ASSEMBLÉE NATIONALE

XIII^e LÉGISLATURE

Compte rendu

Office parlementaire d'évaluation des choix scientifiques et technologiques

Mercredi
9 février 2011
Séance de 17 h

Compte rendu n° 6

SESSION ORDINAIRE DE **2010-2011**

Présidence de M. Claude Birraux, député, *Président*

ASSEMBLÉE NATIONALE

– Désignation de candidats à des organismes extraparlementaires –

M. Claude Birraux, député, président de l'OPECST. – L'ordre du jour appelle la désignation de deux sénateurs membres de l'Office pour siéger en qualité de membres titulaires :

- d'une part, en application des articles L. 531-4-1 et R. 531-12 du code de l'environnement, au sein du Comité économique, éthique et social du Haut conseil des biotechnologies (HCB), en remplacement de M. Jean-Claude Etienne ;

- d'autre part, en application de l'article L. 114-3-3 du code de la recherche, au sein du conseil de l'Agence d'évaluation de la recherche et de l'enseignement supérieur (AERES), en remplacement de M. Christian Gaudin.

Le Premier Vice-président et moi-même avons reçu deux candidatures : celle de notre collègue sénateur Marcel Deneux, pour siéger au Comité économique, éthique et social du HCB, et celle de notre collègue sénateur Christian Demuynck, pour siéger au conseil de l'AERES.

En l'absence d'objection, ces deux candidatures sont approuvées par l'OPECST. J'en informerai rapidement M. Gérard Larcher, Président du Sénat.

M. Daniel Raoul, sénateur, vice-président de l'OPECST. – Actuellement membre suppléant du Comité économique, éthique et social du HCB, je ne souhaite pas être maintenu à cette fonction qui requiert un investissement considérable et me paraît, pour cette raison, incompatible avec l'exercice normal du mandat parlementaire.

M. Jean-Yves Le Déaut, député, vice-président de l'OPECST. – En tant que suppléant de notre collègue député Claude Gatignol à ce même Comité, je trouve toutefois utile d'être l'observateur du Parlement dans le cadre de réunions de bilan ou sur un thème donné, à des dates prévues suffisamment à l'avance, comme ce sera le cas lors de la journée d'étude prochaine du HCB sur les certificats d'obtention végétale.

M. Claude Birraux. – Plus généralement, j'attends les résultats de l'étude entreprise par le Sénat sur les représentations dans les organismes extra-parlementaires. Nous pourrons ensuite repasser au crible de ce que le Sénat aura proposé l'ensemble de nos représentations dans des organismes extra-parlementaires.

Par ailleurs, il serait utile que nos délégués dans ces organismes présentent annuellement devant l'Office un bilan succinct de leur représentation.

***

– Audition de M. Alex Türk, président de la Commission nationale de l'informatique et des libertés (CNIL) –

M. Claude Birraux, député, président de l'OPECST. – Je suis heureux d'accueillir M. Alex Türk, président de la Commission nationale de l'informatique et des libertés (CNIL) et je le remercie de se prêter à cette audition dont le rythme est maintenant annuel.

La CNIL joue un rôle crucial dans la protection du citoyen, de sa vie privée, de ses libertés, dans une ère du tout numérique où le droit à l'oubli et la notion de confidentialité n'existent plus. Le citoyen s'expose en effet chaque jour à des situations à risques dont il mesure mal les conséquences : du jeune adolescent qui publie des photos de soirée sur son compte Facebook au bon père de famille qui se fait subtiliser ses informations bancaires ou son identité sur un site Internet piraté.

Ces risques ne sont généralement pas nouveaux, mais l'échelle à laquelle ils se manifestent crée une situation inédite. Le citoyen, sa vie, ses secrets, ses informations privées, sont potentiellement accessibles au monde entier, en temps réel, et sans retour en arrière possible.

