A/s : Compte-rendu de l'atelier de réflexion Conventions « Quel droit pour les données personnelles à l'ère des méga-données? »

Conventions a organisé un atelier de réflexion consacré au droit d'auteur face au défi des pratiques numériques. Y ont participé :
- Pierre TRUDEL, Professeur à l'Université de Montréal, Titulaire de la Chaire L.R.Wilson sur le droit des technologies de l'information et du commerce électronique
- Jacky RICHARD, Président adjoint et rapporteur général de la section du rapport et des études du Conseil d'État
- Me. Laurent CARON, Avocat au barreau de Paris, expert au sein du comité technologies du Conseil des Barreaux européens
- Me. Bertrand WARUSFEL, Professeur à l'Université de Lille, Chercheur associé à l'IHEJ

L'Union européenne est aujourd'hui à la pointe du combat en faveur d'une protection exigeante et effective de la vie privée des individus. Précurseur en matière de protection du droit fondamental au respect de la vie privée (article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, Directive 95/46, Convention 108 du Conseil de l'Europe), elle doit le rester et œuvrer pour la promotion de ce droit dans un contexte marqué par l'omniprésence de l'écosystème numérique américain et les révélations sur le programme PRISM. L'enjeu est de taille pour l'Europe dès lors qu'elle doit démontrer qu'elle est capable de s'adapter aux nouvelles réalités du numérique - de l'internet aux réseaux sociaux, en passant par l'informatique en nuage ou le Big Data - tout en préservant un haut niveau de protection de ce droit fondamental. L'Europe doit en effet montrer que sur un sujet qui suscite une mobilisation croissante des citoyens, elle est capable d'innover et de construire une gouvernance crédible et légitime des données personnelles en tirant le meilleur profit des approches juridiques latines et anglo-saxonnes et faisant de la protection des données un avantage pour les entreprises, un nouvel espace de droit pour les individus et une opportunité de renforcer l'intégration européenne.

La question fondamentale reste donc celle de l'équilibre à établir entre les attentes des individus, les objectifs des politiques publiques, et ceux des entreprises qui veulent valoriser le potentiel de l'économie numérique qui repose fortement sur le traitement et l'exploitation des données, véritable « carburant » de cette industrie. A l'aune de l'émergence de nouveaux services tels que l'informatique en nuage ou le traitement massif de données, mais aussi des attentes et des inquiétudes que ces évolutions suscitent, et enfin de l'interdépendance croissante en termes de sécurité et d'infrastructures de nos économies, les enjeux générés par la révision du cadre européen en matière de protection des données personnelles sont stratégiques. Cette adaptation du cadre communautaire constitue un objectif d'autant plus délicat que d'autres pays ou régions du monde mènent des réflexions comparables, qu'il s'agisse du « Bill of Rights » de la protection des données personnelles publié par la Maison blanche en février 2012 adossé à l'argumentaire du gouvernement américain en faveur d'un « internet libre, ouvert et sans entraves » – quelque peu mis à mal par les révélations d'Edward Snowden - ou des travaux de l'APEC sur les transferts internationaux de données dans la zone Asie-pacifique. La difficulté sera bien sûr d'aboutir à un niveau élevé de protection, tout en garantissant l'interopérabilité des différents systèmes normatifs entre eux.

La gouvernance qui sera instaurée au niveau européen en matière de protection des données personnelles sera appelée à servir de modèle, et à constituer une référence de la protection de la vie privée au niveau international. La gouvernance en matière de vie privée à travers le monde s'est en effet structurée autour de deux modèles concurrents: l'Europe a rendu inaliénables certains droits individuels et confié des responsabilités aux organismes de protection des données, tandis qu'aux Etats-Unis, les entreprises ont ajouté des clauses de renonciation dans leurs contrats définissant les modalités et les conditions d'utilisation de leurs services, ce qui leur a permis d'exploiter les données de manière exhaustive. Par conséquent l'Europe doit sortir plus forte, plus intégrée, mieux armée suite à cette mise à jour du cadre réglementaire européen pour faire face à la mondialisation des transferts de données, sans renoncer pour autant à ses principes et à ses valeurs, dont le citoyen est le centre de gravité. A cet égard, le projet de règlement proposé par la Commission européenne en 2012 traduit un nouvel équilibre des droits, obligations et sanctions applicables.

1) La consécration du droit à la protection des données à caractère personnel en tant que droit fondamental : quel avenir pour le modèle européen ?

