ASSEMBLÉE NATIONALE

XIVe LÉGISLATURE

Compte rendu

Commission des lois constitutionnelles, de la législation et de l'administration générale de la République

Jeudi
4 octobre 2012
Séance de 10 heures

Compte rendu n° 2

Présidence de M. Jean-Jacques Urvoas, ***Président***

ASSEMBLÉE NATIONALE

La séance est ouverte à 10 heures.

Présidence de M. Jean-Jacques Urvoas, président.

La Commission procède à l'audition de Mme Isabelle Falque-Pierrotin, présidente de la Commission nationale de l'informatique et des libertés.

M. le président Jean-Jacques Urvoas. Nous accueillons ce matin Mme Isabelle Falque-Pierrotin, présidente de la Commission nationale de l'informatique et des libertés (CNIL).

Madame la présidente, la CNIL est mobilisée sur de nombreux sujets. Je pense d'abord aux problèmes d'actualité, tels ceux qui se posent à propos de Facebook et, plus généralement, des réseaux sociaux, ou encore à propos du *cloud computing*, mais le mode de création, la gestion et le contrôle des fichiers continuent également de vous occuper. D'autre part, nous avons aussi à voir ensemble comment articuler au mieux l'action de votre commission avec le travail parlementaire. Je profite de votre venue pour féliciter nos collègues Laurence Dumont et Sébastien Huyghe qui sont membres de notre Commission et viennent d'être nommés membres de la CNIL.

Enfin, nous aimerions vous entendre sur la révision de la directive du 24 octobre 1995 et sur le projet de règlement européen relatif à la protection des données à caractère personnel. Il y a peu, s'est tenue à Nicosie, dans le cadre de la présidence chypriote, une réunion des présidents des commissions des affaires intérieures et de la justice : au nom des citoyens français, qui bénéficient depuis 1978 d'une législation parmi les plus protectrices de l'Union, mon homologue du Sénat, Jean-Pierre Sueur, et moi-même nous sommes fait l'écho de votre extrême préoccupation. Force est de constater qu'insensibles à ces inquiétudes, nos interlocuteurs de la Commission européenne ont plutôt campé sur leurs positions…

Mme Isabelle Falque-Pierrotin, présidente de la Commission nationale de l'informatique et des libertés. Avant d'en venir à ce point, permettez-moi de brosser ce qu'a été l'évolution de l'environnement et du métier de la CNIL.

Nous vivons aujourd'hui, dans tous les compartiments de notre existence quotidienne, les effets d'une explosion des données ; les industries se dématérialisent, les objets communiquent entre eux... Notre univers ambiant est de plus en plus, surtout depuis quatre ou cinq ans, un univers numérique, où tout est connecté et nous oscillons entre le monde physique et le monde virtuel, passant presque insensiblement de l'un à l'autre et consommant des services dans l'un et l'autre.

Cette mutation change considérablement la donne pour la CNIL qui, créée pour encadrer la création et l'utilisation de grands fichiers publics, est mal armée pour piloter un écosystème aussi complexe que celui des données. Elle se traduit par une sollicitation sans précédent de notre institution, confrontée chaque année à une augmentation d'environ 20 % des plaintes et des demandes d'avis ou de conseils qui lui sont adressées.

À cela s'ajoute, depuis 2011, l'attribution de nouvelles missions : le contrôle de la vidéoprotection – il nous faut veiller à ce que les 900 000 caméras qui couvrent le territoire soient utilisées dans des conditions respectueuses des droits individuels –, le traitement des

failles de sécurité notifiées par les opérateurs en application du « paquet Télécom », et, tout récemment, l'octroi de labels.

Le premier défi pour la CNIL consiste à « digérer » cette augmentation du flux de sollicitations.

Le deuxième, d'ordre qualitatif, consiste à adapter notre métier à l'explosion des mouvements de données. Le pilotage ne pouvant passer uniquement par la sanction même si celle-ci reste une arme de dissuasion indispensable, nous devons travailler avec les acteurs eux-mêmes, qu'ils soient publics ou privés, pour les aider à intégrer les principes « informatique et libertés » dans leur offre de services et dans leur pratique professionnelle. Cela implique pour la CNIL, qui était très marquée par une culture administrative, de passer pour ainsi dire à une autre culture, ce qui est appelé à l'occuper beaucoup dans les mois et les années à venir ; cela implique en effet de changer la physionomie et le fonctionnement de l'institution.

D'autre part, les données ayant une valeur économique considérable, tous les pays de la planète sont en concurrence pour élaborer le cadre normatif le plus propre à attirer sur leur territoire les grandes bases de données. Par conséquent, toutes nos réflexions relatives à la protection des données personnelles, tant au niveau national qu'européen, doivent désormais être appréciées à cette aune.

La directive européenne de 1995 est le texte fondateur en matière de protection des données personnelles, mais elle a été élaborée à un moment où Internet, les réseaux sociaux et, plus globalement, les données n'existaient pas. Il est donc temps de la revoir. La commissaire Viviane Reding a présenté en janvier de cette année, en même temps qu'une proposition de directive relative aux données intéressant la police et la justice, un projet de règlement visant à moderniser le cadre juridique européen tout en préservant, selon elle, un haut niveau de protection.

Ce projet est intéressant à certains égards, notamment en ce qu'il reconnaît aux individus un certain nombre de droits nouveaux – droit à l'oubli, à la portabilité –, demande aux acteurs de se conformer dans leur fonctionnement aux principes « informatique et libertés » et vise à porter toutes les autorités de régulation européennes au même niveau, ce qu'on ne peut qu'approuver : les autorités chypriote et même irlandaise, par exemple, sont loin de disposer des pouvoirs, des ressources et de l'expertise de la CNIL, probablement l'une des autorités les plus puissantes d'Europe.

Ce texte présente néanmoins une grande faiblesse, qui tient à ses dispositions relatives à la gouvernance des autorités de régulation et, plus précisément à l'introduction de la notion d'établissement principal, qui certes existe déjà en droit européen, en matière fiscale et dans d'autres domaines du marché intérieur, mais qui serait ainsi appliquée pour la première fois à la protection des libertés individuelles. Dès lors, quand des données font l'objet d'un traitement à l'échelle de plusieurs pays de l'Union, l'autorité nationale du pays où est implanté l'établissement principal de l'entreprise responsable de ce traitement serait seule compétente pour contrôler celle-ci. Il en résulte concrètement qu'un citoyen français ayant à se plaindre d'un traitement des données réalisé en France par une entreprise dont l'établissement principal est situé en Irlande, devra s'adresser à l'autorité de régulation irlandaise, seule compétente en l'espèce ; la CNIL sera alors réduite à un rôle de boîte aux lettres, de relais. On voit bien que cela posera problème tant pour le citoyen que pour les autorités de régulation et pour les entreprises.

Pour le citoyen : s'il conteste la décision prise à son égard, il devra soit saisir l'autorité étrangère ou le juge étranger, soit demander à son autorité nationale de saisir son homologue étranger. Autrement dit, les autorités de régulation devront s'attaquer les unes les autres, ce qui est peu satisfaisant, vous en conviendrez, dans un domaine touchant aux libertés fondamentales.

Pour les autorités elles-mêmes : le risque est grand de voir le travail de régulation se concentrer entre les mains de quelques-unes d'entre elles, désignées comme autorités principales, – celles d'Irlande, de Grande-Bretagne, de Chypre, de Malte et, peut-être, des Pays-Bas –, d'autant que les organismes de traitement pourraient être incités à localiser leur établissement principal là où ces autorités se montreraient les plus compréhensives. Nous pourrions bien alors assister à des phénomènes de *dumping*, les pays les moins disants l'emportant sur les autres à un moment où, face à la concurrence internationale, l'Europe doit au contraire resserrer ses rangs.

Pour les entreprises : si Mme Reding considère que ce projet leur est favorable dans la mesure où il devrait leur simplifier la tâche, ne bénéficieront en réalité de cette simplification que celles dont la gouvernance est centralisée, et nullement les autres, qui souhaitent que chacune de leurs filiales nationales reste responsable des traitements réalisés localement.

