Conférence internationale des commissaires à la protection des données : Madrid – novembre 2009 Internet – *QUO VADIS* ?

Yves Poullet

1. La vie privée n'est pas une liberté parmi d'autres. Elle est la condition de toutes les autres libertés. Dans l'affaire Pretty jugée en 2002, la Cour européenne des droits de l'Homme soulignait en effet que le « droit » à la vie privée s'entend au-delà de garanties solides répondant à notre revendication à l'intimité comme la reconnaissance des conditions nécessaires à l'épanouissement des libertés de chacun et au respect de sa dignité, valeur essentielle pour nos démocraties.

Que devient et que devrait signifier ce droit à l'heure d'une société de l'information et de technologies de plus en plus ubiquitaires entourant voire conditionnant chaque moment de notre vie ?

Notre propos n'est pas de rappeler une fois de plus les capacités aux limites sans cesse reculées de nos systèmes d'information tous convergents et interopérables au sein d'un Internet devenu global, ni d'évoquer leur puissance de stockage, de calcul et de transmission de l'information. Notre propos n'est pas non plus de noter la miniaturisation des terminaux devenus omniprésents (GPS, Mobilophone, RFID...) qui participent à l'intelligence ambiante. Enfin, il ne s'agit pas non plus de s'étendre sur le fait que le web 2.0, les réseaux sociaux et les You Tube, en donnant à chacun la possibilité d'être pleinement acteur sur la toile, le rendent désormais à la fois pleinement responsable et sujet de traitement.

Notre propos part d'une réflexion plus anthropologique sur ce que devient notre autodétermination au gré du développement de la toile. Certes, chacun d'entre nous trouve grâce aux TIC une opportunité d'explorer librement l'infinité des ressources informationnelles disponibles sur la toile, de communiquer avec qui bon lui semble et de s'exprimer librement. Mieux, la dimension ouverte de la société informationnelle permet de rompre avec les contrôles liés traditionnellement à l'appartenance de l'individu à des groupes sociaux qui «normalisaient» le contenu de l'information accessible. L'internaute devant

son ordinateur se sent libre de ces types de contrainte: le cyberespace est le lieu par excellence de libertés.

2. Ce constat encourageant doit cependant être assorti de bémols: nos libertés sont mises à mal par ce développement de la société de l'information. Cinq raisons sont à relever.

La première est à l'évidence le déséquilibre de plus en plus inquiétant entre ceux qui, grâce à ces technologies, détiennent une information de plus en plus considérable, et ceux qui en utilisant ces technologies, créent cette information. On sait que ce déséquilibre, source potentielle de discriminations, a été à la base de nos premières législations de protection des données, mais comment ne pas s'apercevoir que ce déséquilibre s'est accru de manière considérable quand on constate les traces de plus en plus nombreuses et qualitativement bien plus sensibles que révèle l'utilisation d'un navigateur (browser), d'un moteur de recherches, d'un GPS, d'une télévision interactive ou nos déplacements et achats dans un supermarché équipé d'un système RFID. Toujours à propos de cette omniprésence des technologies dans nos vies de tous les jours, on note que certains de nos gestes parce qu'ils sont triviaux ou parce qu'ils répondent à une sollicitation instantanée étaient traditionnellement conçus comme ne laissant pas de traces (si ce ne sont celles recueillies de manière éphémère ou non, consciemment ou non par un voisin). Or, la technologie actuelle permet de collecter ces informations, de les traiter et d'en déduire, connectées ou non à d'autres informations, des profils de personnalité permettant d'agir vis-à-vis des personnes concernées. Elle détruit donc notre «*legitimate expectation*» de vie privée dans ces moments de la vie de tous les jours. On ajoute que les capacités de nos ordinateurs abolissent le droit à l'oubli que les limites de nos cerveaux humains garantissaient.

Deuxième risque: la décontextualisation. Les données qui circulent sur la toile sont «émises» par les personnes concernées pour une finalité précise ou dans un contexte particulier. Le principe de finalité déterminée et l'interdiction de traitements incompatibles assuraient traditionnellement la nécessité de respect de ce contexte. Comment assurer aujourd'hui le respect de ces principes lorsque nous interrogeons le même moteur de recherche à la fois pour choisir la destination de voyage ou un film de cinéma, pour trouver réponse à nos problèmes de santé, pour connaître l'opinion de tel auteur, etc.? Notre référencement sur ces mêmes moteurs de recherche permet de croiser des événements de notre vie que nous espérions maintenus séparés. Notre participation à un réseau social révèle nos activités professionnelles, nos activités de vacances, notre appartenance à un club sportif et mêle sur une même plateforme tous nos centres d'intérêt et les opinions, voire images, à

leurs propos. La possibilité pour certains y compris un futur employeur, un directeur d'école ou des services de police, de prendre ainsi connaissance de ces diverses facettes de notre personnalité et de décider en fonction de cela engendre la crainte que nous soyons jugés «hors contexte».

