ASSEMBLÉE NATIONALE

XIVe LÉGISLATURE

Compte rendu

Commission de réflexion et de propositions sur le droit et les libertés à l'âge du numérique

Mercredi
26 novembre 2014
Séance de 17 heures

Compte rendu n° 08

SESSION ORDINAIRE DE **2014-2015**

Présidence de Mme Christiane Féral-Schuhl,
coprésidente
Et de
M. Christian Paul,
coprésident

ASSEMBLÉE NATIONALE

COMMISSION DE RÉFLEXION ET DE PROPOSITIONS SUR LE DROIT ET LES LIBERTÉS À L'ÂGE DU NUMÉRIQUE

Jeudi 13 novembre 2014

La séance est ouverte à dix-sept heures dix.

(Présidence de Mme Christiane Féral-Schuhl, co-présidente et de M. Christian Paul, co-président)

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

Mme la coprésidente Christiane Féral-Schuhl. Nous avons le plaisir de recevoir Mme Isabelle Falque-Pierrotin, présidente de la Commission nationale de l'informatique et des libertés (CNIL) dont nous suivons avec beaucoup d'intérêt les démarches concernant les données personnelles. Pour notre commission, dont la mission est d'identifier les problèmes qui peuvent se poser en matière de libertés, les données personnelles représentent l'un des points les plus sensibles : cet « or noir de l'internet » touche directement à la vie privée des personnes.

Nos préoccupations tournent autour de trois grands thèmes : les principes à adopter en ce qui concerne la protection et la responsabilisation des individus ; l'usage que font les utilisateurs privés de ces données à caractère personnel ; l'équilibre entre la protection de la vie privée et les impératifs d'ordre public. Il s'agit pour nous de savoir s'il faut légiférer dans ce domaine. À titre personnel, je considère que la très riche loi « *informatique et libertés* » de 1978 a défini les principes fondateurs importants pour internet. La CNIL a pu se prononcer au fil de l'eau, *via* des recommandations qui ont néanmoins un caractère coercitif, sur ses applications. Selon vous, une évolution législative est-elle nécessaire ? Si oui, quelle forme doit-t-elle prendre ?

Mme Isabelle Falque-Pierrotin, présidente de la Commission nationale de l'informatique et des libertés. Merci de me permettre de m'exprimer devant cette commission qui est, m'a-t-on expliqué, un peu atypique, ce qui fait son intérêt pour traiter cette thématique : les données personnelles ne sont pas seulement un objet juridique mais elles ont une dimension sociologique, politique et stratégique. La composition de la Commission fait un peu écho à la dimension très large que revêtent actuellement les données personnelles.

Quelles propositions puis-je vous faire au titre de la CNIL ou du groupe de l'article 29, dit G29, qui réunit les autorités européennes de protection des données ? Avant de répondre à cette question, je vais d'abord passer en revue les constats qui étayent ces propositions.

Premier constat : notre époque se caractérise par une imprégnation des données personnelles dans toutes les activités publiques, professionnelles ou privées. L'individu est de plus en plus pris dans un maillage extrêmement fin d'informations personnelles relayées par des objets de plus en plus communicants : téléphone portable, bracelets électroniques divers, dispositifs électriques, équipements de vidéosurveillance, etc. Cette « datification », cette

mise en données du monde est en marche ; elle illustre ce qui représente une rupture historique dans cette société numérique : l'entrée dans un numérique ambiant. Nous sommes, en effet, désormais plongés en permanence dans ce flux d'informations dont nous ne percevons pas forcément la structure mais qui nous imprègne et nous entoure comme l'air ambiant. La dichotomie qui existait encore il y a quelques années entre les univers physique et virtuel – on « allait » sur internet – a disparu.

Deuxième constat : l'affaire Snowden a révélé que l'infrastructure de ce numérique ambiant, bien que principalement constituée à l'initiative d'acteurs privés désireux de vendre des biens et services, était aussi potentiellement utilisée par des acteurs publics poursuivant d'autres finalités. Même si ces finalités peuvent être légitimes – quand elles répondent à des objectifs de sécurité publique, par exemple – elles sont parfaitement étrangères aux raisons pour lesquelles les données ont été collectées auprès des personnes. Comment faire en sorte que cette infrastructure de données, normalement au service de l'individu, ne se transforme pas en outil de surveillance ?

Troisième constat : cette explosion change le rapport qui existait entre vie privée et données personnelles. Jusqu'à une période récente, les protections de ces deux sphères se superposaient. Sous l'effet des nouveaux comportements et usages, la frontière entre la vie privée et la vie publique commence à se détendre pour donner naissance à une zone un peu grise dans laquelle les personnes veulent exposer leur vie privée et se servent des données personnelles pour avoir une vie publique. Dans le fond, les individus ne sont pas gênés par cette situation et ils recherchent avant tout une maîtrise de leurs données personnelles plutôt qu'une protection de leur vie privée. La demande sociale s'enrichit et devient plus complexe à satisfaire : la notion de maîtrise peut varier d'un individu à l'autre et, pour le régulateur, il s'agit d'un nouveau continent.