S'il comporte quelques avancées et si la notion d'établissement principal peut être séduisante sur le papier, ce projet de règlement propose donc une gouvernance trop centralisée, au bénéfice d'un petit nombre d'autorités de régulation – probablement les plus souples –, mais aussi au profit de l'organe qui succédera au G29 et de la Commission européenne, à qui elle renvoie toute une série de décisions alors que ces questions pourraient être réglées par la coopération entre autorités de régulation nationales. Cette gouvernance est de surcroît inadaptée à la spécificité de notre matière, qui est en relation étroite aussi bien avec des critères nationaux qu'avec le droit pénal et le droit de la santé de chaque pays.

Nous avons dès le début fait part à Viviane Reding de notre réticence à l'égard du dispositif proposé – réticence partagée par l'Assemblée nationale et par le Sénat, comme en témoignent deux résolutions européennes votées par les assemblées. La discussion parlementaire au plan européen va maintenant s'engager, mais elle sera prise dans un calendrier assez resserré puisque l'objectif est de parvenir à l'adoption d'un texte définitif en 2014. Il importe donc d'avancer rapidement des contre-propositions et c'est pourquoi nous avons suggéré quelques amendements aux rapporteurs des commissions concernées.

Si la finance, par exemple, n'intéresse que les professionnels, la protection des données concerne la vie quotidienne de chacun d'entre nous. D'autre part, le monde entier observe ce que va faire l'Europe sur ce sujet éminemment symbolique. Le dispositif de gouvernance qu'arrêtera l'Union doit, par conséquent, à la fois être crédible pour les particuliers et donner à notre continent un atout supplémentaire dans la compétition internationale. Les pays européens ne doivent pas s'épuiser dans une concurrence intracommunautaire, mais au contraire valoriser un haut niveau de protection des données qui amène à s'établir en Europe nombre d'entreprises, sûres d'y trouver un cadre juridique propice et stable. Tout ce que nous pourrons faire ensemble pour améliorer ce projet de règlement sera donc extrêmement positif.

La CNIL se préoccupe depuis de nombreuses années de la question des fichiers de police, question à laquelle nos concitoyens sont aussi de plus en plus sensibles, depuis l'affaire du fichier Edvige ou l'affaire Merah.

Ces fichiers peuvent être divisés en plusieurs catégories.

Il y a d'abord les fichiers d'antécédents judiciaires, qui atteignent des dimensions considérables : ainsi le STIC – le Système de traitement des infractions constatées – concerne 6,5 millions de personnes. Ces fichiers ont fait l'objet de nombreuses critiques. On leur reproche de ne pas être à jour, d'avoir une finalité judiciaire mais également administrative – les entreprises et les administrations le consultent avant de recruter et ce sont ainsi 1,5 million d'emplois qui en dépendraient. De fait, la CNIL dénonce régulièrement le manque de pertinence d'un certain nombre d'éléments enregistrés dans le fichier STIC et les incidences négatives qu'a sa consultation sur l'accès à l'emploi d'un grand nombre de personnes.

Grâce à la seconde loi d'orientation et de programmation pour la sécurité intérieure, dite LOPPSI 2, nous avons enregistré de réels progrès : l'actualisation des données sera facilitée, nous disposerons d'un magistrat référent et, pour ce qui est de la consultation des fichiers à des fins d'enquête administrative, les classements sans suite ne seront plus opposables. Les fichiers STIC et JUDEX seront en outre fusionnés en 2014 au sein d'un fichier TAJ – traitement d'antécédents judiciaires –, dépendant du ministère de l'Intérieur et qui sera interconnecté avec le fichier Cassiopée du ministère de la Justice, de sorte que l'actualisation que nous appelions de nos vœux se fera automatiquement.

Cependant, ces progrès sont encore un peu en devenir et, en attendant, nous nous préoccupons d'améliorer autant que possible l'existant. D'où quelques propositions.

Tout d'abord, nous avons du mal à apprécier la façon dont s'articuleront les fonctions du magistrat référent compétent pour les fichiers d'antécédents judiciaires et de rapprochement judiciaire, qui vient d'être nommé, avec nos propres compétences de contrôle, notamment s'agissant du droit d'accès indirect. Nous sommes convenus avec Mme Taubira et M. Valls de nous réunir afin de préciser les attributions de chacun.

Deuxièmement, dès les prochains jours, la CNIL contrôlera à nouveau le STIC. Nous prévoyons dix contrôles sur place et trente-quatre sur pièces : nous ne nous limiterons pas, en effet, au fichier lui-même et à ce qui relève du ministère de l'Intérieur, mais nous étendrons notre attention à l'environnement de ce fichier et à sa mise à jour par les procureurs, afin de nous assurer de la pertinence des enregistrements. Nous disposerons des conclusions de l'opération au début de l'an prochain, ce qui nous permettra éventuellement d'avancer des propositions complémentaires.

Troisièmement, nous nous demandons s'il ne serait pas temps de faire évoluer le cadre juridique en fixant des durées de conservation des données différentes pour la consultation à des fins judiciaires et pour la consultation en vue d'une enquête administrative.

Les durées de conservation des infractions dans le fichier STIC sont actuellement de quarante ans aussi bien pour un génocide que pour l'accès frauduleux à des systèmes de traitement, qui n'est pourtant passible que de deux ans de prison ; de dix ans pour l'utilisation de stupéfiants par un mineur, de vingt ans s'il s'agit d'un majeur, et cela quelle que soit la quantité détenue ; de vingt ans également pour bizutage, pour vol – quelle qu'en soit encore la gravité – ou pour mendicité agressive !

Pour certaines de ces infractions, ces durées sont beaucoup trop longues. Si elles peuvent à la rigueur se justifier pour la conservation à finalité judiciaire, elles peuvent en tout cas se révéler extrêmement préjudiciables aux personnes qui cherchent un emploi d'agent de sécurité dans un immeuble ou de gardien de parking, par exemple. Nous réfléchissons donc à une scission en fonction des deux finalités et les enseignements que nous tirerons de notre contrôle du STIC ainsi que les consultations que nous organisons ici ou là nous amèneront probablement à prendre position au début de l'année 2013.

En ce qui concerne les autres fichiers de police, nous continuons notre croisade, qui est aussi la vôtre, tendant à faire progressivement reconnaître et légaliser tous ces fichiers par le ministère de l'Intérieur. Celui-ci fait preuve d'une bonne volonté certaine en la matière : nous sommes régulièrement saisis d'actes réglementaires uniques pour certains de ces fichiers, et d'actes-cadres pour des fichiers simplement opérationnels ou constitués localement. Nous entendons néanmoins rester vigilants.

Dernière catégorie : les fichiers de souveraineté. Les enjeux de sécurité nationale et l'intérêt de la puissance publique justifient dans leur cas un régime juridique très particulier et les conditions de leur création, de leur publication et de leur contrôle font l'objet d'aménagements substantiels. La plupart d'entre eux ne sont pas contrôlés par la CNIL et leur création, soumise à une formalité simplifiée, ne fait pas l'objet d'une publication. Cependant, pèse sur ces fichiers une suspicion généralisée, ce qui n'est pas une bonne chose, et j'ai suggéré à M. Valls de faire entrer – de façon forcément limitée – ces fichiers dans le champ du droit commun et de les soumettre à un contrôle de la CNIL. Actuellement, personne ne les contrôle. Dans un État démocratique comme la France, il serait légitime qu'une autorité de régulation le fasse, dans des conditions qu'il convient bien évidemment d'étudier – peut-être en confiant l'exclusivité des résultats de ces contrôles au ministère de l'Intérieur et en soumettant les agents contrôleurs à une habilitation particulière.

La CNIL n'a pas pour vocation d'empêcher de faire, mais bien plutôt d'accompagner l'action de l'administration et des acteurs économiques en sorte que celle-ci soit menée dans le respect des principes « informatique et libertés ». C'est dans le cadre de cette démarche d'accompagnement de l'innovation que nous traitons avec les grands acteurs internationaux que sont Google et Facebook.

