ASSEMBLÉE NATIONALE

XIII^e LÉGISLATURE

Compte rendu

Commission des affaires économiques

Mardi
14 septembre 2010
Séance de 16 heures 15

Compte rendu n° 82

SESSION EXTRAORDINAIRE DE **2009-2010**

Présidence de M. Patrick Ollier
Président

ASSEMBLÉE NATIONALE

La Commission a entendu **M. Alex Türk, président de la CNIL**.

M. le président Patrick Ollier. Nous avons le grand plaisir de recevoir M. Alex Türk, sénateur et président de la Commission nationale de l'informatique et des libertés – créée, je ne l'oublierai jamais, à l'époque où j'étais au cabinet d'Alain Peyrefitte. Très régulièrement, nous recevons les présidents des autorités administratives indépendantes dont l'activité entre dans le champ de compétences de notre commission, la surveillance de ces autorités relevant des missions de contrôle exercées par le Parlement.

Vous êtes, monsieur le président, l'un des mieux placés pour éclairer la représentation nationale sur la problématique de la protection des données personnelles, sujet qui suscite un vrai débat au sein de la Commission des affaires économiques. Ces derniers mois ont été marqués notamment par des interrogations sur la géolocalisation, sur la constitution de fichiers informatiques par l'État ou encore sur le droit à l'oubli sur internet. Sur certains de ces sujets, des dispositions législatives figurent dans la proposition de loi « visant à mieux garantir le droit à la vie privée à l'heure du numérique » qui a été adoptée le 23 mars dernier par le Sénat.

M. Alex Türk, président de la Commission nationale de l'informatique et des libertés (CNIL). Merci de me donner l'occasion de faire le point sur notre activité.

Beaucoup de questions se posent à nous désormais dans le domaine économique. C'est assez nouveau : avant la loi du 6 août 2004 – qui a réformé celle du 6 janvier 1978 –, l'activité de la CNIL était tournée à hauteur de 85 % vers le secteur public ; aujourd'hui, elle l'est à hauteur de 90 % vers le secteur privé. C'est un bouleversement considérable.

En ce domaine, nous sommes sous la pression américaine. Je pense notamment au développement des dispositifs d'alerte professionnelle dans les entreprises, à la stratégie dite *« discovery »* qui permet aux juridictions américaines d'exiger la production de pièces venant d'entreprises françaises, ou encore, s'agissant du fonctionnement des réseaux, au fait que les entreprises américaines considèrent ne pas être soumises au droit européen – ce qui pose non seulement un problème de protection des données personnelles, mais aussi un problème de concurrence : dans le domaine des réseaux sociaux et surtout des moteurs de recherche, les entreprises de taille moyenne pâtissent de la liberté d'action dont bénéficient les grands acteurs venant des États-Unis.

Parmi les sujets les plus brûlants, il y a tout d'abord, bien sûr, la problématique des centrales de crédit. Les choses avancent, le Parlement a pris des initiatives, un délai a été fixé ; la CNIL s'en félicite, ayant clairement dit que pour aller plus loin, il fallait changer le cadre législatif. Nous sommes bien entendu à votre disposition pour éclairer vos travaux.

Un deuxième sujet très important est la normalisation en matière de protection des données. Les entreprises ont besoin d'y voir clair. Dans le cadre du groupe « Article 29 », c'est-à-dire du groupe des « CNIL » européennes, nous avons fait un très gros travail, mais cela n'a pas été sans mal. Il y a environ un an, nous nous étions rendus compte que l'organisme de normalisation ISO travaillait, pour établir des normes à vocation mondiale, sur la base des réflexions de l'Organisation de coopération économique Asie-Pacifique (APEC) – dont font partie les États-Unis et le Canada – et des Lignes de l'OCDE, alors que le niveau de protection des données personnelles y est beaucoup moins élevé que dans la directive européenne et les lois des Vingt-sept. Je ne m'attarderai pas sur nos démêlés avec la

Commission européenne. Aujourd'hui, les choses vont mieux : l'un de nos collaborateurs, chef du service d'expertise technologique de la CNIL, a été désigné par le groupe de l'Article 29 pour participer à l'ensemble des travaux et faire valoir nos positions. Il ne s'agit évidemment pas de bloquer les activités économiques, mais de protéger les libertés individuelles : les normes techniques doivent assurer l'équilibre entre le progrès des premières et le respect des secondes.

