réseaux. [6]
Les normes techniques et les protocoles ainsi que la disposition choisie par les créateurs de systèmes établissent les règles seuil de la protection des données. Ces règles techniques définissent les capacités de réseaux comme l'Internet à porter atteinte à la vie privée ou à la protéger. Par exemple, un usage anonyme de l'Internet peut être incorporé dans l'architecture du réseau tout comme un suivi de surveillance peut aussi être incorporé dans le réseau.

---

[2] Voir Convention du conseil de l'Europe pour la protection des droits de l'homme et des libertés fondamentales, art.8 ; Directive 95/46/CE du parlement européen et du conseil du 24 octobre 1995 sur la protection des individus concernant le traitement des données personnelles et la libre circulation de ces données, J.O.C.E. L.281, 23/11/1995 p. 0031-0050; Convention no. 108 du Conseil de l'Europe (28 janv.1981)

[3] Voir par ex. A Framework for Global Electronic Commerce (1997) [ci-après "U.S. Framework"]

[4] Voir Joel Reidenberg, Lex informatica: The Formulation of Information Policy Rules through Technology, 76 Texas L.Rev. 1315 (1998) [ci-après "Lex informatica"]

[5] Voir Paul Schwartz & Joel R.Reidenberg, Data Privacy Law (Michie:1996)

[6] Voir Lawrence Lessig, Code and Other Laws of Cyberspace (Basic Books: 1999); Lex informatica, supra.

Historiquement, les trois modèles (politique, économique et technologique) classent la réglementation du bon usage en informatique. La perspective politique prenait la loi comme mécanisme principal pour assurer la protection des données, tandis que la perspective économique prenait le marché comme arbitre des protections de la vie privée. En même temps, l'approche technique a incorporé des règles directement dans la transmission des données. Ces différentes approches sont habituellement considérées soit comme autosuffisantes, soit comme en remplaçant une autre. Par exemple, le dialogue transatlantique a pendant de nombreuses années décrit l'ensemble des droits juridiques et politiques comme l'alternative au code de conduite et aux décisions du marché.[7] En même temps, la communauté technique a poursuivi ses processus de normalisation et a prétendu à un certain degré de neutralité de politique.[8] Cependant, ces différents modèles ne sont ni autosuffisants ni des alternatives complètes l'un à l'autre.

II. L'inadaptation des différents modèles

Chacune des différentes formes de réglementation comporte des limites inhérentes qui l'empêchent de suffire à une protection efficace de la vie privée. La *Lex informatica* peut incorporer la capacité dans l'infrastructure soit de protection de la vie privée, soit de violation de la vie privée. Toutefois, à elle seule, l'approche technique ne garantit pas que la mise en œuvre des technologies respectera les principes de protection de la vie privée. Le modèle économique de marché américain minimise ou laisse de côté d'important aspects de la protections des données telles que les valeurs démocratiques non commerciales, tandis que le modèle européen des lois générales est confronté à d'importants problèmes d'application aux contextes spécifiques. En même temps, la protection des données est confrontée à des dimensions internationales critiques que les modèles politique, de marché ou technique ne résoudrent pas séparément.

Le modèle *lex informatica* souffre de l'absence d'un débat politique de l'intérêt public et de la pression commerciale pour une architecture technologique qui maximise la collecte de données et la "dataveillance".[9] Plusieurs exemples clé montrent cette faiblesse actuelle. La privatisation du système d'attribution de noms de domaine par le gouvernement américain et son attribution à Internet Corporation for Assigned Names and Numbers ("ICANN") ont largement ignoré les considérations de la protection de la vie privée inhérentes à la conception du nouveau protocole d'enregistrement du nom de domaine.[10] En effet, le protocole et le processus d'enregistrement exigent la publication en ligne d'informations nominatives sur les inscrits qui mettent en cause des principes fondamentaux de protection des données. La conception du système empêchait la possibilité d'un enregistrement anonyme de nom de domaine. De même, le Groupe d'études techniques de l'Internet ("IETF") s'efforce de créer un nouveau protocole de transmission Internet, IPv6.[11] Ce protocole prévoit que chaque appareil connecté à l'Internet aura un identifiant