Facebook a fait l'objet d'un audit de plusieurs mois, conduit par l'autorité de régulation irlandaise, chef de file pour le compte de toutes les autorités du G29, sur les conditions de service proposées par le réseau. Un premier rapport nous a été transmis il y a près d'un an. Il ne nous satisfaisait pas entièrement, n'étant pas suffisamment exigeant vis-à-vis de Facebook – dont le siège, je le précise, est situé en Irlande. Nous avons été un certain nombre d'autorités à demander une étude complémentaire. L'autorité irlandaise nous a livré récemment ses conclusions définitives, qui nous conviennent en dépit de quelques réserves. Ce résultat montre l'efficacité de la coopération entre autorités de régulation.

J'en donnerai pour exemple le cas de la reconnaissance faciale. Jusqu'en juillet dernier, Facebook constituait par défaut, sans leur avoir demandé leur accord préalable, le profil photographique de tous ses clients. Depuis plusieurs mois, nous insistions auprès des responsables de la société pour qu'ils demandent le consentement de ceux-ci. Il faut savoir qu'une image biométrique est forcément intrusive et que la base de données que constituent les profils des 25 millions de Français qui ont ouvert un compte Facebook – et que dire de la base mondiale ! – peut être utilisée à des fins bien diverses. En juillet, ces responsables ont

accepté d'instaurer le non-paramétrage par défaut – désormais, le détenteur d'un compte doit consentir expressément à ce que Facebook établisse son profil biométrique.

La coopération entre autorités de régulation nous permet donc d'opposer aux acteurs internationaux un front uni pour les pousser à modifier leurs pratiques. Certes, ils ne manquent pas d'arguments – d'ailleurs, la première réponse de Facebook fut de nous rappeler que, n'étant pas localisée en Europe, leur société n'était pas soumise à la législation européenne. En tant qu'autorités de contrôle, nous avons avec ces acteurs un rapport de force permanent, à la fois juridique, sociologique et médiatique, que seule la coopération européenne peut faire tourner au profit de l'usager.

En ce qui concerne Google, c'est la CNIL qui a été mandatée par l'ensemble des autorités européennes pour expertiser la nouvelle politique de protection de la vie privée annoncée par cette société en mars dernier. Cette protection, qui s'applique à soixante des services qu'elle propose, serait selon ses dires plus simple et donc compréhensible pour tous. Avec un certain nombre d'autorités européennes, nous avons constaté qu'elle permettait surtout de procéder entre lesdits services à des échanges de données qui ne sont pas maîtrisés par les clients : par exemple d'afficher une publicité sur Youtube en fonction de l'utilisation faite par l'usager de son téléphone portable, Android étant également un produit Google.

La CNIL, pour le compte du G29, a adressé un questionnaire très précis à Google lui demandant de spécifier quel type d'informations était donné au client et quelle utilisation était faite des données pour quels types de services. Une première salve de réponses ne nous ayant pas parue satisfaisante, nous avons envoyé un deuxième questionnaire, auquel la firme a répondu en juillet dernier. En coopération avec l'ensemble des autorités, nous avons élaboré début septembre un projet de conclusions qui vient d'être adopté par le G29 et sera présenté à la presse le 16 octobre.

Ces conclusions montrent que la situation n'est pas totalement satisfaisante, au moins sur deux points. Tout d'abord, l'information des internautes est trop sommaire : ils ne savent pas, lorsqu'ils utilisent un service, quelles données celui-ci utilise et comment il fonctionne. D'autre part, les échanges de données manquent de base légale lorsqu'ils s'effectuent entre des services qui ne les exigent pas : s'il est admis qu'il peut y avoir communication entre votre téléphone portable et votre carnet d'adresses pour puiser dans celui-ci la date de naissance de vos amis afin de vous permettre de leur souhaiter leur anniversaire comme vous l'avez demandé, un service qui relie Youtube et votre téléphone portable nécessite en revanche un consentement. Or Google n'a pas répondu aux questions concernant un certain nombre de ces services pour lesquels la base légale manque de clarté.

Il est intéressant de noter que, dans cette affaire, d'autres autorités dans le monde se sont jointes au G29 : les Australiens et les Canadiens, qui partagent nos préoccupations, nous ont fait part de leur souhait de signer le courrier adressé à Google. La communauté des régulateurs est en train de se constituer pour offrir aux populations une réponse mondialisée face aux acteurs économiques de dimension internationale !

Quoi qu'il en soit, la discussion n'est donc pas close et Google va sans doute opposer à nos conclusions des arguments juridiques, par exemple sur la compétence. Il n'empêche que la pression des régulateurs et de l'opinion publique est extrêmement efficace pour faire évoluer les pratiques de ces acteurs.

Enfin, je pense que des modifications de la loi « Informatique et libertés » pourraient être envisagées pour aider la CNIL à mieux fonctionner et à mieux s'adapter à l'univers numérique tel qu'il est aujourd'hui.

En premier lieu, si notre commission est consultée sur les projets de loi, elle n'est pas compétente pour donner un avis sur les propositions de loi, sur les amendements ou même sur les projets de loi ayant fait l'objet de modifications substantielles après sa consultation. Cela l'a parfois conduite à s'autosaisir, par exemple à propos de la carte d'identité électronique ou sur la LOPPSI. Ne pourrait-elle être saisie pour avis par les présidents de l'Assemblée nationale et du Sénat, comme peuvent l'être le Conseil d'État et le Conseil économique, social et environnemental (CESE) ? Nous sommes en effet particulièrement désireux de mettre notre expertise juridique et technique à votre disposition dans un cadre plus officiel que celui des auditions auxquelles nous sommes régulièrement conviés.

Une deuxième proposition concerne les expérimentations. On reproche souvent à la CNIL d'être trop lente. Certains d'entre vous ont, je crois, souhaité qu'elle puisse être saisie d'expérimentations. Il faut en effet s'adapter à la nouvelle manière de travailler des administrations. Il serait bon que la CNIL puisse être saisie rapidement de projets qui ne sont pas totalement finalisés, mais sur lesquels elle a un avis à rendre. Nous pourrions expérimenter cette possibilité, par exemple à propos des fichiers de police. Cela nécessiterait de donner à notre bureau la capacité de statuer sur ces expérimentations.

Je ferai une troisième proposition, relative à notre activité de contrôle, qui s'est considérablement développée. Nous avons procédé à plus de 350 contrôles cette année. Certains sont très lourds – ils nécessitent par exemple d'aller sur place – et coûteux. En outre, nous exerçons depuis 2011 une nouvelle mission : destinataires de la notification des failles de sécurité imposée aux opérateurs de télécommunications, nous devons, dans ces cas, diligenter un contrôle sur place. Or les « veilleurs » qui existent sur Internet nous signalent déjà toute une série de ces failles. Pourquoi ne pas ouvrir à la CNIL la possibilité d'exercer un contrôle de système à distance, ce qu'elle ne peut faire aujourd'hui sans tomber sous le coup de la loi Godfrain ? Exercer un tel contrôle à propos d'une faille de sécurité qui nous a été dénoncée est en effet considéré comme une intrusion dans un système informatique et réprimé comme tel par cette loi. Ne serait-il pas intéressant, ainsi que cela a été fait pour les services de lutte contre la pédo-pornographie, d'ouvrir à la CNIL une possibilité – très encadrée – de contrôle à distance, avec la faculté pour les agents concernés d'utiliser une identité d'emprunt ?

M. Sébastien Pietrasanta. Je reviens sur la protection des données personnelles dans l'univers numérique et sur le manque de transparence dans le traitement de ces données, notamment par Facebook. Récemment, une nouvelle polémique est née autour de ce réseau social. Les services de la CNIL ont mené des investigations mais n'ont pas conclu à un dysfonctionnement réel du site. Il n'en reste pas moins que les réseaux sociaux entretiennent une certaine complexité en modifiant de façon récurrente et unilatérale leurs règles de confidentialité, et ce à l'insu des utilisateurs. Je prendrai quelques exemples concernant encore Facebook. Est-il normal que le profil de l'utilisateur soit accessible à tous à partir des moteurs de recherche, notamment Google, si les paramètres de confidentialité ne sont pas correctement paramétrés ? Même en utilisant correctement ces derniers, il est impossible de limiter l'accès à la photo de profil ou de couverture. La photo de profil est visible sur les banques d'images des moteurs de recherche. Il n'est pas possible de supprimer des messages privés : ils vont dans une boîte d'archives qui ne peut être vidée. La géolocalisation peut

également poser problème. Enfin, un ami Facebook peut publier des photos de vous sur son propre mur sans votre autorisation.

