COMMISSION OUVERTE

ITALIE

Responsable : MARTINA BARCAROLI

Mercredi 24 avril 2013

Le futur de la réglementation des données personnelles en Europe : Un dialogue franco-italien

Intervenants :

Giovanni Buttarelli
Contrôleur européen adjoint de la protection des données

Isabelle Falque-Pierrotin
Présidente de la Commission Nationale de l'Informatique et des Libertés (CNIL)

ORDRE DES AVOCATS DE PARIS

LEXBASE l'information juridique

Présentes à cette occasion, les éditions Lexbase vous proposent de retrouver un compte-rendu de cette réunion.

LEXBASE
l'information juridique

Revues

Lexbase Hebdo édition affaires n°345 du 4 juillet 2013

[Internet] Evénement

Le futur de la réglementation des données personnelles en Europe : un dialogue franco-italien — Compte-rendu de la réunion de la Commission ouverte Italie du barreau de Paris du 24 avril 2013

N° Lexbase : N7798BTY

par *Vincent Téchené, Rédacteur en chef de Lexbase Hebdo— édition affaires et Anna Lasseri, Benjamin N. Cardozo School of Law — NY, LL.M in General Studies*

La Commission ouverte Italie du barreau de Paris a tenu, le 24 avril 2013, une réunion sous la responsabilité de Maître Martina Barcaroli, avocat aux barreaux de Paris et de Rome. A cette conférence, qui avait pour thème "Le futur de la réglementation des données personnelles en l'Europe : un dialogue franco-italien", sont intervenus Giovanni Buttarelli, Contrôleur européen adjoint de la protection des données et professeur à l'Université de Rome ; Jean-Paul Amoudry, Sénateur, vice-Président de la CNIL et délégué au groupe de l'article 29 ; Clarisse Girot, conseiller, cabinet de la présidence et du secrétariat général de la CNIL ; et Christiane Féral-Schuhl, Bâtonnier de l'Ordre des avocats de Paris. Présentes à cette occasion, les éditions juridiques Lexbase vous proposent de retrouver le compte-rendu de cette réunion.

Comme l'a exposé Martina Barcarolli, dans ses propos introductifs, le but de cette réunion est, certes d'opérer une comparaison entre les systèmes voisins mais différents, que sont les législations sur la protection des données italienne et française, mais aussi d'exposer les projets européens en la matière. En effet, face à la fragmentation des législations nationales consécutive à la transposition de la Directive de 1995 (Directive 95/46 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 N° Lexbase : L8240AUQ), il est apparu indispensable de renforcer l'harmonisation.

C'est dans cette optique qu'a été présenté par la Commission européenne, le 25 janvier 2012, le projet de Règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (Règlement général sur la protection des données).

– **Présentation du système italien de protection des données, par Giovanni Buttarelli**

L'Italie fut l'un des derniers pays à transposer la Directive 95/46 visant à la protection des données personnelles, quelques mois seulement avant la Grèce.

Cela est notamment dû au fait qu'il n'existait pas de loi sur la protection des données personnelles avant la transposition de ce texte, transposition qui a été réalisée par l'adoption de la loi 675 du 31 décembre 1996 portant protection des personnes et des organismes publics et privés à l'égard du traitement de données à caractère personnel. La loi 676 a été adoptée en même temps. Elle donnait pendant dix-huit mois délégation au Gouvernement, d'une part, pour effectuer par décret des modifications au texte de base et, d'autre part, pour prendre des textes réglementaires complétant le texte de base dans plusieurs domaines (traitement des données à des fins de recherche, règles particulières à certains secteurs comme les télécommunications ou la sécurité sociale, attribution d'un identifiant unique, formes simplifiées de notification, application de la loi aux journalistes et au secteur public...). La loi sur la protection des données concerne les personnes physiques et les personnes morales ; elle s'applique aux fichiers automatisés comme aux fichiers manuels. En revanche, elle exclut un certain nombre de traitements réalisés au sein du secteur public, parmi lesquels ceux qui incluent les données couvertes par le secret d'Etat et ceux qui sont effectués par les services du casier judiciaire ou dans le cadre de procédures pénales en cours. Cependant, cette exclusion n'empêche pas l'application des principes fondamentaux (licéité, loyauté, finalité, exactitude, sécurité...).