Troisième sujet : la problématique de l'externalisation, sur laquelle le Gouvernement a engagé une réflexion. La démarche consiste, pour des entreprises françaises, à passer des contrats avec des entreprises situées à l'étranger, par exemple au Maroc, en Tunisie, au Sénégal ou au Burkina-Faso, afin d'externaliser certaines fonctions comme la gestion comptable ou le secrétariat. Pour ces pays, c'est un enjeu tant économique que social : j'ai visité à Dakar une entreprise où travaillaient 2 200 jeunes de la région, qui avaient ainsi trouvé un emploi ; quant à nos amis marocains, ils développent un plan appelé « Émergence » qui prévoit 120 000 emplois résultant d'externalisation à l'échéance 2012 – contre un peu plus de 50 000 actuellement. Le rôle de la CNIL n'est pas de prendre une position sur l'externalisation en tant qu'option économique, mais de rappeler que si elle a lieu, ce doit être dans un cadre juridique visant tant à protéger les données qu'à éviter les distorsions de concurrence. Je me suis rendu dans beaucoup des pays concernés, dont nous avons en général réussi à convaincre les gouvernements de la nécessité de créer une « CNIL » et de prendre les dispositions législatives nécessaires. Nous leur demandons d'offrir un niveau de protection équivalent à celui demandé par la directive européenne, afin que les entreprises françaises soient autorisées à transférer des données personnelles. Je rappelle que 98 % du commerce international repose sur du transfert de données.

Je voudrais aussi évoquer le processus de labellisation par la CNIL. La loi de 2004 lui avait donné compétence en la matière, mais c'est un article inséré dans la loi de simplification du droit du 12 mai 2009 qui lui donne la possibilité d'avancer de manière concrète. Nous allons donc mettre en place des labels, comme les entreprises françaises nous le réclament afin d'assurer leur développement dans un cadre juridique non vulnérable. Nous allons commencer, très prochainement, par les domaines de la formation et de l'audit. Si tout se passe bien, nous passerons dans un an ou deux à un sujet beaucoup plus difficile, la labellisation de sites internet et de produits logiciels. Mais nous devons prendre garde : les entreprises attendent de nous des labels qui soient reconnus et offrent un gage de stabilité. Nous sommes au début de ce travail ; si vous me faites le plaisir de m'inviter à nouveau l'année prochaine, sans doute pourrai-je vous parler des premières labellisations.

Je terminerai par le sujet le plus préoccupant. Le développement de la biométrie, celui de la vidéosurveillance ou vidéoprotection, le développement prévisible des nanotechnologies dans le domaine des systèmes d'information, notamment pour la géolocalisation des personnes et des biens, le développement du réseau, c'est-à-dire des moteurs de recherche et des réseaux sociaux, sont en train de bouleverser totalement notre conception de la protection des libertés individuelles. J'avoue être extrêmement inquiet et assez pessimiste – car les choses vont tellement vite que nous aurons beaucoup de mal à réagir. Beaucoup de ces systèmes sont mis en place par des entreprises, mais pas tous ; certains le sont par des institutions régaliennes.

La vidéosurveillance ou vidéoprotection et la biométrie ne sont pas ce qui m'inquiète le plus car leur technologie peut en être maîtrisée et, surtout, le problème du passage invisible des frontières ne se pose pas. Le développement de la géolocalisation et celui des réseaux sont

beaucoup plus angoissants ; en la matière, même si nous prenons des initiatives en France, rien ne nous assure que nous serons suivis.

