

## CONFERENCE INTERNATIONALE DES COMMISSAIRES A LA PROTECTION DES DONNEES

LONDRES, 2 ET 3 NOVEMBRE 2006

### REFLEXIONS PROPOSEES PAR ALEX TÜRK, PRESIDENT DE LA CNIL

Dans un peu moins de deux ans, nous allons fêter le 30ème anniversaire de notre Conférence Internationale des Commissaires à la protection des données. Si vous nous donnez votre accord, l'Allemagne et la France auront le grand plaisir de vous accueillir à Strasbourg puisqu'elles fêteront le même jour le 30ème anniversaire de leurs Lois fondamentales et de la création des autorités allemandes de protection des données personnelles et de la Commission nationale de l'informatique et des libertés.

Trente ans pour des institutions telles que les nôtres, est-ce vieux ? Est-ce jeune ? Disposons nous du recul suffisant pour apprécier l'efficacité de notre action ? En vérité, le sens de la réponse à ces questions dépend moins du temps écoulé que de la succession des événements survenus durant cette période. Quels éléments communs entre l'activité de nos Autorités de contrôle au début des années 80 et celle que nous menons aujourd'hui ? Il n'est pas nécessaire d'être un expert pour désigner les facteurs déterminants de cette véritable révolution que nous connaissons depuis le début des années 90 : Internet, téléphone portable, biométrie, puces RFID, WIFI, nanotechnologies, etc..

Nous sommes ainsi confrontés à une **immense vague technologique** qui bouleverse, sur son passage, nos traditions juridiques, l'application de nos concepts et, pour finir, les grandes certitudes que nous pouvions encore entretenir, nous, Autorités de protection des données, sur l'effectivité de notre action. Et voici que, peu après la tragédie du 11 septembre et des autres attentats terroristes survenus par la suite, est apparue une seconde vague que l'on pourrait qualifier de « **sécuritaire** » et qui a déclenché, depuis cinq ans, un mouvement profond, au sein des pouvoirs publics de nombreux États en faveur d'un accroissement des moyens d'action en matière de **lutte antiterroriste**.

Bien entendu, il ne s'agit, en aucune manière, de contester le bien-fondé même de ces politiques qui répondent aux attentes de nos concitoyens. Et d'ailleurs, ces dernières années, nos Autorités de contrôle ont réagi avec un **grand sens de leurs responsabilités** aux différentes mesures anti-terroristes prises par les autorités publiques. Mais cette **vague « sécuritaire », normative** cette fois, qui s'est traduite par la création ou l'extension de nombreux fichiers et la mise en place, au profit des autorités de police, de nouveaux moyens d'investigation dans les systèmes d'information, pourrait bien submerger nos Autorités.

La philosophie même qui sous tend l'existence de celles-ci est, en effet, mise en cause par la conjonction de ces deux vagues. Et l'on éprouve, souvent, un sentiment d'incompréhension lorsque l'on constate que nos Autorités de contrôle, faute de moyens suffisants, ne peuvent accomplir correctement toutes leurs missions, piétinent face à l'émergence des nouvelles problématiques de protection des données, et se sentent parfois, impuissantes face au déferlement de ces vagues alors qu'on attendrait de leur part, tout au contraire, un positionnement fort et un interventionnisme accru .

Dès lors **une prise de conscience collective est nécessaire et urgente** si nous ne voulons pas faillir à notre mission.

Nous devons d'abord faire preuve de lucidité et tenter d'analyser les ressorts de ces deux vagues, à la fois technologique et normative, qui défient nos organisations. Il nous faut aussi, ensemble, proposer des réformes, des stratégies coordonnées pour agir autrement, mieux, plus vite, plus fortement. Enfin, il nous faut déterminer les voies qui nous permettront d'accéder à une autre dimension de façon à retrouver la place qui doit être la nôtre au service de la protection des données personnelles.

Prenons garde ! A défaut d'initiative de notre part, on pourra, un jour, dire de nous : *« La civilisation était en train de changer sous leurs yeux et ils n'ont rien vu venir ; un nouveau droit fondamental des hommes et des femmes vivant dans les sociétés modernes était en train d'être reconnu par les textes et ils n'ont rien fait pour le protéger ».*

## **I – DEUX VAGUES, UN TRIPLE DEFI.**

### **A – La « vague technologique ».**

Il est impossible de formuler des solutions éventuelles à ces questions si on ne prend pas la peine de s'attacher à définir et à circonscrire les caractéristiques inhérentes au progrès technologique dans le domaine de la protection des données personnelles.

#### **1 - Le facteur « accélération ».**

Phénomène bien connu, le progrès technologique s'avance en accélérant sans cesse. Les délais entre la découverte d'un phénomène et sa mise en œuvre technologique se raccourcissent et le temps de passage d'une innovation à une autre innovation, du développement d'un prototype à son déploiement industriel, se réduit sans cesse.

Ainsi, en 10 ans, Internet est devenu omniprésent : près de 1 milliard d'internautes, soit 14,6 % de la population mondiale l'utilisent aujourd'hui<sup>1</sup>. Si l'accès à haut débit représente une première étape dans l'accélération de son usage, la deuxième étape, son accès depuis les mobiles, devrait rendre son usage rapidement incontournable.

Et il ne se sera écoulé que 3 ans entre le moment où la technologie RFID a pu être développée à un stade industriel et celui où elle a été intégrée dans les documents de voyage, dans des cartes de paiement, des cartes d'accès, etc., et la réduction continue du coût de puces et des lecteurs assure la pérennité de ce développement.

---

<sup>1</sup> Sources : world internet statistics citées dans HS du Monde « bilan du monde 2005 » paru en 2006.