L'opacité du fonctionnement tant des terminaux (les cookies, les RFID, les liens «transclusifs» entre sites) que des Infrastructures (voir les «agents distribués» localisés tout au long de systèmes d'information comme ceux dits d'intelligence ambiante) constitue une troisième dimension de cette société de l'information. Cette opacité entraîne la crainte de traitements non sollicités, non voulus et elle justifie, comme le soulignait le tribunal constitutionnel allemand dès 1983, notre souci de nous conformer à un comportement qui est celui que nous pensons être attendus en ces nouveaux lieux de surveillance. La normalisation des comportements dans une société de surveillance ajoutait ce tribunal, est un risque tant pour nos libertés que pour la démocratie.

De plus en plus, quatrième danger, les données collectées à propos des événements mêmes les plus insignifiants de notre vie se multiplient et les systèmes d'information nous analysent à travers ces données qui réduisent les choix et vies humains, de même que nos personnalités, à des «profils» créés à partir d'inférences statistiques aléatoires construites sur base de l'analyse d'un nombre incalculable de données. Ainsi, le contenu du panier d'achats réalisés dans une grande surface révèle le «profil» du consommateur identifié ou non et détermine la publicité ou l'action à mener vis-à-vis de la personne ainsi profilée. Pire, dans les systèmes d'intelligence ambiante où l'homme est mis en réseau avec un ensemble d'objets qui l'entourent, il devient, au sein de ce réseau, un objet communiquant parmi d'autres et la révélation de cette communication peut entraîner telle ou telle décision. L'absence de paiement d'une consommation de boisson réelle ou supposée peut conduire ainsi à la fermeture d'un sas d'entrée ou de sortie dans une discothèque pour la personne munie d'une RFID.

Enfin, on constate l'abolition de la distinction entre sphère publique et sphère privée. L'homme perdu dans la foule que ce soit celle de la rue ou celle d'une grande surface peut être suivi, tracé. Même chez lui, enfermé à double tour, à travers le GSM qu'il a en poche ou les RFID qu'il peut porter, à travers son utilisation de la TV interactive ou de son ordinateur relié à Internet, la personne est repérée, espionnée dans ses actions, voire poursuivie et ses secrets d'alcôve, percés. Or, faut-il le rappeler, la protection du domicile physique, lieu inviolable, apparaissait traditionnellement et, aux yeux du droit, comme quelque chose de fondamental pour la construction de la personnalité de l'individu.

3. À ces risques nouveaux majeurs, que répondre? La solution est sans doute à rechercher dans nos régulations traditionnelles de protection des données, mais ces dernières apparaissent insuffisantes. Sans doute est-il besoin d'une nouvelle génération de législation de protection de la vie privée. Quelques éléments de cette nouvelle « génération » nous apparaissent devoir être mis en évidence. Nous y reviendrons.

À propos de nos législations traditionnelles de protection des données, nous aimerions souligner le besoin de quelques interprétations audacieuses.