Pour faire face à ces défis, j'observe que la CNIL fonctionne dans une double similitude institutionnelle avec notre Office :

- d'une part, une similitude de positionnement avancé quant à la réflexion sur l'innovation technologique ; pour l'OPECST, c'est un devoir ; pour la CNIL, c'est une nécessité ;

- d'autre part, une similitude dans un double ancrage parlementaire et scientifique : l'OPECST est un organe du Parlement, qui s'appuie sur un conseil scientifique ; la CNIL est parlementaire du fait des quatre députés et sénateurs qui y siègent, et scientifique par ses personnalités qualifiées.

Tous deux sont ainsi des rouages entre la communauté politique et la communauté scientifique et technologique.

Nous allons vous laisser présenter les enjeux auxquels la CNIL se trouve confrontée du fait des innovations technologiques. L'actualité récente a notamment donné écho à vos craintes quant à la géolocalisation. J'ajoute une question générique : quels sont les moyens d'investigation scientifiques et technologiques dont dispose la CNIL pour faire face à la diversité des supports de données numérisées qui rendent chacun traçable ?

M. Alex Türk, président de la CNIL. – Merci, Monsieur le Président. Cette audition fait l'objet d'un intérêt réciproque. Nous vous ferons parvenir des réponses écrites aux questions techniques que vous nous avez transmises.

Nous venons de créer au sein de la CNIL une quatrième direction, qui vient de s'ajouter aux trois premières respectivement consacrées aux questions fonctionnelles, à l'expertise juridique et technologique, et au contrôle-contentieux. Cette quatrième direction a été créée pour répondre aux défis des technologies nouvelles. Nous possédions déjà un service d'expertise technologique composé d'ingénieurs, quasiment unique en Europe et dans le monde. Mais il fallait identifier clairement la préoccupation de veille et de prospective au sein de notre autorité.

Cette direction possède de nouvelles armes :

- un budget autonome permettant de faire appel à des experts extérieurs de façon souple ;

- l'assistance d'un comité de prospective composé de membres de la CNIL et de personnalités extérieures à la CNIL ;

- enfin, un laboratoire nouvellement créé au sein de la Commission, car il est indispensable de tester les produits technologiques et de les analyser pour préparer le travail des juristes.

Cette évolution est aujourd'hui le fer de lance du développement de notre autorité.

Quatre technologies méritent une attention particulière :

- la vidéosurveillance ou vidéoprotection, qui rend les services que l'on connaît, mais dont il ne faut pas sous-estimer le potentiel dans le domaine de la géolocalisation ;

- la biométrie c'est-à-dire l'identification d'une personne par certains éléments du corps humain : l'œil, la main (le réseau veineux, l'empreinte digitale, la forme de la main ouverte), la façon de se tenir ou d'écrire, la silhouette, la reconnaissance de l'odeur du corps humain permettent aujourd'hui cette reconnaissance ou la permettront dans un proche avenir. Notre travail est de mesurer le caractère intrusif d'un produit au regard de sa fiabilité technique et de sa performance, dans le cadre juridique existant et en intégrant d'autres facteurs tels que le consentement des personnes. Par exemple, il y a aujourd'hui plus de 400 lycées dotés de systèmes biométriques à l'entrée des réfectoires. Dans ces lycées, nous acceptons la reconnaissance de la main ouverte, dont la trace se perd immédiatement, mais interdisons l'utilisation de l'empreinte digitale, qui pourrait être récupérée à des fins abusives. La biométrie est la seule technologie pour laquelle la CNIL dispose d'un pouvoir d'autorisation expresse.

- la géolocalisation est inquiétante car elle devient diffuse : la vidéosurveillance, la biométrie peuvent servir à géolocaliser. Il existe une géolocalisation par effet, avec l'utilisation des téléphones portables, cartes bancaires, cartes de transport, de télépéage. Il existe également une géolocalisation par objet, avec l'utilisation du bracelet électronique en matière pénale et des puces de radio-identification (RFID), par exemple dans le domaine des transports, pour améliorer la logistique. Mais ce qui modifie la nature du problème, c'est la géolocalisation individuelle par le biais du téléphone portable de dernière génération. C'est un enjeu majeur et, selon moi, il représente la troisième étape de développement du système informatique, après l'ordinateur individuel et le réseau Internet. Je pense erroné de dire que ces problématiques sont analogues à des phénomènes déjà connus et maîtrisés par l'humanité, comme la radio ou la télévision. Nous sommes confrontés à une évolution qui transforme de manière considérable et irréversible l'exercice de nos deux libertés fondamentales que sont la liberté d'aller et venir et la liberté d'expression.