En juin 2003, une nouvelle loi (Code de protection des données) a été adoptée dans le but de consolider et de remplacer entièrement la législation existante pour des raisons essentiellement de sécurité juridique. C'est ainsi qu'en 2003, l'Italie est devenue le seul pays ayant un code unifié de protection des données avec 200 dispositions. Cette loi est entrée en vigueur le 1er janvier 2004.

Concernant la DPA (*Garante per la protezione dei dati personali*), l'idée était de lui donner des pouvoirs forts sachant que l'Italie, comme la Pologne, est l'un des rares pays où une autorité de protection indépendante est habilitée à adopter des décisions concernant certaines affaires judiciaires avec d'importants pouvoirs d'investigation. Elle apporte son aide dans la recherche scientifique notamment dans le but de la protection des données personnelles, elle conseille lors de la création de nouvelles lois. La DPA adopte deux fois par an des documents dans lesquels elle analyse toutes les propositions existantes de la Commission européenne.

La *Garante* a pour principales fonctions de :

— vérifier que le traitement des données personnelles est conforme aux lois et règlements et, si nécessaire, prescrire aux propriétaires ou gestionnaires des mesures à prendre pour mener à bien le traitement ;

— enquêter sur les plaintes et rapports et de décider les appels présentés sous la rubrique "Article 145 du Code en matière de protection des données personnelles" ;

— interdire, en tout ou en partie, ou prendre des dispositions pour le blocage du traitement des données à caractère personnel qui, par leur nature, leur manière ou leurs effets peut représenter un préjudice important ;

— adopter les mesures envisagées par la législation sur les données personnelles, en particulier, l'autorisation générale pour le traitement de données sensibles ;

— promouvoir la signature de codes d'éthique et de bonne conduite dans divers domaines (crédit à la consommation, les activités journalistiques, etc.) ;

— effectuer un rapport, le cas échéant, au gouvernement sur la nécessité d'adopter des mesures réglementaires spécifiques dans le développement économique et social ;

— participer à la discussion sur les initiatives réglementaires avec des audiences tenues devant le Parlement ;

— fournir des avis demandés par le président du conseil d'administration ou par chaque ministre afin de prendre des mesures administratives appropriées susceptibles d'influer sur les questions couvertes par le code ;

— préparer un rapport annuel sur ses activités et sur la mise en œuvre de la législation sur la vie privée transmis au Parlement et au Gouvernement ;

— participer à des activités communautaires et de commerce international ;

— assurer la tenue de registre de traitement formé sur la base des notifications visées à l'article 37 du Code en matière de protection des données personnelles ;

— veiller à l'information et à la sensibilisation du public à l'égard du traitement des données à caractère personnel et sur les mesures de sécurité des données ;

— impliquer les citoyens et tous les acteurs avec des consultations publiques dont les résultats sont pris en compte dans l'élaboration de mesures générales.

L'Europe traverse, aujourd'hui, une phase historique. L'évolution de la réglementation de la protection des données personnelles est marquée par des étapes importantes : les questions soulevées ne portent pas uniquement sur la protection des données et leur confidentialité, mais aussi sur la protection de la dignité et de l'identité personnelle.

Le Règlement européen proposé en 2012, qui sera probablement applicable en 2016 ou 2017, a vocation à s'appliquer au-delà des frontières européennes : toutes les données personnelles recueillies à partir de sites internet hors UE tels que Facebook ou Google, seront soumises aux règles sur la protection des données, ce qui est un grand exploit.