Il est d'ores et déjà prévisible que l'impact des nanotechnologies, qui seront une réalité industrielle massive à échéance 2015, se manifesterait encore plus rapidement que celui des RFID. Et on sait que, avec les nanotechnologies, les performances des futurs « ordinateurs quantiques » pourraient être plus élevées d'un facteur  $10^9$  (dix milliards de fois plus puissant) par rapport aux ordinateurs actuels. Ces chiffres vertigineux laissent imaginer l'ampleur de l'accélération technologique à venir.

Or le temps juridique est lui-même particulièrement lent à la fois parce que les normes et les concepts s'élaborent dans le respect des procédures démocratiques et parce que les enjeux sont de plus en plus complexes.

## **2 - Le facteur « globalisation »**

Autre caractéristique du progrès technologique : ses effets sont marqués par une propension à s'universaliser, à se globaliser. Dans notre domaine, cela se traduit, bien sûr, par le formidable essor des délocalisations de traitements de données : l'émergence dans des pays jusqu'alors peu impliqués dans le traitement de l'information, d'activités de développement logiciel, de sous-traitance et de maintenance à distance. Evoquons également la maîtrise, par les Etats-Unis, des modes de traitement et d'organisation de l'information (systèmes d'exploitation, logiciels, outils de recherche...). De même, il est inutile d'insister sur les problématiques transfrontières qui s'attachent à ces phénomènes. Or notre Droit, nos droits sont, par essence, étroits parce qu'ils s'inscrivent dans le cadre de territoires et de champs de compétences ordonnés et balisés.

Quel constat en tirer pour la protection des données ? Face à des pays où le concept de protection des données est encore peu connu, sinon ignoré du système juridique, les instruments mis en place pour « contrôler » les flux transfrontières de données apparaissent à la fois bien dérisoires et peu compréhensibles.

Nous sommes bien évidemment, aujourd'hui, dans l'incapacité de contrôler, sur le plan international, les échanges de données. Il faut sans doute avoir le courage de reconnaître que nos règles de protection des données sont, en ce domaine, très largement inadéquates et que, de la même façon que l'informatique est aujourd'hui par nature communicante et sans frontières, la protection des données ne peut se concevoir que dans une dimension mondiale. Ceci suppose assurément d'élaborer, sur le plan international, un instrument juridique nouveau. Surtout, il nous faut, en amont, réfléchir à une adaptation (et non à une remise en cause) de nos concepts de base pour assurer une meilleure compréhension de ceux-ci (ex : la notion de donnée à caractère personnel, le concept de droit d'accès, etc.).

## **3 - Le facteur « ambivalence »**

Toutes les réflexions menées dans le domaine de la philosophie du droit dans nos pays respectifs l'ont montré : il est vain de vouloir dissocier, parmi les effets du progrès technique, les aspects positifs et négatifs. Toute innovation technologique porte, en elle, « le bien et le mal » et renvoie aux usages que souhaitent en faire ses promoteurs<sup>2</sup> ou ceux à qui on remet le pouvoir de décision en la matière. Or le droit -c'est un élément intrinsèque à sa vocation- se doit d'être univoque et se trouve donc être, bien souvent, par nature, en inadéquation avec cette ambivalence du progrès technique.

---

<sup>2</sup> Cf les propos ambigus tenus par les deux fondateurs de GOOGLE, Larry Page et Sergey Brin : « Notre mission est d'organiser l'information du monde et de la rendre accessible à tous ».

La difficulté majeure vient de ce que, aujourd'hui, l'informatique est devenue une informatique de « confort » indispensable dans tous les actes de la vie quotidienne (pour se contacter, se localiser, s'informer, se sécuriser...). Mais nos concitoyens se préoccupent-ils de la traçabilité et de la surveillance potentielle de leurs déplacements, de leurs comportements, de leurs relations ? L'individu est-il pleinement conscient de cette ambivalence de la technique ? Force est de constater le peu de réactions de nos concitoyens vis-à-vis de ces questions. A qui la faute ? N'avons-nous pas notre part de responsabilité dans ce manque de vigilance citoyenne ?

#### **4 - Le facteur « imprévisibilité »**

Largement lié à la conjonction des trois caractéristiques précédentes, le développement parfois imprévisible de certains usages de l'outil informatique crée des situations de porte-à-faux pour ceux qui sont en charge de l'élaboration des normes et rend l'exercice de nos missions malaisé. C'est l'exemple du téléphone portable, qui aurait pu ne rester qu'un simple outil de communication, mais qui est également devenu un moyen de paiement et un outil de traçage et de géolocalisation des utilisateurs. De même, Internet, simple instrument d'information et de communication, peut se transformer en un redoutable système d'espionnage par le biais d'applications comme Google Earth, par exemple. Pouvait-on prévoir que l'on pourrait être identifié à distance par son passeport ou encore que l'on pourrait rechercher un passé judiciaire sur internet « grâce » aux formidables capacités d'investigation dans la vie privée qu'offrent aujourd'hui les moteurs de recherche ?

#### **5 - Le facteur « invisibilité ». (Invisibilité virtuelle / Invisibilité physique ou réelle).**

On est loin aujourd'hui du gros ordinateur trônant dans « la » salle informatique... Le traitement de l'information est de plus en plus « invisible », impalpable, de moins en moins maîtrisable, que ce soit par les individus ou par nos Autorités.

Ce facteur « invisibilité » est double :

- d'une part, la technologie tend à devenir invisible du fait du développement des traitements de données virtuelles réalisés à l'insu des personnes (c'est l'invisibilité virtuelle, liée aux processus);
- d'autre part, la technologie tend à devenir invisible du fait de son extrême miniaturisation (c'est l'invisibilité physique ou réelle) .