Quatrième constat : le droit à la protection des données personnelles était spécifique, isolé des autres droits en raison de sa technicité et de son caractère très procédural, connu d'experts et doté d'une logique interne très forte ; il est en train de vivre une interpénétration avec d'autres droits. C'est ainsi qu'en mai dernier, la Cour de justice de l'Union européenne (CJUE) a rendu un arrêt sur le déréférencement. Le régulateur est chargé de trouver un équilibre entre la protection des données et le droit du public à l'accès à l'information. Par ailleurs,,il vient d'être décidé en France le blocage administratif d'accès à des sites faisant l'apologie du terrorisme et le rôle de la CNIL est de contrôler ce blocage et d'éviter le surblocage. Il faudra trouver un équilibre entre protection des données et protection de la liberté d'expression. On assiste aussi à une interpénétration croissante entre le domaine de la protection des données personnelles et le droit de la concurrence. Au nom du respect de la concurrence, l'Autorité de la concurrence a récemment obligé un acteur à ouvrir un fichier client à ses compétiteurs. Le droit de la protection des données personnelles doit donc intégrer ces relations de plus en plus intimes avec d'autres droits.

Cinquième constat : les analyses sur ce droit à la protection des données personnelles – et donc les propositions qui en découlent – ne peuvent pas être menées dans un cadre franco-français. Comme le disait Christiane Féral-Schuhl, les données personnelles sont au cœur de tout, notamment d'affrontements stratégiques entre les différentes zones du globe. Elles deviennent une arme au service d'entreprises et d'États, y compris étrangers. Nous devons assurer la protection du citoyen français et européen en accord avec nos valeurs fondamentales qui viennent d'être réaffirmées par la CJUE, mais nous devons aussi assurer la compétitivité de l'espace économique européen par rapport aux acteurs internationaux car la capacité de contournement de l'Europe est forte en ces matières.

Ces constats nous incitent à formuler des propositions dont la traduction ne serait pas forcément de nature législative.

Première proposition : la constitutionnalisation de la protection des données personnelles. Certains rétorquent que la protection constitutionnelle de la vie privée existe déjà et qu'il est inutile d'y ajouter celle des données personnelles. Ce n'est plus exact car ces deux sphères s'autonomisent de manière croissante. La constitutionnalisation de la protection des données personnelles existe dans treize pays européens sur vingt-huit et aussi dans les textes européens, notamment dans l'article 8 de la charte des droits fondamentaux auquel l'arrêt de la CJUE se réfère. Elle nous permettrait d'afficher une protection du plus haut niveau dans ce domaine, ce qui serait très utile lors des négociations internationales.

Deuxième proposition : le renforcement du droit des personnes. Construit autour de l'utilisateur, l'univers du numérique innove à partir de lui. Il est assez logique de donner à l'individu des droits renouvelés et adaptés au fur et à mesure du développement de cette société numérique, et nous avons fait des propositions en ce sens dans le cadre de la préparation du projet de loi sur le numérique qui sera présenté l'année prochaine.

Le Conseil d'État propose de reconnaître une sorte de droit nouveau à l'autodétermination. Je ne suis pas sûre qu'il faille créer un nouveau droit expressément libellé comme tel, mais il est certain que nous recherchons tous cette autodétermination des individus, c'est-à-dire cette capacité de maîtrise renouvelée qu'ils demandent. Tous les droits seraient déclinés à partir de ce droit chapeau.

Il nous paraît important de renforcer les droits existants et, le cas échéant, d'en reconnaître d'autres. La décision rendue en mai par le CJUE sur le déréférencement est un bon exemple de renforcement des droits : les moteurs de recherche se voient rappelés à leurs obligations en tant que responsables de traitement de données personnelles, c'est-à-dire qu'ils doivent faire droit à une demande d'effacement. On demande aux moteurs de recherche d'appliquer le droit à l'effacement qui existe déjà dans la directive de 1995.

Le G29, réuni à Bruxelles, a élaboré des lignes directrices permettant une application harmonisée sinon uniforme de ce droit sur le territoire européen. Qu'ils exercent ce droit à Paris, Berlin ou Dublin, les citoyens européens sont sûrs que les autorités de protection auront les mêmes pratiques concernant le contrôle de la décision du moteur de recherche. Nous avons aussi demandé que soient concernées toutes les extensions liées au traitement de données, soumis au droit européen, qui fait l'objet d'un déréférencement demandé par un individu. Dans le cas particulier de Google, *google.com* doit appliquer la décision de déréférencement.