Parallèlement, est né aux Etats-Unis, le *Cyber Intelligence Sharing and Protection*, projet de loi déposé en 2011 à la Chambre des représentants des Etats-Unis, qui avait pour objectif de faciliter l'accès de différentes agences gouvernementales aux données personnelles des fournisseurs d'accès à internet, lorsqu'existent, à l'égard d'un internaute, des soupçons d'action délictuelle ou criminelle sur le réseau. Ce texte, adopté par la Chambre des représentants, ne l'a pas été par le Sénat américain. En tout état de cause, le Président Obama a annoncé qu'il aurait opposé son veto, dans la mesure où le projet portait atteinte au respect du droit sur la protection de la vie privée.

– **Présentation de l'institution française de protection des données : la CNIL, par Jean-Paul Amoudry**

La CNIL est une autorité mature, instituée en 1978 (loi n° 78-17 du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés N° Lexbase : L8794AGS) au lendemain de l'initiative Safari qui avait pour objet de regrouper l'ensemble des fichiers publics du pays.

La CNIL est aujourd'hui composée d'un collège de 17 membres : deux sénateurs et deux députés, des personnalités qualifiées, issues du Conseil d'Etat, de la Cour de cassation et de la Cour des comptes. Le mandat de ses membres, qui élisent leur président, est de 5 ans. A côté de ce collège, des équipes hautement qualifiées de juristes et d'informaticiens effectuent le travail quotidien. Ils sont organisés en divisions : la division juridique et international, numériquement la plus importantes ; la division de l'expertise et de la prospective ; la division des plaintes, des contrôles et des sanctions. Elle comprend également un cabinet attaché au président et au secrétaire général composé de conseillers techniques. La CNIL compte un effectif d'environ 170 personnes.

Contrairement à la DPA, la CNIL n'est pas une autorité judiciaire mais une AAI qui ne dispose donc pas des mêmes pouvoirs d'investigation. Les décisions de la CNIL sont des décisions administratives soumises au contrôle du Conseil d'Etat. Ses pouvoirs ont toutefois été renforcés par une loi de 2004, en créant notamment la formation restreinte pouvant prononcer des sanctions en cas de manquement constatés. Elle peut ainsi prononcer des sanctions pécuniaires, mais aussi des avertissements simples ou rendus publics, ainsi que des mises en demeure. Le prononcé de sanctions rendues publiques a souvent un impact beaucoup plus fort que celui de sanctions pécuniaires.

En 1978, la CNIL avait vocation à contrôler et autoriser en matière de fichiers publics. L'évolution du monde est telle que la CNIL a aujourd'hui à faire pour l'essentiel à des fichiers privés. Un autre phénomène marquant est celui de l'internationalisation des échanges et le passage d'une logique de fichiers à une logique de fichiers de données, qui s'est traduite par le passage d'un régime d'autorisation préalable et de déclaration préalable à un univers qui exige un contrôle dynamique et permanent. Dans cette optique ont été créés les CIL, correspondants informatique et liberté, qui jouent un rôle essentiel d'assistance et d'accompagnement dans la mission de protection des données.

L'activité de la CNIL se caractérise par sa transversalité puisqu'elle connaît de dossiers ayant trait au droit du travail, au droit bancaire, au droit de la consommation, ou encore au droit des télécommunications. A la différence de l'autorité italienne, la Commission française ne dispose pas d'un *corpus* de droit qui servirait de base juridique codifiée. Les services de la CNIL ont recensé les textes avec lesquels la loi de 1978 devait être interconnectée, ce qui représente plus de 350 textes.

La CNIL souhaite aujourd'hui se positionner à l'avant-garde des innovations et des progrès technologiques afin d'accompagner l'ensemble des acteurs et adopter un rôle, non pas de censeur et de contrôleur, mais de prévention

et d'information par un travail en amont et se préparer ainsi à ce que réserve le futur Règlement européen, c'est-à-dire une plus grande responsabilité des acteurs et un pouvoir renforcé de la CNIL.