Le premier facteur d'invisibilité résulte de la multiplication des traitements qui, s'ils sont effectués par des technologies visibles physiquement, sont toutefois réalisés à l'insu des personnes, si bien qu'ils sont, en pratique, pour celles-ci, parfaitement invisibles. Ce sont ces traitements qui permettent de tracer les personnes de manière virtuelle : traçabilité de leurs déplacements physiques dans les transports en commun, de leurs consultations sur Internet, de leurs communications téléphoniques et électroniques, etc.

L'indifférence de nos concitoyens à l'égard des enjeux de protection des données, le manque sinon l'absence de perception qu'ils ont des risques d'atteinte à leurs libertés individuelles par l'usage de telle ou telle technologie, tiennent aussi sans doute à cette invisibilité croissante du traitement de l'information, à ces traces informatiques - actives ou passives - que chacun laisse désormais derrière soi.

Le second facteur d'invisibilité réside, lui, dans l'extrême miniaturisation de la technologie elle-même. Les téléphones portables, les ordinateurs, les assistants personnels diminuent en taille et en poids chaque année. La taille des puces diminue, tandis que leur durée de vie s'allonge, et que les capacités de mémoire et les puissances de traitement des ordinateurs se développent.

Mais **une autre vague technologique pointe à l'horizon 2015, celle des nanotechnologies**, dont on nous promet des applications déconcertantes dans le domaine des systèmes d'information. Avec les nanotechnologies, la difficulté ne consistera plus à avoir conscience de l'existence d'un traitement, visible par ailleurs. Il ne sera même plus question d'avoir ou non conscience de l'existence d'un traitement : il sera devenu impossible de voir à l'œil nu que la technologie est présente dans un objet !

Avec la tendance à la virtualisation des traitements, nos concepts menaçaient déjà de voler en éclat : comment définir le responsable du traitement et la finalité avec le « data mining », le lieu du traitement avec le « peer to peer », quel sens cela a-t-il de définir aujourd'hui une durée de conservation... ? Mais de manière encore plus préoccupante, l'évolution vers l'invisibilité réelle de la technologie elle-même pourrait aboutir, à échéance de quelques années, à placer notre droit et nos Autorités de contrôle dans une situation d'impuissance puisqu'il leur reviendrait d'encadrer et de contrôler des traitements effectués par le recours à une technologie invisible...

## 6 - Le facteur « irréversibilité »

Les évolutions liées au progrès technologique sont par nature irréversibles<sup>3</sup>. Nous ne vivrons plus jamais dans un monde sans ordinateurs, sans Internet, sans téléphones portables, sans identification biométrique, sans géolocalisation, sans vidéosurveillance. Bien au contraire, ces technologies ont tendance à s'imbriquer les unes dans les autres. Outre les problèmes majeurs que pose cette caractéristique d'irréversibilité à nos systèmes juridiques, elle doit probablement constituer, en termes d'intérêt général, le facteur le plus dangereux. Nous aurons l'occasion d'y revenir plus longuement en conclusion.

## B – Les politiques de sécurité : la vague normative

Il s'agit, cette fois, d'un défi socio-juridique qui nous est lancé par l'ensemble des nouvelles législations et réglementations produites en matière de lutte antiterroriste des deux côtés de l'Atlantique. Ces politiques liées aux nouvelles exigences de sécurité publique ont abouti à la mise en place d'un maillage en matière d'utilisation de fichiers informatiques susceptibles de constituer un **choc de civilisation**.

---

<sup>3</sup> Si l'on exclut, bien entendu, l'hypothèse de catastrophes naturelles majeures aboutissant à des destructions globales auquel cas d'ailleurs les réflexions ici menées se verraient ipso-facto dépourvues de tout intérêt...

Si l'on prend l'exemple de la France, les événements du 11 septembre se sont traduits par un renforcement des mesures de sécurité intérieure et de maîtrise des flux migratoires, même si notre pays est déjà doté, depuis 1986, d'une législation antiterroriste<sup>4</sup>. Plusieurs lois sont ainsi intervenues, depuis 2001, pour étendre la consultation des fichiers de police en particulier à des fins administratives (pour le recrutement à des emplois de sécurité, les décisions de naturalisations, l'octroi des titres de séjours des étrangers...), pour élargir sensiblement les possibilités d'accès par les autorités judiciaires et les services de police aux fichiers informatiques privés (et en particulier à ceux des opérateurs de communications, des cybercafés, des fichiers des compagnies aériennes), ou encore pour prévoir la création de nouveaux fichiers de police (ex : fichier de domiciliation des délinquants sexuels), l'extension de fichiers existants (ex : fichier des empreintes génétiques), le développement de la vidéosurveillance ou encore la mise en place en tous points appropriés du réseau routier et autoroutier de dispositifs fixes ou mobiles de lecture des plaques minéralogiques et de prise des photographies des occupants des véhicules.

Ces différentes mesures, qui s'inscrivent dans le prolongement de la politique de lutte anti-terroriste, ont, bien entendu, eu un impact certain sur la protection des données personnelles et on sait que les mesures adoptées en France ont connu leurs équivalents dans les autres pays.

Au niveau européen, les politiques de lutte contre le terrorisme ont donné un coup d'accélération au développement des bases de données sur les visas et de la seconde version du Système d'information Schengen (SIS II), à la rétention des données de trafic, au contrôle des listes de passagers aériens, etc. Elles ont également conduit nos gouvernements, via l'OACI, à soutenir l'incorporation de données biométriques dans les passeports et les documents de voyage.

Aux Etats-Unis, ces mêmes politiques ont conduit à l'adoption emblématique du Patriot Act -une loi de 342 pages !- adoptée seulement un mois et demi après les attentats du 11 septembre. Cette loi, comme les divers programmes de surveillance ultérieurement mis en place par l'administration Bush, accordent des pouvoirs considérables aux autorités administratives américaines pour saisir et intercepter des documents, des communications téléphoniques et électroniques, pour interconnecter des fichiers, tout en limitant l'intervention de l'autorité judiciaire et en autorisant l'exécutif à ne pas publier ces mesures.