- l'évolution d'Internet est, elle aussi, un facteur de risques : dès lors que nous sommes entrés dans un système, il n'existe plus aucune garantie absolue d'en sortir un jour. Ici, le traçage n'est pas physique et dans l'espace, mais mental et dans le temps. Le présent se dilate à un point tel que l'on perd la capacité à corriger les informations entrées dans le système.

On voit apparaître des phénomènes qui compliquent encore ces évolutions :

- la concentration des dispositifs : Roissy sera par exemple bientôt un « parapluie technologique » utilisant à la fois la vidéo, les puces RFID pour localiser les voyageurs retardataires, la biométrie, la récupération de nombreuses informations sur les passagers. La même évolution peut être observée dans les gares et dans les stades.

- la dilution des dispositifs dans le « nuage » numérique : des milliards de données personnelles sont gérées dans des « fermes numériques » pour une durée potentiellement infinie, les informations pouvant réapparaître à tout instant.

- la miniaturisation des dispositifs par le recours aux nanotechnologies : avec ces systèmes d'information, devenus invisibles, nous perdrons la certitude de ne pas être vus ou entendus dans notre vie courante.

- enfin, la dématérialisation : l'air que nous respirons sera teinté d'informatique. On est en train d'admettre l'idée que l'intelligence et l'émotion seront elles-mêmes intégrées à la société numérique.

Face à ces défis, quelles sont les solutions envisageables ?

D'abord, la pédagogie auprès des jeunes et du corps enseignant, par l'intermédiaire du ministère de l'éducation nationale : nous avons consacré un budget important à une action ciblée sur les élèves, les centres de documentation et les professeurs, sous forme de réunions et de guides pratiques. Il est indispensable de créer une sorte d'« instruction civique » au numérique pour inculquer aux jeunes les valeurs de l'intimité et de l'identité.

Il convient ensuite d'étudier dans quelle mesure la technologie serait capable de juguler la technologie : en limitant par construction l'intrusivité d'une technologie donnée, ou en intervenant de façon curative pour en limiter les effets. Se pose toutefois la question du financement de tels dispositifs.

Enfin, la solution juridique consisterait à convaincre les Etats-Unis, le Japon, la Russie, la Chine et l'Inde qu'il n'est pas concevable que des mastodontes économiques tels que Google ou Facebook développent leurs activités en Europe, sans reconnaître le droit européen. Le Canada et quelques autres pays, soit moins de 500 millions d'habitants, partagent le point de vue de l'Europe et son niveau élevé de protection. Il faut donner une valeur juridique contraignante au processus dit de Madrid, c'est-à-dire à un certain nombre de principes fondamentaux reconnus lors de la Conférence de Madrid il y a deux ans. Le Sénat et l'Assemblée nationale vont examiner des résolutions en ce sens, mais il faudra ensuite que le Gouvernement français et ses homologues européens entreprennent de faire de cet objectif une priorité. Il est malheureusement probable que ce processus sera trop long pour aboutir, avant qu'il ne soit trop tard, à une convention internationale. Dans l'attente, il faut souligner l'utilité de la pédagogie et l'intérêt de progresser sur le plan technologique.

M. Claude Birraux. – Mes questions sont les suivantes :

- A propos du « Pass Navigo » anonyme, avez-vous obtenu des résultats auprès de la RATP ?

- Avez-vous des outils permettant de contrôler les informations recueillies par les sites Internet ?

- Quel regard portez-vous sur les réseaux sociaux ? Comment instaurer le droit à l'oubli ?

- Disposez-vous de pouvoirs sur les fichiers de police et de renseignements ?

- Comment détectez-vous des croisements de fichiers susceptibles de porter atteinte à la vie privée des personnes ?