Le renforcement du droit des personnes peut aussi passer par la création de nouveaux droits. La nouvelle réglementation européenne sur la protection des données définit le droit à la portabilité, qui est extrêmement puissant même s'il a été moins évoqué que le droit à l'oubli : il permet en quelque sorte à l'individu de transporter sa maison numérique avec lui et de ne pas être prisonnier des interlocuteurs, commerciaux ou non, avec lesquels il dialogue. Lorsqu'une personne noue une relation avec un prestataire, un réseau social, ou un site de e-commerce, des données la concernant sont agrégées et accumulées. En vertu de ce droit à la portabilité, la personne peut demander à ce que ces données lui soient rétrocédées afin qu'elle puisse apporter son profil à un autre prestataire. Ce droit permet une autonomisation de l'individu et un rééquilibrage de la relation qu'il entretient avec ceux qui collectent des données sur lui.

À la CNIL, nous avons la conviction qu'une quatrième génération de droits est en train d'émerger. Chaque génération précédente a correspondu à une rupture historique : les Lumières, les droits sociaux, les droits collectifs. À chaque époque, on a cristallisé le besoin démocratique dans de nouveaux droits pour l'individu. La protection des données personnelles et ses enrichissements successifs – jurisprudence, projet de règlement – appartient à une nouvelle génération de droits qui correspond aussi à une rupture historique. L'individu y trouve le moyen de garder la maîtrise de la complexité de l'univers dans lequel il évolue. Même s'ils sont marqués par les technologies, ce ne sont pas des droits sur les technologies. À la différence des droits précédents, ils sont positifs et non pas réactifs : on les reconnaît positivement à l'individu sans qu'ils le protègent nécessairement contre tel ou tel danger. Ils conditionnent beaucoup l'exercice d'autres droits, notamment la liberté d'aller et de venir et la liberté d'expression. Ces réflexions nous paraissent donc consacrer une nouvelle génération de droits qui correspondent à la complexité accrue des sociétés contemporaines.

Troisième proposition : le renforcement de la voix européenne. L'Europe dispose d'un actif juridique et éthique d'une qualité exceptionnelle. Dans la grande bataille internationale qui se noue sur la question des données personnelles, il est absolument nécessaire que nous renforcions la voix de l'Europe, pas de façon défensive mais en montrant que cet actif légal et éthique peut aussi être une arme positive au service de l'Europe et de son rayonnement international.

Sur cette question de l'identité juridique et éthique européenne, nous devons être très vigilants, en cette phase finale de négociation du règlement européen sur la protection des données. Au nom de la volonté d'aboutir, nous risquons de construire des équilibres différents de ceux que nous souhaiterions. A ce titre le Conseil conduit des négociations qui mettent en avant une approche par le risque, l'enjeu des débats actuels étant : la démarche européenne est-elle pertinente pour digérer la modernité digitale ?

L'Europe s'appuie sur des principes extrêmement robustes – fondés sur la finalité et le consentement – mais qui deviennent très lourds et trop complexes dans l'univers actuel des données massives, le « *big data* », où les croisements se font à l'aveugle, sans finalité *a priori*. Quant au principe de consentement, il est encore moins évident en raison des multiples échanges qui interviennent bien au-delà de la collecte. Dans ces conditions, comment demander un consentement informé aux personnes ?

Dans ce contexte, certains bons esprits internationaux préconisent de substituer à l'approche européenne classique, une approche par le risque : on ne s'intéresse qu'aux traitements et aux usages les plus risqués et c'est l'entreprise elle-même – et non l'individu – qui évalue le risque. Au nom du pragmatisme, de la complexité de l'univers digital et du souci de l'allocation des ressources, on change d'approche. Dans un cas, la protection des données personnelles est un droit fondamental ; dans l'autre, les acteurs économiques l'envisagent comme une balance d'intérêts.

Alors que cette approche par le risque gagne chaque jour de nouveaux partisans, il est important que nous puissions en fixer précisément les contours pour que ne soit pas abandonnée la notion de droit fondamental dans le règlement européen. Cet élément de négociation est très important. Dans son projet de règlement, l'Europe doit définir très clairement les adaptations du cadre juridique qu'elle souhaite, tout en restant attachée à ses principes fondamentaux.

Quand elle s'engage dans la construction d'un cadre juridique compétitif et attractif, l'Europe se situe dans une démarche relativement offensive. Elle peut aussi adopter une position défensive, comme après les révélations de M. Snowden. Comment nous défendons-nous d'une aspiration massive et indistincte de données relatives à des citoyens européens ?

Le G29 propose de faire reconnaître le bloc de protection des données personnelles comme une loi de police, dans la mesure où il participe à l'ordre public. Il ne s'agit pas de demander une application mondiale du droit européen ; il s'agit d'éviter que des lois extraterritoriales ne puissent déroger, sur notre sol, à nos lois de protections des données. Ce n'est pas une épée mais un bouclier.

