

A S S E M B L É E   N A T I O N A L E

X I I I <sup>e</sup>   L É G I S L A T U R E

# Compte rendu

## Commission des affaires culturelles et de l'éducation

- Audition, ouverte à la presse, de M. Alex Türk,  
président de la Commission nationale de l'informatique  
et des libertés (CNIL) ..... 2
- Présences en réunion ..... 19

Mercredi

2 mars 2011

Séance de 10 heures 30

Compte rendu n° 29

SESSION ORDINAIRE DE 2010-2011

**Présidence de  
Mme Michèle Tabarot,  
*présidente***



## COMMISSION DES AFFAIRES CULTURELLES ET DE L'ÉDUCATION

**Mercredi 2 mars 2011**

*La séance est ouverte à dix heures trente.*

*(Présidence de Mme Michèle Tabarot, présidente de la Commission)*

*La Commission procède à l'audition, ouverte à la presse, de M. Alex Türk, président de la Commission nationale de l'informatique et des libertés (CNIL).*

**Mme la présidente Michèle Tabarot.** Nous avons le plaisir d'accueillir M. Alex Türk, président de la CNIL. Monsieur le président, vous aviez appelé mon attention sur l'action que la CNIL entendait mener pour sensibiliser les jeunes, tout particulièrement en milieu scolaire, à l'usage des technologies de l'information et aux risques d'internet. Cela rejoint nombre des préoccupations de notre Commission au sujet de la révolution numérique ; j'envisage d'ailleurs d'organiser prochainement une table ronde sur les enjeux de l'école numérique.

Nous sommes très attachés à votre institution. De ma part, il s'agit aussi d'un attachement personnel puisque j'ai eu l'honneur d'être membre de la CNIL.

Le numérique imprègne désormais notre jeunesse. Dans un monde où les modes de fonctionnement, les habitudes de travail et les relations aux autres sont bouleversés, les plus fragiles ont particulièrement besoin d'informations et de conseils susceptibles de leur éviter les dérives et les dangers des univers virtuels. Nous avons déjà abordé ces thématiques au sujet de la régulation des contenus audiovisuels sur internet, en entendant le Conseil supérieur de l'audiovisuel. Notre Commission a également créé avec la Commission des lois une mission d'information commune sur les droits de l'individu dans la révolution numérique, dont notre collègue Patrick Bloche est co-rapporteur.

Monsieur le président, vous allez nous présenter ce rôle d'information et de conseil joué par la CNIL auprès des jeunes. J'aimerais que vous évoquiez à ce sujet vos relations avec le monde de l'éducation : dans son plan de développement des usages du numérique à l'école présenté en novembre 2010, le ministère de l'éducation nationale met l'accent sur la sensibilisation aux questions de libertés et de fichiers et sur l'éducation à internet ; comment inscrivez-vous votre propre démarche dans ce cadre ?

**M. Alex Türk, président de la Commission nationale de l'informatique et des libertés (CNIL).** Merci, madame la présidente, de me donner l'occasion de présenter les préoccupations de la CNIL, voire ses angoisses.

La CNIL n'a bien sûr aucun jugement a priori à porter sur les technologies liées au numérique. Seul nous intéresse leur usage : la même technologie peut être utilisée à des fins détestables comme à des fins de progrès. Quels sont, à nos yeux, les grands enjeux du numérique, non seulement pour les jeunes mais pour nous tous ? Notre attention se porte prioritairement sur le développement simultané, et largement conjugué, de quatre technologies : vidéoprotection ou vidéosurveillance, biométrie, géolocalisation, réseau internet.

La vidéosurveillance n'est pas une technique nouvelle. Nous sommes convaincus qu'il en existe des usages intelligents et raisonnables, d'autres inutiles et inefficaces. La loi ayant récemment donné à la CNIL la possibilité d'exercer des contrôles sur l'ensemble du territoire, nous pensons pouvoir présenter chaque année, dans un rapport public, des propositions tendant à harmoniser l'ensemble des systèmes.

Dans ce domaine, notre objectif est l'application effective des lois existantes. Bien souvent, nous découvrons lors de nos contrôles que la mise en place des caméras par le responsable du système ne s'est pas accompagnée de l'organisation de la protection des données personnelles, et, plus largement, des libertés individuelles. Il peut s'agir de la durée de conservation des données, de la fixation des zones placées sous surveillance vidéo, ou encore de la détermination des personnes ayant accès au système. De même, très peu d'élus locaux admettent l'idée, pourtant inscrite dans la loi, que le citoyen doit pouvoir accéder aux images de lui-même prises par un dispositif de vidéosurveillance ; très souvent, ils m'expliquent que cela n'a pas de sens. Pourtant, un citoyen qui a le sentiment d'avoir été pris dans une séquence d'images a bel et bien le droit de demander à vérifier cette séquence – et elle seule ; il appartient au maire de lui en ouvrir l'accès, et de satisfaire son éventuelle demande d'effacement de son image.

On appelle biométrie, en second lieu, l'ensemble des technologies qui permettent d'identifier la personne à partir d'éléments du corps humain. On les voit fleurir aujourd'hui, qu'il s'agisse de reconnaissance à partir de l'œil – la cornée, l'iris, la rétine –, de la main – contour géométrique de la main ouverte, réseau veineux de l'index ou de la paume, empreinte digitale numérisée du doigt... –, de la silhouette, voire – des experts coréens y travaillent – de l'odeur du corps humain. L'inventivité dans ce domaine ne connaît pas de limites.

La loi a fixé un régime spécifique à la biométrie. Elle a d'abord interdit l'installation d'un dispositif de reconnaissance biométrique sans l'accord exprès de la CNIL. En 2004, le législateur a en effet sagement considéré que les éléments intangibles du corps humain devaient faire l'objet d'une protection spéciale.

C'est ainsi, par exemple, que plus de 400 établissements scolaires en France se sont dotés d'un système de reconnaissance biométrique à l'entrée du réfectoire, pour contrôler les allées et venues et le paiement de la cantine. Les premiers chefs d'établissement intéressés voulaient utiliser l'empreinte digitale numérisée des élèves, mais la CNIL s'y est opposée en raison du risque d'une utilisation à l'insu et au détriment des adolescents. Que ferait un établissement de l'empreinte digitale d'un élève une fois que celui-ci l'aurait quitté ? En revanche, nous avons donné notre accord pour l'utilisation de la main ouverte. C'est bien à tort que certains se sont gaussés de cette distinction : la reconnaissance de la main ouverte est celle de sa forme extérieure – une fois le poing fermé, la trace de la main disparaît ; au contraire, la reconnaissance de l'index est celle de son empreinte digitale numérisée. Il est toujours possible d'en récupérer la trace à l'insu de la personne ; je viens moi-même de laisser la mienne sur le micro devant lequel je parle. La CNIL considère qu'il faut, dans chaque cas, utiliser le système le moins intrusif au regard de l'enjeu – lequel n'est pas le même lorsqu'il s'agit de vérifier, à l'entrée du réfectoire, qu'un élève a payé son repas, ou lorsqu'il s'agit d'entrer sur le tarmac de Roissy ou dans un laboratoire où l'on manie des produits hautement toxiques : la CNIL acceptera, dans ces derniers cas, le recours à l'empreinte digitale numérisée. La CNIL applique ce raisonnement à l'ensemble des techniques biométriques.