Les paramètres protecteurs de la vie privée sur les réseaux sociaux sont-ils aujourd'hui réellement garantis ? Les préconisations du G29, notamment celle d'une meilleure transparence pour les usagers, ont-elles été prises en compte par les acteurs des réseaux sociaux ? Comment comptez-vous inciter ces derniers à faire évoluer leurs pratiques ?

Mme Isabelle Falque-Pierrotin. L'incident Facebook est symptomatique de la situation. Il n'y a pas eu de *bug* technique, au sens strict du terme, mais il y a bien un *bug* sociologique et comportemental, lié à l'opacité absolue de ces réseaux et de leur fonctionnement, et si la panique a pu gagner les internautes français en l'espace de vingt-quatre heures, c'est bien parce qu'ils ont brusquement découvert qu'ils n'avaient pas la maîtrise de cet univers.

Vous avez raison, il y a un manque de transparence et de simplicité dans les offres que ces réseaux sociaux font à leurs clients. Le communiqué de presse que nous avons rédigé à l'issue de l'affaire n'a d'ailleurs pas dédouané Facebook de ses responsabilités. Au contraire, nous avons dit que cet incident montrait que l'opacité prévaut sur les règles de paramétrage, et que Facebook n'avait pas satisfait à la demande de la CNIL et du G29 de mettre en place un paramétrage par défaut beaucoup plus protecteur des données personnelles. De façon plus générale, nous sommes déjà intervenus auprès de Facebook sur les divers points que vous avez énumérés, et c'est pourquoi nous n'étions pas entièrement satisfaits de l'audit irlandais.

Nous allons continuer à exercer une pression sur Facebook, et voir comment nous pouvons agir sur un plan juridique vis-à-vis de cette société, établie je le rappelle en Irlande. Mais, en complément, nous attirons également l'attention de l'utilisateur final sur la nécessité d'être vigilant. Nous nous attacherons plus particulièrement dans les prochains mois à lui fournir des conseils et des outils pour la maîtrise de son activité en ligne.

Mme Axelle Lemaire. La majorité des grands acteurs de l'innovation dont vous avez parlé se trouvent sur le territoire de ma circonscription, en Europe du nord. Le *cloud computing*, ou informatique en nuage, progresse de manière exponentielle à travers le monde, notamment en Europe, que ce soit auprès des entreprises ou des particuliers. Le déploiement de ces services est une source potentielle de croissance et de création d'emplois – selon la Commission européenne, jusqu'à 2,5 millions d'emplois pourraient ainsi être créés d'ici à 2020. Dans le contexte de concurrence que vous avez évoqué, je m'interroge néanmoins sur la possibilité de protéger effectivement les données des utilisateurs. En effet, l'utilisation de ce type de services par le grand public pour partager des documents, de la musique ou des photos tend à se traduire par un renforcement des groupes internationaux utilisant des hébergements mutualisés à travers le monde. Si la stratégie numérique dévoilée par la Commission européenne le 27 septembre 2012 propose une certification pour identifier les prestataires fiables, elle ne comporte aucun élément précis en matière de législation permettant de renforcer la protection des données. Or, en ce domaine, le droit est assez nébuleux. Comment mieux protéger les données des utilisateurs français, alors que le droit applicable doit être modifié par une nouvelle réglementation européenne ?

Mme Isabelle Falque-Pierrotin. Le *cloud* est aujourd'hui présenté comme *l'alpha et l'oméga* des infrastructures informatiques : sa souplesse et son faible coût le rendraient très intéressant pour tout type d'utilisateur, particulier ou entreprise. C'est vrai à certains égards,

mais il y a une contrepartie : le client perd la maîtrise de la localisation de ses données – donc de leur sécurité et de leur confidentialité.

Nous étudions depuis plusieurs mois ces offres de *cloud*, qui sont extrêmement variées. Après avoir auditionné et consulté la plupart des acteurs, nous avons émis en juin une recommandation qui s'adresse principalement aux professionnels. L'enjeu est réel : beaucoup d'entreprises et d'universités mettent dans le *cloud* des travaux et des données confidentiels, et il faut s'assurer que ceux-ci ne soient pas accessibles à tous. Nous avons donc rédigé à l'intention de ces clients professionnels une sorte de guide d'accompagnement, pour les aider à décider de mettre ou non certaines informations dans le *cloud* et pour mettre à leur disposition des clauses contractuelles types, leur permettant de s'assurer auprès de leur prestataire de la réalité des garanties de sécurité et de confidentialité offertes. En l'état actuel du droit, où il n'existe pas de responsabilité du prestataire au regard de la loi « Informatique et libertés », cela devrait leur permettre de se prémunir.

La situation des particuliers est différente, puisque leur capacité de négociation avec l'offreur est nulle. Vous avez parlé de certification. Peut-être pourrions-nous faire appel à la notion de label – puisque nous avons désormais la possibilité d'en délivrer.

L'argument « informatique et libertés » peut aussi être promu comme un élément de compétitivité auprès des offreurs de *cloud*. La concurrence est en effet telle sur ce marché que si l'Europe veut être attractive, elle doit offrir quelque chose de plus. Cela peut être des garanties en termes de protection des données personnelles et de sécurité. Aussi encourageons-nous les acteurs du *cloud* à en faire un argument concurrentiel.

M. Lionel Tardy. Que pensez-vous du rapprochement envisagé entre autorités administratives indépendantes ? On parle d'une fusion entre le Conseil supérieur de l'audiovisuel (CSA) et l'Autorité de régulation des communications électroniques et des postes (ARCEP), et nous allons discuter cet après-midi dans l'hémicycle de l'intégration de la présidente de la CNIL dans le collège de la Commission de régulation de l'énergie (CRE).

Ma deuxième question porte sur le *cloud computing*. J'ai assisté hier au colloque organisé par la Fédération des industries électriques, électroniques et de communication (FIEEC) et la CNIL : il faut avant tout diffuser les principes « informatique et libertés », car il est évident que l'on ne pourra pas tout sanctionner. Le problème majeur est celui de l'extra-territorialité des données et, à cet égard, il ne faut pas rater le coche : si tous les serveurs sont à l'étranger, nous ne pourrons pas faire grand-chose, sauf à l'échelle européenne. Je suis allé aux États-Unis avec mon collègue Patrice Verchère : nous avons bien compris que l'État américain laisserait faire Google et Facebook. Quelles sont les solutions envisageables ? Il n'en existe hélas guère, sauf à nous mobiliser pour faire en sorte qu'il y ait des centres et des serveurs en France. C'est l'objet du projet Andromède. Je me félicite que Mme Pellerin ait assisté hier à la présentation du projet Cloudwatt. Nous devons absolument maintenir ce cap.

Comment envisagez-vous le développement de l'*open data* sous l'angle de la protection des données personnelles ? Quelles sont vos recommandations ? Quelles évolutions législatives préconisez-vous ?

Ma dernière question porte sur les moyens de la CNIL. Le nombre de plaintes, de conseils et d'avis a progressé de 20 %, avez-vous dit, et seule la direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) connaît une hausse comparable des sollicitations. Dans le même temps, vos missions se sont considérablement accrues. Comment voyez-vous l'avenir de votre institution ?

Mme Isabelle Falque-Pierrotin. Le CSA et l'ARCEP sont des autorités de régulation d'opérateurs économiques qui sont connus et en nombre limité. Le métier de la CNIL est tout autre. Notre population cible est extrêmement hétérogène : collectivités locales, administration, grandes entreprises internationales, particuliers… En réalité, la CNIL régule une thématique ; et dans la mesure où celle-ci est horizontale, elle est difficilement soluble dans un « meccano » institutionnel du type CSA-ARCEP.