Force est de constater que le hiatus entre les conceptions américaine et européenne de la protection juridique des données personnelles s'aggrave. L'inscription au *Safe Harbor* était, pour des entreprises américaines, une manière de donner aux Européens la garantie qu'elles respecteraient les règles européennes dans les transferts de données vers l'Union. Or l'Australie, qui n'est pas suspecte d'être plus proche de l'Europe que des États-Unis, vient de faire savoir qu'elle ne croyait plus en cette solution, étant désormais persuadée que les entreprises américaines ne respectent pas les règles – ce dont, pour ma part, je suis convaincu depuis longtemps. Quant au système des BCR, permettant aux grands groupes internationaux de mettre en place un système juridique assurant, à l'intérieur de l'ensemble de leurs filiales, l'adéquation avec le niveau de protection des données européen, c'était une solution qui nous paraissait intelligente ; mais nos amis britanniques et néerlandais sont en train de lui donner un coup de frein. Bref, les quelques systèmes qui avaient été trouvés pour compenser l'absence d'une législation américaine comparable à la législation européenne sont en train de se déliter.

Il y a un an à Madrid, à une soixantaine de délégations, nous avons réussi à nous mettre d'accord sur un corpus de principes fondamentaux, ou « standards internationaux », l'objectif étant d'avoir des standards communs à l'Europe, aux États-Unis et à l'Asie. Nous avons pu les définir dans leur contenu mais, bien entendu, il ne nous appartient pas de le faire dans leur valeur juridique contraignante. C'est l'une des raisons pour lesquelles je suis très heureux d'être aujourd'hui devant vous : les « CNIL » européennes considèrent qu'il revient maintenant aux pouvoirs publics des États, et notamment aux Parlements, de passer à la deuxième étape, la mise en place des standards de valeur juridique contraignante équivalents en Europe, en Asie et aux États-Unis. Pour y parvenir, il faut probablement s'orienter vers une convention internationale.

Ce que nos homologues espagnols ont obtenu du Parlement de leur pays, et que sont également en train de le demander nos homologues allemands, nous nous permettons de vous le suggérer. Nous sommes prêts à vous adresser tous les documents nécessaires à votre réflexion. Il nous paraît urgent que le Parlement français adopte une résolution pour attirer l'attention du Gouvernement sur la nécessité de mettre en place ce corpus de principes à valeur juridique contraignante. C'est un enjeu majeur pour nous : les « CNIL » ont le sentiment d'être arrivées au bout de ce qu'elles peuvent faire ; aux pouvoirs publics de prendre le relais.

M. le président Patrick Ollier. Votre suggestion ne restera pas sans suite, j'en prends l'engagement. Je vous remercie d'inviter la Commission des affaires économiques, très absorbée au quotidien par l'examen des nombreux textes qui relèvent de sa compétence, à entrer dans une réflexion qui engage l'avenir.

Avant de donner la parole à mes collègues pour vous interroger, je voudrais moi-même formuler une question. Il y a deux mois, lors de la discussion parlementaire, j'avais demandé à Mme Lagarde de créer un groupe de travail pour examiner l'opportunité d'instituer un fichier positif dans le cadre du crédit à la consommation. Il y a des arguments pour et des arguments contre ; il faut donc trancher. Ce groupe de travail semble être réuni, mais j'aimerais avoir votre sentiment personnel.

M. Serge Poignant. Je serai moi aussi très intéressé par la réponse à cette question ; pour ma part, j'étais de ceux qui souhaitaient la mise en place d'un fichier positif.

En ce qui concerne les standards internationaux, tous les États européens partagent-ils le même point de vue, ou y a-t-il des différences ? Que pouvons-nous faire pour convaincre les Américains, les Chinois, les Indiens ? Quelle peut être l'autorité compétente, s'agissant à la fois de protection des données et de concurrence ? L'OMC se penche-t-elle sur cette question des transferts de données ?

Enfin, pourriez-vous nous en dire un peu plus au sujet de la géolocalisation ?