---

[7] voir "U.S. Framework", *supra* en 14 (question 5)

[8] voir par ex. About IETF, http://www.ietf.org

[9] Roger Clarke a inventé l'expression "dataveillance" pour décrire la pratique de surveillance des données par la saisie des informations de suivi électronique comme les enregistrements interactifs de circulation. Voir Roger Clarke, « Information Technology and Dataveillance », Commun.ACM 31,5 (Mai 1998) <http://www.anu.edu.au/people/Roger.Clarke/DV/CACM88.html>

[10] voir Michael Fromkin: A critique of WIPO's RFC3 Ver. 1.0a (14 mars 1999). Avant que les responsables publics ne réalisent les implications du WIPO, une grande partie de la norme avait été terminée. Voir 3e rapport annuel du Groupe de l'Art.29 de la Directive européenne 95/46/EC, Doc.50066/00/en/final WP 35, p. 59 <http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp35en.pdf>

[11] Internet Engineering Task Force, Internet Protocol, version 6 (Ipv6) Spécification: Draft Standard RFC2460 (décembre 1998) http://www.ietf.org/rfc/rfc2460.txt?number=2460

unique - un genre d'empreinte digitale numérique pour les utilisateurs d'Internet. D'un point de vue technique, les empreintes digitales numériques ont peut-être beaucoup d'avantages, mais du point de vue de la vie privée, une telle architecture est très inquiétante. Il est important que ces décisions soient prises par le groupe des techniciens intéressés de l'IETF (groupe d'études techniques de l'Internet)[12] plutôt que par une combinaison de techniciens et d'acteurs politiques.

Alors que les décisions d'architecture technique sont souvent prises en forums peu connus, les grands produits sont aussi fréquemment développés avec une ignorance des conséquences aux libertés publiques. Les pressions commerciales poussent les informaticiens vers des produits qui recueillent autant d'informations que possible sur les utilisateurs. La personnalisation des produits du marché et les impératifs de sécurité des données exigent tous deux des informations détaillées sur les individus et leurs interactions en réseau. Habituellement, ces données "furtives" sont soit non transparentes pour l'utilisateur, soit incompréhensibles. [13] En effet, ces décisions techniques dissimulent d'importants problèmes politiques de la protection des données. Par exemple, les serveurs ont habituellement des fichiers comptes-rendus (« fichiers log ») contenant des données sur le comportement des utilisateurs. Ces fichiers sont utiles pour l'entretien du système, mais permettent aussi la surveillance massive d'individus. Cependant, les décisions politiques importantes selon lesquelles les fichiers auront la possibilité d'anonymat ou seront rapidement effacés échappent en général à l'attention du public. [14] De même, les moteurs de recherche sont pour les utilisateurs des outils puissants pour trouver des informations sur l'Internet. Toutefois, ils ont aussi d'étonnantes capacités de surveillance. DejaNews et Hotbot ont apparemment configuré le moteur de recherche pour relayer les informations de la chaîne de recherche à des tiers. [15] D'autres logiciels célèbres contenaient des caractéristiques cachées qui permettaient de repérer l'utilisateur jusqu'à un point surprenant. RealNetworks a même incorporé une fonction qui a déclenché un appel secret à RealNetworks quand un utilisateur écoutait la musique sur l'Internet . [16] Chacun de ces exemples illustre le pouvoir qu'ont les entreprises privées d'établir les règles de la vie privée et le poids des intérêts commerciaux sur les libertés publiques.