- Les données sensibles de l'Etat sont-elles suffisamment protégées ? Quelles conséquences tirez-vous de l'affaire « Wikileaks » ?

M. Alex Türk. – Sur le « pass Navigo », nous sommes toujours en discussion avec la RATP, car nous avons obtenu un pass anonyme mais payant, ce que nous n'acceptons pas. Nous avons constaté, par ailleurs, que les responsables aux guichets de la RATP ont tendance à décourager les clients souhaitant se procurer ce « pass » anonyme.

Le droit à l'oubli n'a jamais voulu dire déresponsabilisation. Il s'agit de circonscrire le périmètre du droit à l'oubli, de fixer des durées de conservation qui pourraient être distinctes selon que les informations sont ou non entrées par la personne qu'elles concernent ou par quelqu'un d'autre. Ce droit à l'oubli pourrait être intégré à la Constitution au sein d'une charte numérique. Il pourrait y jouer le même rôle que le principe de précaution au sein de la charte de l'environnement. A défaut, le risque est que l'on finisse par accepter que les technologies restreignent un certain nombre de libertés acquises au cours de l'histoire par les peuples.

C'est ainsi que Mark Zuckerberg, fondateur de Facebook, pense qu'il faut admettre que la norme sociale a glissé, que la vie privée est un concept qui s'est modifié. De même que les patrons de Google, Larry Page et Eric Schmidt, nous expliquent que Google a vocation à digérer la connaissance du monde entier et à donner le moment venu aux Etats des informations sur leurs citoyens, ou encore qu'il va falloir admettre de vivre avec des séquences d'identité, c'est-à-dire plusieurs états-civils successifs au cours du temps. Des juristes développent le concept de banqueroute de réputation, impliquant un changement d'identité, ce qui consiste à faire de cette valeur fondamentale qu'est l'identité de la personne humaine une valeur marchande.

J'en viens aux fichiers de police et de renseignements, qui sont contrôlés en France, ce qui n'est pas courant dans le monde. Sur demande, les magistrats de la CNIL vérifient le contenu de ces fichiers. Pour les plus sensibles d'entre eux, il est possible que les magistrats de la CNIL ne divulguent pas au demandeur le résultat de ce contrôle.

Les croisements de fichiers doivent être autorisés par la CNIL. Une personne est en moyenne intégrée dans environ 400 fichiers.

Dans tous les cas, la CNIL ne saurait être considérée comme un frein par le législateur qui l'a créée et peut à tout moment en modifier le rôle.

M. Claude Birraux. – Qu'en est-il des croisements de fichiers, par exemple en cas d'épidémie ?

M. Alex Türk. – Nous rendons un avis, généralement favorable, car nous n'avons pas d'a priori sur les interconnexions de fichiers, mais il faut que cela soit cadré juridiquement.

Wikileaks ne nous pose pas de problème particulier et nous reconnaissons par ailleurs l'utilité des réseaux sociaux par exemple dans les événements qui se déroulent en ce moment en Tunisie et en Egypte. Mais il faut réfléchir plus généralement au concept de transparence. Pour nous, une démocratie se caractérise par la transparence des fichiers régaliens, mais par l'opacité de la vie privée des personnes. Le problème de Wikileaks est qu'il n'existe pas de cadrage juridique. Il faut que le législateur réfléchisse à ce concept de tranparence.

M. Gwendal Le Grand, chef du service de l'expertise de la CNIL. – Au sujet des outils technologiques, nous agissons sur plusieurs axes :

- Au sein de la CNIL, des experts techniques ont des compétences spécifiques et variées pour analyser les nouvelles technologies en collaboration avec nos homologues européens, afin de donner un avis juridique. Par exemple, nous avons adopté cette année un avis sur la publicité comportementale, qui pose la question de la géolocalisation.

- Cette démarche s'articule avec les pouvoirs de contrôle de la CNIL : nous contrôlons des sites Internet, par exemple l'année dernière Google Street View.

- Enfin, le développement du laboratoire de la CNIL nous permet de décortiquer les nouvelles technologies, pour pouvoir parler d'égal à égal avec des sociétés comme Apple. Un certain nombre d'industriels nous prêtent des prototypes en amont pour pouvoir les modifier éventuellement avant leur mise sur le marché, en fonction de nos recommandations.