M. François Brottes. Il arrive que le Parlement s'intéresse à des choses essentielles : cela fait plaisir…

Concernant l'action de la CNIL, je m'apprêtais à vous demander, monsieur le président Türk, si le temps de la désespérance n'était pas arrivé, mais vous avez déjà répondu… Merci en tout cas pour l'action très courageuse que vous menez, à une époque ou *Big Brother* n'est plus un fantasme. Les tenants de la liberté absolue de dire tout et n'importe quoi acceptent que la liberté de l'individu soit parfois piétinée, les tenants de la liberté de la concurrence trouvent normal que l'on fouille dans la vie privée des gens pour voir ce que l'on pourrait leur vendre, les tenants du contrôle policier prônent une traçabilité générale : il y a convergence entre ces trois types d'acteurs sociaux, en dépit de leurs différences, pour saboter les libertés individuelles.

Que faire ? Je souscris à votre approche globale, mais dans l'immédiat il faut être pragmatique. Dans le domaine des télécoms, des activités postales, de l'énergie, nous avons institué des régulateurs, dont la mission essentielle est de faire en sorte que la concurrence s'exerce entre les différents opérateurs. Ne faudrait-il pas, comme tend par exemple à le montrer le débat sur le « compteur électrique intelligent », que la CNIL soit systématiquement associée aux décisions de ces instances, afin qu'elle puisse tirer la sonnette d'alarme quand la manière dont un marché est régulé porte atteinte à la liberté individuelle ? Seriez-vous prêt à être, de droit, membre des autorités de régulation ?

M. Jean Dionis du Séjour. Je m'associe à la question sur le fichier positif. Le montage envisagé autour de la Banque de France vous convient-il ?

En ce qui concerne la géolocalisation, je partage vos inquiétudes. Quels moyens avons-nous de contraindre un acteur comme Google ? Est-ce au niveau du droit européen qu'il faut agir ?

Comment jugez-vous les débuts de l'HADOPI ? Que dites-vous du délit de non-sécurisation de son PC ?

S'agissant de la lutte anti-spam, les dispositifs législatifs existent maintenant depuis six ans. Considérez-vous qu'ils sont suffisants ?

M. Daniel Paul. Moi qui conteste l'existence de certaines autorités administratives dites indépendantes, je voudrais dire tout le bien que je pense de la CNIL. À l'évidence, elle répond à un besoin. Néanmoins, n'est-elle pas arrivée au bout de ce qu'elle pouvait faire dans le cadre législatif actuel ? Vous semblez dire qu'il est temps de passer à une autre phase. Quelles améliorations attendez-vous en termes de missions et de moyens ? Contrairement aux

responsables d'autres autorités, le respect que vous inspirez vous autorise à nous faire des suggestions.

S'agissant des inquiétudes suscitées par la géolocalisation, j'aimerais que vous nous précisiez la manière dont vous pensez procéder pour ce qui concerne la surveillance des salariés, eu égard à l'arrêt de la Cour de cassation.

Mme Frédérique Massat. Le projet « Loppsi 2 » adopté par le Sénat vous confie le contrôle de la vidéoprotection. Sur quoi celui-ci va-t-il exactement porter ? Avez-vous les moyens de l'exercer ?

Vous avez autorisé le recours à un système biométrique pour lutter contre la fraude à un examen. Pourquoi ? Ne craignez-vous pas que cette autorisation entraîne d'autres demandes que vous aurez du mal à refuser ?

Les compteurs Linky d'ERDF vont rendre accessibles des informations sur le mode de vie des consommateurs. N'y a-t-il pas là un risque ?

Enfin, pouvez-vous nous donner votre sentiment sur le système de traitement des infractions constatées (STIC), qualifié par certains de « monstruosité policière gérée par des moyens juridiques courtelinesques » ?

M. Francis Saint-Léger. Ma première question concerne la publicité ciblée en ligne. Comment pouvez-vous lutter contre le manque de transparence de cette technique ? Les internautes ignorent bien souvent que leur comportement est constamment sous surveillance.

S'agissant par ailleurs du vote électronique, qui a déjà donné lieu de votre part à des contrôles et même à des sanctions, pensez-vous que les moyens techniques soient suffisants pour garantir la confidentialité des données recueillies ?