L'ancrage du principe de protection des données à caractère personnel dans la sphère des libertés publiques et droits fondamentaux est présent dans la Directive 95/46, laquelle se réfère à l'article 8 de la Convention européenne des droits de l'homme. Si les grands principes fondateurs de la protection des données à caractère personnel restent pertinents, leur mise en œuvre effective semble néanmoins poser problème dans un écosystème numérique reposant de plus en plus sur l'exploitation intensive des données. Face aux différentes évolutions technologiques se pose la question fondamentale de la capacité de la réglementation européenne à composer avec les nouveaux défis posés par une société de l'information en constante mutation alors que certains concepts devraient être revisités afin de permettre une protection effective des personnes contre les atteintes à leurs droits et libertés. Le besoin de réforme au niveau européen est donc né de la nécessité d'adapter la réglementation existante à la protection de la vie privée dans un monde en réseau et de l'insuffisance d'harmonisation des cadres nationaux.

Les nouvelles modalités de circulation de l'information donnent naissance à une architecture « réseautique », interconnectée, nécessitant des rapports de dialogue approfondis. Deux phénomènes ont changé la donne: (i) l'automatisation du traitement des données à caractère personnel relativise et minimise *de facto* l'exigence de consentement éclairé, lequel est d'autant plus formel ou entravé que les conditions d'utilisation de ces données sont présentées d'une manière inintelligible ou subreptice ; (ii) la massification des données (« Big data ») et le développement corrélatif des techniques d'agrégation et de profilage affaiblissent les principes garantissant la qualité des données. Or, en Europe, ces dernières doivent, comme le prévoit l'article 6 de la directive du 24 octobre 1995, être traitées d'une manière loyale, être collectées pour des finalités déterminées, de manière proportionnée et pour une durée limitée, mais aussi être exactes, complètes et mises à jour.

Dans un contexte marqué par une monétisation et une exploitation de plus en plus poussée des données (cf. la sophistication croissante des algorithmes prédictifs de Google, Amazon ou de Netfix), la question de leur statut cristallise différents antagonismes culturels, politiques et juridiques. Force est de reconnaitre que les Etats-Unis et l'Europe ont une conception assez opposée de la protection des données à caractère personnel : si l'Europe articule des principes de protection de la personne et de libre circulation ; les Etats-Unis favorisent plutôt les libertés du commerce ainsi que la liberté d'expression. De manière schématique, ce clivage opposerait ainsi une conception philosophique « personnaliste » mobilisant la bannière des droits fondamentaux à une conception plus pragmatique et économique. Ainsi, pour les anglo-saxons, le régime européen de la protection des données personnelles serait devenu obsolète, les principes de finalité et de proportionnalité étant inapplicables à l'univers du Big data. Seule l'autorégulation pensée et mise en œuvre par les acteurs économiques – fondée sur une approche reposant sur une analyse des risques - complétée par l'intervention *ex post* de tribunaux chargés de veiller à la défense des libertés individuelles, permettrait ainsi de préserver l'innovation et le dynamisme de l'économie numérique. L'Union européenne, de son côté, peine à articuler sa philosophie dans ce domaine, partagée entre le souhait de voir se développer un marché unique du numérique et la préservation d'un socle de droits fondamentaux dans lequel la vie privée figure à la première place. Cette divergence d'approche met donc en lumière l'importance et les enjeux de la protection des données dans l'environnement économique, juridique et numérique actuel. Par conséquent, comment éviter les dérives de la « prédictivité sytématique » (tant en matière de santé, que de comportement social ou de marketing) sans brider l'innovation? Cela impose-t-il une redéfinition des quatre principes cardinaux sur lesquels repose le régime juridique de la protection des données personnelles, à savoir le principe de finalité, de proportionnalité, de sécurité, et le droit pour tout individu de consentir ou de s'opposer à leur collecte, d'y accéder et d'en obtenir rectification ? Les mécanismes actuels d'articulation entre les points de vue divergents des États-Unis et de l'Union européenne (safe harbor, corporate binding rules, …) doivent-ils être revus en conséquence ?

L'approche anglo-saxonne - fondée sur la responsabilisation des acteurs (« accountability »), plus que sur l'encadrement de la collecte, du traitement et de l'exploitation des données - a le mérite de la flexibilité, d'autant qu'il n'existe pas – outre des dispositions sectorielles – de législation « généraliste » sur la protection des données à caractère personnel aux Etats-Unis. Les enjeux juridiques ne se conçoivent alors plus en termes de mise en conformité avec une mosaïque de dispositifs nationaux mais en termes d'examen des risques pouvant découler des traitements inhérents aux pratiques analytiques considérées (Big Data, Cloud computing, etc.). Ainsi, pour cerner

effectivement les enjeux posés par ce genre de traitement massif d'information et assurer une réelle protection des droits fondamentaux, il s'agit tout d'abord d'identifier les « gisements d'information » concernés et d'examiner ensuite quels sont les traitements d'information qui sont effectués. Il devient alors possible d'identifier les risques que peuvent comporter certaines activités d'analyse. Selon cette approche, les fondements du cadre européen deviennent obsolètes dans ce nouvel environnement technologique caractérisé par la massification des flux de données :

