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

Maison du Barreau
Paris, 24 avril 2013

Giovanni BUTTARELLI
Contrôleur européen adjoint de la protection des données

La protection des données personnelles traverse une phase historique.

Dans l'agenda politique et institutionnel des pays européens des quarante dernières années, la manière dont nous avons renforcé les garanties des droits de la personnalité a évolué par étapes importantes.

Cependant, nous n'avions jamais enregistré un moment aussi délicat.

Les choix que nous effectuons aujourd'hui, cette fois principalement au niveau européen et non plus en ordre dispersé, pays par pays, auront un impact décisif et de longue durée sur la manière dont les institutions publiques, les grandes multinationales, les petites entreprises et chaque utilisateur individuel d'internet opéreront à l'ère du numérique.

Il est vrai que cette législation ne traitera, une fois encore, que d'un aspect de la société de l'information, à savoir le «traitement des données personnelles», qui n'est ni le seul ni le principal aspect.

Cependant, il est vrai aussi qu'aucune organisation publique ou privée ne peut se dispenser de collecter des informations à caractère personnel pour poursuivre ses propres objectifs.

En d’autres termes, la protection des données est «horizontale»; elle englobe quasiment toutes les activités, y compris celles des forces de police, des autorités judiciaires et des services d’espionnage.

Si nous analysons la manière dont les principes de légalité, de correction, de nécessité, de proportionnalité doivent être concrètement respectés dans ces secteurs, ou si nous débattons sur la manière de garantir réellement le droit à l’oubli sur l’internet, de concilier le droit à l’information et à la transparence avec le droit à la protection de la vie privée, nous nous rendons compte que la protection des données est une question omniprésente. Nous la retrouvons dans de nombreuses autres réglementations de secteur; elle nous oblige à repenser la manière dont l’administration publique ou une entreprise doivent se conformer à ces réglementations sectorielles qui ne tiennent, peut-être, nullement compte des aspects liés à la protection des données.

Ainsi, la protection des données, qui est d’ailleurs née en relation avec la protection des droits et libertés fondamentaux et spécialement ceux relatifs à la personnalité, devient partie intégrante et parfois prépondérante des règles et des pratiques de bonne administration, en influençant de manière décisive toutes les activités dites de *core business*. Elle influence également votre activité, en qualité de juristes, défenseurs, consultants, acteurs des procédures civiles, pénales, commerciales et du droit de la famille, dont l’exercice requiert la collecte de très nombreuses informations à caractère personnel ou très sensibles, parfois impérativement, parfois de manière incorrecte ou intrusive.

Comment, de quelle manière, jusqu’à quel point et pour quelle durée est-il possible de collecter légalement des données personnelles aux fins d’une meilleure défense d’un droit devant les tribunaux? Selon quelles précautions ces informations doivent-elles être conservées et diffusées par l’avocat, l’enquêteur privé, le ministère public, le juge?

Parfois le droit primaire ou secondaire au niveau national parvient à fournir des réponses précises à ces questions.

À titre d’exemple, étant donné que ce soir nous devrions également comparer les systèmes italien et français de protection des données, c’est avec fierté que je vous informe que mon pays est probablement le seul dans lequel les avocats

civilistes et pénalistes et les enquêteurs privés peuvent bénéficier d'indications raisonnables et spécifiques sur la manière de trouver un équilibre entre une activité de défense efficace et la protection des données des tiers en ce qui concerne la collecte, la production des éléments de preuve devant les tribunaux et leur conservation, et ce, au moyen d'un instrument souple tel que le code de déontologie promu par l'autorité compétente (votre Cnil) sur impulsion législative, lequel revêt, toujours sur base législative, une valeur contraignante à leur égard.

Cependant la législation nationale ne fournit pas toujours des réponses concrètes. Ainsi, parfois, vous devez trouver vous-même les réponses aux demandes de certitude formulées par les opérateurs, vous qui êtes appelés à appliquer dans votre activité des principes de protection des données qui sont, peut-être, de caractère général et n'indiquent pas les bonnes pratiques que vous attendez.

Cependant revenons à mon affirmation introductive. Pourquoi sommes-nous dans une phase historique, pourquoi parle-t-on du moment de vérité pour la protection des données?

La réponse devient plus simple si l'on remonte rétrospectivement aux origines de cette matière, qui a connu plusieurs générations de règles.