En outre, dans tous nos pays, une tendance se crée qui consiste à utiliser des bases de données de sociétés privées à des fins de lutte contre le terrorisme. Les affaires PNR et SWIFT sont caractéristiques de cette tendance.

Confrontées à une telle situation, les Autorités de contrôle en matière de protection des données doivent éviter les pièges, dénoncer les illusions et combattre les mythes.

## 1 - Le piège du manichéisme.

L'ensemble des Autorités de contrôle nationales en charge de la protection des données reconnaît, bien évidemment, **la légitimité des politiques de lutte antiterroriste** mises en place dans leurs États respectifs. Et les accusations d'irresponsabilité qui sont parfois portées à leur égard en la matière sont inacceptables.

<sup>4</sup> La France s'était dotée d'une telle législation après une première vague d'attentats en 1986 (Loi du 9 septembre 1986). Celle-ci avait été renforcée par une seconde série d'attentats en 1995.

Les Autorités de contrôle se situent en dehors du champ politique. On ne peut les confondre ni avec certaines associations militantes qui professent des opinions très engagées, ni avec les autorités publiques en charge de la sécurité ou de la justice. Il serait si facile de stigmatiser les comportements de ces autorités de contrôle si elles versaient d'un côté ou de l'autre !

Au contraire, elles examinent les textes de niveau législatif ou réglementaire en recourant aux principes et aux instruments que les textes fondateurs, de chaque pays, leur ont confiés. Quelle est la finalité poursuivie par tel traitement de données dans une politique de lutte antiterroriste ? Y a-t-il adéquation entre l'objectif poursuivi et les moyens mis en œuvre ? Quel est le champ de garanties prévues pour assurer la confidentialité et le respect des droits des personnes ?..., etc. Et c'est très exactement ce qu'attendent d'elles les citoyens des pays concernés : il s'agit d'éclairer leur propre analyse avantages-inconvénients qui doit leur permettre de **mesurer à quelles limitations de leurs droits individuels ils sont prêts à consentir pour accroître le niveau de sécurité publique**, et donc leur propre sécurité.

Les Autorités de contrôle sont rompues à ce genre d'exercice et elles ne doivent donc pas se laisser entraîner dans le piège du manichéisme - à condition que les Gouvernants veuillent bien leur délivrer les informations nécessaires pour leur permettre de formuler leur appréciation en pleine connaissance de cause ! Or force est de constater qu'en ces domaines, certes politiquement très délicats, nos Autorités de contrôle peuvent éprouver parfois le sentiment de ne pas disposer de la part des autorités concernées de tous les éléments de contexte utiles. On imagine les motifs pour lesquels les autorités gouvernementales, de l'ensemble des États, peuvent ainsi être enclines à retenir l'information.

## 2 - Le risque de l'engrenage.

Si l'on prend l'exemple des politiques de sécurité (mais nous pourrions en dire autant dans le domaine de la Justice, de la politique sociale ou de la Santé), on constate que, en pratique, dans aucun pays on n'a procédé par la mise en œuvre d'une loi fondamentale, suivie aussitôt d'un ensemble de textes d'application. Compte tenu de la complexité et de la sensibilité de ces questions, il est compréhensible que les pouvoirs publics de nos pays puissent être contraints de recourir à la pratique du train des lois successives.

Mais parfois il s'agit, en réalité, d'une **véritable stratégie de contournement** à l'égard des autorités de protection des données. Peu importe d'ailleurs, car du point de vue du comportement qui doit être le nôtre, cela ne change rien. Dans tous les cas, nous sommes confrontés au risque de l'engrenage juridico-politique.

Ce risque est le suivant. L'Autorité de contrôle est saisie d'un projet de loi portant création d'un nouveau traitement. Conformément aux principes fondamentaux de finalité et de proportionnalité, elle formule un avis qui repose sur un équilibre à un instant donné et en admet la pertinence. Mais quelque temps plus tard, on lui soumet un nouveau projet de loi qui élargit le champ du traitement ou accroît sa puissance. Les promoteurs de ce second texte font valoir que l'Autorité de contrôle ayant déjà donné un accord de principe au premier texte, on voit mal comment elle pourrait s'opposer à une simple extension, et ainsi de suite si nécessaire...

Ajoutons que le problème est rendu encore plus aigu par le fait qu'en la matière, 1 + 1 peut faire 3 ! On veut dire par là que la conjugaison des dispositions des deux textes produits peut créer une synergie telle que les risques engendrés à l'égard de la protection des droits individuels se multiplient au lieu de s'ajouter seulement.

Ce phénomène est parfaitement illustré par le développement progressif, selon des processus identiques, des fichiers nationaux d'empreintes génétiques en France et en Grande-Bretagne. Dans les deux cas, ces fichiers ont été créés dans un but spécifique : centraliser les empreintes génétiques de criminels sexuels condamnés afin de faciliter leur identification en cas de récidive. Puis on a augmenté le nombre des personnes concernées, pas forcément de façon concomitante, ni dans le même texte. Ensuite c'est la nature des infractions prises en compte qui est étendue. Enfin on diversifie les situations des personnes vis-à-vis de la procédure pénale : s'agit-il d'une personne accusée ou simplement mise en cause, est-ce une personne seulement suspectée ? Y a-t-il des indices graves *et* concordants, ou s'agit-il d'indices graves *ou* concordants ? C'est ainsi qu'en quelques années, on est passé d'un fichier spécifique dédié à la prévention de la récidive des délinquants sexuels à un instrument général d'investigation au service de l'élucidation de quasiment toutes les affaires par la police judiciaire.

Comment réagir face à ce type d'engrenage législatif ? Question délicate surtout si l'on rappelle qu'elle se pose sur la toile de fond de l'irréversibilité des phénomènes décrits plus haut.