Il y a en effet des enjeux majeurs dans la régulation de l'énergie : quoi que l'on puisse en penser, ce secteur est appelé à utiliser de plus en plus les traitements de données et l'analyse de fichiers. La CNIL a donc son mot à dire. Doit-elle pour autant être représentée au collège de la CRE ? Nous ne l'avions en tout cas pas demandé. Il y a d'autres moyens d'associer étroitement ces deux autorités. On peut par exemple imaginer une consultation obligatoire sur les sujets ayant une incidence en matière de traitement des données. Nous pouvons faire des propositions, comme nous l'avons fait dans le cadre des auditions de cet été au Sénat et à l'Assemblée nationale. Bref, s'il est important que la dimension « informatique et libertés » soit pleinement prise en compte, la réponse institutionnelle peut être variable.

J'en viens au *cloud* et à l'extra-territorialité. Ce sujet majeur appelle au moins deux réponses. Pour ce qui est du *cloud* souverain, c'est-à-dire du *cloud* de l'administration ou des données publiques, il est impératif que les serveurs soient localisés en France ou en Europe. Je l'ai redit récemment aux responsables des différents projets de *cloud* français. Outre que c'est une garantie physique indispensable, c'est en effet la question du droit applicable qui est posée. C'est pourquoi le dispositif de Mme Reding ne nous convient pas. Nous lui avons demandé dans notre contre-proposition d'introduire un critère de résidence. Il y a aujourd'hui deux critères : la loi européenne s'applique s'il y a un établissement en Europe ou s'il y a des moyens de traitement, ce deuxième critère étant accessoire. Les grandes entreprises internationales arguent bien sûr toutes qu'elles n'ont pas d'établissement en Europe, ou bien qu'il n'y a pas de moyens de traitement, mais simplement des moyens commerciaux. Il est indispensable que nous puissions « rapatrier » le traitement éventuel du conflit en Europe. Pour cela, il faut un critère de résidence. Le règlement en cours d'élaboration répond *a priori* à cette exigence : même si un opérateur de traitement n'est pas établi en Europe, s'il cible un résident européen, le règlement européen sera applicable.

L'*open data* est à la fois un sujet de société et un enjeu économique. C'est un sujet de société, car il répond à l'attente de transparence qui est désormais portée par le numérique. C'est un enjeu économique, car la mise à disposition de ces données publiques va permettre de créer de nouveaux services et de stimuler la croissance. La CNIL ne peut donc qu'y être favorable. En revanche, les données personnelles concernées ne peuvent perdre la protection qui leur est attachée simplement parce qu'elles appartiennent à l'*open data*. Au moment de l'implantation d'Etalab en France, nous avons donc demandé à ses responsables qu'une licence spécifique soit mise en place dès lors que l'*open data* concernerait des données personnelles. La discussion n'est pas aisée car, ce faisant, on créera un obstacle à la mise en ligne, que ce soit à travers une demande d'anonymisation ou que cela résulte de l'obligation de respecter un droit d'opposition.

La prise en compte de la protection des données personnelles est une contrainte supplémentaire qui coûte, mais elle est indispensable si l'on veut éviter que l'*open data* ne rencontre l'opposition de nos concitoyens voyant livrer en pâture au grand public des informations personnelles les concernant. Nous sommes donc actuellement dans cette phase de dialogue avec les responsables de l'*open data*, afin d'instiller cette préoccupation dans leur politique.

La question de nos moyens est posée de façon récurrente depuis 2004-2005, mais ces moyens ont déjà considérablement augmenté depuis cette date. Notre budget de fonctionnement s'établit aujourd'hui à environ 16 millions d'euros et nous employons 180 personnes. La difficulté vient de ce que nos compétences ne cessent de s'étendre avec l'expansion du numérique. Nous avons fait valoir ce point auprès du Premier ministre dans la négociation budgétaire triennale qui s'engage. Nous avons obtenu 21 créations de postes sur trois ans, soit 7 postes par an. Notre budget de fonctionnement enregistre en revanche une légère baisse, ce qui nous pose problème. L'éducation numérique, objectif fondamental de la CNIL et « couche de base » de la régulation, coûte cher, alors que nos moyens sont relativement limités. Notre département d'expertise est l'un des meilleurs d'Europe – c'est d'ailleurs pour cette raison que nous avons été mandatés dans l'affaire Google mais, là encore, cela exige d'investir dans des matériels et dans des expérimentations. J'espère donc que nous aurons les ressources nécessaires pour faire face à ces obligations.

Mme Marietta Karamanli. Je constate que, dans le règlement et la directive, les formalités préalables à la mise en œuvre d'un traitement de données à caractère personnel à effectuer auprès de la CNIL constituent la partie immergée de l'iceberg. Le projet de règlement ne devrait-il pas réduire ces formalités déclaratives, dont un certain nombre d'avocats ou d'organismes remettent en cause l'efficacité ? Existe-t-il une étude ou une évaluation – qu'elle soit française ou européenne – de l'utilité de ces déclarations ? Comment revoir cette question pour mieux protéger le citoyen et le rapprocher de l'autorité de traitement ?

Au vu de ce règlement et des avis qui ont été donnés, dont celui de la CNIL, il apparaît que la consultation de l'autorité de contrôle, préalable à la mise en œuvre d'un traitement de données à caractère personnel, n'est pas totalement supprimée. Dans ce cadre, certains traitements resteraient soumis à un contrôle préalable de la CNIL, dans trois cas importants : les transferts hors de l'Union européenne lorsque le responsable du traitement et le destinataire des données ne sont pas liés par des clauses contractuelles types conformes à celles adoptées par la Commission européenne ; les transferts de données hors de l'Union européenne, vers des pays n'offrant pas un niveau de protection adéquat ; et les traitements de données sensibles – analyse comportementale, profilage, *scoring*, données relatives à la vie sexuelle. Pensez-vous que la liste de ces traitements doive être allongée et, si oui, pour couvrir quels domaines ?

En mars 2012, le contrôleur européen indiquait que le rôle et les pouvoirs des autorités nationales de contrôle seraient renforcés. Cette assertion vous semble-t-elle exacte ?

Mme Isabelle Falque-Pierrotin. Le principe de la directive, c'est de substituer à des formalités lourdes de contrôle *a priori* une politique de sanctions fondée sur la responsabilisation des contrôleurs de traitement, l'*accountability*. Cela passe par la constitution d'une documentation, d'études d'impact ou par la désignation de correspondants Informatique et libertés. Le règlement constitue par conséquent un changement de paradigme radical en termes de régulation.

Sont substituées aux formalités déclaratives de nouvelles modalités. Aujourd'hui, nous délivrons un récépissé dans un délai de quatre jours et cela n'est pas un gros mot de dire que le contrôle que nous exerçons est faible. Au reste, la délivrance du récépissé ne garantit pas la conformité à la loi Informatique et libertés. L'abandon des obligations de déclaration n'a donc rien de dramatique, d'autant que celles-ci sont remplacées par des obligations de

documentation, que certains des acteurs concernés trouvent déjà trop lourdes, demandant à ce qu'elles soient modulées en fonction du type d'entreprise ou de la nature des données traitées.

La consultation et le recueil de l'avis des autorités demeurent, mais dans un très faible nombre de cas, qui concernent notamment les transferts internationaux. Il nous semblerait plus pertinent de pouvoir redemander du contrôle en amont pour ce qui concerne les données sensibles, mais ce serait aller à rebours de la directive. La liste des données sensibles y est fixée de manière tout à fait limitative : à titre d'exemples, les données génétiques et la biométrie n'y figurent plus. C'est un point sur lequel nos propositions n'ont pas été entendues et nous le regrettons vivement. Réintégrer les données génétiques et la biométrie dans la liste nous paraîtrait d'autant plus essentiel que leur exploitation va se développer énormément et que les risques afférents ne sont pas totalement maîtrisés. Désormais, lorsqu'on couplera de la vidéoprotection avec de la reconnaissance faciale, ce ne sera plus considéré comme l'exploitation de données sensibles et les autorités de contrôle ne seront pas consultées *a priori*. Sans doute disposera-t-on d'autres moyens pour récupérer des connaissances sur ces traitements, mais il nous incombera d'aller chercher une information qui nous est aujourd'hui fournie.