– **Evolution de la protection des données en Europe et projet de Règlement par Giovanni Buttarelli, Jean-Paul Amoudry et Clarisse Girot**

Sur le plan de la protection des données, personnelles, comparé au bloc anglo-saxon, la France et l'Italie sont très proches. La législation de ces deux pays déclare solennellement la nécessité de veiller à ce que tous les types de données personnelles soient respectueux de toutes les libertés et droits fondamentaux, notamment le droit à la vie privé et à la dignité. Toutefois, selon la culture du pays, la façon dont les droits sont protégés change.

Monsieur Buttarelli est ainsi revenu sur l'évolution historique de la protection des données personnelles, laquelle se divise en trois grandes périodes.

La première des trois étapes historiques est initiée par le droit allemand en 1977 et le droit français en 1978. L'idée était de permettre un examen préliminaire par une autorité indépendante. Par ailleurs, la Convention du Conseil de l'Europe de 1981, qui est toujours un modèle valide aujourd'hui et qui se distingue par sa souplesse et son caractère international puisqu'elle a été ratifiée par 45 pays, vise à imposer un niveau minimal d'uniformité dans le domaine de la protection des données pour qu'ensuite, chaque pays puisse constituer ses propres orientations en matière de protection de données.

La deuxième grande période de la protection est marquée par la tentative, dans plusieurs pays européens dans les années 1980, de mise en place d'une réglementation des catégories plus spécifiques de données personnelles, telles que celles possédées par la police. Quoi qu'il en soit, chaque pays a fini par légiférer en la matière, si bien que dans les années 1990, tous les pays européens disposaient de systèmes différents de réglementation.

Enfin, la troisième phase est celle de l'harmonisation des lois des différents Etats membres de l'UE, initiée en octobre 1998, concomitamment à l'échéance du délai imparti pour la transposition de la Directive européenne 95/96. Si elle demeure satisfaisante en ce qui concerne ses objectifs et ses principes, la Directive 95/46/CE n'a pas permis d'éviter une fragmentation de la mise en œuvre de la protection des données à caractère personnel dans l'Union, une insécurité juridique et le sentiment, largement répandu dans le public, que des risques importants subsistent, notamment dans l'environnement en ligne. Il est donc apparu nécessaire d'assurer la cohérence et un degré élevé de protection des personnes, mais aussi de lever les obstacles à la circulation des données à caractère personnel, le niveau de protection des droits et des libertés des personnes à l'égard du traitement de ces données devant alors être équivalent dans tous les Etats membres. Il convient dès lors d'assurer une application cohérente et homogène des règles de protection des libertés et droits fondamentaux des personnes physiques à l'égard du traitement des données à caractère personnel dans l'ensemble de l'Union.

L'article 16, paragraphe 1, du Traité sur le fonctionnement de l'Union européenne (N° Lexbase : L2462IPU TFUE), introduit par le Traité de Lisbonne, établit le principe selon lequel toute personne a droit à la protection des données à caractère personnel la concernant. En outre, avec l'article 16, paragraphe 2, du TFUE, le Traité de Lisbonne a créé une base juridique spécifique pour l'adoption de règles en matière de protection des données à caractère personnel. Par ailleurs, l'article 8 de la Charte des droits fondamentaux de l'Union européenne (N° Lexbase : L8117ANX) consacre la protection des données à caractère personnel en tant que droit fondamental.

La proposition de Règlement est donc fondée sur l'article 16 du TFUE, qui est la nouvelle base juridique, introduite par le Traité de Lisbonne, pour l'adoption de règles en matière de protection des données. Cette disposition permet d'adopter des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les Etats membres dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union. Elle permet également l'adoption de règles relatives à la libre circulation de ces données, y compris les données à caractère personnel traitées par les Etats membres ou des personnes privées.