S'ajoute à cela le fait que les Latins, à commencer par les Français, considèrent que le consentement – d'un salarié dans une entreprise, d'un élève dans un établissement scolaire... – ne peut être que relatif. Comment pourrait-il être « explicite et éclairé », comme le disent les textes, dès lors qu'il est formulé dans le cadre d'un lien de subordination hiérarchique ? C'est la raison pour laquelle, au contraire des Anglo-Saxons, si dans notre analyse des dispositifs biométriques nous intégrons le critère du consentement, nous ne considérons pas que celui-ci « lave tout » : il n'autorise pas à utiliser n'importe quel système.

La troisième technologie, la géolocalisation des personnes et des biens, est celle qui, de très loin, nous préoccupe le plus.

La géolocalisation est d'abord la conséquence indirecte de nos propres décisions : lorsque j'utilise une carte bancaire, un téléphone portable, un passe Navigo ou une carte de télépéage, je me sers d'un instrument qui permettra de me géolocaliser. Mais il s'agit d'une géolocalisation par effet, et non par objet. De même, la biométrie et la vidéosurveillance sont indirectement des outils de géolocalisation.

Mais il existe aussi des instruments de géolocalisation par objet : la géolocalisation des personnes dans le temps et dans l'espace, de façon séquentielle ou continue, en temps réel ou différé, est bien l'objet des puces d'identification par radiofréquences, dite puces RFID (pour *Radio Frequency IDentification*), et des systèmes GPS.

Là encore, si certains usages ne posent pas de difficultés, d'autres méritent une réflexion approfondie. Ainsi, chacun comprend que, pour peu qu'elle s'effectue selon des règles médicales et juridiques strictes et en liaison avec la famille, la géolocalisation de malades atteints de la maladie d'Alzheimer permettra à la fois de venir plus rapidement en aide à ceux qui se trouveraient en situation de vulnérabilité et de les faire bénéficier, dans un périmètre déterminé, d'une autonomie accrue. À l'inverse, nous sommes nettement moins convaincus par l'idée, dans les maternités, de poser un bracelet à la cheville des nourrissons. Notre réflexion n'est pas achevée sur ce point mais les différences entre les deux situations sont notables : la conscience va croissant chez les nourrissons, alors que pour les personnes atteintes de la maladie d'Alzheimer elle va hélas en s'amenuisant, et avec elle l'intrusivité du système ; et pour le nourrisson, l'argument du surcroît d'autonomie ne vaut pas. Un certain nombre de maternités se sont dotées de ce système, avec mise en place d'un périmètre de sécurité de 50 ou 100 mètres. Au vu du nombre de bébés enlevés dans les maternités françaises – 1,6 par an en moyenne de ces dernières années, ce qui, bien sûr, est déjà beaucoup trop, dont un peu plus de 1 – chiffre statistique – retrouvé dans les vingt-quatre heures –, la CNIL estime nécessaire de bien évaluer, au regard de l'enjeu, l'intrusivité de la technique. Par ailleurs, est-il pédagogique de dire à de jeunes mères que, pendant les cinq ou six jours qui suivent la naissance, elles n'auront pas à surveiller leur bébé ? Ne faudrait-il pas au contraire leur expliquer que, sauf cas particulier, à partir du moment où l'enfant est né, elles sont au premier chef responsables de sa sécurité et qu'aucun système ne pourra les remplacer ? Les études menées à l'étranger montrent que si la personne en charge du système a une défaillance, alors il n'y a plus du tout de contrôle.

La CNIL n'exprime pas un désaccord de principe, mais souhaite ardemment que le Parlement engage une réflexion très approfondie sur l'ensemble de la problématique de la géolocalisation. Celle-ci peut en effet donner lieu à des usages contaminants : si les parents s'habituent à l'idée que leur enfant va être surveillé les cinq premiers jours de sa vie, ils ne seront pas étonnés que d'ores et déjà, dans certaines villes de France, des réflexions soient en

cours pour installer des systèmes de géolocalisation dans les crèches. Aux États-Unis, en Californie notamment, il existe des dispositifs de géolocalisation des élèves du primaire et du secondaire pendant toutes les heures de cours. N'est-ce pas oublier que la pédagogie doit permettre à l'enfant d'acquies progressivement son autonomie ? Éduquer, c'est apprendre à l'enfant à gérer sa propre vie, non pas le suivre à la trace. On mesure à travers ces exemples les enjeux considérables auxquels nous devons réfléchir.

Il existe aussi des utilisations absurdes et détestables de la géolocalisation. À Mexico, Madrid ou Rotterdam, des boîtes de nuit proposent à leurs meilleurs clients, les « *happy few* », pour un bénéfice aussi dérisoire que d'entrer avant les autres, l'injection dans le bras d'une puce RFID, de la taille d'un grain de riz cru. Un « rayon vert », paraît-il, permet ainsi non seulement à l'entrée, mais aussi à chaque commande de boisson, d'opérer le prélèvement correspondant sur la carte bancaire. J'attire votre attention sur la manière dont se pratique ce système imbécile : les clients acceptent de se faire injecter dans le bras un corps étranger, au moyen d'une seringue d'un diamètre double de celui d'une seringue classique, et cela non par un médecin ou un infirmier, mais par un vigile. Lors d'un débat sur la chaîne Arte, un chirurgien madrilène m'a dit qu'il lui arrivait de pratiquer une opération pour extraire une puce...

Or si demain, une boîte de nuit française décidait de se doter d'un tel système, la CNIL n'aurait aucunement le pouvoir de l'en empêcher. En effet, si la loi lui a donné un pouvoir d'autorisation en matière de biométrie, elle n'a pas prévu ce genre de cas : en 2004, personne n'avait imaginé que les techniques de géolocalisation se développeraient à ce point.

Enfin, les instruments de géolocalisation qui seront désormais les plus performants et les plus répandus sont les téléphones portables de troisième génération. Après l'ordinateur portable dans les années 1980, le réseau internet dans les années 1990, ils constituent une nouvelle grande étape dans le développement des technologies du numérique. L'utilisateur se sert d'ailleurs souvent du téléphone portable uniquement pour savoir où se trouve la personne à laquelle il s'adresse, celle-ci lui demandant elle-même où il se trouve : fréquemment, la conversation s'arrête là. Cette géolocalisation pour elle-même devrait évidemment être suivie par le développement d'usages nouveaux, notamment en liaison avec le commerce de proximité.

J'en arrive – quatrième technologie – au réseau internet.

Aujourd'hui, aucun utilisateur d'internet ne peut avoir la certitude absolue, quand il quitte le réseau, de ne pas y laisser des informations, sans parler de celles qui ont été confiées à son insu par quelqu'un d'autre. Les dirigeants des grandes sociétés – Éric Schmidt et Larry Page, de Google, ou encore Mark Zuckerberg, le fondateur de Facebook – développent à ce sujet des théories.

Selon Mark Zuckerberg, nous sommes obligés de nous adapter au développement des technologies du numérique ; il faut donc faire évoluer la norme sociale. Dans quelque congrès ou colloque où je me rends, j'entends des Anglo-Saxons, reprenant cette thèse, militer en faveur d'une évolution de nos législations. L'adaptation souhaitée porte essentiellement sur les notions d'identité et de personnalité, c'est-à-dire d'intimité de la personne.

Éric Schmidt part quant à lui du constat que le système ne peut plus garantir la « virginité » – c'est le terme qu'il utilise – de l'identité, c'est-à-dire sa préservation totale ; il en tire la conclusion qu'il faut effectuer un retournement : nous devons désormais considérer que nous vivons sur le réseau des « séquences d'identité », dont les experts américains évaluent la durée à six ou huit ans ; autrement dit, après six à huit ans d'un usage courant du réseau, notre identité est tellement altérée que le droit à un changement d'identité devrait être ouvert.