Mme Marie-Lou Marcel. Après la publication au Journal officiel d'un décret concernant l'installation, à partir de 2012, de compteurs électriques "intelligents" dans les logements neufs, la CNIL a fait une mise au point sur ce type de compteur et émis des réserves. Le décret précise les conditions du remplacement progressif des compteurs électriques classiques par ces compteurs dits "intelligents", capables de communiquer avec les systèmes informatiques des distributeurs d'énergie. Ces compteurs sont en mesure de relever la consommation électrique pratiquement en temps réel et de la transmettre aux distributeurs. La CNIL, à l'attention des usagers, répond à une série de questions concernant notamment les avantages de ces compteurs, les informations collectées, les informations transmises au distributeur du réseau d'énergie, les risques de traçage, l'installation des compteurs. Pourriez-vous nous apporter quelques précisions ?

M. Alain Suguenot. Sans revenir sur les interrogations relatives au fichier positif, j'observe que les pouvoirs publics tentent depuis quelque temps, dans beaucoup de pays d'Europe, de faire pression sur les mastodontes d'internet et les puissants sites d'e-commerce afin qu'ils limitent la durée de conservation de leurs données. Pensez-vous que l'on puisse avancer sur la suppression des cookies et des adresses IP ?

M. William Dumas. Le STIC pose problème depuis sa création. Près de 85 % des classements sans suite ne font pas l'objet d'une mise à jour et 300 000 personnes restent dans le fichier de façon indue. Que pouvez-vous faire ?

M. Alex Türk. Petite remarque préalable : je ne m'attendais pas du tout à ces questions. Elles concernent – et j'en suis ravi – la protection des libertés et des données, beaucoup plus que des problèmes d'ordre économique. Ce n'était pas le cas il y a deux ans – ce qui explique, d'ailleurs, que j'aie consacré mon intervention liminaire aux seules questions économiques.

Certains pays ont déjà accepté le fichier positif. Dans le cas américain, on récupère toutes les informations que l'on peut sur des personnes. En Europe, on se limite aux informations touchant réellement à la situation bancaire – et en France, on s'interroge sur l'opportunité d'aller vers ce système. Il revient au Parlement de trancher sur cette question de société. La CNIL ne peut qu'appeler à une extrême prudence quant à la nature des informations recueillies. Il ne faudrait certainement pas aller jusqu'à la solution américaine, qui conduit à cerner la vie personnelle à travers ces éléments d'information bancaire.

La pratique est au moins aussi importante que le texte : si la maintenance n'est pas bien assurée, si des personnes accèdent au fichier alors qu'elles ne le devraient pas ou si des informations demeurent dans le fichier alors qu'elles auraient dû être enlevées, le système deviendra très dangereux. C'est la raison pour laquelle nous pensons qu'il faudrait choisir une voie moyenne, permettant de vérifier la réalité des incidences sur le surendettement – point sur lequel les Belges émettent des réserves. Pour le reste, vous savez que les banques sont réticentes, mais pour les raisons qui sont les leurs.

En ce qui concerne les standards, une résolution serait un début. Aujourd'hui, il n'y a rien. Or je suis extrêmement angoissé de voir que nous sommes dépassés par la technologie. La CNIL a dû créer un service d'expertise, qui compte aujourd'hui sept ingénieurs experts de haut niveau ; on me demande du renfort car tous les jours, nous sommes saisis d'applications technologiques nouvelles. En ce qui concerne la biométrie, lorsque j'ai pris mes fonctions 54 appareils avaient été installés dans l'année ; il y en a eu 3 500 cette année. Le problème est le même pour la vidéosurveillance et pour la géolocalisation – qui est ce qui m'inquiète le plus car elle se développe par tous les vecteurs : il s'agit aussi bien des puces RFID, des systèmes GSM, des utilisations quotidiennes de cartes bancaires, de cartes de télépéage, de pass navigo et de téléphones portables, ou encore du réseau. La CNIL – à laquelle un pouvoir exprès d'autorisation a été donné en 2004 sur la biométrie, n'a aucun pouvoir pour juguler la géolocalisation. Et si on lui donnait un pouvoir d'autorisation en la matière, il faudrait doubler son budget…