Claude Moraes, le président de la commission des libertés civiles, de la justice et des affaires intérieures (LIBE), propose quant à lui d'intégrer un article 43A dans le projet de règlement précisant que, lorsqu'une autorité étrangère publique demande accès à des données relatives à des citoyens européens, elle doit avoir l'accord d'une autorité européenne. On ne peut pas laisser une autorité publique étrangère siphonner les données des citoyens européens ; les conditions de l'accès à ces données doivent avoir été précisées lors d'une négociation avec une autorité européenne compétente.

Quatrième proposition, qui ne relève pas entièrement du champ législatif : les acteurs économiques doivent jouer un rôle privilégié afin d'éviter que les données collectées, qui permettent un ciblage toujours plus fin des individus, ne se transforment en un puissant outil de surveillance. D'une manière ou d'une autre, il faut leur imposer des obligations supplémentaires de transparence de leurs clauses sur les conditions générales d'utilisation, et aussi des algorithmes utilisés, ainsi que l'a suggéré le Conseil d'État dans un récent rapport. D'une façon générale, l'utilisation de cet or noir que sont les données internet doit se faire dans la transparence.

Dernière proposition, qui ne relève pas du tout du champ législatif : l'éducation au numérique doit faire l'objet d'un effort collectif beaucoup plus important que celui qui est consenti actuellement. Une manière vraiment efficace de rééquilibrer le rapport entre l'individu et ceux qui collectent des données sur lui, qu'il s'agisse d'acteurs privés ou publics, c'est de développer la connaissance afin de donner au grand public les moyens de comprendre cet univers digital. Actuellement, le citoyen moyen en connaît les usages – et encore ! – mais il n'en appréhende pas nécessairement les ressorts. L'usager doit acquérir la culture générale de l'homme numérique, c'est-à-dire un mélange de connaissances techniques, juridiques et historiques.

L'an dernier, avec un collectif de plus de soixante-dix acteurs, nous avions proposé que l'éducation au numérique puisse être une grande cause nationale. *In fine*, ce n'est pas celle qui a été retenue pour 2014. Avec un autre collectif, nous reprenons notre bâton de pèlerin et nous allons déposer une nouvelle demande pour que l'éducation au numérique soit une grande cause nationale en 2015. Si nous voulons que se développe dans notre pays un monde numérique respectueux des libertés, il faut que les usagers soient bien conscients des caractéristiques et des modes de fonctionnement de cet univers. À l'heure actuelle, nous n'avons pas tous les clefs pour nous protéger, sans parler de nous emparer de toutes les potentialités de cet univers.

Mme la coprésidente Christiane Féral-Schuhl. Merci pour la richesse de vos propositions et des différentes pistes de réflexion que vous nous avez offertes.

Tout d'abord, je voudrais rebondir sur la dimension internationale que vous avez soulignée. Le principe d'effacement, inscrit dans la loi, peut-il s'appliquer actuellement ? Avons-nous, sur le plan matériel, les moyens de contrôler la durée des traitements, sachant qu'il y a une obligation de supprimer certains d'entre eux ?

Quelle place accorder aux acteurs ? La décision rendue en mai dernier par la CJUE a en effet ouvert la voir au déréférencement. Google a mis en place un comité chargé de répondre aux demandes qui sont extrêmement nombreuses. Dans son rapport, le Conseil d'État a proposé une formule consistant à permettre un débat judiciaire lorsque le site veut réagir ou contester ce type de décision. Comment vous positionnez-vous par rapport à ce débat ?

Mme Isabelle Falque-Pierrotin. À ce jour, la loi n'oblige pas le collecteur de données à les détruire à l'expiration de la durée de conservation, sachant que celle-ci correspond à la finalité de la collecte. Dans le cadre de ses missions de contrôle et de sanction, la CNIL constate bien souvent un dépassement des durées de conservation. Une partie du métier de la CNIL consiste à faire respecter ces durées de conservation.

La décision de la CJUE sur le déréférencement a eu diverses conséquences. Nous avons constaté une attente sociale considérable en la matière : Google a reçu 150 000 demandes de personnes qui veulent contrôler leur vie numérique. Le droit à l'oubli n'est pas seulement une invention de technocrates mais il répond à une volonté affirmée des gens. L'affaire n'est pas anodine pour Google : il s'agit de ses clients. La construction du numérique repose sur la confiance et la maîtrise des clients sur leurs données .

Cette décision a aussi fait apparaître l'existence d'un rapport singulier entre la personne qui demande un déréférencement et le moteur de recherche, Google ou un autre. Mais, dans certains cas, il y a un troisième acteur : le site initial. Jusqu'à présent, dans le droit de la protection des données, on ne connaît que la relation entre le demandeur et le responsable du traitement. À présent, on voit que la décision de déréférencer affecte un tiers : journaux, sites divers.