Le modèle américain a un ensemble parallèle de limites. Le fait qu'il se fie à l'autorégulation pour laisser le marché déterminer la protection de la vie privée minimise les aspects non économiques de la protection des données. [17] En particulier, la vie privée est un élément central de la démocracie et est une valeur très humaniste.[18] Les éléments fondamentaux de la démocratie et de la dignité humaine se prêtent peu au marché économique. Même au-delà de cette limite inhérente, la capacité d'un citoyen d'agir sur un marché de vie privée sera limitée par un important effet de réseau. Tout citoyen peut perdre la capacité de prendre des décisions sur ses informations personnelles du fait des divulgations par des tiers. Par exemple, un individu qui divulgue ses informations génétiques divulgue aussi les informations génétiques de ses parents. Au fur et à mesure que plus d'informations circuleront et que les possibilités d'établir des profils en recroisant des informations seront plus étoffées, tout individu perdra la capacité de faire des choix de participation.

---

[12] voir Overview of the IETF, http:/www.ietf.org/overview.html

[13] par exemple, l'utilisateur moyen de l'Internet a peu de chances de comprendre la technologie des "cookies" ou 'web bugs' et encore moins de savoir ce qu'il peut y faire.

[14] les avis habituels des sites web sur la confidentialité sont si vagues que même un utilisateur informé aurait des difficultés à trouver la réponse à ces questions.

[15] *Deja News Privacy Breach Raises Red Flag*, Information Security 13 (juin 1999)

[16] voir RealNetworks Federal Class Action, http://www.internetnews.com/streaming-news/article/0,1087,8161_235141,00.html

[17] voir Joel R.Reidenberg, Restoring Americans' Privacy in Electronic Commerce, 14 Berkeley Tech. L. J. 771(1999).

[18] voir Paul Schwartz , Privacy and Participation: Personal Information and Public Sector Regulation in the United States, 80 Iowa L. Rev. 553 (1995); Spiros Simitis, Reviewing Privacy in an Information Society, 135 U.Pa. L.Rev. 707 (1987); Alan Westin, Privacy and Freedom, 23-26 (1967).

Un marché pour la protection de la vie privée ne peut fonctionner efficacement que s'il y a transparence. Cependant, ce marché est l'illustration du problème classique d'échec du marché. Les usages actuels de l'information par les entreprises sont très dissimulés au public. En effet, la relation entre les entreprises de traitement des données et les individus est habituellement basée sur des informations asymétriques : " l'entreprise a le plus grand pouvoir de contrôler quelles informations sont diffusées sur elle tout en dissimulant simultanément la nature et l'étendue des informations qu'elle a obtenues sur les individus" [19] Les barrières empêchant les individus de découvrir comment les entreprises utilisent leurs informations personnelles sont souvent insurmontables. En même temps, les entreprises profitent énormément d'un commerce des informations personnelles dissimulé au public. Les victimes n'ont aucun recours, et il n'existe pas de mécanisme indépendant qui détermine si les bons usages en informatique sont respectés. Dans ces conditions, le marché n'offre pas et ne peut pas offrir aux individus la possibilité de négocier de bons usages constructifs en informatique pour l'utilisation de leurs informations.

La réponse traditionnelle aux problèmes de l'approche américaine autorégulatrice est l'adoption de lois ciblées pour combler les lacunes de protection. [20] Cependant, l'éclectisme de la réponse réglementaire aux Etats-Unis illustre les limites de cette méthode. Les réglementations sectorielles sont réactives et incohérentes. Par exemple, les agences de renseignements sur le crédit fournissant des informations sur les antécédents en relation avec les décisions d'accord de crédit sont réglementées, [21] mais les organisations de marketing direct fournissant des informations similaires à des buts de marketing ne le sont pas. [22] Cette méthode de comblement des lacunes législatives laisse aussi de côté beaucoup d'aspects du traitement des informations et va à l'encontre de la nature trans-sectorielle du traitement de données moderne.

Les lois générales de protection des données, toutefois, sont nécessairement trans-sectorielles avec une grande portée. Mais le modèle européen aussi présente ses propres problèmes qui limitent l'autosuffisance de l'approche réglementaire générale. La vie privée est contextuelle et l'interprétation de règles générales dans un contexte spécifique sera souvent extrêmement difficile et complexe. En effet, les principes généraux laissent une large marge pour l'interprétation et l'application. En conséquence, la complexité toujours croissante du traitement des données est un défi fondamental à la clarté et au traitement équitable des individus et des utilisateurs de données.