Lors de la conférence internationale « informatique et libertés » tenue cet automne à Jérusalem, je me suis trouvé croiser le fer avec des Américains, professeurs de droit comme moi, qui développaient le concept de « banqueroute de réputation » : de la même manière qu'une personne surendettée demande la suspension du remboursement de ses dettes, quelqu'un ayant le sentiment que, du fait d'une grave altération causée par l'usage du réseau, son identité a perdu une partie de sa valeur pourrait présenter à un État, dans sa fonction de gestionnaire de l'état-civil, une demande officielle de changement d'identité, pour une nouvelle séquence de quelques années. Autrement dit, faute de pouvoir contrôler le système, on préconise de modifier les concepts d'identité et d'état-civil.

Quant à Larry Page, à partir des concepts de connaissance universelle et d'intelligence artificielle, il développe des thèses intellectuellement séduisantes mais extraordinairement dangereuses. Pour lui, Google a vocation à absorber l'ensemble de la connaissance, y compris sur l'identité des personnes, puis à la redistribuer, notamment aux États. Comme tous les États d'Europe occidentale, notre pays est aujourd'hui largement engagé dans cette réflexion et dans cette logique.

Tous ces développements appellent de la part du pouvoir législatif des réflexions très approfondies.

On voit par ailleurs se profiler pour les années qui viennent quatre évolutions déterminantes.

La première est la concentration des systèmes, comme on la constate à l'aéroport de Roissy, qui va toucher aussi les stades et les gares. Même si cette évolution est légitime, la réflexion sur les changements de comportements collectifs qui en découleront est insuffisante. Aujourd'hui, sont présents à l'aéroport de Roissy le système biométrique de passage automatique des frontières *PARAF*, la vidéosurveillance, le « body scanner », des systèmes d'information permettant aux compagnies aériennes de savoir quel menu – hallal, cachet par exemple – servir à bord à quels passagers, des *no fly lists* interdisant à certains Européens de prendre l'avion pour les États-Unis – la CNIL, en possession d'une copie, ne parvient pas à faire extraire de la liste originale américaine des Européens qui y figurent. Avant 2020 vont s'y ajouter des systèmes de reconnaissance de comportements erratiques. Ces systèmes vidéo, déjà opérationnels dans d'autres pays, permettent de repérer les comportements anormaux en salle d'embarquement, notamment ceux traduisant une nervosité telle qu'elle pourrait poser difficulté pour l'accès à l'avion. Dans les années qui viennent sera également mis en place le système OpTag. Conçu par l'Union européenne, il couple la vidéosurveillance avec une puce RFID intégrée dans le billet de transport : il s'agit – cet objectif est mentionné dans le document de présentation – de permettre aux compagnies aériennes d'identifier les flâneurs dans les galeries commerciales *duty free*, pour les ramener aussi vite que possible dans la zone d'embarquement. En effet, arrivant à l'embarquement avec retard, ces flâneurs provoquent des retards au décollage, la sortie de l'avion du plan de vol, et donc, à l'aéroport d'arrivée, de l'attente avant l'atterrissage avec la consommation supplémentaire de kérosène qui s'ensuit.

Quant aux projets d'équipement des stades dans les trois ans qui viennent – nous sommes aujourd'hui saisis d'expérimentations – ils consistent, pour lutter contre la violence, en un double couplage, d'une vidéosurveillance avec un système de reconnaissance faciale biométrique d'une part, et de cet ensemble avec des puces RFID d'autre part. Couplé avec un système de reconnaissance faciale biométrique, le balayage des tribunes par une caméra signalera tout visage qui a déjà été numérisé, autrement dit tout visage de hooligan déjà répertorié. La puce RFID intégrée dans le billet de stade permettra alors de retrouver la personne.

Je ne conteste pas la nécessité d'utiliser certaines de ces techniques, mais il faut bien comprendre qu'en matière numérique,  $1+1=3$  : la combinaison de certaines technologies aboutit à des dispositifs ultra-performants. Nous devons donc mieux réfléchir à leur usage.

La deuxième évolution concerne la dilution des systèmes, ce qu'on appelle le « nuage numérique ». De puissantes sociétés, dont celles évoquées plus haut, ont installé dans le monde entier des milliers d'entrepôts, sous des formes assez prosaïques – des « fermes numériques » gardées par des vigiles accompagnés de chiens – où des systèmes font tourner en permanence des milliards de données personnelles. Selon de très hauts responsables informatiques des plus grandes sociétés mondiales, dans quelques années plus personne ne saura quel est le statut de chacune de ces données – que j'appelle « déchets infoactifs ». Là aussi, la réflexion est insuffisante.

La troisième évolution est la miniaturisation, autrement dit l'utilisation des nanotechnologies dans les systèmes d'information. Selon tous les experts rencontrés, avant 2020 il sera possible de créer des systèmes capables de voir, entendre et communiquer à distance, et invisibles à l'œil nu. Je ne mets bien sûr nullement en cause de façon globale l'utilisation des nanotechnologies : dans le domaine médical notamment, elles seront à coup sûr à l'origine de progrès fulgurants pour l'humanité. En revanche, si réellement – et je pense qu'avant dix ans, ce sera une réalité – nous devons vivre dans une société où des systèmes disséminés par milliers, dont plus personne ne saura à qui ils appartiennent ni qui les contrôle, nous entendront, nous verront et communiqueront à distance les résultats de leurs constatations, que restera-t-il de notre vie privée, de notre intimité ? Le développement très rapide de ces technologies est extrêmement préoccupant. Si nous pouvons toujours interdire des dispositifs de vidéosurveillance et de biométrie à l'intérieur de nos frontières, en revanche nous serons impuissants face à des milliers de systèmes de géolocalisation devenus invisibles du fait de la miniaturisation.

La quatrième évolution, enfin, est la dématérialisation des systèmes. L'on s'oriente de plus en plus vers ce qu'on appelle l'informatique ambiante, contextuelle : des ingénieurs de très haut niveau nous disent que bientôt, l'informatique ne sera plus palpable ; nous la respirerons comme l'air qui nous entoure, parce qu'elle sera totalement dématérialisée.

Face à ces évolutions, on peut agir sur le plan juridique et sur le plan technologique ; mais nous considérons que l'urgence est avant tout à la pédagogie.

Il nous faut absolument prendre très rapidement des mesures solides pour aider les membres du corps enseignant à traiter l'ensemble de ces problématiques dans leurs cours ; aujourd'hui, ils sont désemparés face aux élèves.

Je me rends régulièrement dans des classes primaires – en CM1 et CM2 – de collège – quatrième et troisième – et de lycée – première et terminale. Les élèves de quatrième que j’ai rencontrés récemment passaient deux heures et demie par jour en moyenne sur Facebook – sans compter le week-end –, sans aucune préparation. Si les parents sont rassurés de savoir leur enfant dans sa chambre plutôt qu’on ne sait où dehors, en réalité, ces enfants se trouvent seuls face à un système devant lequel leurs parents sont dépassés et leurs professeurs désarmés.

La CNIL a consenti un effort budgétaire considérable pour faire face à cet enjeu de société majeur. Il a été longtemps très difficile de faire prendre conscience au ministère de l’éducation qu’il y avait urgence, mais les choses commencent à bouger. Pour notre part, nous avons préparé un guide pratique à l’attention des enseignants, rédigé des brochures à l’intention des élèves. L’ensemble de ces documents a été adressé par dizaines de milliers d’exemplaires à des professeurs et des établissements scolaires. Il s’agissait pour nous d’engager une action de sensibilisation mais, comme nous l’avons clairement exposé au ministère, la CNIL ne dispose pas des ressources financières suffisantes pour la poursuivre chaque année ; c’est à lui désormais de mobiliser les moyens nécessaires.