Dans les années 1970, les premières expériences, pionnières en ce domaine (par exemple, en Suède ou en Allemagne au niveau des Landers), se basaient essentiellement sur des mécanismes d'interdiction, d'autorisation préalable au traitement des données personnelles, de «recensement» public des banques de données automatisées qui, à l'époque, était principalement de grande taille et détenues par quelques personnes dont on se méfiait. On craignait en effet la naissance des grands ordinateurs, leur capacité d'emmagasiner des informations et de les traiter, en parvenant à des résultats inimaginables en utilisant uniquement des supports papier. Les flux de données vers l'étranger n'étaient autorisés que vers des pays, également européens, qui garantissaient une protection des données «équivalente».

La première loi allemande de 1977 et votre loi de 1978 ont constitué une élaboration plus évoluée des premières expériences. Toutefois, même au cours de cette phase, on a continué de prévoir des mécanismes qui, aujourd'hui, semblent dépassés, tels que la notification préalable des traitements de données à une

autorité publique. L'idée est de permettre à une autorité indépendante de procéder à un examen préliminaire, de sorte qu'il soit presque possible de contrôler au préalable les principales activités de traitement de données.

Au cours des années suivantes, on a cherché aussi au niveau international de donner une première dimension homogène à la matière, tant au moyen de la Convention du Conseil de l'Europe de 1981 (qui reste aujourd'hui encore un modèle valable en raison de sa souplesse et de sa neutralité technologique, ce qui a facilité sa ratification par 45 pays) que par les lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontaliers de données.

À partir des années 1980, une deuxième génération de lois est apparue dans plusieurs pays européens. Le besoin d'indications plus spécifiques sur la manière de réglementer certaines catégories de données personnelles (telles que celles sur la santé, ou les données traitées par les forces de police par exemple) se faisait sentir.

Durant cette phase, l'expérience acquise au cours des années précédentes conduit à une approche plus réaliste et sélective (par exemple, à travers des notifications simplifiées à l'égard de l'autorité de contrôle), notamment parce que les systèmes d'information ne sont plus concentrés dans les mains de quelques organisations, mais sont basés sur des ordinateurs de petite/moyenne taille utilisés par une palette bien plus large de personnes. Chaque pays a cependant suivi son propre chemin. En substance, jusqu'à la deuxième moitié des années 1990, l'Europe présentait un cadre très diversifié, avec des systèmes réglementaires très différents selon les pays, systèmes qui conditionnaient la libre circulation des marchandises, des personnes, des services, des capitaux et des professions (rappelons-nous le fameux cas d'école «Fiat S.p.A», dans lequel la succursale française ne pouvait initialement envoyer des données à la maison mère italienne, en raison de l'absence de loi sur la protection des données en Italie. L'affaire a été résolue sur la base de clauses contractuelles qui sont aujourd'hui largement utilisées dans la pratique des flux transfrontaliers).

Je voudrais évoquer enfin une troisième phase dont le début peut être situé au moment de l'expiration, en octobre 1998, du délai de transposition de la directive européenne n° 95/46, qui a marqué le début d'un parcours très lent pour tenter

d’obtenir un premier niveau d’harmonisation entre les lois des différents pays de la Communauté européenne.

Sur la base de la directive européenne de 1995 et de la première directive-fille sur les télécommunications de 1997 (97/66/CE), tous les pays européens se sont dotés d’une loi plus organique en la matière, ainsi que de certaines lois sectorielles et de règles secondaires et ont tenté de relever les premiers défis de la biométrie et de la génétique, de l´*e-government* (l’administration en ligne), de l’évolution technologique, et ceux d’un monde dans lequel nous subissons progressivement et de plus en plus l’*ubiquitous computing* (informatique ubiquitaire), dans lequel nous sommes connectés mais aussi surveillés en ligne, où nous interagissons sur les réseaux sociaux mais auxquels nous sommes aussi soumis.

Dans cette nouvelle phase, le monde des premiers ordinateurs de grande taille ou des grands systèmes reliés à différents serveurs-clients, des petits réseaux individuels a disparu: les ressources informatiques, l’éducation technologique et la navigation à risque sur l’internet, bien que la fracture numérique reste encore une réalité pour trop de minorités, sont notre pain quotidien, surtout pour des nouvelles générations. Les informations ne sont plus emmagasinées dans de grands «conteneurs» dont le législateur doit régir l’utilisation et auxquels quelques privilégiés ont accès, mais ces informations naissent, sont partagées par un nombre infini de personnes puis deviennent dépassées, en temps réel.