- Premièrement, il est indéniable que le concept d'« identifiabilité » devrait être élargi à ceux de traçabilité et de contactibilité, et ce, notamment, pour résoudre l'éternelle question de la nature de données à caractère personnel comme l'adresse IP, les cookies, voire la possession d'un tag muni d'une RFID. Il va de soi que les utilisations dénoncées de telles données reliées à un objet ne concernent pas la recherche du nom, du prénom ni de toutes autres caractéristiques traditionnelles de l'identité d'une personne, mais permettent de tracer voire de contacter la personne X à travers la possession de l'objet identifié, qu'il s'agisse d'une session sur le disque dur d'un internaute, le caddie sur lequel est placé la puce RFID ou le terminal auquel est liée une adresse IP.
- Deuxièmement, de la même manière que le numéro de registre national a été considéré comme une donnée sensible, non par sa nature comme le sont les données médicales ou politiques, mais à cause des risques d'interconnexion entre fichiers que ce numéro permet, il serait utile de soumettre à examen et réglementation particuliers les multiples « digital identifiers » qui permettent cette même interconnexion, ainsi à nouveau les numéros de tag RFID, les cookies, etc..
- Troisièmement, l'interdiction d'utilisation pour des finalités incompatibles doit être réaffirmée en réponse aux risques de décontextualisation déjà dénoncés.
- Quatrièmement, le souci de réaffirmer ce principe de proportionnalité se justifie au moment où les logiques de l'efficacité tant sur le plan de la rentabilité que sur le plan de la sécurité se voient renforcées grâce aux technologies de l'information et de la communication de manière incroyable. Ainsi, la sécurité publique, mais également privée des organisations et des citoyens exige toujours davantage de systèmes de contrôle, de surveillance et d'alerte. La rentabilité économique, au sens le plus large, l'efficacité tout court, viennent comme une justification complémentaire où se rejoignent les préoccupations des administrations et des organisations, d'une part, et les intérêts des consommateurs

et des citoyens, intérêts soigneusement mis en évidence par les administrations ou organisations.
En particulier, si le consentement peut à juste titre être considéré comme une des conditions nécessaires de légitimité des traitements, il ne peut comme l'affirment certaines théories néolibérales être une cause suffisante de légitimité. Ce point est important dans la mesure où la technologie crée l'illusion en tout cas d'un possible « *user empowerment* » (*Privacy settings, P3P*) où l'internaute serait lui-même apte à décider des traitements qu'il autorise. Le rejet de la doctrine du consentement comme fondement suffisant du traitement des données ne prend en compte le fait que les nécessités ou avantages liés à la vente de données peuvent être attractives pour des personnes fragiles socioéconomiquement parlant, ni la théorie des dominos qui fait que l'octroi par l'un de données personnelles entraîne les autres à donner la même information, sous peine de suspicions envers eux. Sans doute notre jugement serait moins sévère si le consentement s'appuyait sur une réelle « négociation collective » entre un site ou une plateforme et ses utilisateurs. Récemment, une plateforme de réseau social soumettait ainsi les améliorations de ses « *Terms of use* » à ses utilisateurs. Peut-être, est-ce une voie pour l'avenir qui trouve sa validité dans l'article 16 de la directive « Commerce électronique » de juin 2000 qui encourage les codes de conduite des prestataires de service de la société de l'information, mais réclame la consultation préalable de leurs utilisateurs?

- Cinquièmement, il est essentiel que les droits de la personne concernée soient réévalués et élargis : quelques exemples, meilleure information sur les privacy policies rendues obligatoires pour les entreprises présentes sur la toile ; droit d'accès électronique y compris via des identifiants non personnalisés comme les cookies ; obligation pour les responsables de traitement de construire les systèmes d'information des responsables de traitement pour satisfaire à un droit d'accès en ligne instantané, etc. Il s'agit de traduire un principe de réciprocité des avantages : dans la même mesure où les TIC favorisent la collecte et le traitement des responsables, dans la même mesure, faut-il prévoir une amélioration de la transparence de leurs traitements vis-à-vis des personnes concernées.

4. Au-delà de l'amélioration de nos réglementations traditionnelles, nous plaidons pour un élargissement de nos réglementations à de nouveaux objets. Notre autodétermination suppose en effet une maîtrise de notre environnement informationnel. Cette maîtrise n'est possible que si des réglementations

sont proposées dans des matières nouvelles: le profilage, les terminaux et l'infrastructure.