La solution n’est pas de consacrer un module de formation, parmi d’autres, à ces questions : les jeunes générations vont vivre toute leur vie avec une informatique ambiante, « au bout de leurs doigts », d’un maniement naturel et spontané ; la bonne solution est donc de teinter toutes les disciplines de la préoccupation « informatique et libertés ». Il faut en quelque sorte mettre sur pied une « instruction civico-numérique », s’étendant à tous les domaines actuels de l’enseignement.

Nous devons aussi fixer des règles dans les relations entre les chefs d’établissement, les professeurs et les élèves, faute de quoi les uns ou les autres vont se trouver en porte-à-faux. Il faut également réfléchir à la manière dont on peut protéger les professeurs, ainsi que les élèves les uns par rapport aux autres : il est inconcevable que de jeunes enseignants d’université ou des étudiants puissent avoir le sentiment que leur vie est brisée, en raison du harcèlement dont ils font l’objet sur le réseau.

À ces questions, ce n’est pas à la CNIL qu’il revient d’apporter des réponses. Elle invite le Parlement à s’emparer de toute urgence de ces sujets. Il appartient par ailleurs au ministère de l’éducation de prendre le relais dans les actions à mener auprès des élèves pour qu’ils puissent, tout à la fois, profiter de ce qu’apporte le réseau en termes de dialogue et d’accès à la connaissance, et assurer la préservation de leur identité et de leur intimité – qui, une fois qu’on y a porté atteinte, ne se reconstituent pas.

**M. Michel Herbillon.** Monsieur le président, nous avons été passionnés par votre exposé très brillant et très documenté. Extrêmement préoccupés par les évolutions dont vous avez parlé, nous sommes conscients de l’enjeu majeur que constitue le respect de la vie privée. En vous écoutant, on a envie de demander à Alain Souchon d’actualiser sa chanson *Foule sentimentale* : oh là là, la vie qu’on nous propose... À côté d’aspects très positifs, il en est d’autres qui font froid dans le dos.

Vous militez de longue date en faveur du droit à l’oubli sur internet. Aujourd’hui, lorsqu’un abonné clôture son compte Facebook, cette société reste propriétaire des photos qu’il a insérées sur le web. Pour y remédier, le Sénat a voté une proposition de loi – qui doit venir devant notre Assemblée. Cependant, y a-t-il un sens à ce que la France adopte un texte



au niveau national, alors que, du fait de leur domiciliation à l'étranger, les sociétés concernées par la problématique du droit à l'oubli, comme Facebook ou Google, ne seront pas tenues par les obligations ainsi posées ?

La LOPPSI 2 autorise le filtrage de certains sites internet hors de la décision d'un juge. Comment évaluez-vous ce dispositif au regard des principes fixés par la CNIL ?

Enfin, quelle appréciation portez-vous sur les premiers mois de fonctionnement de la Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet (HADOPI) ? Quelles devraient être selon vous ses interactions institutionnelles avec la CNIL ?

**M. Patrick Bloche.** Nous nous réjouissons d'autant plus de cette audition que sur tous les bancs de l'Assemblée, nous avons dû nous mobiliser en ce début d'année pour dire tout notre attachement à l'action de la CNIL, préserver son originalité ainsi que son actuelle présidence par le parlementaire que vous êtes, monsieur le président.

Vos réflexions nous conduisent à cette question : que faire ?

En matière de géolocalisation, que peut-on faire, par exemple, à l'égard de la RATP qui, alors qu'elle devrait veiller à l'anonymisation des données, réclame sans le dire un supplément de cinq euros aux usagers qui souhaitent disposer d'un passe anonyme ? Ce passe anonyme – qui du reste ne s'appelle pas « Navigo », mais « Découverte », est principalement destiné aux touristes. Une grande entreprise comme la RATP ne devrait-elle pas, dans un tel domaine, être exemplaire ?

La ministre alors en charge du numérique, Mme Nathalie Kosciusko-Morizet, avait pris l'initiative d'une charte sur le droit à l'oubli. Or deux acteurs majeurs du secteur, Google et Facebook, ne l'ont pas signée. Même si nous sommes conscients des difficultés techniques de mise en œuvre d'un droit à l'oubli absolu, avec effacement total des données personnelles, cette attitude concorde avec la description que vous avez faite de l'état d'esprit des dirigeants de ces sociétés. L'argument de la transparence absolue, mis en avant notamment par M. Schmidt, n'est-il pas un prétexte pour dessiner tranquillement les profils comportementaux des internautes et faire de ceux-ci des cibles idéales de publicité ?

L'Union européenne envisage-t-elle de faire évoluer la législation en ce domaine ? Aux États-Unis, l'approche est très différente de celle qui prévaut en Europe, notamment en France depuis la loi « Informatique et libertés » du 6 janvier 1978. Lorsque, à l'occasion d'un déplacement avec les membres de la mission d'information sur les droits de l'individu dans la révolution numérique, j'ai exposé à nos amis américains que le fait de cibler des publicités à partir des données personnelles laissées sur le réseau était une atteinte à la vie privée, ils ont répondu que les internautes ainsi démarchés avaient ainsi l'opportunité de bénéficier d'avantages commerciaux... Plutôt que comme un citoyen, l'internaute est considéré aux États-Unis comme un consommateur, la régulation étant assurée par le marché.

Au-delà d'un effort d'éducation aux médias, présent depuis longtemps – je pense aux débats sur la violence à la télévision – la loi ou le règlement ne devraient-ils pas instaurer des contraintes d'information au profit des internautes, notamment les plus jeunes ?

Enfin, quand aurons-nous connaissance de l'avis de la CNIL sur le volet pénal de la HADOPI ? Pouvez-vous nous en dévoiler quelques éléments ?

**Mme Marie-George Buffet.** Merci, monsieur le président, pour la qualité de votre exposé et le travail réalisé à la présidence de la CNIL. Nous devons nous mobiliser afin que cette institution dispose des moyens nécessaires pour répondre aux enjeux que vous avez présentés. Vos propos peuvent faire peur, mais ils doivent surtout amener les élus de la Nation que nous sommes à élaborer une législation susceptible au moins de freiner la volonté de grands groupes de transformer les citoyens en consommateurs, en allant jusqu'à leur faire perdre leur identité. Comment la législation peut-elle contribuer à limiter les mauvais usages de l'informatique ?

En ce qui concerne la géolocalisation, qu'attendez-vous de la loi ?

Quelles réponses le ministère de l'éducation nationale apporte-t-il à votre demande que la thématique de l'informatique et des libertés traverse l'ensemble du spectre de l'enseignement ?

Enfin, êtes-vous satisfait des moyens, notamment humains, mis à la disposition de la CNIL ? Pensez-vous qu'il conviendrait de les élargir ?

**M. Daniel Spagnou.** Le département dont je suis l'élu compte 200 maires, dont 195 dirigent des communes de moins de 500 habitants. En réponse à un questionnaire que je leur ai adressé en ma qualité de président de leur association, ils ont placé parmi les cinq formations prioritaires qu'ils souhaitaient recevoir dans le courant de l'année une information sur la CNIL et l'application sur le terrain des mesures de garantie dont elle a la charge. Ils sont très inquiets et soucieux de bien faire. Des spécialistes pourraient-ils venir sur place assurer ces formations ? Une action ne pourrait-elle pas être organisée à l'échelle nationale, en lien avec l'Association des maires de France ?