L'ambiguïté et l'application des principes généraux ont un impact important sur les communications en ligne. Souvent, les lois générales de protection des données présentent des divergences importantes.[23] Par exemple, les lois de l'informatique et de la liberté se rapportent à des informations qui concernent une personne "identifiable". [24] Mais ce que recouvre une personne "identifiable" est interprété très différemment selon les diverses lois

---

[19] Philip Agre, Introduction in Technology and Privacy: The New Landscape (Philip E.Agre & Marc Rotenberg eds. 1997), 11.

[20] voir Schwartz &Reidenberg, supra.

[21] voir 15 U.S.C. § 1681b

[22] voir In re: Trans Union, rôle 9255 Federal Trade Commission, Opinion de la commission, 12-13 (1er mars 2000) http://www.ftc.gov/os/2000/03/transunionopinionofthecommission.pdf (notant que les organismes non classés comme agences de renseignements sur la santé financière peuvent fournir d'une façon non réglementée des données qui sont similaires, mais pas aussi fiables, que les données réglementées des agences de renseignements sur la santé financière) affaire Trans Union Corp contre FTC, 245 F.3d 809(DC Circ., 2001) <http://laws.findlaw.com/dc/001141a.html>

[23] voir par ex. Peter Swire &Robert Litan , None of Your Business: World Data Flows, Electronic Commerce and the European Directive 188-96 (Brookings:1998); Joel R.Reidenberg &Paul Schwartz, Data Protection Law and Online Services: Regulatory Responses (Comm. Eur. 1998)

générales. Certains pays européens adoptent une conception plus large des critères pour les données anonymes et excluent des protections de la loi plus de données concernant les transactions que d'autres. [25] Pour les transmissions de données en Europe, la conséquence est que certains pays peuvent considérer certaines données comme non soumises aux lois de protection des données, tandis que d'autres leur appliqueront la gamme complète des normes juridiques.

Le caractère exécutoire présente une autre limite à l'efficacité des lois générales de protection des données. La crédibilité de la protection des données dépend de son caractère exécutoire. Alors que les lois européennes établissent des mécanismes d'application importants par des amendes et des commissions de protection des données, de problèmes de conformité avec les exigences d'avis et d'enregistrement apparaissent néanmoins. [26] Les poursuites pour infraction aux lois de protection des données ne sont toutefois pas fréquentes en Europe même face à des violations flagrantes. [27] Ce qui est plus grave, le traitement transnational des données remet en question les pouvoirs d'exécution territoriale.

Les dimensions internationales de la protection des données mettent à l'épreuve chacun des différents modèles. La croissance spectaculaire des industries de service globales entraîne des conflits et pressions d'importance dans les formes politiques, économiques et techniques de régulation de l'informatique et de la liberté. Alors que les législations nationales et même les accords privés ont des rôles à jouer dans le nouvel âge de l'information globale, il existe un besoin croissant d'une coordination internationale de la protection de la vie privée. L'inévitabilité du conflit entre les normes juridiques et générales que l'on trouve en Europe, et les protections ad hoc que l'on voit aux Etats-Unis, place la question du traitement équitable des informations personnelles au centre des flux transfrontiers des données. Même en Europe, le traitement transnational des informations crée des conflits entre des régimes généraux fondés sur la loi. En effet, au début des années 1990, les différentes lois nationales ont fait de l'harmonisation des normes de protection des données une composante essentielle du projet de marché interne. La directive européenne 95/46/EC a cherché à harmoniser les lois nationales des états membres à un haut niveau commun de protection pour "les droits et les libertés fondamentales des personnes physiques et en particulier leur droit à la protection de la vie privée." [28] La stratégie était double: premièrement, la directive établissait les principes obligatoires, essentiels pour le traitement des données personnelles, puis deuxièmement, elle demandait aux Etats membres de l'Union européenne de faire que leurs lois nationales soient pleinement conformes à ces normes. Toutefois, les divergences entre normes qui étaient autorisées par la marge de manœuvre accordée par la directive ont laissé d'importants obstacles pour les services en ligne. [29] La directive a aussi obligé à un examen minutieux des régimes de protection des données étrangers par l'interdiction