- « rigidification » du principe de finalité de la collecte de données imposant l'utilisation des renseignements à des fins limitées ou uniquement aux fins pour lesquelles ils ont été recueillis à l'origine ;
- manque d'efficience de la règle imposant la collecte du minimum de renseignements personnels et de l'obligation d'éliminer les renseignements une fois que l'objectif de leur collecte a été atteint ;
- « mythologie » du consentement lié à la difficulté d'obtenir un accord explicite des personnes ;
- difficulté d'envisager concrètement un véritable droit à l'oubli, etc.

Ces exigences, mises en place préalablement à la généralisation de ces technologies, seraient, dans une certaine mesure, susceptibles d'engendrer des effets pervers tels que la « sur-collecte » de données. Or, les ressources consacrées à ces collectes redondantes seraient mieux investies dans la sécurisation des données déjà disponibles.

Les possibilités ouvertes par les nouvelles modalités de traitement massif supposerait donc de penser la protection de la vie privée autrement qu'en limitant l'accès aux données. Les cadres règlementaires sur la protection des données à caractère personnel devraient être revus en fonction des dynamiques associées aux façons actuelles de traiter des informations. L'avènement et la généralisation des traitements massifs de données requiert donc un cadre juridique garantissant que les informations soient traitées de façon loyale et que les risques soient effectivement identifiés et efficacement pris en charge. Reste que l'approche anglo-saxonne repose sur le concept de « privacy » qui se distingue de l'approche européenne fondée sur le caractère personnel de la donnée et de la légitimité du traitement. Ainsi, le concept de « privacy » induit de contextualiser l'information se rattachant à la personne sans avoir, comme dans l'approche européenne, à définir une catégorie de donnée spécifique. Il est dès lors concevable d'envisager des clauses de renonciation à la protection offerte par la notion de « privacy » dans les contrats définissant les modalités et les conditions d'utilisation des services numériques proposés par des opérateurs régis par des codes de conduite. Cette approche n'est plus valable dès lors que l'on envisage la notion « personnaliste » européenne liée à l'existence d'un droit fondamental et à la dignité de la personne. Le défi consiste à tenter de concilier ces deux approches afin de garantir, dans ce nouveau contexte technologique, l'imputabilité des pratiques à ceux qui collectent, conservent et exploitent effectivement ces données, notamment en cas de sous-traitance, tout en définissant des garanties solides pour les individus qui ne soient pas que formelles.

2) Vers un nouvel équilibre des droits et obligations en matière de protection des données à caractère personnel fondé sur « l' autodétermination informationnelle » des individus ?

La question de la protection des données personnelles se pose aujourd'hui avec une urgence nouvelle du fait d'un contexte législatif et règlementaire marqué par l'adoption promise d'un « paquet législatif » européen. La question est également très sensible du côté des opinions publiques dans un contexte post-PRISM avec la prise de conscience des risques de surveillance généralisée, mais aussi des gouvernements mobilisés dans la lutte contre le terrorisme international, et enfin, pour les acteurs économiques européens, inquiets des risques qu'il y aurait à brider l'innovation et entraver le développement de l'économie numérique en Europe, aujourd'hui en retard sur celui des grands champions américains. Par conséquent, il s'agit de s'interroger sur les enjeux essentiels de la refondation d'un droit des données personnelles, ou d'un droit adapté aux nouveaux usages culturels, sociaux et économiques de ces données, qui leur donnent une importance et une valeur accrue. En effet, la première loi Informatique et Libertés de 1978 – visant à prémunir le citoyen contre les violations des droits et libertés perpétrées par l'Etat (cf. en France l'affaire « Safari » qui révélait en 1974 un projet gouvernemental visant à interconnecter les bases de données du secteur public à partir du numéro de sécurité social) - comme la directive européenne « relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données » de 1995, datent d'avant la seconde révolution numérique qui s'opère aujourd'hui.