**M. Marcel Rogemont.** Que faire ? Telle est la question, comme l'ont dit mes collègues, que nous devons nous poser. Quant à la CNIL, monsieur le président, que fait-elle ?

A-t-elle procédé à une analyse qualitative des nombreuses plaintes – plusieurs milliers – qu'elle reçoit chaque année ? Quelles réponses y a-t-elle apportées ? Pourriez-vous nous transmettre ces éléments ?

L'Allemagne a, semble-t-il, obtenu que les maisons visibles sur *Google Street View* puissent être rendues floues. Pour quelles raisons la France n'a-t-elle pas réussi à encadrer au préalable les caractéristiques de certains nouveaux services de Google ?

Pour la HADOPI, une adresse IP n'est pas une donnée personnelle ; que pensez-vous de cette position ?

Au niveau européen, un comité d'experts vient d'être constitué. J'ai cru comprendre qu'il comportait quatre Américains. Est-ce à dire que le Groupe des « CNIL européennes », dit G 29, que vous avez présidé pendant deux ans, a d'ores et déjà opté pour une conception de l'internaute sous l'angle du commerce, plutôt que comme citoyen ?

Quelles sont les réflexions de la CNIL sur le recueil du consentement éclairé de l'internaute pour l'utilisation des données le concernant ?

Enfin, face à l'essaimage des systèmes, l'éducation ne sera-t-elle pas toujours en retard ?

**M. Jacques Groperrin.** On a parlé des chefs d'établissement, des enseignants et des élèves, mais ne faut-il pas également assurer la sensibilisation des parents ?

Par ailleurs, à l'instar de ce qui se fait pour certains films, ne pourrait-on examiner avec les constructeurs d'ordinateurs ou d'outils informatiques la possibilité que des bandeaux d'alerte s'affichent à l'ouverture du système ?

**Mme Monique Boulestin.** La CNIL a effectué plusieurs contrôles auprès des principaux réseaux sociaux français. Dans votre rapport d'activité 2009, vous notiez que les personnes ne faisant pas partie du réseau ne sont pas toujours informées lorsqu'elles sont identifiées sur une photo de groupe, et par ailleurs que les mesures de protection des mineurs sont parfois inexistantes. Récemment, vous avez lancé un plan d'urgence à destination du monde de l'éducation pour sensibiliser au bon usage des nouvelles technologies et à la protection de la vie privée sur internet.

Cependant, malgré tous vos efforts, nous sommes régulièrement alertés d'utilisations frauduleuses de données personnelles. Une jeune femme a ainsi découvert que depuis deux ans, à partir de ses photos, une autre personne s'était inventé une vie. D'autres exemples montrent que tout un chacun peut être la cible d'actes malveillants.

Or le vol d'identité numérique est reconnu depuis peu comme un délit. Usurpation d'identité, vol d'identité : quelle est la position de la CNIL sur le fait que des clichés puissent être répandus sur des forums, à l'insu de la personne et sous un autre nom ? Pour vous, une nouvelle loi est-elle nécessaire ? Et surtout, que pouvons-nous faire au niveau européen ?

**M. Alain Marc.** L'information de la jeunesse doit être assurée dans le cadre scolaire, mais la distribution d'une documentation est souvent inopérante. L'essentiel passe par les enseignants, dont il faut donc assurer la formation. Comment faire pour que chaque enseignant soit bien conscient qu'il doit aiguïser l'esprit critique des élèves et les alerter sur les risques de l'outil informatique ?

**M. Pascal Deguilhem.** En juillet dernier, le Conseil d'État a invalidé sur plusieurs points les fichiers « Base élèves » et BNIE (Base nationale des identifiants des élèves). Où en est-on ? Quel regard la CNIL porte-t-elle sur ces fichiers ?

**Mme Marie-Josée Roig.** Le guide « Informatique et libertés » que vous avez établi à destination de l'enseignement du second degré met à juste titre l'accent sur la nécessaire sensibilisation des jeunes, souvent bien inconscients des répercussions des activités auxquelles ils se livrent sur internet avec les réseaux sociaux et les blogs. Comment ne pas s'émouvoir que des jeunes soient invités à noter leurs professeurs ? Ou encore que des passages à tabac soient filmés en cour de récréation pour être ensuite mis en ligne ?

Certains de ces actes ont des conséquences pénales, sans que leurs auteurs en aient conscience. Quelles actions de sensibilisation pourriez-vous mener, éventuellement en partenariat avec les autorités de police, auprès des parents et du jeune public ?

**Mme Françoise Imbert.** Comment mettre fin au développement des spams dans le courrier électronique ? Existe-t-il des solutions juridiques ?

Concernant la sécurité des systèmes informatiques, où en est-on de la protection contre le piratage ?

**Mme Sophie Delong.** La presse a révélé que les préfetures, par le biais des données individuelles figurant sur les cartes grises, ont permis aux constructeurs automobiles d'établir le profil des consommateurs. Quels sont les dysfonctionnements qui ont abouti à cette situation ? Comment peut-on y remédier – afin que chacun de nos concitoyens ne soit pas regardé avant tout comme un consommateur ?

**Mme Martine Martinel.** Pour participer à des conseils d'administration de collège, j'entends souvent les discours enthousiastes des chefs d'établissement sur la mise en place d'espaces numériques de travail (ENT), mais les problèmes que vous avez abordés sont rarement évoqués. Certes le guide que vous avez établi est de qualité, mais sa lecture est un peu difficile et je n'en avais pas encore entendu parler sur le terrain ; quels sont les partenariats et les moyens mis en œuvre pour veiller à la protection des droits ?

**M. Lionel Tardy.** Nous avons tous compris votre appel concernant le partenariat avec l'Éducation nationale.

Le Gouvernement vient de lancer le projet Etalab, portail unique pour la réutilisation des données publiques de l'État et des collectivités locales. Quel rôle la CNIL peut-elle jouer dans ce domaine ? Êtes-vous associés à ce projet et aux démarches touchant à la réutilisation des données publiques ?

Que pensez-vous d'une éventuelle fusion entre la CNIL et la CADA (Commission d'accès aux documents administratifs) ? Dans le rapport de la mission sur les autorités administratives indépendantes (AAI), à laquelle j'ai participé, nos collègues Vanneste et Dosière, rapporteurs, ont préconisé des rapprochements. Quelle est la position de la CNIL ?

**Mme Marie-Odile Bouillé.** Les espaces numériques de travail (ENT) se développent dans les établissements scolaires, mais la mise en place d'une charte de l'utilisation de ces outils informatiques, d'une part, et la désignation d'un correspondant « Informatique et libertés » au sein de l'établissement, d'autre part, sont actuellement facultatifs. Au regard de la place grandissante de l'informatique et des dérives constatées, ne faudrait-il pas rendre obligatoires ces deux dispositifs ?

**M. Hervé Féron.** Monsieur le président, vous avez à plusieurs reprises réduit les pouvoirs de la CNIL, sous prétexte d'un manque de moyens financiers et humains. Par exemple, la loi a retiré à la CNIL le pouvoir de bloquer la mise en œuvre de fichiers dits de sûreté, mais lui a accordé un pouvoir de sanctions. Il en résulte que des fichiers policiers sont avertisés sans tenir compte des remarques de la CNIL. De même, vous avez procédé à de nombreuses simplifications des procédures pour les déclarations de fichiers – dont les entreprises profitent aujourd'hui – au motif que vous n'aviez pas les moyens de procéder aux contrôles. Pourquoi en dix-huit ans n'avez-vous pas, en tant que parlementaire, déposé une proposition de loi visant à doter la CNIL des moyens humains et financiers nécessaires à l'accomplissement de ses missions ? Cela ne peut pas être pour éviter le mélange des genres, puisque vous avez par ailleurs voté les lois HADOPI et LOPPSI.