---

[25] voir Reidenberg &Schwartz, supra, pp. 124-26

[26] par exemple le faible nombre des enregistrements dans des pays comme la France et un examen anecdotique des avis sur la divulgation de la vie privée sur les sites web européens montrent des problèmes de conformité. En effet, une recherche des enregistrements exigés de grands fournisseurs de services en ligne dans au moins un pays européen a révélé que de grandes sociétés tout à fait en évidence ne s'étaient pas enregistrées et que cette non conformité à la loi était ignorée. Voir aussi *Existing case-law on compliance with data protection laws and principles in the Member States of the European Union.* Annexe au rapport annuel de 1998 de la commission de travail créé selon l'art.29 de la directive 95/46/EC (1998)

[27] par exemple, le nombre d'enregistrements dans les pays comme la France ou la Belgique indique un problème de conformité. En effet, une recherche des enregistrements exigés de grands fournisseurs de services en ligne dans au moins un pays européen a révélé que de grandes sociétés tout à fait en évidence ne s'étaient pas enregistrées et étaient apparemment ignorées.

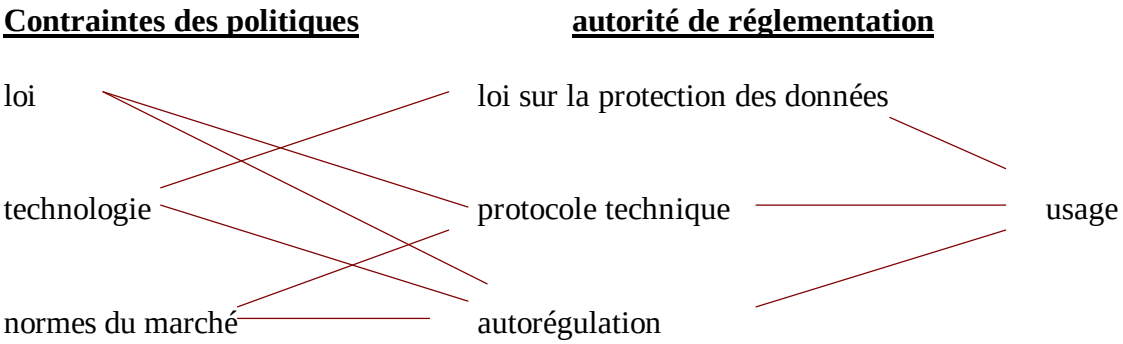
[28] Directive 95/46/CE [29] Reidenberg &Schwartz, supra.

des transferts d'informations personnelles vers des pays n'offrant pas de protection "adéquate". [30] Comme les combinaisons complexes de traitements d'informations impliquent souvent des juridictions multiples, cette disposition a amené à un conflit entre les différentes approches politique et économique de l'Europe et des Etats-Unis . En même temps, l'émergence de l'Internet et de ses capacités sophistiquées de traitement international des données a montré que les règles techniques se développaient à leur façon sans considération des normes nationales de protection des données . [31] Ceci signifiait que les diverses technologies déployées pouvaient ne pas offrir aux utilisateurs la capacité de se conformer aux normes locales de protection des données.

III. Le modèle d'interdépendance des protections de l'informatique et de la liberté

Les problèmes de chacun des différents modèles montrent que les trois approches ne peuvent être isolées. En effet, les approches politique, économique et technologique s'influencent mutuellement et donnent des aperçus importants pour la création d'une protection des données efficace. La véritable mise au point des bons usages en informatique exige la reconnaissance d'un modèle d'interdépendance des protections de l'informatique et de la liberté. Le diagramme ci-dessous illustre ce modèle.