Le plus inquiétant, c'est l'utilisation des nanotechnologies dans les systèmes d'informations. Les experts du monde entier nous disent que dans moins de dix ans, il sera possible d'installer des systèmes qui verront, qui entendront, qui communiqueront à distance, mais qui ne seront pas visibles à l'œil nu. Nul ne sera plus jamais certain de ne pas être vu ou entendu. Plus que pour moi, je m'inquiète pour mes enfants et petits-enfants… Je revendique – mes étudiants s'en étonnent – le droit de vivre sans que l'on me voie et sans que l'on m'entende, même si je n'ai rien à me reprocher – car je ne confonds pas l'intimité et l'innocence. Sur ce sujet, j'observe qu'une pédagogie est nécessaire : quand je vais dans des classes de cm2, je constate que les élèves n'ont aucune idée de ce qu'est l'intimité. Ceux que j'ai rencontrés dernièrement dans une petite commune proche de Lille étaient à 90 % sur Facebook, qui est en principe interdit aux moins de 13 ans… C'est dans les maisons qu'il faudrait instituer un couvre-feu ! Pour un enfant de 10 ans, il y a probablement beaucoup plus de risques à aller seul sur internet qu'à se trouver dans la rue à 22 heures…

S’agissant de la pédagogie, la CNIL vient de décider de consacrer la quasi-totalité des crédits de communication qui restaient disponibles à une action en direction des professeurs de lycée, des chefs d’établissement et des élèves. Cette opération représentera un budget de 500 000 euros.

La voie de la résolution me semble utile. Ensuite, il faut que les gouvernements prennent le problème en mains, puis que l’Union européenne se saisisse du sujet et qu’elle entre en relations avec les États-Unis et l’Asie afin de mettre en place une convention à valeur juridique contraignante. Cela demandera sans doute dix ou quinze ans – et d’ici là les puces seront partout… Le temps démocratique d’élaboration du droit est beaucoup plus lent que le temps du développement technologique. Il ne faut pas pour autant en conclure qu’il ne faut rien faire : au contraire, il faudrait une résolution le plus vite possible.

Désespoir non, pessimisme oui, monsieur Brottes. Nous allons incontestablement vers une société de surveillance. Je crains même que l’on finisse par regretter le bon vieux temps du *Big Brother* : comment faire pour s’insurger contre des milliers de puces invisibles, ces « *Nano Brothers* » qui, telles des cellules cancéreuses, vont se développer partout dans la société ? Le Parlement, de même qu’il s’est formellement opposé à tout clonage humain, aura-t-il le courage politique d’envisager l’interdiction des nanotechnologies dans les systèmes d’information ? Le fait de savoir que l’on est entendu et vu conduit en effet à reproduire spontanément un modèle commun, donc à pratiquer le clonage mental. J’espère que le Parlement français, mais aussi les autres Parlements d’Europe et du monde s’interrogeront sur cette question, une action limitée à notre pays ne pouvant être efficace.

La tendance est à ce que la CNIL soit représentée dans les diverses autorités. C’est une bonne chose car elle est désormais compétente dans tous les domaines de la vie sociale, l’informatique étant présente quasiment partout. Si on nous le demande, nous participerons aux instances dont vous avez parlé.

Monsieur Dionis du Séjour, la position de la CNIL est de s’écarter au maximum de l’HADOPI, les objectifs étant totalement différents et il ne faut pas que les gens confondent. Sur HADOPI, d’ailleurs, les membres de la CNIL ont été très partagés. Certains, à commencer par votre serviteur, ont été préoccupés mais ont voté pour ; et j’avoue rester impressionné par ceux qui sont capables de se prononcer dans un sens ou dans l’autre sans émettre la moindre réserve : entre la protection du droit des auteurs et la préservation des libertés de l’internaute, j’ai beaucoup de mal à trancher. L’HADOPI doit faire ses preuves – et chacun jugera. Aura-t-elle tous les moyens technologiques d’intervenir ? La réponse est, à terme, non. Il faudra donc que le Parlement réagisse. Sur l’ensemble de ces technologies, il va devoir travailler quasiment en temps réel, tellement les choses bougent rapidement.