Quelle a été la nature des échanges entre le G29 et *Google* sur ce point ? Tout d'abord, nous avons rappelé que, contrairement à ses dires, *Google* n'avait pas l'obligation légale de notifier systématiquement sa décision de déréférencement à l'éditeur initial. Nous avons ensuite expliqué que, pour que l'écosystème fonctionne bien et qu'il n'y ait pas de déréférencement excessif, le groupe devrait donner aux régulateurs des éléments nous permettant de comprendre sa politique en la matière. Nous lui avons demandé des statistiques plus précises qui nous permettraient de savoir quels types de sites sont concernés par les décisions de déréférencement. C'est d'autant plus intéressant que plusieurs acteurs peuvent être concernés.

Cette affaire a aussi illustré le rôle croissant joué par les acteurs économiques, dans la régulation du numérique. D'aucuns trouvent anormal qu'une société privée devienne l'arbitre des élégances sur le sujet. En fait, ce n'est pas le cas. Il se trouve que, du fait de la très forte présence de Google dans notre vie numérique, la décision de cette société a un impact considérable. Pour autant, sa situation n'est pas différente de celle d'un autre responsable de traitement auprès duquel nous formulons une demande d'effacement depuis déjà sept ou huit ans. Jusqu'à présent, on ne s'est jamais préoccupé des sites de journaux et des blogs auxquels nous adressions des demandes comparables. La décision de cette société

n’est pas prise en l’absence de contre-pouvoirs et d’instances de contrôle : la CJUE a explicitement indiqué qu’elle était sous le contrôle des autorités de protection et du juge.

L’imbrication croissante entre les régulateurs et les acteurs économiques se fait avec le souci croissant que chacun soit dans son rôle. Dans certains cas, toute la difficulté est de délimiter le rôle des régulateurs afin qu’ils sachent à quel moment intervenir, que ce soit pour réprimer ou pour encadrer les acteurs économiques.

M. le coprésident Christian Paul . Depuis la loi « informatique et les libertés », et singulièrement depuis dix ou quinze ans, les préoccupations ont évolué : s’ils s’intéressent toujours à la sécurité et à la protection, les gens s’interrogent aussi sur la propriété et la valorisation des données personnelles. Qu’est-ce que cela change pour le régulateur ? La CNIL a-t-elle besoin de nouveaux outils juridiques et de moyens supplémentaires ? Un changement de fond est-il en train de s’opérer ? Si oui, quelles en sont les conséquences ?

Dans son récent rapport, le Conseil d’État propose que nous débattions d’une notion jurisprudentielle allemande ancienne, datant du début des années 1980 : le droit à l’autodétermination informationnelle. Qu’en pensez-vous ?

Mme Isabelle Falque-Pierrotin. La valorisation économique des données introduit, en effet, un changement fondamental. Au moment de l’adoption de la loi de 1978, on raisonnait en termes de protection. À notre époque, les données personnelles sont au cœur des modèles économiques et des innovations de la plupart des secteurs industriels. C’est un terrain d’innovation considérable.

Qu’est-ce que cela change pour nous ? Cela ne change pas les principes de la loi de 1978, qui sont parfaitement capables de digérer cette valorisation économique des données. Des réflexions ont été menées sur la notion de propriété des données personnelles. Certains ont estimé que, dans cet univers de valorisation économique des données, la solution était peut-être de reconnaître à l’individu un droit à la propriété de ses données personnelles.

Pour notre part, nous sommes absolument convaincus que ce n’est pas une bonne voie car on perdrait des leviers d’action considérables sur lesdites données : étant propriétaire de ses données, l’individu pourrait les vendre, notamment à des acteurs étrangers. Or la grande supériorité intellectuelle du droit à la protection des données personnelles réside dans le fait qu’il reconnaît le droit d’un individu même si les données sont traitées par d’autres. Même si elles sont détenues par Google, la FNAC, mon médecin ou la caméra de vidéosurveillance, j’ai des droits, en tant qu’individu, sur mes données. Il ne faut pas lâcher cette approche qui est extrêmement puissante.

Faut-il innover pour intégrer cette dimension économique des données ? Je pense qu’il faut innover dans des approches ou des outils nouveaux. La protection intégrée de la vie privée, *privacy by design*, consiste à se préoccuper de la protection des données dès la conception d’un produit ou de l’offre d’un service.

Dans les secteurs de l’assurance et de la banque, nous sommes en train de développer des *packs* de conformité, excusez l’anglicisme qui traduit notre volonté d’européaniser notre démarche. Dès lors que les données prennent une aussi grande importance économique, leur protection ne passe pas seulement par le respect de formalités administratives préalables mais elle implique une relation continue entre le secteur industriel concerné et le régulateur. Cette démarche trouve sa traduction concrète dans le *pack* de conformité.