Ce manque de moyens et de volonté pour garantir les libertés publiques aboutit à une impunité dans les faits : trop peu d'affaires sont portées devant le parquet, tant par rapport au nombre de plaintes qu'en comparaison des autres pays européens.

Par ailleurs, où en est-on dans les suites de l'enquête de la Cour des comptes sur la gestion de la CNIL ? La Cour a considéré que la pratique de la CNIL n'offrait pas une

« présentation objective et rigoureuse de ses missions » et était « dépourvue d'un cap clair ». Elle a également contesté les indemnités que vous avez perçues, non pas au regard du travail effectué, mais quant à la procédure. Comment ferez-vous pour les prochains exercices ?

Enfin, on se souvient d'Ali Soumaré, tête de liste socialiste dans le Val-d'Oise aux élections régionales de mars dernier, qui avait été accusé par deux maires UMP d'être un « délinquant récidiviste ». Leur source était le fichier STIC, voire CASSIOPEE. Pourquoi la CNIL a-t-elle mis cinq jours pour intervenir alors que la situation était urgente et que la procureure de Bobigny, elle, est intervenue tout de suite ? Est-ce parce que l'un des maires, Francis Delattre, est un ex-commissaire de la CNIL ? Un an après les faits, où en est l'enquête ?

**Mme la présidente Michèle Tabarot.** Monsieur Féron, votre intervention est réellement déplacée. L'exposé de M. Türk a été salué par tous nos collègues, je regrette que vous ayez gâché la tonalité de cet échange.

La parole est à Mme Marietta Karamanli, qui a rejoint notre commission et à qui j'ai le plaisir de renouveler mes souhaits de bienvenue.

**Mme Marietta Karamanli.** J'ai été stupéfaite de constater qu'un certain nombre d'établissements scolaires, et donc d'équipes administratives, n'appliquent pas du tout le droit à l'oubli et ne savent pas toujours comment procéder. Il me paraît important d'assurer non seulement la formation des enseignants, mais aussi celle des personnels administratifs.

Par ailleurs, monsieur le président, vous avez évoqué les recommandations de la CNIL mais renvoyé au Parlement et au Gouvernement le soin de prendre les initiatives. Il en est cependant une que vous pouvez prendre : à l'occasion de la sortie de votre guide, avez-vous saisi officiellement le président de l'Assemblée nationale et le président du Sénat ? Quant au ministre de l'éducation nationale, a-t-il répondu à l'ensemble de vos recommandations ? Madame la présidente, permettez-moi d'ailleurs de vous suggérer que nous auditionnions le ministre à ce sujet.

**Mme Colette Langlade.** La fiche n° 12 du guide « Informatique et libertés » est intitulée « Communication à des tiers autorisés d'informations relatives aux personnels et aux élèves ». Elle rappelle que la loi permet à des autorités publiques de se faire communiquer, dans le cadre de leurs missions et sous certaines conditions, des informations issues de fichiers. Elle rappelle ensuite que de façon générale, un établissement scolaire ne peut communiquer à des tiers des informations nominatives relatives à ses personnels, aux représentants légaux des élèves mineurs ou aux élèves majeurs. Puis elle explique que la communication par un établissement, à des « tiers autorisés », de renseignements sur ses personnels et ses élèves « ne peut être effectuée que sur demande ponctuelle écrite ». Cependant il est indiqué dans la phrase suivante que « l'établissement n'est pas tenu de répondre à une simple demande téléphonique », ce qui signifie qu'il a la faculté d'y répondre : n'y a-t-il pas là une contradiction ?

Dans la fiche n° 16, relative à la commission locale informatique et libertés (CLIL), on peut lire, s'agissant de la composition de la commission, que parmi les membres de droit devrait figurer, outre le proviseur, l'administrateur du réseau informatique ; et par ailleurs, que le correspondant informatique et libertés peut être chargé d'animer cette commission. Quels sont les résultats de vos échanges avec le ministre de l'éducation nationale à ce sujet ? Comment les membres de ces commissions seront-ils rémunérés ? S'agira-t-il de professeurs ou d'autres personnels ?

**M. Michel Pajon.** Monsieur le président, j'ai eu grand plaisir à vous écouter, et j'ai beaucoup appris. À quoi attribuez-vous l'intérêt pointilleux, pour ne pas dire l'acharnement, dont vous semblez faire l'objet de la part de la Cour des comptes ? L'indépendance dont jouit l'autorité administrative que vous présidez serait-elle en cause ?

**M. Alex Türk.** Étant donné le nombre de questions, permettez-moi d'y répondre en les regroupant par thèmes et, sur certains points précis, de compléter ultérieurement mon propos par des réponses écrites.

Premier thème abordé : le droit à l'oubli.

Au niveau national, la proposition de loi Détraigne-Escoffier, adoptée par le Sénat, permet d'avancer. Je crois savoir qu'une réflexion est menée à l'Assemblée nationale dans le même esprit. Nous espérons donc que ce dossier va aboutir.

Mais l'élément déterminant sera la directive européenne. Le débat est engagé, tous les jours des collaborateurs de la CNIL participent aux réunions à Bruxelles. En ce qui concerne le comité d'experts, voici ce qui s'est passé : il y a un peu plus d'un an, alors que je présidais le groupe des 27 « CNIL » européennes, la Commission européenne m'avait demandé de désigner l'un des cinq membres d'un groupe de travail chargé de réfléchir à la directive ; j'ai désigné mon vice-président de l'époque, le président de la « CNIL » néerlandaise. J'ai appris ensuite à l'occasion d'une réunion à Barcelone, dans un couloir, que les quatre autres membres étaient américains. Particulièrement mécontent, je suis allé voir M. Fillon, Premier ministre, ainsi que M. Barrot, vice-président de la Commission, qui tous deux ont immédiatement réagi. Le groupe a été dissous. Dans cette affaire, je ne critique pas les Américains, mais les Européens : il m'avait paru invraisemblable – et c'était un fonctionnaire français qui en avait eu l'idée – qu'ils puissent demander à quatre Américains de réfléchir au droit européen ! M. Obama chargerait-il des Européens de proposer une législation pour les États-Unis ?

Il reste que la plupart des problèmes ne trouveront leur solution qu'au niveau international. Actuellement, les pays dotés d'une loi protectrice des personnes à l'égard du traitement des données ainsi que d'une autorité chargée de veiller à cette protection représentent moins de 500 millions d'habitants. Les États-Unis, la Russie, la Chine, l'Inde, le Japon n'en font pas partie. Néanmoins, la réunion à Madrid, en novembre 2009, de la cinquantaine de « CNIL » existant dans le monde a abouti au « processus de Madrid » : ces autorités se sont mises d'accord sur des principes. Pour qu'ils soient inscrits dans le droit positif, il faut évidemment que le relais soit pris par les pouvoirs publics, à commencer par les Parlements nationaux. C'est la raison pour laquelle j'ai été auditionné par la Commission des affaires économiques de votre Assemblée, où une proposition de résolution a été déposée – proposition de résolution de M. Patrick Ollier et plusieurs de ses collègues *visant à apporter le soutien de l'Assemblée nationale à l'élaboration d'une convention internationale relative à la protection de la vie privée et des données personnelles* – ainsi que par les commissions compétentes du Sénat, où il en a été de même. Permettez-moi d'insister pour que le sujet soit inscrit à l'ordre du jour, de telle manière que le Gouvernement soit lui-même saisi, à l'instar de ce qui s'est passé en Allemagne et en Espagne. Si les Gouvernements français, allemand et espagnol poussaient ensemble l'Union européenne à agir, on peut imaginer que celle-ci se saisirait du sujet et se tournerait vers prioritairement vers les États-Unis et la Chine pour les convaincre de la nécessité d'une régulation. En disant cela, je réponds aussi à la question sur les *spam* – dont la résolution suppose d'agir au niveau international.