### 3 – L'illusion de « l'exemplarité »

Il s'agit là d'un autre risque qui présente quelques analogies avec le précédent mais qui concerne peut-être plus particulièrement les pays membres de l'Union européenne qui représentent à eux seuls la moitié des États dans le monde disposant d'une Autorité de contrôle et d'une loi de protection des données.

Par exemple, de nombreux pays en Europe disposent de fichiers nationaux de population et font usage d'un seul numéro d'identification, d'autres pays, tels que la France, ont fait des choix différents. Tel pays développe puissamment un système de traitement des empreintes génétiques qui devient une « référence » pour d'autres exécutifs. Tel autre pays développe de manière très significative le recours à la biométrie ou à la vidéo surveillance.

Or, les exécutifs nationaux, prenant appui sur ces exemples étrangers, ont bien souvent tendance à utiliser l'argument analogique suivant : « *Comment vous, Autorité de contrôle, pouvez-vous vous opposer à tel ou tel développement de traitement alors que cela a été accepté dans tel autre pays ?* » On devine alors les problèmes d'harmonisation que cela pose et, en tout état de cause, on mesure à quel point il est **nécessaire de recourir à des raisonnements fondés sur la définition de dénominateurs communs.**

### 4 – Le mirage du fichier « remède miracle »

Nos autorités doivent ensuite se battre contre le mirage du « fichier, remède miracle ». On dit parfois que lorsque l'autorité publique est confrontée à un problème, elle crée une commission. Désormais, à cette propension s'ajoute un nouveau réflexe : la création d'un fichier !

Or nos Autorités savent pertinemment que la création d'un fichier informatique ne règle pas tout. Il nous revient de **désacraliser le caractère supposé infallible du fichier informatique**.

Combien de fois d'ailleurs nous sommes-nous prononcés sur des fichiers supposés régler un problème qui n'auront finalement jamais vu le jour ? Ainsi en France, le législateur a prévu, en 1997, l'obligation de relever et de traiter les empreintes digitales des ressortissants sollicitant un titre de séjour en France. Près de dix ans après, ce fichier n'a toujours pas vu le jour ! Ceci n'a pas empêché le législateur de modifier la loi pour étendre cette obligation aux demandeurs de visas, pour lesquels des expérimentations sont en cours. La réglementation européenne aura ici, sans aucun doute, contribué à l'accélération du processus.

Parfois également nos Autorités se prononcent sur la création d'un fichier en sachant que celui-ci a des chances de ne pas être la réponse adaptée au problème que l'on cherche à régler. Ainsi, les exigences de transmission par les compagnies aériennes des données des passagers aériens aux autorités américaines et les diverses mesures prises pour contrôler le déplacement des personnes ne sont-elles pas parfois disproportionnées, quand on sait que les mouvements terroristes ont désormais tendance à recruter en « local », et à user de moyens de déplacement plus discrets que l'avion ... ?

Un dernier exemple illustrera encore de manière emblématique cette course, toujours inachevée, entre la création d'un nouveau fichier, son effet escompté en terme de sécurité et l'imprévisibilité des comportements humains les plus odieux. En France le fichier judiciaire des infractions sexuelles recense les personnes condamnées pour des délits et des crimes sexuels et oblige celles d'entre elles ayant été le plus lourdement condamnées à se présenter tous les six mois au commissariat et à signaler tout changement de domicile. L'intérêt d'un tel fichier est indéniable car connaître la localisation de personnes dont la dangerosité est avérée, et qui se savent surveillées, peut contribuer à améliorer la prévention de la récidive. Or, ce fichier n'était pas encore entré en vigueur que, à la suite d'un fait divers particulièrement dramatique, impliquant un récidiviste sexuel, plusieurs propositions de modifications ont été avancées afin d'obliger quasiment tous les délinquants sexuels à venir au commissariat non plus tous les six mois mais tous les trois mois, voire tous les mois. Ces propositions n'ont pas encore été suivies d'effet mais, une fois encore, le mythe du contrôle absolu par l'instrument informatique est à l'œuvre.

On le voit, croire que la création d'un fichier va permettre, en tant que tel, de résoudre un problème constitue trop souvent un leurre pour l'opinion publique.

## **5 – Le mythe du fichier infallible et la problématique « Majorité-Minorité »**

Les systèmes se développent et se perfectionnent sur le plan technologique. Ainsi, les traitements devenant de plus en plus performants, de moins en moins de personnes sont censées s'y trouver de manière non justifiée. Mais, de ce fait même, le problème est encore plus aigu pour les personnes qui figurent dans ces fichiers de manière indue, car tout portera à croire qu'il est impossible d'être dans ce fichier, aussi sophistiqué technologiquement, sans que cela soit justifié.

Sur le plan technique, il est impossible d'affirmer qu'un traitement de données peut être considéré comme fiable à 100%. Il est donc indispensable, sur le plan éthique, de continuer à affirmer que **l'informatique peut être faillible** et de proscrire, tout particulièrement dans certains domaines tels que celui de la sécurité ou de la justice, la prise de décision automatique par ordinateur.

Comment dès lors faire prendre conscience aux exécutifs et aux législatifs que la création de fichiers, lorsqu'ils concernent potentiellement des millions de personnes, appelle au préalable une réflexion de fond et une évaluation à la fois de la mesure et de la technique utilisée ? L'exemple de la biométrie est sur ce point révélateur : considérée comme la panacée en matière d'identification et d'authentification, alors même qu'elle n'a jamais fait l'objet d'une évaluation officielle, concertée sur le plan international, la biométrie est aujourd'hui amenée à se développer massivement sans qu'aucune réflexion réelle n'ait été conduite sur les conséquences à l'égard des personnes des erreurs d'identification biométriques.