M. Jean-Yves Le Déaut, député, vice-président de l'OPECST. – Je m'interroge sur le droit à l'oubli dans le domaine du permis à points car les relevés fournis par les préfectures remontent très loin dans le temps. Par ailleurs, vous n'avez pas abordé la question des fichiers génétiques, qui me paraît pourtant cruciale avec le développement de la connaissance du génome. Les neurosciences sont également un risque pour la vie privée puisque des techniques permettent de détecter le mensonge et même les pensées des individus, dépassant ainsi la fiction.

A propos des puces RFID, quelles sont les limites du passage de l'identification d'un objet à l'identification d'une personne ?

Enfin, la question de la sécurité des systèmes informatiques constitue un enjeu de taille. Comment éviter l'immixtion des systèmes informatiques dans la vie privée ? Comment mettre fin à la profusion de spams dans le courrier électronique ?

M. Alex Türk. – Il n'y a pas de solution à la question des spams car 90 % d'entre eux viennent des Etats-Unis, pays qui n'applique pas les mêmes règles que nous. C'est un problème juridique qui devrait être examiné au niveau international.

Il existe un débat à l'échelle européenne sur la façon de traiter les puces RFID mises sur les produits des supermarchés : soit elles restent actives après la caisse du supermarché et il faut accomplir une démarche particulière pour les désactiver, soit c'est l'inverse. Je pense malheureusement que la première conception, qui est anglo-saxonne, l'emportera.

La géolocalisation, qui ne fait pas l'objet d'un pouvoir d'autorisation de la CNIL, me paraît devoir faire l'objet d'une réflexion particulière. Une même technologie peut être jugée acceptable ou non en fonction de sa finalité. Par exemple, les puces RFID peuvent être utiles pour les malades d'Alzheimer, à qui elles redonnent une certaine autonomie. Mais surveiller

ainsi les nourrissons dans les maternités, voire les enfants ensuite dans les crèches et les écoles, est autrement plus problématique. Dans certaines communes de Californie, on dote de puces des enfants de 10-12 ans. Ira-t-on jusqu'à mettre des puces à des adolescents alors que ceux-ci ont, au contraire, besoin de faire l'apprentissage de l'autonomie ? On succombe à la tentation d'utiliser des technologies sous prétexte qu'elles sont disponibles. Le rôle du Parlement est d'évaluer l'impact de ces technologies.

Mme Sophie Vulliet-Tavernier, directrice des études, de l'innovation et de la prospective de la CNIL. – Nous allons vérifier si la durée de conservation des données du permis à points est conforme à ce qui a été défini en accord avec la CNIL.

La loi française, au contraire de la loi européenne pour le moment, traite de façon particulière les fichiers génétiques. L'absence de cadrage juridique international et notamment l'absence de règles américaines font que des sites Internet peuvent effectivement proposer aujourd'hui des tests génétiques.

M. Gwendal Le Grand. – Il faut souligner que le développement de l'administration électronique et notamment du permis électronique est aussi un facteur d'amélioration de l'exercice du droit d'accès par les personnes.

Il devient impossible d'échapper à la technologie aujourd'hui. La transmission d'informations se fait parfois de façon invisible, par exemple lorsque des sociétés tierces collectent des informations sur Facebook. Je suis pessimiste sur cet aspect, en raison de la dissémination des données et des acteurs.

Mme Sophie Vulliet-Tavernier. **–** La CNIL vient de diffuser sur son site Internet un guide pratique sur la sécurité, complété d'une simulation permettant à chacun de vérifier quel est son niveau de sécurité.

Mme Marie-Christine Blandin, sénateur. – Malheureusement, les actions de communication de la CNIL auprès des jeunes se heurtent aux valeurs répandues par la télévision, qui promeut au contraire le dévoilement de l'intimité.

Les puces RFID sont parfois exigées aujourd'hui pour le transport aérien des animaux : le seront-elles bientôt pour le transport des enfants ? Il conviendrait de savoir anticiper de telles évolutions.