Il faut maintenant, donc, donner une valeur juridique contraignante à des principes dont nous, autorités de protection, n'avons pu que définir le contenu : tel est le volet juridique de la réponse à apporter aux problèmes actuels, à côté du volet pédagogique et du volet technologique.

Mais il existe une différence de fond entre la conception européenne – de « l'internaute » – et la conception américaine – du « client ». À ce client, je souhaite qu'on donne au moins les droits d'un consommateur : il faut ramener la relation entre Google ou Facebook et l'individu sur un terrain juridique connu, celui du droit de la consommation. Les Américains considèrent que les données personnelles peuvent être analysées comme un bien marchand, alors que dans la logique européenne, issue du droit latin, ces données sont un attribut de la personnalité. Ces deux systèmes juridiques sont, en réalité, intellectuellement incompatibles. Les Américains considèrent l'identité comme une variable et la personnalité comme une constante, alors que nous faisons le contraire : les Européens considèrent que l'identité est intangible ; elle est le socle sur lequel nous exprimons notre personnalité qui, elle, évolue. Aux États-Unis, on admet l'idée de « séquences d'identité », ce qui signifie que l'identité n'est pas considérée comme un socle intangible ; quant au fait de ne pas reconnaître le droit à l'oubli, il signifie qu'on dénie à quelqu'un la capacité d'évoluer cours de sa vie. Dans la conception européenne, l'identité est intangible – et elle doit l'être également sur les réseaux ; en revanche, on juge légitime que chacun puisse évoluer.

Bien entendu, le droit à l'oubli ne veut pas dire l'absence de responsabilité : celui qui a prononcé des paroles diffamatoires doit les assumer, de même que la trace d'actes répréhensibles peut être conservée dans le casier judiciaire. En revanche, on ne peut pas admettre que des données, par exemple des photos, soient utilisées à l'insu de la personne. Le droit à l'oubli me paraît donc pouvoir se développer, avec plus de circonspection lorsqu'il s'agit d'informations fournies par la personne elle-même pour des informations données à son insu. Il faut considérer ce droit à l'oubli comme une méthode permettant de « limiter la casse » dans un domaine qui n'a jamais fait l'objet d'une réflexion juridique approfondie – le réseau étant une sorte de *no man's land* entre la vie privée et la vie publique.

Dans les établissements scolaires – où il faut de même expliquer le statut des SMS envoyés sur les téléphones portables, à mi-chemin entre l'oral et l'écrit –, il faut réapprendre aux élèves le sens du mot « intimité ». Il faut leur dire qu'elle est un bien sacré, qu'il convient de protéger. Cela signifie que le citoyen doit avoir droit à l'opacité : il ne faut pas que le pouvoir voie en lui ou à travers lui. Or ses deux éléments d'opacité sont l'identité – d'où la volonté de beaucoup de pays africains de créer un système d'identité, car il n'y a pas de citoyenneté sans identité – et l'intimité, cette carapace invisible qui protège de l'extérieur. Le travail de pédagogie est urgent ; pour notre part, nous y contribuons notamment à travers les « rencontres régionales » que nous organisons, ainsi qu'à travers les informations que nous mettons sur notre site.

J'ai voté la loi HADOPI, mais comme chacun des membres de la CNIL, j'étais déchiré. La CNIL elle-même ne s'est exprimée ni pour, ni contre puisqu'elle ne fait qu'émettre des avis circonstanciés. Sur le fond, nous avons une très grande inquiétude sur un point précis : le fait que la HADOPI ne considère pas l'adresse IP comme une donnée personnelle est à nos yeux une catastrophe. Dans les pays des vingt-six autres autorités, il n'y a aucun doute sur le sujet. Remettre en question ce principe, c'est enlever à la protection des données personnelles un de ses piliers. Je suis en train d'entrer en relation à ce sujet avec Mme Marais, présidente de la HADOPI. On fait référence à un arrêt de la Cour de cassation qui, à notre sens, n'a pas tranché la question. Il y a là un enjeu considérable pour nous.

En ce qui concerne le passe Navigo, le dialogue que nous avons eu avec la RATP a été jusqu'à présent infructueux. Nous considérons qu'il n'est pas normal de devoir payer pour préserver son anonymat. Pour nous, chacun devrait pouvoir choisir entre un passe donnant certains avantages mais assorti d'une géolocalisation et un autre offrant moins d'avantages et dépourvu des mêmes effets géolocalisants. Nous désapprouvons le fait qu'il faille payer cinq euros pour rester – comme cela devrait être naturel – incognito.

La charte sur le droit à l'oubli, qui n'a pas été signée par les grands groupes, ne l'a pas été non plus par la CNIL. Nous ne voulons pas en effet d'une charte dont les signataires ne prendraient pas l'engagement de se doter de correspondants Informatique et libertés.

S'agissant du contenu de la législation nécessaire en matière de géolocalisation, la question du consentement est évidemment au cœur du problème. Il en va de même pour les réseaux, avec le débat sur le système *opt-in, opt-out*. Je suis très choqué que *Street View* puisse introduire dans le système des références concernant l'habitation d'une personne sans avoir recueilli son consentement. Pour l'entrée dans le système, le consentement doit être nécessaire. À l'étape suivante, il faut assurer la transparence – c'est-à-dire l'information : quand je suis dans le système – Facebook ou Google par exemple –, je dois disposer de l'information relative à l'usage fait par le système des données que je lui ai confiées. Enfin, au sortir du système, il faut assurer un droit à l'oubli – droit non absolu, mais relatif, qu'il convient de définir. En respectant ces règles – consentement, information, oubli –, on arrive à une relation quasi-contractuelle. À défaut de l'un des trois éléments, la construction est bancal.

Or aujourd'hui, les grandes sociétés américaines ne reconnaissent pas l'applicabilité du droit européen en Europe. Il n'y a pourtant pas de raison que nous Européens supportions d'être soumis au droit du comté de Santa Clara en Californie pour les problèmes que nous pouvons avoir avec Google ou Facebook, alors qu'une société française ou allemande aux États-Unis est soumise au droit américain. L'Union européenne doit avoir le courage politique de résoudre cette question avec les États-Unis. La situation actuelle pose également problème au regard de la concurrence : elle a abouti à la création de deux mastodontes, en face desquels les acteurs européens ont bien du mal à exister.

Quelles sont les réponses du ministère de l'éducation nationale à nos demandes ? Il a fallu un peu de temps, mais les choses commencent à bouger. Le ministère perçoit l'ampleur de la tâche : il faut à la fois former les enseignants, préciser le rôle des chefs d'établissement, établir des liens avec les parents...