La proposition de la Commission est de maintenir un système dans lequel les litiges sont jugés au niveau national. Si elle contient de nouveaux systèmes de régulation, elle souhaite donc conserver les compétences nationales. La proposition de Règlement prévoit l'introduction de la notion d'établissement principal. C'est le principe du "*main establishment*". Le principal établissement ne correspond donc pas nécessairement au lieu où se trouve le serveur mais au lieu où sont prises les principales décisions quant aux finalités, aux conditions et aux moyens du traitement de données à caractère personnel. Le projet envisage ainsi de donner une compétence exclusive à la "CNIL" du pays de l'établissement principal de l'entreprise responsable du traitement pour prendre l'ensemble des décisions applicables (y compris les contrôles et sanctions éventuelles). Ce dispositif du "guichet unique" proposé par la Commission européenne, attribue donc la compétence pour instruire les requêtes des citoyens européens à l'autorité de contrôle du pays dans lequel le responsable de traitement en cause a son principal établissement. L'objectif avoué

de ce dispositif est de faciliter les démarches administratives des entreprises qui n'auront plus qu'un interlocuteur unique à l'échelle européenne.

Jean-Paul Amoudry a indiqué, sur ce point de l'établissement principal et de la désignation de la commission de régulation de l'établissement principal, que, pour la CNIL, un tel mécanisme serait insatisfaisant car il aurait pour conséquence d'obliger les citoyens à faire valoir leurs droits dans un pays autre que celui de leur résidence, celui de l'établissement principal, leur CNIL nationale devenant une simple "boîte aux lettres". Le citoyen se verrait à la fois privé de la possibilité de voir sa demande instruite par l'autorité de contrôle qui lui est la plus proche et la plus accessible, et privé de la possibilité de se voir appliquer le cas échéant les dispositions de droit national plus favorables. De plus, les entreprises seraient incitées à choisir leur lieu d'établissement principal en fonction des contraintes locales, encourageant les risques de concurrence intra-communautaire en la matière. La CNIL a donc proposé un mode de gouvernance à la fois intégré et décentralisé : intégré, parce que les autorités de contrôle doivent pouvoir prendre conjointement des décisions à l'égard des traitements transnationaux ; décentralisée, parce que chaque CNIL doit rester compétente pour les résidents de son territoire.

Comme le relève Clarisse Girot, des cas très concrets illustrent les difficultés qui se posent en termes de gouvernance et les deux options qui sont mises sur la table. Ainsi, dans le cas Facebook, un audit a été diligenté par l'autorité de contrôle irlandaise qui a demandé aux autres autorités européennes ses commentaires sans les diffuser, et a publié seule ses conclusions selon lesquelles aucun problème de protection des données n'était identifié. Ce mécanisme est assurément insatisfaisant. Quant au cas Google, plusieurs autorités ont décidé de se saisir ensemble du dossier et de désigner la CNIL comme techniquement la mieux équipée pour faire face à cet exercice complexe. Des réunions de travail avec Google et les homologues européens de la CNIL se sont tenues conjointement. Si cette voie est plus difficile, elle est préférable car elle participe d'une logique européenne et empêche toute prime à la délocalisation intra-Union européenne qui serait préjudiciable au citoyen mais aussi à l'Union européenne.

Sur le fond la proposition de Règlement permet d'améliorer sensiblement la protection des personnes. Elle prévoit notamment que le consentement de la personne à l'utilisation de ses données personnelles devra être exprès. Elle reconnaît aux internautes un "droit à la portabilité" de leurs données, qui leur permettra de s'affranchir de l'autorité de traitement, sans perdre l'usage de leurs données. Elle réaffirme le droit d'opposition de chacun au traitement de ses données personnelles et encadre strictement la possibilité pour les responsables de traitement de soumettre les données qu'ils ont recueillies à un "profilage" informatique. Elle consacre un droit à l'oubli numérique, permettant à chacun d'obtenir l'effacement des données personnelles qui lui portent préjudice.

La proposition de Règlement contient de nouvelles règles d'autorisation des fichiers, qui reposent, notamment, pour les fichiers les plus sensibles, sur l'obligation de les soumettre à une étude d'impact. Elle modifie la règlementation relative au transfert de données vers des pays tiers à l'Union européenne.