Nous séparons-nous des conclusions du contrôleur européen des données personnelles (*European Data Protection Supervisor - EDPS*) ? Non, mais il s'agit d'une vérité textuelle plutôt qu'opérationnelle. L'objectif de Mme Reding tel que l'exprime le texte, c'est que toutes les autorités soient dotées des mêmes pouvoirs et, autant que faire se peut, des mêmes ressources. Le texte fixe des orientations et des obligations de moyens, mais qu'en sera-t-il dans la réalité ? Les Vingt-Sept ont-ils tous le même appétit en matière de protection des libertés et l'adoption du règlement se traduira-t-elle par leur « mise à l'équerre » sur ces questions dès 2015 ? Je n'en suis pas persuadée.

M. Patrice Verchère. Si l'on veut du *cloud computing* dans les pays européens, il faut absolument qu'il soit européen à 100 % puisque, sur le sol des États-Unis comme dans les autres pays, les entreprises américaines sont soumises au *Patriot Act* qui fixe des obligations en matière d'information des services de renseignement américains.

Le rapport d'information que, sous la législature précédente, j'ai rédigé avec Patrick Bloche sur les droits de l'individu dans la révolution numérique proposait notamment de modifier l'article 25 de la loi de 1978 afin de soumettre les demandes de traitement des données de géolocalisation – en plein essor – à un régime d'autorisation plutôt que de simple déclaration. Votre prédécesseur, M. Alex Türk, s'était montré très sensible à cette préoccupation. La géolocalisation permet véritablement d'entrer dans la vie des gens en suivant leurs déplacements : que pouvez-vous nous dire à ce sujet ?

Une proposition de loi, en cours de discussion, instaure une tarification progressive de la consommation énergétique des ménages. J'ai bien compris – et je trouve logique – que les propositions de loi ne soient pas soumises à la CNIL. Néanmoins, je crois savoir que le rapporteur vous a consulté car il s'agit ni plus ni moins que de constituer un fichier énorme, de plus de 30 millions de foyers et entrant véritablement dans l'intimité des gens. Quel a été l'avis de la CNIL ? Bien qu'il n'y en ait aucune trace dans son rapport écrit, le rapporteur a semblé dire que vous n'aviez pas soulevé d'objection mais, comme la confiance n'exclut pas le contrôle, je préfère poser la question.

Mme Isabelle Falque-Pierrotin. Il est certain que la collecte, *via* les grands acteurs économiques du *cloud* ou d'autres, de données extrêmement sensibles pouvant aller jusqu'à la

connaissance de secrets d'entreprise, au nom de la sécurité ou de l'intelligence économique, présente un intérêt considérable pour les États-Unis, et le danger est d'autant plus grand que le *Patriot Act* autorise la transmission de ces données à des autorités étrangères. C'est une des raisons qui nous ont poussés à appeler l'attention des clients professionnels sur l'importance de leur décision de localiser certaines catégories de données dans le *cloud*. Même si cela devait leur coûter moins, il serait assez irresponsable par exemple que toutes les universités françaises recourent à des offres de *cloud* d'opérateurs américains, au risque de communiquer les secrets de notre recherche !

Une réflexion collective s'impose sur l'ensemble des paramètres à prendre en compte dans ce type d'offre, qu'il s'agisse de la confidentialité, du respect des personnes, de l'intelligence économique, du renseignement ou de la sécurité. J'ai fait connaître ce point de vue de manière très insistante au président de la République et au Premier ministre car je considère que cet enjeu dépasse très largement les frontières d'une relation contractuelle entre deux parties.

Faut-il soumettre le recueil des données de géolocalisation à un régime de déclaration ou d'autorisation ? On sent bien qu'au fil du temps, ces données tendent à devenir des données sensibles. Les individus sont à la fois très friands des services conçus à partir de la géolocalisation – situer ses amis, un restaurant, une boutique…– mais ils en voient bien le revers. Faut-il pour autant retenir un régime d'autorisation ? Il faut y réfléchir car la géolocalisation peut être couplée à d'autres services et il ne faudrait pas faire obstacle à la mise en place de services utiles dont la géolocalisation ne constitue pas l'élément essentiel.

S'agissant de la proposition de loi instaurant une tarification progressive de l'énergie, nous avons effectivement été auditionnés par les rapporteurs du Sénat et de l'Assemblée nationale. Ne pouvant être saisie, la CNIL n'a pas exprimé de position officielle. L'enjeu de traitement est énorme puisque les forfaits de base seront établis à partir des déclarations de revenu, puis transférés à un tiers gestionnaire, lui-même chargé d'élaborer les profils de base qui seront transmis aux fournisseurs d'énergie pour qu'ils en fixent le tarif. Le dispositif est assez pertinent dans la mesure où il limite la circulation de l'information et l'accès des fournisseurs d'énergie aux données personnelles en partant de la déclaration de revenu et en faisant intervenir un tiers délégataire de la puissance publique. Le problème, c'est que l'on n'en sait pas tellement plus en ce qui concerne l'informatique et les libertés puisque tout a été renvoyé à des décrets. Certes, ceux-ci seront pris après consultation de la CNIL – laquelle publiera des avis motivés – et du Conseil d'État. Cependant, cela me semble encore trop peu eu égard à l'importance de cette affaire pour les Français...

M. Patrice Verchère. 33 millions de foyers concernés !

Mme Isabelle Falque-Pierrotin. … et cela suscite d'ailleurs une certaine mobilisation. Ce fichier entre littéralement dans les maisons des consommateurs et nous ferons donc preuve de la plus extrême vigilance.

M. Sergio Coronado. La CNIL a été très attentive au respect des principes « informatique et libertés » dans l'organisation des primaires d'Europe Écologie Les Verts (EELV) et du Parti socialiste. Dès lors, il eût été assez logique qu'elle se penche avec la même attention sur l'élection, pour la première fois et par vote électronique, des onze députés représentants des Français de l'étranger. Des alertes avaient été lancées par les partis politiques, par les candidats, par les associations attachées au respect des libertés fondamentales et par le parti Pirate. Elles se sont malheureusement révélées fondées : le vote

électronique ne s'est pas déroulé dans de très bonnes conditions. La CNIL va-t-elle rendre un rapport sur ce processus électoral ? Quel sera notamment le devenir des listes électorales comportant des données personnelles, très largement diffusées ?

Vous avez rappelé les pouvoirs que vous confère la loi dite LOPPSI 2 en matière de vidéosurveillance. S'agissant du fichier STIC, vous allez vous attacher non seulement au contrôle formel mais aussi, avez-vous dit, à celui de l'environnement. Allez-vous procéder de même pour la vidéosurveillance, sachant que la ville d'Amiens a conduit une étude dont les conclusions convergent avec les travaux du sociologue Tanguy Le Goff et mettent en évidence la prégnance du regard discriminatoire des agents en charge de la vidéosurveillance ?

Mme Isabelle Falque-Pierrotin. En 2011, nous avons en effet été assez actifs dans le suivi des nouveaux processus électoraux. À la suite de l'action menée pour les primaires internes de certains partis, nous avons même mis en place un observatoire pour être à même de rappeler au respect des principes « informatique et libertés » dans toutes les nouvelles techniques de propagande et d'accès à l'électeur. Force est de reconnaître que ces pratiques ne sont pas pleinement satisfaisantes et, dans la perspective des élections à venir, nous organiserons bientôt des réunions avec les partis politiques pour leur rappeler les règles relatives à l'utilisation des données personnelles.