- Une régulation des terminaux et des infrastructures est proposée de manière à ce que leur fonctionnement soit «privacy compliant». Trois pistes sont proposées. Ne faut-il pas, première suggestion, rendre obligatoire la transparence de leur fonctionnement? Les terminaux opèrent de telle manière que certains traitements opérés à partir de nos terminaux restent invisibles et sans contrôle ou réelle maîtrise par les utilisateurs de ces terminaux. Il est donc important que par la réglementation de leur fonctionnement et leur standardisation technique, l'usager dispose, au moins par défaut, de la pleine maîtrise des données envoyées et reçues. Au-delà, l'usager devrait pouvoir connaître de manière conviviale l'étendue exacte du bavardage de son ordinateur, les informations transmises et reçues, leur finalité, leur émetteur ou leur destinataire. Le débat européen récent sur les RFID a amené des conclusions sur la responsabilité des constructeurs d'équipements terminaux et des fournisseurs des systèmes RFID, c'est-à-dire des infrastructures qui englobent tant les systèmes de collecte, de transmission, des données générées par les terminaux RFID que les bases de données dans lesquelles ces données seront analysées et grâce auxquelles les décisions ad hoc seront prises.
  Cet élargissement de la protection des données à une réglementation des infrastructures et des terminaux est indispensable. Comment assurer la protection des données de manière effective, si des solutions techniques ne prennent pas en compte ces exigences et ne les traduisent point efficacement? Ainsi, pour reprendre l'exemple des RFID, souhaite-t-on, avec le Groupe de l'article 29, permettre que le porteur de la puce puisse aisément désactiver la puce, que le système de transmission utilise les solutions de la cryptographie. Cette approche dite «*privacy by design*» se fonde sur une réflexion fondamentale traduite pour la première fois par les rédacteurs de la loi française de 1978, «L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.» À partir de ce texte, les organes de protection des données ont à plusieurs reprises affirmé le principe de la responsabilité des fournisseurs d'équipements terminaux et des concepteurs d'infrastructures quant aux risques que l'utilisation de leurs infrastructures ou terminaux pouvait engendrer vis-à-vis de la protection des données de leurs utilisateurs.

  Une troisième piste serait d'obliger, comme la recommandation récente de l'Union Européenne à propos des RFID, le propose, d'obliger les designers de systèmes d'information collectant et traitant des données collectées automatiquement auprès des personnes, de veiller à ce que le fonctionnement de leurs systèmes réponde aux exigences des réglementations de protection des données et de procéder à un réel «*privacy impact assessment*», motivé et publié.
- Les dangers particuliers nés du profilage ont été dénoncés. Ils conduisent à réduire les personnes à des profils et à prendre ainsi des décisions vis-à-vis de personnes identifiées ou non. L'utilisation de telles techniques requiert un encadrement réglementaire aux motifs de leur opacité ou invisibilité, mais surtout vu les risques de discrimination et d'absence de proportionnalité des données utilisées. On peut songer, pour celui qui met en œuvre de telles techniques, à une obligation comme celle d'indiquer à la personne profilée le fait qu'il y a eu recours à une telle technique, à la nécessité de limiter les données utilisées lors du profilage aux seules données pertinentes et à les coder, à l'obligation de vérifier périodiquement la qualité tant des données utilisées que des inférences obtenues. Un droit d'opposition à être profilé devrait de même être reconnu.

5. Curieusement, le développement des technologies et la volonté de répondre aux préoccupations nouvelles qu'il suscite en matière de vie privée nous amènent à réaffirmer, mais dans un contexte nouveau, deux droits indiscutables déjà affirmés par l'article 8 de la Convention européenne des droits de l'Homme et corollaires (voire facettes du droit à la vie privée): l'inviolabilité du domicile et le secret de la correspondance.

- L'inviolabilité du domicile doit s'entendre désormais de l'inviolabilité du domicile virtuel? Une récente décision du Tribunal constitutionnel allemand du 27 février 2008 crée sur la base du droit général à la personnalité un tout nouveau droit fondamental à la protection de «la confidentialité et l'intégrité des systèmes d'information technologiques». Ce nouveau droit fondamental en matière de technologie de l'information doit compléter les droits fondamentaux existants là où ils font défaut, et ce, eu égard à l'évolution des technologies et des risques nouveaux liés à cette évolution. Ne constitue-t-il pas l'affirmation du droit à la protection du domicile virtuel que serait le terminal détenu par la personne concernée et ne donne-t-il pas le droit à une désactivation du terminal chaque fois que la personne souhaite être en paix.
- De même, il serait utile d'affirmer avec la même vigueur le droit au secret de la communication électronique, au moment où nombre de

communications sont échangées via des plateformes ou prennent la forme de simples consultations de site web sans que nul ne s'émeuve que ces consultations puissent être portées à la connaissance de tiers.

6. Qu'il nous soit permis également d'évoquer l'importance pour le droit de la protection des données de chercher des synergies nouvelles avec d'autres branches du droit. La première se déduit naturellement des deux dernières réflexions. La violation du secret de la correspondance est punie par le droit pénal et pénétrer sans son consentement, ne serait-ce que par un cookie ou un spyware dans le terminal d'un utilisateur, n'est-il pas un «*hacking*» au sens des lois nouvelles dites de cybercriminalité? De même, le vol d'identité, dans nombre de cas, s'identifie à un faux en informatique. Bref, il y a là matière à réfléchir sur l'intérêt de travailler avec les spécialistes du droit pénal.