Modèle de l'interdépendance des protections de l'informatique et de la liberté



L'interdépendance des protections de l'informatique et des libertés commence par une compréhension des contraintes des politiques et des autorités de réglementation pour la protection des données qui dérivent de chacun des trois modèles. Les contraintes des politiques sont les mécanismes d'établissement des règles de protection des données. Le modèle politique utilise la loi, le modèle économique emploie les normes du marché et le modèle de la *Lex informatica* utilise les technologies. Les véritables règles de protection des données sont établies par les autorités de

---

[30] Directive 95/46/EC, art.25

[31] voir Recommandation 1/99 sur Le traitement invisible et automatique des données personnelles sur l'Internet fait par logiciels et matériels du groupe de travail établi d'après l'art.29 de la directive 95/46/EC., Eur.Doc. DG MARKT 5093/98 WP 17 - (23 février 1999)
<http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp17en.htm>

réglementation. Dans le modèle politique, l'autorité de réglementation est une loi de protection des données, tandis que dans un modèle économique, c'est l'autorégulation. Dans un modèle de *Lex informatica*, l'autorité de réglementation est un protocole technique.

Comme le montre le diagramme ci-dessus, les contraintes des politiques n'agissent pas d'une façon sectorielle sur les autorités de réglementation. La loi affecte les protocoles techniques et l'autorégulation. Des exemples les plus clairs de cette interaction entre la loi et la technologie se produisent en matière de cryptographie. La loi a fourni des limites controversées sur la disponibilité des produits de cryptage que ce soit par une réglementation de contrôle à l'exportation ou sur la concession de licences portant sur l'utilisation de ces produits.[32] De même, la loi a motivé des mécanismes d'autorégulation. La directive 95/46/EC a été une grande incitation à la création pour l'Internet aux Etats -Unis une petite industrie de labelisation attestant des traitements de données personnelles par des entreprises sur leurs sites web. [33]

En même temps, la technologie affecte les lois de protection des données et l'autorégulation. Les développements technologiques influencent à la fois le besoin et l'orientation de la loi. Par exemple, les premières lois de protection des données étaient centrées sur les "fichiers" et les systèmes de fichiers parce que l'environnement était composé d'ordinateurs centralisés. Aujourd'hui, la décentralisation de l'informatique et les communications sans fil modifient la relation de traitement, et la protection de données moderne est centrée sur les "contrôleurs", "traitement" et "données structurées", reflétant ainsi ces développements techniques. En outre, la globalisation des réseaux a signifié que les lois de protection des données ont dû décider comment traiter les normes étrangères. L'Europe a opté pour les contrôles des flux transfrontiers si les normes étrangères étaient trop insuffisantes. [34] De même, la technologie a influencé la capacité des mécanismes d'autorégulation. Les premiers "cookies" permettaient de repérer les utilisateurs de l'Internet sans leur accord. Au fur et à mesure que les utilisateurs se sont alarmés et que les logiciels de navigation se sont perfectionnés, les options pour les "cookies" se sont développées pour permettre aux utilisateurs un meilleur contrôle sur un tel repérage. [35] Cette interdépendance est aussi illustrée par l'apparition de lois sur la protection des données qui répondent spécifiquement à la technologie. L'Allemagne , par exemple, a adopté une loi spécifique "d'alerte aux cookies" pour exiger que les utilisateurs soient informés de l'emploi de la technologie des cookies. 36

Les normes du marché ont aussi un impact important sur les protocoles techniques et l'autorégulation. Les acteurs du marché entraînent le développement de nouvelles architectures techniques. Par exemple, au fur et à mesure que les développements de la technologie donnaient aux utilisateurs plus de contrôle sur le repérage de leur comportement par l'emploi des cookies, les sites web et les annonceurs commencèrent à découvrir des moyens techniques de tourner les contrôles des utilisateurs par des bogues ou des images GIF vides. Le bogue web profite de certaines caractéristiques des commandes HTML qui permettent à un site web ou à un annonceur d'obliger le navigateur des utilisateurs à charger une image de la taille d'un seul pixel d'un site distant. Cette image est imperceptible pour l'utilisateur et ne peut pas être bloqué par lui, mais l'action permet au site web ou à l'annonceur de repérer l'utilisateur. 37

Au cas échéant, les normes du marché reflétant l'importance de la protection de la vie privée pour le commerce

---

[32] Les Etats-Unis, par exemple, réglementent l'exportation de produits de cryptage tandis que la France a toujours demandé une licence pour les produits de cryptage utilisés en France. De même, aux Etats-Unis, la loi Computer Assistance for Law Enforcement Act, 47USC§§ 1001-1010, exige que les réseaux numériques soient "écoutables".