S'agissant des listes électorales consulaires, vous avez eu raison de rappeler qu'il y avait eu un « souci », ce qui nous a conduits à solliciter le ministère des Affaires étrangères à plusieurs reprises. Le vote s'est toutefois déroulé et nous allons à nouveau rencontrer les représentants de ce ministère pour revenir sur l'utilisation de ces listes électorales. Se pose avec une acuité particulière le problème des adresses *e-mail* des Français de l'étranger, qui, en principe, ne sont pas collectées pour des opérations de prospection électorale. Nous avons recommandé l'existence de deux adresses *e-mail* distinctes, mais nous n'avons pas encore été entendus sur ce point. Il convient de rectifier le tir et de faire en sorte que les prochains scrutins se déroulent différemment.

En matière de vidéoprotection, nous avons mené plus de 150 opérations de contrôle au cours de l'année 2011, sur les 900 000 caméras installées au titre de la loi du 21 janvier 1995.

M. Sergio Coronado. Les contrôles de la CNIL sont formels et portent pour l'essentiel sur les autorisations préalables et sur l'orientation des caméras. Je vous interrogeais plus précisément sur la prégnance du regard discriminatoire des agents en charge de la vidéosurveillance et sur le temps effectif qu'ils y consacrent. La CNIL peut-elle élargir son champ de contrôle à cet environnement ?

Mme Isabelle Falque-Pierrotin. Peut-être ne me suis-je pas exprimée assez clairement. Lorsque j'indique que nous allons prendre en compte l'environnement du fichier STIC, cela ne signifie pas que nous allons piloter des études sociologiques sur la manière dont travaillent les officiers de police. Ce n'est pas notre métier et nous ne disposons pas des ressources nécessaires. Lorsque j'évoque l'environnement du fichier, je distingue ce qui relève du ministère de l'Intérieur de ce qui incombe à la Chancellerie, c'est-à-dire les mises à jour demandées par les procureurs. Notre département des études et de la prospective pourrait sans doute conduire le type d'étude sociologique que vous évoquez, mais, dans les mois à venir, il va plutôt concentrer ses efforts sur la biométrie et sur la reconnaissance faciale.

M. le président Jean-Jacques Urvoas. Je donne la parole à Laurence Dumont dont la nomination à la CNIL a été publiée ce matin même au *Journal officiel*.

Mme Laurence Dumont. J'entends y siéger dès la semaine prochaine.

Mme Isabelle Falque-Pierrotin. Et nous serons ravis de vous accueillir !

Mme Laurence Dumont. Il est fou de constater comme le droit court après les évolutions technologiques. Si nous sommes tous d'accord sur la nécessité de protéger les données personnelles le plus en amont possible, les puces d'identification par radiofréquence *RFID* offrent un contre-exemple extraordinaire. Votre prédécesseur avait du reste fait part de ses inquiétudes sur le développement de cette technologie. Quelques industriels et États ont adopté un code de bonne pratique, le *Privacy impact assessment (PIA)*, mais il est dépourvu de portée normative et des milliards de puces circulent aujourd'hui sur la planète hors de tout contrôle.

En sus de l'absence de vigilance des citoyens, il y a aussi sans doute, dans notre pays en particulier, une absence de moyens légaux. S'agissant des *RFID*, des associations de consommateurs allemandes ou américaines ont réussi à faire bouger les lignes en obtenant que les puces puissent être désactivées. Il n'existe pas en France de telles procédures, permettant à des acteurs non gouvernementaux de porter ces questions sur le devant de la scène politique. Peut-être sont-ce les plus vigilants qui ont le plus de mal à se faire entendre ?

S'agissant des fichiers de souveraineté, vous n'avez pas précisé jusqu'où allait la bonne volonté du ministère de l'Intérieur. Qu'en est-il ?

À titre anecdotique, je souhaite enfin rappeler que, sauf erreur de ma part, l'Assemblée nationale impose toujours un *Pass Navigo* nominatif aux députés.

M. Lionel Tardy. Cela ne me pose aucun problème !

Mme Laurence Dumont. Il y a quelques années, j'avais adressé une lettre ouverte à mes 576 collègues pour obtenir un *Pass* anonyme et je n'ai recueilli que deux réponses. L'absence de vigilance des citoyens et d'éducation au numérique s'étend donc sans conteste aux parlementaires.

Mme Isabelle Falque-Pierrotin. Vous avez déploré que le droit soit toujours à la remorque de la technique. Ce que nous apprend surtout la période actuelle, c'est que, pour réguler, on doit mobiliser d'autres outils en complément du droit. Le droit n'est pas en retard mais il n'a pas toujours le degré de granularité et de souplesse adapté aux mutations de l'ère numérique. S'agissant des puces *RFID*, le *PIA* – qui était en fait une étude d'impact – définit une norme qui s'impose aux industriels pour que leur gestion de ces étiquettes communicantes soit respectueuse des droits et libertés. Cela complète l'encadrement législatif et réglementaire. Le régulateur dispose désormais d'une boîte à outils plus riche que par le passé, avec tout à la fois des instruments juridiques classiques et des référentiels de standardisation ou de labellisation qu'il faut tous mobiliser en même temps.

Le métier de régulateur est devenu plus compliqué mais cela ne discrédite pas le droit car certains choix ne peuvent être faits que par lui. Lorsque l'on dit que pour les *cookies*, il faut un *opting*, c'est bien le Parlement qui l'impose à un moment donné. Il faut envisager une complémentarité en forme de poupée russe, du droit le plus contraignant à la régulation la plus douce.

Hier, lors d'une rencontre à la Fédération des industries électriques, électroniques et de communication (FIEEC) à laquelle participait M. Tardy, il a été dit que nous entrions dans un univers où les objets vont communiquer, y compris malgré nous. C'est à l'évidence potentiellement porteur de services très intéressants. Mais il faut aussi veiller à ce que ces outils ne deviennent pas des mouchards ou des espions et tout doit être fait pour en conserver la maîtrise. Il doit toujours rester possible de les désactiver, lorsque l'on n'en a pas l'utilité. Or le droit français est loin de s'opposer à une telle désactivation. C'est du *opt out* et rien dans notre droit ne fait obstacle à une telle neutralisation des puces.

Quel a été le degré de bonne volonté de M. Valls et de ses services en matière de fichiers de souveraineté ? Nous n'en sommes qu'au stade exploratoire et le ministre a exprimé une position d'ouverture quant à la nécessité de contrôler ces fichiers.

Mme Marie-Anne Chapdelaine. Il faut être attentif au fait que les mentions relatives au droit d'accès et de rectification des données personnelles sont souvent noyées dans les conditions générales de vente, ce qui les rend peu accessibles à certaines personnes. Un effort de transparence s'impose par conséquent.

Comment va-t-on passer outre la législation américaine ? Amnesty International s'est beaucoup préoccupée du *Patriot Act* mais parviendra-t-on jamais à lever cet obstacle ?

Nombre de fichiers concernent le domaine de la santé en général, pour ne pas parler de l'informatisation des dossiers médicaux. Comment se donner les moyens de les réguler ? Un problème s'est posé récemment à propos d'un hébergeur mais j'imagine mal que lui soient appliquées des sanctions financières.

Enfin, j'aimerais comprendre ce que sera le rôle réel d'un correspondant « informatique et libertés » dans les entreprises.

Mme Isabelle Falque-Pierrotin. Votre première remarque sur la transparence fait écho à ce que nous disons depuis longtemps. Face à des services de plus en plus sophistiqués, il y a à l'évidence un déficit de transparence et tout ce qui peut accroître la lisibilité des conditions d'utilisation des données personnelles doit être recherché. À titre d'exemple, c'est un point sur lequel nous avons insisté auprès de Google, dont la nouvelle politique relative à la protection de la vie privée, si elle semble plus simple et fédérative, est aussi plus opaque. Dans notre rapport, nous avons fait des recommandations très précises pour ménager trois niveaux d'information progressifs : une information de base, un niveau intermédiaire et une information plus complète. Un seul texte ne peut tout résoudre et il faut donc organiser l'information de façon graduée.

La question du *Patriot Act* relève du pouvoir politique et non des prérogatives de la CNIL. Faut-il permettre à des autorités étrangères d'avoir accès à des données – de voyages, médicales, financières, etc. – qui concernent d'autres États ? Le problème n'est pas technique, mais politique.