La Commission européenne a rendu public, le 25 janvier 2012, un projet de règlement relatif à la protection des données à caractère personnel, qui refond l'ensemble du cadre juridique européen

issu de la directive de 1995. L'ambition est de concilier deux objectifs qui peuvent paraître parfois contradictoire : (i) sur le versant économique, faciliter les flux transfrontières de données afin d'encourager le développement de « champions » numérique au sein du marché intérieur ; (ii) sur le volet protection des données personnelles, ne pas fragiliser les droits fondamentaux des citoyens de l'UE. Il est donc proposé de mettre en place une autre gouvernance, tirant le meilleur des approches juridiques latines et anglo-saxonnes et faisant de la protection des données personnelles un avantage pour les entreprises, un nouvel espace de droit pour le citoyen et une opportunité de renforcer l'intégration européenne. Le règlement opère, en effet, un changement de paradigme dans la régulation des données personnelles, non sur les principes eux-mêmes mais sur les outils de régulation mis à disposition des acteurs et des régulateurs. Le système actuel est en effet marqué par l'importance des formalités préalables, notamment dans le cadre du régime des « déclarations » de traitements automatisés auprès des autorités de contrôle nationales. Ces formalités sont contrôlées *a priori* par le régulateur. Concrètement, une fois les formalités préalables effectuées, le principal moyen de s'assurer de la conformité effective d'un dispositif est le mécanisme de contrôle *a posteriori* susceptible de déboucher sur une mesure coercitive comme une mise en demeure, voire une sanction. En réponse à cette logique forte mais quelque peu binaire, le projet de règlement propose une vision nouvelle qui consiste à atténuer considérablement le poids des formalités préalables, à renforcer les pouvoirs de contrôle et de sanction et, entre les deux, à construire un nouveau cadre de responsabilisation des acteurs, fondé sur la notion d'*accountability*. L'idée est simple : face à l'explosion des données personnelles, il faut que les responsables de traitements intègrent dans leurs pratiques mêmes les principes « informatique et libertés » car la seule politique de sanction ou de formalités préalables ne saurait tout encadrer. La mise en place de politiques internes de conformité mobilisant un certain nombre d'outils prévus par le règlement est donc un nouvel objectif des régulateurs. La proposition de Règlement vise ainsi à établir un nouvel équilibre entre le renforcement des droits des personnes (principe du consentement explicite, droit à l'oubli, droit à la portabilité des données) et la simplification des formalités pour les entreprises (suppression de la déclaration préalable des traitements, guichet unique…).

La protection des données personnelles est un droit à part entière, qui se trouve à la croisée d'autres droits fondamentaux, notamment le droit de propriété, le droit au respect de la vie privée et la liberté d'expression. Elle interagit également avec des principes économiques et commerciaux, en particulier dans le domaine de la protection du consommateur et de règles publicitaires. Elle influe aussi sur l'organisation des entreprises. C'est précisément cette situation centrale dans l'exercice des libertés et essentielle en matière économique, notamment pour l'économie numérique, qui est la cause des attentes, mais aussi des inquiétudes profondes des citoyens. Il est parfois proposé de reconnaître aux individus un véritable droit de propriété sur leurs données, en pariant sur leur plus grande implication du fait qu'ils deviendraient financièrement intéressés à une bonne gestion de leurs données. Néanmoins, la reconnaissance du droit de propriété ne permettrait pas de rééquilibrer la relation entre les individus et les acteurs économiques et compliquerait l'exercice de la régulation par les pouvoirs publics.

Le droit à « l'autodétermination informationnelle », concept dégagé par la Cour constitutionnelle allemande en 1983, est à la différence du droit de propriété un droit attaché à la personne, tendant à garantir la capacité de l'individu à décider de la communication et de l'utilisation de ses données à caractère personnel. Ce droit ne devrait pas être défini comme un droit supplémentaire s'ajoutant aux autres droits (droit d'information, droit d'accès...), mais comme un principe donnant sens à tous ces droits. Ce droit à l'autodétermination informationnelle (« Informationnelle Selbstbestimmung ») a été consacré par la Cour constitutionnelle fédérale de l'Allemagne dans un arrêt du 15 décembre 1983, relatif à une loi sur le recensement. La Cour le déduit des articles 1er (dignité de l'homme) et 2 (droit au libre développement de sa personnalité) de la Loi fondamentale. Alors que le droit à la protection des données peut-être perçu comme un concept défensif, le droit à l'autodétermination lui donne un contenu positif. Il ne s'agit plus seulement de protéger le droit au respect de la vie privée mais d'affirmer la primauté de la personne qui doit être en mesure d'exercer sa liberté. En ce sens, le droit à l'autodétermination répond d'avantage à l'aspiration croissante des individus à l'autonomie de décision. C'est cette aspiration que la proposition de droit de propriété sur les données essaie de saisir ; le droit à l'autodétermination y apporte une réponse à la fois plus efficace et plus conforme à la logique personnaliste et non patrimoniale qui a toujours prévalu en Europe en matière de protection des données. Là où le droit de propriété prétend faire des individus

des gestionnaires d'un patrimoine, le droit à l'autodétermination rappelle qu'ils doivent demeurer en mesure de décider de leur existence.