En même temps, les goûts, les préférences et les habitudes de millions d’utilisateurs d’internet font de plus en plus l’objet de surveillance et cela de manière peu transparente.

Nous qualifions les données de «personnelles» parce qu’elles nous appartiennent. Elles sont une projection de notre personne; nous devrions pouvoir nous même définir, à tout le moins dans certaines hypothèses, quelles personnes peuvent les utiliser et dans quel but. Nous devrions pouvoir être en mesure d’identifier facilement tous ceux qui les utilisent et pouvoir exercer de fait nos droits si ceux-ci sont violés.

Et pourtant, les utilisateurs d’internet font l’objet de «profilages» intensifs et renouvelés sur l’internet de la part d’autres personnes qui, même si elles

n’utilisent pas directement nos noms et prénoms, suivent attentivement nos comportements en analysant nos traces et les «bouts» de notre identité que nous laissons sur le réseau (l’adresse IP, par exemple). Nous sommes sectionnés, classés et catalogués en temps réel de mille façons que nous ignorons. Plus les données que nous laissons en ligne sont récentes et analytiques, plus grande est leur valeur commerciale. On nous demande continuellement de fournir des informations afin de faciliter la navigation en ligne, mais en réalité nous faisons l’objet d’un grand commerce sans que nous nous en rendions compte. Des personnes que nous ne connaissons pas forcément créent nos identités, plus d’une, qui peut-être ne correspondent nullement à notre façon d’être, même si elles ont été élaborées par un ordinateur sophistiqué.

Vous devez vous demander pourquoi j’ai effectué ce long *escursus* historique. Je pense qu’il peut vous être utile pour comprendre les éléments important à protéger à l’ère du numérique et quels sont les choix que le législateur européen doit faire aujourd’hui.

Certainement la société du futur réduira de plus en plus les plages de notre vie privée. À certains égards, il est raisonnable que cela se produise, spécialement si nous prétendons gérer toute notre vie privée à travers une *tablette* ou un *smartphone,* en lisant un journal en ligne, en nous connectant à notre banque, en demandant et en obtenant des certificats administratifs, des réservations aériennes et des prises de rendez-vous médicales, en socialisant avec tant d’autres personnes sur des blogs, en utilisant des systèmes d’appels gratuits et des réseaux sociaux.

La solution ne consiste donc pas à réduire les flux de circulation des informations dont le développement est désormais inéluctablement au niveau global, sur l’ensemble de la planète.

La réduction de nos plages de vie privée sera de plus en plus inévitable dans un monde dans lequel, à côté des caméras, des satellites et des systèmes GPS, nous utilisons pour économiser et pour des exigences d’ordre écologique, des calculateurs dits «intelligents» (qui mesurent de manière analytique notre consommation domestique), ou des automobiles «intelligentes» (qui nous informent de tout ce qui nous entoure: risques, circulation, vols et accidents, mais suivent de manière analytique nos déplacements).

De plus, nos démocraties fragiles continuent d'être exposées à des risques en matière de sécurité, de petite et grande criminalités. L'efficacité des forces de police, des services de sécurité et de la magistrature se base encore une fois sur l'obtention d'informations fiables en temps réel. Vie privée et sécurité ne sont pas incompatibles, mais il est incontestable que les grandes bases de données et les contrôles aux frontières posent plusieurs défis.

Nous payons donc un prix pour tout cela, en termes de droits des personnes et de liberté de circulation, laquelle signifie, dans notre vision moderne, non seulement la liberté de se déplacer physiquement, mais aussi la liberté de mouvement physique et en ligne sans devoir laisser une quantité déraisonnable de traces de nos déplacements.

Ce prix doit être compensé par un renforcement considérable de nos possibilités de contrôler les flux de données qui nous concernent, en sachant, surtout, quelles sont les personnes qui détiennent des informations sur notre compte et à quelles fins. Être informés signifie pouvoir effectuer librement des choix surtout lorsque nous devons décider en toute connaissance de cause de renoncer à des plages importantes de notre vie privée.

C'est pour toutes ces raisons que plus de trente ans après l'adoption de la Convention de Strasbourg et presque vingt ans après l'entrée en vigueur de la première directive européenne, nous voulons faire un pas en avant afin de disposer de règles modernes plus harmonisées, ambitieuses et orientées vers l'avenir.

Les changements ne concernent pas seulement les technologies, qui sont d'ailleurs en évolution constante et que nous ne pouvons suivre avec des règles détaillées.