S'agissant des dossiers médicaux, je rappelle que les hébergeurs de données de santé doivent faire l'objet d'un agrément particulier assorti d'obligations spécifiques. En cas de problème, nous pouvons prendre des sanctions et nous avons été très réactifs, en liaison avec l'agence des systèmes d'information partagés de santé, l'ASIP Santé, dans le cas que vous avez évoqué.

Jusqu'à présent, le correspondant « informatique et libertés » avait pour mission d'alléger les formalités préalables, l'obligation de tenir un registre se substituant à l'obligation

de déclaration, et d'entretenir une relation régulière avec la CNIL. Dans le futur, son rôle sera plus ambitieux, et même déterminant pour évoluer vers une régulation fondée sur la responsabilisation des acteurs et sur un contrôle *a posteriori* : il sera chargé de piloter la conformité. Dans les entreprises comme dans les administrations et les collectivités, ce sera un agent permettant à son organisme de respecter strictement ses obligations, en dispensant des formations internes ou en établissant des études d'impact. Il devient ainsi un acteur clé dans la mise en œuvre de la responsabilité sociale de l'entreprise.

Mme Anne-Yvonne Le Dain. Dans le monde de l'entreprise, des codes de bonne pratique se développent à un rythme soutenu et cela est intéressant à observer car l'on pourrait y puiser des solutions à l'échelle nationale et internationale, en complément d'un droit qui ne doit être ni en retrait ni trop en avance.

Pouvez-vous nous apporter des précisions sur la notion de droit à l'oubli ? Qui en bénéficie et comment y accède-t-on ?

S'agissant de Google, vous avez donné des indications très précises sur la nécessité qui lui était faite d'obtenir un accord explicite pour la communication de données personnelles : comment une forme de rétroactivité pourrait-elle trouver à s'appliquer ? Sans rétroactivité en effet, le système n'est pas efficace puisqu'il ne permet pas de sanctionner l'exploitation de données déjà effectuée par le moteur de recherche.

Mme Isabelle Falque-Pierrotin. Le droit à l'oubli doit être plus qu'un slogan car les internautes sont inquiets. En un an, le nombre de plaintes a augmenté de plus de 42 %, ce qui correspond à une véritable explosion. Les Français sont de plus en plus nombreux à éprouver un malaise en étant confrontés à une image d'eux qui remonte à plusieurs années et qui ne correspond plus forcément à celle qu'ils souhaitent diffuser aujourd'hui. Sur les quelque 6 000 plaintes que nous enregistrons chaque année, plus de 1 000 concernent le droit à l'oubli !

Comment procédons-nous concrètement ? Nous disposons de lignes dédiées avec les grands acteurs de l'Internet. Lorsqu'une plainte concernant par exemple Google ou Facebook nous parvient, nous entrons en contact avec un interlocuteur privilégié et, la plupart du temps, après examen, les réseaux suppriment les contenus. Dans le cadre du règlement européen, le droit de rectification et d'opposition sera facilité par l'inversion de la charge de la preuve. Si vous voulez obtenir aujourd'hui l'effacement d'un contenu, il vous revient de prouver qu'il vous porte préjudice ; demain, ce sera à l'entreprise d'apporter la preuve que cette demande de suppression n'est pas justifiée. C'est un progrès, mais nous souhaitions aller au-delà en assortissant l'obligation de suppression à la demande d'une obligation de déréférencement. Car, en réalité, même supprimé, le contenu continue à tourner sur Internet et il est donc toujours visible *via* les moteurs de recherche. Nous n'avons pas obtenu gain de cause et il y a tout lieu de le regretter.

Nous sommes au cœur d'un sujet qui met en évidence de façon très emblématique la différence entre la logique humaine et la technique. Le numérique est conçu pour ne rien oublier, alors que l'humain oublie, voire pardonne. Si l'on veut réconcilier l'individu avec le numérique, il est très important d'introduire dans celui-ci un peu d'oubli. À l'évidence, beaucoup reste à faire en ce domaine.

Votre remarque sur la rétroactivité me semble fondée, et me rend un peu perplexe. Lorsqu'un individu demande d'accéder à ses données en vue de les supprimer – comme l'a fait récemment un internaute autrichien auprès de Google, ce qui lui a valu de recevoir des

liasses de données le concernant ! –, il faut s'assurer que la myriade d'acteurs qui agissent masqués accèdent eux aussi à cette demande. Or il s'est déjà constitué un véritable écosystème qui a prospéré sur l'exploitation de vos données. Dès lors, comment assurer la disparition totale de la donnée dans un système dont on ne peut percevoir qu'une partie ?

M. Lionel Tardy. Les sujets qui ont été évoqués ce matin reposent sur trois fondamentaux : éduquer, encadrer, protéger.

En matière d'éducation, on s'en tient pour l'essentiel aux réseaux sociaux, ce qui est insuffisant. Il faut aussi prendre en compte l'arrivée imminente de l'Internet des objets. Si le fournisseur d'accès Internet (FAI) représente aujourd'hui le principal lien avec l'internaute, demain tous les appareils de la maison seront connectés, du réfrigérateur au système de chauffage. Indépendamment des FAI, nombre de services vont se créer pour développer ces appareils, sans garantie valable quant à la protection des données personnelles. Comment prévenir le risque de revente de ces données à ceux qui ont intérêt à en disposer ?

À côté de la génération des *digital natives* qui maîtrise ces différents outils, nous avons toute une population qui sait à peine envoyer des *e-mails* ou qui est coupée d'Internet. Comment l'aiderons-nous à faire face à ces évolutions ?

Je voulais enfin évoquer la réalité augmentée, qui va bien au-delà de la géolocalisation. Demain, dès que vous franchirez le seuil d'un restaurant McDonald's, vous recevrez une publicité pour un restaurant Quick. Cela pose des questions qui excèdent le champ du droit de la consommation et doivent intéresser l'ensemble de nos commissions.

Mme Anne-Yvonne Le Dain. Parallèlement à la question de la réalité augmentée, il y a celle de la fabrication d'images par voie informatique, prenant la forme du réel et susceptibles de générer de fausses informations sur Internet.

Mme Isabelle Falque-Pierrotin. Toutes les questions abordées ce matin montrent que nous sommes entrés dans un nouvel univers, tant aux plans technique que sociologique et même anthropologique. L'individu se retrouve en forte tension par rapport à l'ensemble des possibilités ouvertes par le numérique. La CNIL s'attache à accompagner ces changements, en restant fidèle à l'approche humaniste propre à la France et à l'Europe. Nous ne sommes pas seulement un nuage de données ! Sous les traces que produisent nos activités en ligne, il y a toujours des personnes et des liens et notre commission évolue en permanence pour défendre cette vision des choses dans tous les domaines.

M. le président Jean-Jacques Urvoas. Madame la présidente, merci pour la précision de vos réponses et bon courage dans l'ouverture de tous ces nouveaux chantiers ! Au cours de cette législature, notre Commission aura à cœur d'y participer, en veillant tout particulièrement au respect des libertés publiques et à la défense de l'intérêt général.

*

* *

La séance est levée à midi dix.

Membres présents ou excusés

Présents. - M. Gilles Bourdouleix, Mme Marie-Anne Chapdelaine, M. Sergio Coronado, Mme Françoise Descamps-Crosnier, Mme Laurence Dumont, M. Philippe Gosselin, M. Sébastien Huyghe, Mme Marietta Karamanli, M. Jean-Yves Le Bouillonnec, Mme Anne-Yvonne Le Dain, Mme Axelle Lemaire, M. Sébastien Pietrasanta, M. Pascal Popelin, M. Dominique Raimbourg, M. Bernard Roman, M. Jean-Jacques Urvoas, M. Patrice Verchère

Excusés. - M. Marc Dolez, M. Matthias Fekl, M. Guy Geoffroy, M. Daniel Gibbes, M. Alfred Marie-Jeanne, Mme Corinne Narassiguin, Mme Elisabeth Pochon, M. Didier Quentin, M. Roger-Gérard Schwartzenberg, M. Jean-Luc Warsmann, Mme Marie-Jo Zimmermann

Assistait également à la réunion. - M. Lionel Tardy