En ce qui concerne la lutte anti-spam, on fait ce que l’on peut, sachant que dans 90 % des cas, les pays d’origine n’ont pas les mêmes règles que nous. Cela fait partie des éléments à mettre dans la corbeille d’une convention internationale car aujourd’hui les Européens sont les seuls à agir ; il faut nous employer à convaincre les autres pays.

S’agissant de nos moyens, monsieur Paul, les choses avancent. Lorsque je suis arrivé il y a six ans à la présidence de la CNIL, nous étions 65 ; nous sommes aujourd’hui environ 150, grâce au plan de rattrapage mis en place en 2004 et qui va se poursuivre pendant encore au moins deux ans. Est-ce suffisant ? Cela ne le sera jamais, eu égard à l’ampleur de la tâche…

La surveillance des salariés est devenue pour nous un sujet à part entière car elle passe par différents vecteurs – la biométrie, la vidéosurveillance, la géolocalisation, la surveillance des réseaux, le développement des techniques *discovery*, celui des dispositifs d'alerte professionnelle, donc de dénonciation de faits qui peuvent poser problème. Une grande partie de nos contrôles se fait dans les entreprises car le salarié doit être protégé. Je rappelle que pour la France et les autres pays européens, la notion de consentement est relative : nous considérons que le consentement d'un cadre d'entreprise, soumis à un lien de subordination hiérarchique, à utiliser un véhicule géolocalisé ne peut être comparé au consentement libre d'un individu à se doter d'un téléphone portable. C'est une différence avec les Américains, pour qui le consentement n'a pas de caractère relatif.

Quant à la vidéosurveillance, si comme je l'espère le texte voté par le Sénat est définitivement adopté, la CNIL aura désormais la possibilité d'en assurer le contrôle national. Cela nécessitera le recrutement de quelques contrôleurs assermentés supplémentaires. Chaque année, nous ferons un rapport, à destination du Parlement, du Gouvernement, mais aussi de la Commission nationale de vidéosurveillance et aux préfectures, afin d'améliorer le dispositif de protection des données. Je fais partie de ceux qui considèrent qu'en elle-même, la vidéosurveillance n'est ni bonne, ni mauvaise ; tout dépend de la manière dont elle est utilisée. Il appartient aux décideurs de faire leurs choix, et à la CNIL de vérifier que les prescriptions législatives relatives aux droits individuels sont respectées.

En ce qui concerne le système développé par GMAC, destiné à vérifier l'identité des étudiants qui passent les concours et utilisé par 2 000 grandes écoles dans le monde entier, la CNIL, consciente de l'enjeu pour les étudiants français, a accepté l'utilisation d'une technologie de reconnaissance biométrique du réseau veineux de la paume de la main – en exigeant diverses garanties, concernant notamment la durée de conservation. En revanche, nous avons refusé l'utilisation d'empreintes digitales numérisées, technique qui peut être utilisée à l'insu et au détriment de la personne.

Les compteurs « intelligents », considérés isolément, ne posent pas de problème. Là encore, c'est le lien avec d'autres systèmes qui peut être dangereux. C'est pourquoi nous avons fixé des contraintes, touchant notamment à la sécurité du dispositif et à l'information des personnes. Soyez sûrs que nous ferons des contrôles et que nous vérifierons que les choses se passent conformément au texte qui nous a été présenté – faute de quoi nous n'hésiterons pas à le faire savoir.

Sur le STIC, nous avions rendu il y a un peu moins de deux ans un rapport qui faisait état d'un grand nombre de problèmes. Les choses progressent. Au ministère de l'intérieur, l'impératif est de rappeler certaines règles que la routine conduit à oublier, qu'il s'agisse de confidentialité des mots de passe des ordinateurs ou de traçabilité. Au ministère de la justice, c'est lorsque la mise en place du système Cassiopée sera complète que la plupart des problèmes devraient se trouver réglés. Je suis en contact permanent avec les deux ministères. Nous avions indiqué dans la conclusion de notre rapport que nous ferions un nouveau contrôle dans les trois ans qui allaient suivre : il aura donc lieu dans l'année qui vient.