La même réflexion conduit à rechercher des alliances du côté de la protection des consommateurs. Au-delà des questions de droits de l'homme, le développement des technologies de l'information et de leurs applications présente des enjeux économiques importants pour la défense des consommateurs. L'économie de l'Internet repose largement sur les ressources publicitaires et les technologies qui l'animent permettent de donner à ceux qui désirent maximiser l'intérêt de la publicité, les moyens appropriés pour le faire. Le marketing *one-to-one* est en pleine expansion et l'apparition de sociétés spécialisées dans cette technique de prospection et d'entreprises – comme les plateformes du web 2.0 ou comme Google – en relation directe avec les individus qui «consomment» leurs services hautement personnalisés, font craindre une exploitation de plus en plus pointue de l'expression des choix des consommateurs ou des données à caractère hautement personnel que ces derniers confient à la toile (liste d'amis, hobbies, photos de vacances, etc.). Bref, protection des consommateurs et protection de la vie privée trouvent une occasion de cause commune, que les dispositions légales encouragent: utilisation des dispositions en matière de pratiques commerciales déloyales ou agressives, possibilité d'actions collectives et, au-delà, intérêt d'un rapprochement des autorités de protection des données, des associations de libertés civiles et des associations de protection des consommateurs. L'intérêt de cette approche commune est attesté par l'action remarquable de la *Federal Trade Commission* américaine en matière de *Privacy*. Cette juridiction administrative spécialisée en matière de protection des consommateurs a pu, nonobstant l'absence de législation en matière de protection des données, développer une réflexion et des actions importantes dans les domaines qui nous concernent, qu'il s'agisse des utilisations à des fins commerciales, des RFID ou des techniques de profilage. Cette action a pu être menée sur base de la loi américaine relative aux

pratiques déloyales, sur la base notamment du «*False and Deceiptive Statement Act*», et devrait inspirer nos propres autorités publiques de protection de la vie privée.

7. Il apparaîtra peut-être étrange qu'en définitive, nous plaidions pour une relativisation de nos réglementations de protection des données. Pourtant, ce qui est en jeu dépasse de loin le simple champ des réglementations de protection des données, voire la constitutionnalisation de ce droit. Nous sommes convaincus qu'il est important que les autorités dites de protection des données prennent l'exacte dimension des défis posés par nos sociétés de l'information. Il s'agit bien d'une revendication en faveur de nos libertés, qui appelle à une défense de la dignité et de l'autodétermination de la personne. Si les technologies de l'information et de la communication constituent une chance inouïe pour le développement personnel de chacun, ces mêmes technologies représentent un enjeu d'autant plus grand pour nos libertés que les avantages de ces technologies mis en avant nous amènent à multiplier les risques d'atteinte à notre vie privée, non seulement, à accepter d'être suivis, à nous voir réduits à un numéro, à subir les messages qui nous arrivent à tout moment sur nos boîtes aux lettres, sur nos écrans voire dans nos corps, mais, au-delà, à jouer le jeu de la marchandisation de l'information personnelle, en nous exhibant sur le net à travers les réseaux sociaux et autres.

L'enjeu essentiel du droit à la protection de la vie privée est la défense de l'humain, de son développement et de sa dignité comme valeurs absolues et le renvoi des logiques absolues de sécurité et d'efficacité économique à leur dimension toute relative. La protection des données n'épuise pas le débat de la vie privée. Au contraire, la réflexion fondamentale que suscite le devenir de nos libertés nous oblige à repenser nos législations de protection des données qui ne sont jamais qu'un instrument au service de la vie privée et non une fin en soi. Ceci doit vous conduire, messieurs les commissaires, à envisager votre rôle combien précieux non comme un rôle juridictionnel au service d'une législation qui deviendrait un dogme et qui vous enfermerait sur vous-mêmes, mais comme des avocats de nos libertés, capables d'entrer en dialogue avec l'ensemble des autres acteurs et de chercher avec eux, au-delà des législations actuelles, des solutions courageuses.

Internet, quo vadis? Mais surtout, nous, où vont nos libertés?