Le traité de Lisbonne a changé l'architecture des droits en Europe.

La charte des droits fondamentaux de l'Union reconnaît solennellement le droit fondamental à la protection des données, spécifique et faisant l'objet d'une disposition autonome en ce qui concerne la vie privée. Qu'est-ce que cela signifie?

Cela signifie que la manière dont une personne de droit public ou de droit privé gère nos informations, garantit la transparence, met en œuvre des mesures de

sécurité, identifie ses responsabilités internes et celles de ses collaborateurs externes en offrant par exemple un service de *cloud computing* (l'informatique en nuage), conserve les informations pendant un délai justifié, etc., fait l'objet d'un droit qui nous appartient, qui est classé par la charte en tant que droit fondamental.

Ce droit existe indépendamment du fait que la violation de l'ensemble de ces règles sur le traitement des données personnelles nous crée éventuellement aussi un préjudice moral ou patrimonial. Ce droit fondamental peut-être revendiqué devant un juge indépendamment de la circonstance qu'il existe d'autres dispositions au degré de détail qui en établissent les caractéristiques, ou du fait que le traitement des données comporte également une interférence injustifiée dans la sphère de notre vie privée.

En d'autres termes, le respect des règles du jeu en matière de légalité et de correction dans le traitement des données fait partie intrinsèquement de nos droits même lorsque nous ne subissons aucun préjudice concret.

C'est pourquoi l'attention se déplacera de plus en plus d'une dimension de protection statique du droit (selon laquelle on se borne à ne demander que bureaucratiquement à la personne concernée l'autorisation préalable au traitement des données) à une dimension de protection dynamique qui garantit à la personne concernée un contrôle effectif, même si parfois a posteriori, sur la manière dont ses données sont traitées.

L'autorisation préalable, libre et informée ne disparaîtra pas, surtout en ce qui concerne la surveillance et le «profilage» en ligne, mais n'aura pas toujours l'importance centrale qu'elle avait dans les lois de première génération.

Les traités relatifs à l'Union européenne et sur son fonctionnement indiquent clairement qu'une intervention au moyen de règles européennes uniformes en cette matière est aujourd'hui non seulement une faculté, mais aussi une obligation pour l'Union. Les traités reprennent, bien qu'implicitement, la jurisprudence de la Cour européenne des droits de l'homme sur l'article 8 de la Convention européenne des droits de l'homme, selon laquelle les pays adhérents à la Convention ont des obligations tant «négatives» (en ce sens que les États ne doivent pas interférer de manière disproportionnée dans la vie privée des personnes), que «positives» (en ce sens que les États doivent se mobiliser pour

introduire les mesures nécessaires, y compris de nature réglementaire, pour garantir un niveau raisonnable de vie privée aux personnes et interdire à d'autres personnes de droit public et privé d'interférer de manière illégale dans la sphère privée des personnes).

Le monde entier (pas seulement les États-Unis d'Amérique où l'administration américaine tente de soumettre au congrès un «Bill of Rights» susceptible de favoriser une interopérabilité de principes au niveau international) observe actuellement avec une extrême attention le débat en cours au Parlement européen et au Conseil européen sur le paquet présenté par la Commission européenne en janvier de l'année dernière, qui s'articule autour d'une proposition de réglementation horizontale et une proposition de directive pour les activités de police et de justice.

Les règles que nous serons en mesure d'introduire et qui devraient être applicables vers 2016, devront tenter de dépasser le cadre fragmenté résultant des 27 lois en vigueur dans les pays de l'Union. Nous devrons tenter de prendre le meilleur de ce qui existe dans certains pays et mettre fin aux expériences moins positives. Nous devrions tenter de préserver les spécificités culturelles qui existent dans certains pays, et nous efforcer surtout de prendre en considération le point de vue du citoyen, agir de manière telle que, même si les traitements de données sont de plus en plus globalisés au niveau mondial, la protection de ses droits continue à constituer pour l'autorité nationale de contrôle un point de référence important.

Le moment n'est pas venu de réinventer la protection des données. Nous devons rendre plus effectifs ses principes et les compléter avec de nouveaux principes adaptés à l'ère numérique, tels que le *privacy by design* (prise en compte du respect de la vie privée dès la conception), *privacy by default* (protection par défaut de la vie privée) et l'a*ccountability* (gestion des responsabilités). Nous avons besoin de règles technologiquement neutres, capables de résister à une rapide obsolescence, au moins jusqu'en 2025.