Les moyens de la CNIL ont été considérablement développés : alors que nous étions 70 quand je suis arrivé à la présidence, nous serons 160 dans quelques semaines ; le budget a également beaucoup progressé. Sans être dans le peloton de tête européen – l'autorité allemande compte 400 personnes, l'anglaise 240 –, notre institution est vraiment opérationnelle. Nous avons mis en place ces jours-ci une quatrième direction, dite de l'innovation et de la prospective, ainsi que des budgets autonomes de recherche. En effet le temps démocratique de l'élaboration du droit est toujours plus long que le temps du développement technologique.

Dans les établissements scolaires, nous croyons beaucoup au rôle des correspondants Informatique et libertés. La formule se développe fortement dans les collectivités locales et les entreprises ; on en est à plus de 7000 en France. En revanche l'administration centrale est rétive – et nous espérons qu'elle évoluera. Nous sommes également favorables aux



commissions locales Informatique et libertés – qui pourraient rendre de très grands services à l'intérieur des établissements scolaires. Actuellement, il n'en existe qu'une – sur 10 000 établissements ; une autre a disparu parce que le proviseur a changé d'affectation. Cette formule permet à tous – élèves, professeurs, parents d'élèves, rectorat... – de réfléchir ensemble et de retenir les meilleures solutions.

Le guide à destination des collectivités locales est prêt. Nous sommes en train de passer avec l'AMF une convention qui devrait permettre à chaque maire de le recevoir au mois de juin.

Je ne répondrai pas à la question sur la fusion entre la CNIL et la CADA, par déontologie. Il revient au Parlement de décider.

La question sur les constructeurs d'ordinateurs me fait revenir sur le volet technologique de la réponse à apporter aux problèmes actuels, c'est-à-dire à l'utilisation de la technologie pour juguler les effets néfastes de la technologie – selon le concept de *Privacy by Design*, protection des données et de la vie privée dès la conception de nouvelles technologies. Tous les ingénieurs nous disent que c'est possible ; le problème est celui du financement : les grandes sociétés aptes à financer les recherches n'ont pas forcément intérêt à le faire.

En ce qui concerne le contrôle sur les réseaux sociaux et la lutte contre les utilisations frauduleuses, il faut savoir que tout le monde n'est pas d'accord. En France même, certains journalistes déclarent que le fait de mettre sur le réseau des informations sur une autre personne relève de la liberté d'expression. Pour ma part, je suis outré par ce type de comportement. Le Parlement devrait réfléchir également à cette question, vitale pour les années à venir.

En Allemagne, on ne réagit pas nécessairement plus vivement qu'en France : s'agissant de *Google Street View*, la CNIL, saisie à la suite de plaintes, a fait un contrôle sur place ; la procédure interne suit son cours et dans une quinzaine de jours, la CNIL rendra publique sa première prise de position contentieuse.

Je rappelle par ailleurs que nous contrôlons tous les fichiers de police. Notre contrôle du STIC (Système de traitement des infractions constatées) a duré un an. Tous les jours, les membres magistrats de la CNIL se rendent au ministère et dans les commissariats pour procéder à des contrôles de droit d'accès – mais les demandes de nos concitoyens s'étant multipliées, il peut y avoir un peu de retard.

Dans l'affaire Ali Soumaré, nous sommes intervenus aussi vite qu'il était possible pour nous : en jours francs, au bout de quarante-huit heures. Nos contrôleurs passant leur temps à sillonner la France, il a fallu rappeler une équipe. Nous avons rendu publiques les constatations qui ont été faites ; il s'est avéré que le problème relevait moins du ministère de l'intérieur que du tribunal de Bobigny – et Mme le procureur a traité le sujet avec nous.

S'agissant du contrôle de la Cour des comptes, le rapport définitif va sortir ces jours-ci. Une grande partie de ce qui avait été initialement affirmé a été retirée. Pour ma part, lorsque j'ai été convoqué devant la quatrième chambre, j'ai clairement dit que si on m'avait demandé mon point de vue, je l'aurais donné. Alors que va sortir chez Odile Jacob dans trois semaines le livre de 270 pages que je consacre à l'ensemble de ces problématiques, je n'ai pas bien compris les reproches qui m'étaient adressés quant à une absence éventuelle de vision

stratégique ! Il est vrai que le contrôle a eu lieu pendant le mois d'août, époque de l'année où la CNIL n'est sans doute pas la plus performante... Le rapport définitif de la Cour nous donne acte des réponses que nous avons apportées.

Sachez enfin qu'en ce qui concerne les indemnités, le président de la CNIL n'est pas seul en cause : tous les membres de la CNIL, et même ses anciens membres, sont visés. Le problème vient de ce que le fonctionnement financier de la CNIL n'a pas été révisé depuis douze ans. J'ai en conséquence demandé à notre direction financière de prendre contact avec Matignon pour obtenir des revalorisations ; mais, semble-t-il, je n'ai pas choisi la bonne procédure juridique. De manière à ne pas être attaqué, j'ai remboursé, en souscrivant il y a quelques semaines un prêt bancaire, les 52 000 euros correspondant aux trois années d'indemnités que l'on me reproche. Et maintenant, la Cour des comptes me demande de poursuivre mes collègues et les anciens membres de la CNIL qui ont pu bénéficier du même système ! Il ne me paraît pourtant pas aberrant qu'un collègue qui se lève à 5 heures du matin pour aller travailler une journée entière à Lyon touche 221 euros... Quant au reproche que l'on m'a fait d'avoir un déjeuner par semaine au titre de mes activités de président, chacun en jugera. Il en inquiète d'autres... Mais je réduis encore le nombre de déjeuners !

**Mme la présidente Michèle Tabarot.** Monsieur le président, tous nos remerciements pour cette matinée passionnante.

*La séance est levée à douze heures trente.*



### **Présences en réunion**

#### **Réunion du mercredi 2 mars à 10 heures 30 :**

*Présents.* - Mme Marie-Hélène Amiable, M. Pierre-Christophe Baguet, M. Eric Berdoati, M. Marc Bernier, M. Patrick Bloche, Mme Marie-Odile Bouillé, Mme Monique Boulestin, M. Bruno Bourg-Broc, Mme Marie-George Buffet, M. Édouard Courtial, M. Bernard Debré, M. Pascal Deguilhem, Mme Sophie Delong, M. François Deluga, M. Bernard Depierre, M. Marc Dolez, Mme Marianne Dubois, M. Yves Durand, M. Gilles d'Ettore, Mme Martine Faure, M. Hervé Féron, M. Sauveur Gandolfi-Scheit, M. Jacques Groperrin, M. Michel Herbillon, Mme Sandrine Hurel, Mme Françoise Imbert, Mme Jacqueline Irles, Mme Marietta Karamanli, M. Christian Kert, Mme Colette Langlade, Mme Geneviève Levy, M. Apeleto Albert Likuvalu, M. Alain Marc, Mme Jeanny Marc, Mme Martine Martinel, M. Gilbert Mathon, M. Jean-Philippe Maurer, M. Michel Pajon, M. Jean-Luc Pérat, M. Franck Riestler, M. Jean Roatta, M. Marcel Rogemont, Mme Marie-Josée Roig, M. Daniel Spagnou, Mme Michèle Tabarot

*Excusés.* - Mme Sylvia Bassot, Mme Joëlle Ceccaldi-Raynaud, M. Jean-François Copé, M. Guy Delcourt, Mme Jacqueline Farreyrol, M. Gérard Gaudron, Mme Françoise Guégot, M. Yvan Lachaud, Mme Françoise de Panafieu, M. Patrick Roy, Mme Marie-Hélène Thoraval

*Assistaient également à la réunion.* - Mme Pascale Crozon, M. Lionel Tardy