Avec le secteur de l'assurance, nous avons ainsi élaboré un *pack* qui intègre les formalités préalables mais qui permet aussi aux assureurs d'innover en matière de tarification grâce à des informations qui prennent en compte toutes les dimensions de l'assuré et pas seulement le nombre de kilomètres qu'il parcourt avec sa voiture dans l'année. Ces données massives – *big data* – sont intégrées au fil de l'eau et leur conformité est négociée dans le cadre d'une relation continue avec le régulateur. Un tel outil n'était pas nécessaire dans les années 1980 ; à un moment où les données deviennent le cœur des modèles et des activités économiques des entreprises, il est très utile.

M. Winston Maxwell. J'aimerais revenir sur le droit chapeau et le renforcement de la capacité de maîtrise de l'individu. Comment insérer ce principe général dans le droit ? De telles dispositions vont-elles trouver leur place dans l'article 9 du code civil ?

Mme Isabelle Falque-Pierrotin. Pardonnez-moi, monsieur Paul, j'ai oublié de répondre à votre question sur le droit à l'autodétermination. Nous le voyons, en effet, comme une sorte de droit chapeau qui abriterait les droits spécifiques sur la protection des données personnelles. Il peut aisément s'insérer dans le préambule de la loi « informatique et libertés » revue. Je ne suis pas sûre qu'il faille en faire un droit en tant que tel.

M. Christian Paul, coprésident. Nous allons rester sur notre faim, si une juriste aussi précise que vous en restez là !

Mme Isabelle Falque-Pierrotin. C'est clairement la clef de voûte de tous nos droits mais faut-il pour autant l'intégrer dans un article additionnel du code civil ? Faut-il que nous ayons un droit spécifique intitulé de cette manière ? Pour être tout à fait honnête, nous n'avons pas encore mené totalement cette réflexion au sein de la CNIL. Pour le moment, nous le voyons davantage comme une synthèse des droits existants que comme un droit nouveau spécifique.

M. Philippe Aigrain. Madame la présidente, en ma qualité de membre fondateur de l'association La Quadrature du net et en tant que promoteur des droits positifs et des droits à capacités, je voudrais tout d'abord vous remercier d'avoir donné une importance à ces nouveaux types de droits que le développement du numérique et son appropriation massive par les citoyens ont mis en évidence jusqu'à les rendre incontournables.

Les choses deviennent plus compliquées quand nous nous interrogeons sur la manière de les rendre effectifs. Comme vous l'avez souligné dans votre exposé, la notion de donnée comporte désormais plusieurs facettes : trace, information, donnée, expression. Notre droit a été construit autour des concepts de donnée, de fichier, de finalité et de consentement, et nous avons tendance à penser que tout le reste va s'y intégrer.

Qu'est-ce j'appelle une information ? C'est, par exemple, le fait que vous soyez par hasard sur une photo prise lors du passage de la voiture qui alimente le site *Google street view*. Qu'est-ce que j'appelle une trace ? C'est un parcours de navigation capturé et analysé. Tout cela ne va évidemment pas relever des mêmes dispositions. Les individus n'ont souvent aucun moyen de savoir quelles traces de leurs activités sont recueillies. Si l'on se crispait sur la notion de donnée parce que nous avons tout un droit matériel accumulé sur le sujet, on risquerait d'être en décalage par rapport à la réalité des problèmes.

Qu'en est-il de l'érosion de la distinction entre vie privée et vie publique ? En réalité, je ne suis pas sûr de l'existence du phénomène. Les analyses des comportements effectifs des

internautes montrent que la sphère de l'intimité reste au centre de leurs préoccupations, y compris quand ils s'exposent. Faites l'expérience et dites à quelqu'un que l'on peut lire les brouillons d'articles qu'il n'a pas encore publiés, sur une plateforme de blog. Décrivant son activité d'analyste, Snowden disait : « je peux lire vos pensées au moment où elles se forment, en suivant vos frappes, vos retours en arrière et vos corrections ». Quand ils apprennent ce genre de choses, les gens ne sont généralement pas contents.

Quand ils s'exposent, c'est avec un projet. Même s'ils n'en sont pas toujours explicitement conscients, ils font très rapidement l'expérience que la volonté de maîtriser une identité dans l'espace numérique est, en fait, une négociation sociale. C'est bien beau d'essayer de se construire une réputation mais celle-ci peut être mise à mal par des commentaires dépréciateurs. Les usagers de n'importe quel média social s'en rendent compte assez rapidement. En outre, ils sont confrontés à un espace public où la dimension d'anonymat a été extrêmement réduite notamment par la généralisation de la vidéosurveillance.

C'est lorsque l'on entre dans le registre des solutions que ces digressions un peu philosophiques prennent un vrai sens. La notion de portabilité fonctionne quand on l'applique au téléphone, par exemple : l'usager souhaite garder le même numéro, même en cas de changement d'opérateur. En revanche, le concept se heurte très vite à des limites quand on l'applique au champ des données, notamment lorsqu'il s'agit de traces et d'interactions qui unissent des personnes. Dans une architecture centralisée où les données ne sont pas dans les mains de l'individu, la portabilité va se heurter à des difficultés majeures. Or celui qui quitte un média ou un réseau social veut partir avec tous ses amis, pas tout seul.