Par ailleurs, la commission d'enquête sur la pandémie grippale s'est interrogée sur les fichiers utilisés pour diffuser les invitations prioritaires à la vaccination. La CNIL peut-elle émettre des préconisations dans des situations d'urgence ?

Enfin, dans le cadre des prélèvements d'ADN par le système pénal, le législateur n'a pas obtenu la destruction de l'ADN des simples témoins, au motif que cet ADN était non codant. D'après certains travaux scientifiques récents, cet ADN non codant pourrait toutefois devenir déchiffrable. Les données sont centralisées et informatisées. Qu'est-ce qui nous garantit qu'une compagnie d'assurance ne pourra pas s'en emparer à l'avenir ?

M. Bruno Sido, sénateur, premier vice-président de l'OPECST. – Je remercie notre collègue Alex Türk, président de la CNIL, pour ses propos éclairants sur un certain nombre de sujets. Je souhaiterais souligner que l'Etat a contribué à certains aspects de la situation actuelle, si l'on songe par exemple à l'encouragement donné aux paiements par cartes (cartes bancaires, cartes de télépéage et autres cartes diverses). Par ailleurs, la capacité

d'observation des satellites militaires et l'utilisation des données ainsi collectées devraient être étudiées. Plus généralement, on peut se demander parfois en consultant des dossiers d'archives si l'Etat applique bien à ses propres fichiers le principe du droit à l'oubli.

Mais ma question est plus générale : peut-on faire confiance à l'homme ? Est-ce vraiment très préjudiciable d'être tracé et de recevoir du courrier indésirable ? Parviendra-t-on à lutter contre ces dérives et en quoi est-ce vraiment important ?

M. Alex Türk. – Est-ce important ? Oui. Va-t-on y arriver ? Je crains que non. Pourtant, une société dans laquelle nous perdrions notre anonymat, notre incognito, me paraît dangereuse. En 1974, René Dumont a tenté de nous alerter sur les dangers d'un changement climatique. Or, ce changement se produit maintenant car on a laissé passer le moment où il fallait agir. C'est ce qui risque d'arriver aussi dans le domaine de la protection des données numériques. Dans le premier cas, il s'agissait de protéger notre environnement collectif ; dans le second, notre environnement individuel. Or, si l'on vit dans une société où tout peut être vu et entendu, on risque de lisser notre discours, d'y perdre notre identité et notre personnalité. C'est pourquoi il faut que l'humanité maîtrise l'usage de l'informatique.

A propos des fichiers de l'Etat, il faut distinguer entre les dossiers « papier », enfermés dans des placards, et l'Internet qui peut faire resurgir à tout moment des informations, ce qui crée le danger.

Mme Marie-Christine Blandin a évoqué les dangers des valeurs promues par la télévision, notamment par la téléréalité. Pour traiter cet aspect, nos crédits de recherche pourront être alloués à des économistes, philosophes ou sociologues, car une réflexion en sciences humaines est nécessaire. En effet, pourquoi les jeunes éprouvent-ils aujourd'hui le besoin de vivre leur vie privée au vu et au su de tout le monde ?

Mme Sophie Vulliet-Tavernier. – Lors de la pandémie grippale nous avons été saisis d'une demande d'autorisation de la Caisse nationale d'assurance maladie (CNAM) et nous avons contrôlé la fusion de nombreux fichiers pour cibler en priorité certaines catégories de population, mais de façon sécurisée.

Le fichier des empreintes génétiques devait, à l'époque, utiliser de l'ADN non codant, mais il serait opportun de réexaminer cette question au regard de l'évolution scientifique. Par ailleurs, le principe de finalité empêche la réutilisation par des compagnies d'assurance de ces données. Le détournement de finalité est passible de sanctions pénales. Les compagnies d'assurance ont d'ailleurs l'interdiction d'utiliser toute donnée génétique, même transmise par l'assuré lui-même.

M. Claude Birraux. – Je vous remercie infiniment pour ce débat passionnant, qui confirme que notre société est en proie à une perte de repères et de relations sociales.