Pour conclure sur ces différents pièges, insistons sur le fait que **la problématique de sécurité présente toutes les caractéristiques d'un cheval de Troie**. Ce qui peut être finalement admis, dans ce domaine d'intervention, par les Autorités de contrôle et les opinions publiques et individuelles peut devenir un précédent pour d'autres domaines d'action des fonctions régaliennes de l'État.

Si l'on n'y prend garde, il y a là, en germe, le risque de voir se vider de sa substance toute la philosophie qui sous-tend les textes fondamentaux en matière de protection des données personnelles.

### **C – Un troisième défi : la réputation de la protection des données et des autorités de contrôle**

Au moins dans un certain nombre de pays, la protection des données et les autorités de protection des données ne jouissent pas de la réputation positive qu'elles méritent.

Les règles de protection des données peuvent être perçues comme complexes et difficiles à appliquer de manière cohérente, prévisible et réaliste. D'autres critiquent les règles de protection des données comme trop abstraites, et pas assez recentrées sur les dommages réels ou supposés – causés aux personnes ou à la société dans son ensemble – si ces règles ne sont pas observées. D'autres encore critiquent la manière dont ces règles sont interprétées ou mises en œuvre, ce qui les dissuade de se mettre en conformité ou d'investir dans des efforts de mise en conformité.

De telles perceptions négatives peuvent être celles d'hommes politiques, d'administrations, d'entreprises, des médias mais aussi de particuliers. Il est nécessaire de combattre ces perceptions, en démontrant l'importance pratique de la protection des données, en matérialisant la réalité des droits et libertés fondamentaux, et en reconsidérant certaines pratiques, si cela s'avère nécessaire.

## **II – LIGNES D'ACTION. INITIATIVES.**

Pour faire face à de tels défis, il importe avant tout de reconsidérer nos méthodes d'action. Des initiatives germent ou existent sous l'impulsion de certains Etats à propos du rôle de la Conférence internationale, de l'OCDE à propos des instruments d'action des Autorités de contrôle, de la Francophonie à propos de l'exigence d'une Convention internationale et de l'inventaire des moyens d'action des Etats... Tout cela concourt au même objectif et pourrait emprunter deux axes principaux.

Les Autorités de contrôle doivent réfléchir ensemble :

- d'une part, à la manière de rendre plus efficace leur action,
- d'autre part, à faire reconnaître celle-ci de manière institutionnelle sur le plan international.

## **A – Les instruments.**

### **1 – La capacité d'expertise, de prospective et d'intervention dans le champ technologique**

Face à ces deux vagues qui menacent de nous submerger, il nous faut trouver un **second souffle**. Il est crucial et urgent de développer et d'affûter nos capacités d'expertise et de prospective. Notre crédibilité se joue en ce moment même chaque fois que nous allons devant l'opinion publique pour exprimer notre point de vue face aux projets développés par les pouvoirs publics et le secteur privé.

Au-delà, l'expertise technique nécessaire pour apprécier les enjeux du développement de telle ou telle technologie devient de plus en plus pointue. Ces enjeux nécessitent un suivi permanent qui s'avère de plus en plus difficile à réaliser pour les autorités de protection des données. Force est de constater qu'aujourd'hui nos Autorités sont plus présentes sur le terrain juridique que technique et que la protection des données « souffre » aujourd'hui de son image trop juridique. **Or la crédibilité de nos institutions est et sera de plus en plus liée à notre capacité à comprendre et à anticiper les développements technologiques.** C'est un enjeu de taille pour les Autorités de contrôle, mais il n'est pas concevable que se développent des techniques telles que le peer-to-peer, des applications comme Google Earth ou le Customer Experience Improvement Program de Microsoft sans que nous ne procédions, de façon coordonnée et concertée, à l'expertise de leurs potentialités. Le peer-to-peer signifie la libre circulation de quantités illimitées d'informations entre des acteurs situés en tous points de la planète, sans qu'il soit possible d'encadrer, sur le plan juridique, les échanges d'information en question. Google Earth, dans sa forme actuelle, constitue le socle idéal pour mettre en place des applications de géolocalisation d'une efficacité de plus en plus redoutable. Enfin, pour ceux qui ont accepté de participer aux programmes d'amélioration de ses logiciels, Microsoft reçoit, à Seattle, toutes les informations qu'il a jugé nécessaire de recueillir sur la façon d'utiliser ses logiciels (quand, comment, à quelle fréquence, etc.), construisant ainsi un profil détaillé de ses utilisateurs.

Pour analyser toutes ces nouveautés, est-il nécessaire chaque fois d'inventer ce qui existe déjà ? Nos Autorités de contrôle ne sont-elles pas capables de mettre en place des structures de coordination nécessaires pour élaborer **des stratégies de division du travail entre les Autorités** en fonction de leurs expériences, de leurs responsabilités, de leurs moyens et des enjeux qui sont les leurs ?

Face aux puissances planétaires, économiques, créatives et financières que sont Microsoft ou Google, il est aujourd'hui indispensable et urgent de repenser notre mode d'expertise, de coordonner, en ce domaine, nos actions, de développer et de mettre en commun notre savoir technologique. Ceci suppose aussi et surtout de réfléchir aux relations que nous souhaitons et devons entretenir avec la communauté des chercheurs et les industriels des technologies de l'information et de la communication.

## 2 - Évaluer notre efficacité et adapter nos pratiques

Le dialogue régulier et fructueux qui existe entre l'ensemble des Autorités de contrôle permet de très vite toucher du doigt l'un des paradoxes qui aujourd'hui obère notre efficacité globale.

Prenons l'exemple de l'Union européenne. L'ensemble des 25 Etats de l'Union européenne s'est donné un corpus de règles communes dans le cadre de la directive de 1995, et nombre de ces Etats travaillent ensemble sur les questions de protection des données depuis 20 ans. Pourtant, dès que l'on observe de plus près les pratiques des uns et des autres issues de leurs textes de référence, on se trouve devant une mosaïque, une incroyable diversité.