Du coup, deux éléments se retrouvent au cœur de la réflexion et qui restent difficiles à appréhender pour le législateur lorsqu'il a l'habitude de penser en termes procéduraux : il s'agit des architectures et des modèles commerciaux.

Je crains que l'idée que les données représenteraient le troisième « or noir » du XXI^{e} siècle nous empêche de comprendre que, sans promotion de tel ou tel modèle commercial, sans limites apportées aux modèles commerciaux, nous n'aboutissions à rien en matière de construction des droits-capacités.

Vous avez mentionné le fait que *Google* devait tout de même bien respecter ceux que vous avez appelé ses clients ; mais les usagers de *Google* ne sont pas ses clients. Qu'il s'agisse du moteur de recherche, de *You Tube* ou de la géolocalisation, les clients de *Google*, ce sont les annonceurs publicitaires. Les usagers sont en fait la marchandise que *Google* vend à ses annonceurs

Si nous laissons dominer des modèles qui retirent aux individus l'un des principaux moyens de faire respecter leurs droits, à savoir la capacité, en tant que consommateurs, de choisir les produits qu'ils ont à disposition, le système risque de ne pas fonctionner. De même qu'en ce qui concerne le concept de *privacy by design* : si l'on ne réfléchit pas aux architectures techniques et qu'on se contente de vérifier qu'il y a bien une couche de respect de protection des données, on créera une petite industrie du *privacy by design* mais je ne suis pas sûr que l'on servira réellement le respect de l'intimité.

Certains ont une autre approche et proposent que les fournisseurs de systèmes soient obligés, au moins, d'offrir le chiffrement de bout en bout des communications, afin de

garantir qu'eux-mêmes n'ont pas accès au contenu des communications dont ils fournissent les services. Ils proposent de légiférer sur ce point.

Mme Isabelle Falque-Pierrotin. On ne peut pas reprocher au cadre juridique en vigueur d'être archaïque et trop rigide puisque la définition de la donnée personnelle a progressivement évolué, prenant en compte toute une série de nouveaux types de données personnelles – notamment les métadonnées.

Vous doutez que la portabilité fonctionne dans la mesure où ce droit ne serait pas seulement individuel mais qu'il aurait une dimension communautaire : je voudrais bien récupérer mes propres données mais également celles de ma tribu, de ma communauté. Cette remarque est très intéressante et il est relativement difficile de donner une réponse définitive car il est vrai que nous en sommes au stade expérimental. Reste que ce droit à la portabilité correspond tout à fait aux travaux de la Fondation internet nouvelle génération (FING) qui consiste à permettre la rétrocession de ses données à l'individu afin que, le cas échéant, il les offre à un autre prestataire ou, dans certains cas, les lui vende. Sera-ce une démarche purement individuelle ou bien une démarche collective ? Il faut expérimenter un droit de ce type avant de le ciseler.

Faut-il se limiter aux grands principes ou bien faut-il également aborder les modèles économiques et les dispositifs techniques ? Car en effet, vous avez raison : il s'agit d'un levier supplémentaire dont on souhaite disposer. Comment procéder ? Nous-mêmes, en tant que régulateurs, nous intéressons déjà aux modèles économiques mais sur la pointe des pieds, si j'ose dire, car on nous objecte qu'il ne nous revient pas de définir les modèles économiques d'acteurs comme *Google*, modèles qui reposent largement sur le croisement de données. Nous avons expliqué aux représentants de *Google*, dans le cadre de l'action répressive que nous avons menée contre cette société dans six pays, qu'elle peut croiser les données recueillies par ses plus de soixante services – *Gmail*, *You Tube*, la géolocalisation… –, mais à condition de le faire savoir. L'incidence sur le modèle économique de l'obligation supplémentaire de transparence au bénéfice de l'individu est ici indirecte.

Selon vous, tant que les données seront concentrées entre les mains d'un nombre trop limité de personnes, on aura beau légiférer, ce sera de peu d'effet. Vous avez raison, mais on sort du cadre de la protection des données personnelles pour entrer dans celui du droit de la concurrence. On constate bien, justement, une interpénétration croissante des deux sphères, la réglementation de la concurrence au sujet des données visant justement à fragmenter, le cas échéant, ces grandes bases de données étant donné le risque encouru par les individus.

Enfin, concernant les aspects techniques, on peut en effet placer la protection des données le plus en amont, notamment à travers la normalisation. La CNIL est d'ailleurs très présente au sein des instances de normalisation internationales comme l'Organisation internationale de normalisation (ISO) ou le G29, afin que la protection des données soit intégrée dans lesdites normes.