Parallèlement, le texte fait peser sur les responsables de traitement des obligations nouvelles comme la désignation d'un délégué à la protection des données dans les entreprises de plus de 250 salariés, ou le renforcement des sanctions contre les entreprises ne respectant pas les règles fixées. La proposition de Règlement adapte aussi le système de contrôle des responsables de traitement en créant notamment un comité européen de la protection des données, auquel sera associé le Contrôleur européen de la protection des données, qui se substituera à l'actuel groupe de travail réunissant les "CNIL européennes", dit "G29".

Le projet de Règlement prévoit également l'introduction de la notion d'*accountability* qui se traduit par l'obligation faite aux responsables de traitement et aux sous-traitants de mettre en place des règles internes et des politiques transparentes en la matière et, en particulier, effectuer une analyse d'impact pour les traitements présentant des risques pour les données personnelles, avertir la personne concernée en cas de violation de ses données personnelles, désigner un délégué à la protection des données et mettre en œuvre des mesures techniques et opérationnelles afin d'assurer la sécurité des données. Ils doivent, selon le concept *accountability*, être à même de démontrer, que le traitement des données à caractère personnel est effectué dans le respect de la réglementation.

En ce qui concerne plus spécifiquement les transferts de données à caractère personnel vers des pays non membres de l'Union européenne, Clarisse Girot rappelle que la Directive 95/46/CE pose un principe général d'interdiction vers un pays tiers dont le droit applicable n'offre pas un niveau de protection "adéquat" des données personnelles, c'est-à-dire un niveau de protection équivalent à celui qui existe au sein de l'Union européenne. Pour se conformer à cette obligation, les sociétés disposent de différents instruments juridiques reconnus par la Commission européenne et par les autorités nationales de protection des données personnelles comme apportant un niveau de protection adéquat, telle que des clauses contractuelles. Toutefois, les contraintes liées à la mondialisation de l'économie, à la globalisation des échanges de données et aux développements technologiques, ont soulevé des problèmes notamment en ce qui concerne le transfert de données intra-groupe. Dans ce contexte, la Commission européenne propose d'introduire expressément le concept de règles d'entreprise contraignantes (*binding corporate*

rules) afin de faciliter le transfert de données personnelles hors de l'Union européenne. L'adoption et l'implémentation *binding corporate rules* pour encadrer les flux transfrontaliers de données est une mise en pratique du principe d'*accountability*.

Mais, la proposition de Règlement n'est pas le seul mouvement actuel et la protection des données personnelles s'inscrit dans une problématique beaucoup plus large qui doit en fait être traitée au niveau mondial. Les Etats-Unis, le Conseil de l'Europe, l'OCDE, notamment ont lancé des initiatives qu'il convient d'articuler concrètement.

– **Conclusion par Madame le Bâtonnier, Christiane Féral-Schuhl**

Les données personnelles sont un vrai sujet qui préoccupe tous les pays. Pour les avocats, cette thématique présente d'abord des défis et des opportunités qui peuvent être regroupés en quatre grands axes :

- une future réglementation beaucoup plus lisible juridiquement, ce qui est un prérequis pour l'avocat, lorsqu'il conseille ses clients ;

- le nouveau cadre juridique renforce le pouvoir de contrôle et de sanctions des autorités nationales et l'avocat pourra y jouer tout son rôle ;

- ce nouveau cadre fait émerger la notion de l'*accountability*, puisque l'application des règles doit être prouvée, démontrée, tracée et l'avocat a toute sa place dans la production de la preuve ;

- le maintien du correspondant informatique et liberté qui permet à l'avocat d'être au cœur de l'entreprise.

Mais les données personnelles soulèvent également des difficultés :

- la lisibilité de l'application réelle des mécanismes prévus par le texte ;

- l'interaction du droit européen avec les droits nationaux ;

- le risque d'amoindrissement des droits et libertés, au profit de l'harmonisation.

Les données personnelles sont au cœur de la discipline des avocats et de la protection des libertés individuelles.