Alors que toutes les Autorités ont la même vocation, les mêmes missions à accomplir, défendent les mêmes principes, elles disposent de pouvoirs et utilisent des moyens parfois totalement différents les uns des autres. Certains pays mettent l'accent en forte priorité sur la politique de contrôle et de sanction, pour certains de ceux qui en disposent, d'autres privilégient le rôle des correspondants à la protection des données, d'autres encore donnent la primauté aux procédures de déclaration. Et d'autres pays enfin, s'efforcent de développer une stratégie généraliste.

Probablement certains de ces mécanismes sont-ils plus efficaces que d'autres. Personne n'en sait rien. Probablement certains de ces mécanismes sont-ils complémentaires des uns et des autres. Personne n'en sait rien.

Il est donc absolument nécessaire de procéder à une **évaluation complète et sans fard de cette diversité dans l'utilisation des moyens d'action** pour en tirer des enseignements permettant d'améliorer les résultats des Autorités concernées.

Mais ceci passera alors par la remise en cause de pratiques de fonctionnement mais aussi parfois par des revendications tendant à faire évoluer les législations en vigueur.

## **B - Nécessité d'une reconnaissance institutionnelle**

Pour porter ces messages et ces actions vis-à-vis des responsables des Etats concernés mais aussi pour prolonger notre politique d'action, d'information et de dialogue à l'égard des pays qui entreprennent aujourd'hui une réflexion sur leur niveau de protection des données, nous devons, le plus rapidement possible, parvenir à une reconnaissance institutionnelle et donc une existence internationale plus forte.

### 1 - Structuration de la Conférence Internationale

**La Conférence Internationale des Commissaires à la Protection des Données doit devenir le fer de lance de l'action de nos autorités sur le plan international.** Pour ce faire, nos Autorités ont besoin d'en structurer le fonctionnement, pour la rendre plus visible et plus efficace. Une réflexion est indéniablement nécessaire pour en assurer la viabilité et proposer des améliorations de fonctionnement. **Il convient dès lors de soutenir avec vigueur la résolution très opportune proposée en ce sens par nos collègues néo-zélandais.**

Peut-être est-il déjà possible, à ce stade, d'évoquer quelques pistes de réflexion, quelques objectifs. A court terme, nous devons sans doute réfléchir à la manière dont nos conférences doivent permettre, plus que cela n'a été possible jusqu'à présent, la discussion et la remontée d'idées de portée concrète, **dans un but avoué d'harmonisation de nos pratiques et d'adoption de positions communes**. A moyen terme, il nous faudra trouver le moyen de faire vivre notre conférence tout au long de l'année, et non seulement deux ou trois jours par an, élaborer un plan d'action, un programme de communication.... Notre conférence devra également se donner les moyens d'être considérée sur le plan international comme un interlocuteur privilégié pour les initiatives internationales ayant une incidence sur le droit de la protection des données. Ceci impliquera sans doute, à terme, de doter la conférence d'un **secrétariat permanent**. La tâche est donc importante, et elle est urgente.

## 2 – Elaboration d'une Convention Internationale

Par la **déclaration de Montreux**, nos Autorités appelaient au développement d'une **Convention universelle de protection des données**. Cette initiative doit être soutenue, portée par nos Autorités en parallèle du renforcement de la Conférence Internationale.

Cette Convention devrait être une grande Déclaration de droits, consacrant la reconnaissance **d'un droit universel à la protection des données et à la vie privée**. Sous la forme d'un instrument juridiquement contraignant, elle doit reprendre et mettre en valeur tous les travaux effectués en matière de protection des données jusqu'à nos jours, sur le plan mondial.

Elle devra constituer également un outil indispensable à la collaboration entre Autorités de contrôle, notamment dans les affaires sensibles de portée internationale, et permettre d'œuvrer pour le renforcement de leurs capacités, à se concerter face à l'accélération des nouvelles technologies. Elle favorisera des activités d'accompagnement aux démarches législatives, réglementaires et institutionnelles nécessaires à la mise en œuvre du droit à la protection des données.

Une longue marche sera sans nul doute nécessaire pour faire en sorte qu'une telle convention soit élaborée sous l'égide de l'organisation internationale compétente. Nous devons toutefois réaliser que nous avons parfois accès à des champs d'influence immenses qui peuvent être autant d'appuis pour faire avancer le projet. Je pense par exemple aux organisations régionales et aux zones linguistiques espagnole, francophone, lusophone, sans oublier le Commonwealth. Et **il reviendra à chacune de nos autorités de faire progresser cette idée et de la soutenir auprès de son gouvernement et des organisations auxquelles elle appartient**<sup>5</sup>, en fonction bien sûr de nos positionnements institutionnels respectifs, et, éventuellement, après coordination avec les autres autorités compétentes en matière de protection des données au niveau national.

---

<sup>5</sup> A titre d'exemple, l'action de la CNIL a mené les chefs d'État et de gouvernement de la Francophonie à appeler, dans la déclaration adoptée à l'issue de leur sommet de Bucarest, les 28 et 29 septembre 2006, à l'intensification des travaux nécessaires à l'adoption de législations et réglementations de protection des données, et, conscients de l'accroissement de la circulation de données personnelles au-delà des frontières, marqué leur intérêt pour examiner l'opportunité d'élaborer un instrument international garantissant le droit des personnes à la protection des données à caractère personnel.

### III – POUR UNE NOUVELLE STRATEGIE DE COMMUNICATION

Nous devons, de manière urgente, concevoir et mettre en œuvre une nouvelle stratégie de communication, chacun en ce qui nous concerne mais également sur le plan international.

Cette nouvelle stratégie doit être conçue à la fois comme une fin et comme un moyen.