[33] Truste and BBBOnline , en particulier, cherchait à être une réponse autorégulatrice au niveau de protection exigé par l'art.25 de la directive 95/46/EC.

34 Directive 95/46/EC, art.25

[35] Les dernières versions de Netscape Communicator et d'Internet Explorer permettent chacune plusieurs choix concernant les cookies qui n'étaient pas disponibles dans les versions antérieures de ces logiciels de navigation.

[36] IuKDG, art.2

[37] voir Richard Smith, FAQ: Web bugs <http://wwww.privacyfoundation.org/education/webbug.html>

électronique ont été aussi une motivation importante pour le développement d'un protocole technique qui permettrait aux sites web de divulguer leurs politiques de traitement des données d'une manière lisible par ordinateur. Ce protocole, P3P, est développé par le World Wide Web Consortium. De même, les normes du marché influencent l'autorégulation à la fois dans un sens positif et dans un sens négatif. Au fur et à mesure que la protection de la vie privée préoccupe plus les citoyens, le génie de certains acteurs de l'industrie a adopté la protection des données comme usage essentiel de la profession. De grandes sociétés financent maintenant le développement d'outils de protection de la vie privée. Mais dans la mesure où les citoyens ne connaissent pas les usages des entreprises ou que les acteurs de l'industrie suivent des codes de conduite écrits par les associations professionnelles, les normes du marché apportent plus de relations publiques qu'une véritable protection des données.

L'impact collectif des différentes contraintes des politiques sur les autorités de réglementation et les règles qui en résultent elles-mêmes, conduisent aux traitements réels concernant les données dans la société. En effet, les autorités de réglementation ne sont pas indépendantes [38] ; chacune exerce une influence sur les bons usages en informatique et sur le niveau réel de protection des données. Comme les éléments ne sont pas indépendants, la protection efficace des données ne peut venir que d'une combinaison des contraintes politiques et des autorités de réglementation travaillant de concert plutôt qu'en opposition. Les relations de la loi, de la technologie et des normes du marché avec la législation de protection des données, les protocoles techniques et l'autorégulation sont entrecroisées. Chaque autorité de réglementation peut réduire ou soutenir les objectifs des autres. Par exemple, quand la loi de protection des données cherche à empêcher la collecte d'informations personnelles, des protocoles techniques exigeant l'identification des utilisateurs peuvent être créés , ou des options techniques peuvent être développées pour créer l'anonymat. De même, les contraintes des politiques peuvent réduire mutuellement leurs objectifs, et aller à l'encontre des objectifs de diverses autorités de réglementation. Par exemple, les normes du marché tendent à favoriser la maximisation de la collecte des données aux fin commerciaux tandis que la loi préfère que les données soit minimisées et servent aux besoins sociaux et des citoyens. Dans la mesure où ces préférences sont incorporées dans les protocoles techniques et les mesures d'autorégulation, ces autorités de réglementation seront en contradiction avec les objectifs de la loi de protection des données. En bref, il y a une interdépendance de la loi, de la technologie et de l'autorégulation du marché.