Monsieur Saint-Léger, la publicité ciblée en ligne nous ramène toujours au même problème : comment faire pour assurer la défense de nos concitoyens face aux grandes sociétés américaines ? Face aux réseaux, l'usager a un triple droit : il doit exprimer son consentement avant, se voir assurer la transparence pendant, obtenir l'oubli après. Il faut donc se replacer dans le champ du droit de la consommation. Arrêtons de parler d'internautes : parlons d'usagers, d'utilisateurs, de consommateurs, de clients ; et disons à ces grands réseaux

que le développement de leur activité doit se faire dans le respect du droit des utilisateurs. Mais le problème est non seulement qu'ils le veuillent – si leur volonté fait défaut, on peut leur imposer des standards – mais aussi qu'ils le puissent – ce dont je m'inquiète beaucoup : c'est toute la problématique du nuage informatique. À ce sujet, je suis d'ailleurs très frappé qu'une société à si haute technologie et aussi performante que Google mette ses appareils – ce qui constitue la « ferme numérique » – dans des entrepôts gardés par des vigiles avec leurs chiens… Il y a là des milliards de déchets que j'appelle « infoactifs » parce qu'un jour, ils resurgiront. On ne connaît pas de solution à ce problème. Lorsque quelqu'un quitte un réseau, il ne peut jamais avoir la certitude absolue d'emporter la totalité de ses données.

S'agissant du vote électronique, la CNIL souhaite que, au cas où les pouvoirs publics décideraient de passer à ce mode de vote à distance pour les élections nationales, les systèmes informatiques utilisés apportent exactement les mêmes garanties que le vote en mairie : il ne faut pas que les risques de tricherie soient plus grands. Mais quelles que soient les précautions prises, il sera impossible d'être absolument sûr de l'identité de la personne qui est devant l'ordinateur. À titre personnel, je considère que la démarche du vote en mairie fait partie des rares ciments démocratiques qui nous restent et que nous ne devrions pas y renoncer.

S'agissant enfin de la durée de conservation des données par les moteurs de recherche, Google, après être passé de l'absence de limite à dix-huit mois, se dit prêt à passer à neuf mois, mais pas moins ; en revanche, Microsoft et Yahoo pensent que six mois, voire trois mois, pourraient suffire. Le G29 tente actuellement de faire comprendre à Google que pour conserver la confiance des usagers, il faudrait adopter une attitude plus raisonnable. Pour notre part, nous pensons que trois mois suffiraient largement ; nos collègues allemands, eux, réclament que ce soit zéro jour. C'est dire que la bataille est ardue – et elle nous ramène à la problématique des standards internationaux.

M. le président Patrick Ollier. Merci infiniment pour cette audition passionnante. Nous mesurons la tâche qui nous attend. Vous serez toujours le bienvenu et je suggère que vous reveniez faire le point avec nous avant l'été.

Membres présents ou excusés

Commission des affaires économiques

Réunion du mardi 14 septembre 2010 à 16 h 15

Présents. - M. Jean-Pierre Abelin, M. Bernard Brochand, M. François Brottes, M. Jean Dionis du Séjour, M. William Dumas, M. Jean Grellier, M. Pierre Lasbordes, Mme Marie-Lou Marcel, Mme Frédérique Massat, M. Jean-Marie Morisset, M. Patrick Ollier, M. Daniel Paul, M. Serge Poignant, M. Francis Saint-Léger, M. Alain Suguenot, M. Alfred Trassy-Paillogues, M. René-Paul Victoria

Excusés. - M. Gabriel Biancheri, M. Jean-Michel Couve, Mme Geneviève Fioraso, M. Jean-Louis Léonard, M. Jean Proriol, M. Michel Raison

Assistaient également à la réunion. - M. Jean-Luc Pérat, Mme Anny Poursinoff