#### **A – Un objectif : Communiquer**

La communication doit être conçue d'abord comme un objectif prioritaire. Est-il concevable, par exemple, que dans les pays de l'Union européenne où l'on inscrit le droit à la protection des données parmi les droits fondamentaux imprescriptibles tels que la liberté d'aller et venir ou la liberté de la presse<sup>6</sup>, l'immense majorité de nos concitoyens n'ait aucune conscience d'en être titulaires ? Or nous ne disposerons jamais d'assez de moyens pour nous interposer entre chacun d'entre eux et leurs gouvernants respectifs. Dès lors nous devons nous engager dans des **actions pédagogiques puissantes et à long terme, visant à les informer de l'existence et du contenu de ces droits, et à créer le réflexe de la protection des données personnelles**. Nos concitoyens devraient refuser de transiger sur leurs droits à la protection des données comme ils refuseraient de le faire pour la liberté de réunion ou la liberté de la presse.

Or, tel n'est pas le cas, loin de là ! Nous avons donc à engager un immense effort de pédagogie et il peut nous arriver de défendre le droit des individus, si l'on ose dire, malgré eux. Toute la population est ainsi concernée, le citoyen en tant que tel, les salariés des entreprises, les fonctionnaires des administrations, etc.

Mais deux catégories doivent être visées en priorité :

- Il s'agit d'abord des élus nationaux et locaux qui ont, par nature, une responsabilité particulière en la matière et dont l'information doit être améliorée ;
- En second lieu, il faut s'adresser aux jeunes générations qui, bien souvent, font preuve d'une grande indifférence vis-à-vis de ces questions tant ils sont habitués à manipuler ces nouvelles technologies au fur et à mesure qu'elles font l'objet d'usages publics. Chacun comprend que l'usage précoce de cette technologie dépourvue de référence aux principes de la protection des données personnelles, ne favorise pas l'accès des jeunes à une **citoyenneté de l'informatique et des libertés**. Il faut donc **agir dans le secteur éducatif** le plus tôt possible. Si l'on osait risquer cette image : il faut faire en sorte que dès l'instant où un enfant pose le doigt, pour la première fois, sur un clavier d'ordinateur, il intègre à son apprentissage l'impératif de la protection des données.

---

<sup>6</sup> Cf l'article 8 de la Charte des droits fondamentaux de l'Union européenne.

## **B – Un levier d'action : communiquer**

Les réflexions qui précèdent montrent combien il est important et urgent de doter les Autorités de moyens d'action supplémentaires et de leur assurer une reconnaissance sur le plan international.

Seules les organisations assurant une communication fondée sur des **thèmes largement accessibles au grand public** et tournés vers l'ensemble des médias disposeront de la **puissance nécessaire pour être entendues par les opinions publiques et donc par les Etats et la communauté internationale**. C'est à cette condition qu'ils pourront obtenir ces moyens d'action indispensables. Ceci passe probablement par une professionnalisation de la fonction de la communication au sein de nos autorités.

## **CONCLUSION**

Nos Autorités de contrôle occupent une place singulière et sans précédent au sein de l'organisation des pouvoirs publics de nos Etats respectifs. Nous ne sommes pas des législateurs mais certains d'entre nous peuvent émettre des réglementations à caractère contraignant. Nous ne sommes pas des sociétés de consultants mais nous nous honorons d'exercer, avant tout, un rôle de conseil auprès des acteurs de l'informatique et de nos concitoyens. Enfin, nous ne sommes pas des juridictions, mais certaines de nos autorités peuvent prendre des sanctions. En réalité notre mission consiste à rechercher en permanence, au nom de la société, **un équilibre entre les impératifs de sécurité publique ou du développement économique, d'une part, et d'autre part, les exigences de la protection de la vie privée et des données personnelles**.

L'extrême difficulté de notre tâche réside dans le fait que nous devons définir la légitimité et les ressorts de cet équilibre en nous projetant 5 à 10 ans plus tard. Nous devons éclairer le chemin que s'apprête à parcourir notre civilisation dans les usages qu'elle fait de l'informatique et **prévenir les dérives éventuelles** engendrées par la création de tel ou tel traitement de données. Et il est très difficile, alors même que nous savons que le résultat peut s'avérer catastrophique pour nos libertés, de se faire entendre lorsqu'il s'agit d'alerter nos concitoyens et nos gouvernants à propos de menaces éventuelles. Les éléments mis en place par tel ministère vont s'ajouter à d'autres éléments, se conjuguer, se combiner pour créer des synergies et aboutir à des situations échappant à notre contrôle. Et le risque serait qu'un jour, on constate que notre civilisation est totalement engluée. Les responsables seront alors tout désignés et l'on comptera parmi eux les Autorité de contrôle...

C'est pourquoi une piste intéressante consisterait à réfléchir à un thème qui pourrait être développé en commun par l'ensemble des Autorités permettant de mettre chacun face à ses responsabilités et de sensibiliser fortement nos concitoyens. Il s'agirait, par analogie avec le thème du capital naturel de notre planète mise en danger par la pollution issue de l'activité humaine, de reprendre la notion de capital à préserver.

Chaque homme, et l'humanité dans son ensemble est à la fois détenteur et responsable d'un capital. De même qu'on ne peut pas agir impunément en matière de protection de l'environnement, nous devons être extrêmement vigilants dans notre domaine, à l'égard de toute avancée technologique non maîtrisée comme de toute mise en œuvre de normes nouvelles consenties plus ou moins consciemment, parce que **ce capital de garantie de nos libertés et de notre identité peut alors être amputé ou menacé dans son existence même.**

Et il ne se renouvellera pas précisément en raison du **phénomène d'irréversibilité des effets du progrès technologique.**

Il y a donc là une **situation d'urgence** qu'il s'agit d'exposer à nos concitoyens.