Dans ce contexte d'interdépendance, la protection de la vie privée ne peut donc être garantie convenablement que par la canalisation des contraintes des politiques et des autorités de réglementation. Les éléments doivent fonctionner ensemble d'une manière cohérente pour arriver à une protection efficace des données. La canalisation des contraintes des politiques et des autorités de réglementation tournera autour de quatre conditions clé. Premièrement, la participation des citoyens à la conception de la loi, des technologies et des marchés est essentielle pour une protection efficace des données. La participation des citoyens est nécessaire afin que les valeurs et les objectifs publics soient cohérents dans les trois sphères du droit, de la technologie et du marché. Deuxièmement, l'anonymat à l'âge du numérique devient une caractéristique essentielle pour les systèmes techniques et les produits du marché. L'anonymat incorporé dans les systèmes informatiques favorise la cohérence de la protection de la vie privée dans la loi, la technologie et le marché. Troisièmement, la minimisation des données doit être la pierre angulaire des normes de la loi, de la technologie et du marché. La nécessite des données pour les besoins de la technologie et du marché préserve la cohérence dans le traitement des informations personnelles dans les trois sphères. Enfin, l'automatisation doit jouer un rôle important dans la garantie de la protection des données. Les mécanismes qui rendent automatique l'application des politiques concernant les données permettront une uniformité dans les zones de la loi et du marché.

L'interdépendance signifie que des technologies de la protection de la vie privée sont nécessaires, que les normes du marché doivent adopter ces technologies et que la loi doit protéger les citoyens. Cependant, dans le contexte de la protection des données, les incitations du marché et les informaticiens ne soutiennent pas régulièrement la protection de l'informatique et des libertés et n'aboutissent pas à des règles cohérentes. [39] Pour que

---

38 voir par ex. Lawrence Lessig, Code and other Laws of Cyberspace (1999)

39 voir Joel R.Reidenberg, Restoring Americans' Privacy in Electronic Commerce, 14 Berkeley Tech. L.J. 771 (1999) http://www.law.berkeley.edu/journals/btlj/articles/14_2/Reidenberg/html/reader.html

l'autorégulation et les règles techniques jouent ensemble en faveur d'une protection efficace des données, il faut qu'il existe un cadre d'objectifs. Dans une société démocratique, les objectifs publics et les valeurs publiques sont traditionnellement fixés par les représentants politiques au moyen du système juridique. Cela signifie que la loi doit établir les objectifs pour les autorités de réglementation de la protection des données. En effet, pour canaliser les règles techniques et l'autorégulation et les faire correspondre aux règles juridiques, la loi peut et doit attribuer une responsabilité au marché et aux architectes de réseaux pour leurs choix. [40] En d'autres termes, les règles de la responsabilité juridique deviennent un mécanisme clé pour inciter les règles techniques et l'autorégulation à s'harmoniser avec les objectifs publics. Cette motivation nécessaire entraînera le développement et l'extension de technologies de protection de la vie privée et d'actions de protection de la vie privée du marché. Si, d'après la loi, les technologies doivent contenir des options de protection de la vie privée et si la responsabilité doit être intégrée aux régimes autorégulateurs, alors ces autorités de réglementation - protocoles techniques et autorégulation - agiront de manière complémentaire au lieu de se développer de manière contradictoire.

Conclusion

Le modèle juridique, le modèle technologique, et le modèle du marché des bons usages informatiques , quoique conçus comme des ensembles de règles distincts, sont en fait interdépendants en tant qu'instruments d'une protection efficace des données. Cette interdépendance de la loi, de la technologie et de l'autorégulation montre, toutefois, que les trois autorités de réglementation doivent être canalisées dans la même direction afin que les règles se renforcent au lieu de se contrecarrer. Trois principes directeurs peuvent être dégagés pour cette canalisation des autorités de réglementation:

1. La loi est nécessaire pour établir les objectifs d'intérêt public, mais insuffisante pour garantir l'application des bons usages en informatique.
2. Dans une société démocratique, l'établissement des règles par la technologie doit être dirigé par les objectifs et le débat des libertés publiques.
3. La responsabilité juridique sera un instrument essentiel pour le développement de produits de protection de la vie privée.

Les relations complexes entre la loi, les choix techniques et le marché demandent une vigilance accrue des citoyens à propos de la collecte et de l'utilisation de leurs informations personnelles. Des citoyens vigilant et actifs resteront la défense essentielle contre l'érosion de la vie privée à l'âge informatique.

---

[40] voir par ex. *Lex informatica* supra