La réponse n'est donc pas exclusive quant à la volonté de maîtriser l'environnement numérique au niveau individuel et au niveau collectif. Il faut, pour y parvenir, utiliser plusieurs leviers en même temps.

M. Daniel Le Métayer. En relisant le rapport du Conseil d'État déjà évoqué, j'ai noté que la CNIL apparaissait comme l'un des vecteurs d'application d'au moins dix recommandations parmi celles énumérées, qu'il s'agisse de la promotion d'outils de

protection de la vie privée, de la standardisation des politiques de protection des données personnelles, de standards d'anonymisation, du contrôle des algorithmes, des discriminations illicites, ou encore de l'animation de la délibération collective sur les questions d'éthique du numérique – soit, si j'ai bien compris, une sorte de comité d'éthique du numérique.

Quel est votre sentiment sur ces recommandations ? Les reprenez-vous volontiers à votre compte ? Ou alors sortent-elles, selon vous, du périmètre d'activité naturel de la CNIL ? Ou encore conduisent-elles à la mobilisation de moyens disproportionnés ?

La seconde partie de ma question porte sur l'équilibre entre les missions de conseil et la mission de sanction. On a vu que la dimension de conseil prend de l'importance et c'est une très bonne chose de ne pas voir systématiquement ces questions sous le seul angle des rapports de force. La culture informatique et libertés traverse toutes les dimensions de la société – vous avez évoqué l'éducation numérique, qui est capitale – et il me tient à cœur qu'elle prenne place dans le monde économique. Aussi, comptez-vous donner une plus grande ampleur à l'activité de conseil – vous l'avez évoquée avec les *packs* de conformité ?

Je me pose donc la question de la conciliation de cette activité avec celle du juge qui sanctionne. Dans de nombreux domaines, on a en effet tendance à vouloir séparer les deux. Or j'imagine qu'une entreprise ne s'adressera pas à vous de la même manière pour obtenir un conseil si elle sait qu'en même temps vous pouvez la sanctionner. Je ne prétends pas avoir de réponse à cette question – il faut bien prévoir des sanctions, *a fortiori* si on se dirige, avec le projet de règlement, vers des contrôles *a posteriori* qui devront être dissuasifs. Cela étant, ne faudra-t-il pas, à terme, séparer les deux rôles ?

Mme Isabelle Falque-Pierrotin. Nous souscrivons pour une large part aux propositions du Conseil d'État et ne sommes du reste opposés à aucune. Le fait qu'elles soient nombreuses correspond à l'importance des données dans ce nouvel univers numérique. Il est donc assez naturel que le régulateur des données personnelles se trouve très concerné par une réflexion sur l'adaptation de la régulation aux nouvelles réalités pour la rendre plus efficace. Je n'ai pas d'autre remarque à formuler sur ce rapport.

La seconde partie de votre question est fondamentale pour les autorités de protection des données : comment équilibrer la sanction avec, le cas échéant, autre chose ? Par « autre chose » j'entends le conseil, l'accompagnement, le suivi. À titre personnel, je suis convaincue qu'on ne peut pas réguler uniquement par la sanction qui est une arme de dissuasion certes indispensable mais qui ne constitue pas une arme de régulation au quotidien. En effet, la CNIL rend une quinzaine de sanctions par an. Vous imaginez donc bien qu'en nous limitant à la sanction, nous nous condamnerions à ne toucher que l'écume de cet univers numérique. Si nous voulons que ce dernier se développe dans le respect de la protection des données personnelles, il faut agir autrement, à savoir en amont, donc par le biais d'outils qui étaient jusqu'à présent les formalités préalables mais qui demain n'existeront plus ou quasiment plus et qui donc seront de plus en plus des outils de mise en conformité. Comment éviter le conflit d'intérêts ? On peut avancer deux réponses.

D'abord, concernant les outils de mise en conformité, nous ne proposons pas de travail à façon pour une entreprise ; nous ne travaillons qu'au bénéfice d'un secteur : l'assurance, la banque, le logement social, les compteurs communicants… Nous ne réalisons pas de *pack* de conformité pour une entreprise – c'est là le travail des avocats, des sociétés de conseil. Le rôle du régulateur est d'ouvrir un parapluie générique pour une industrie qui veut développer ses usages dans le respect de la loi « informatique et libertés ».

Un second garde-fou permet d'éviter le conflit d'intérêts : la formation restreinte est une activité très spécifique, compartimentée, avec des règles de fonctionnement *ad hoc*, une présidence *ad hoc*, différente du fonctionnement de la CNIL en séance plénière. De ce fait, on limite, on interdit largement les conflits d'intérêts entre les pouvoirs répressifs et ceux de conseil.

La position dont je vous fais part n'est pas partagée par tous les régulateurs européens. Pour certains d'entre eux, la régulation, c'est uniquement la sanction. Demain, quand les sanctions représenteront 2 à 5 % du chiffre d'affaires et donc deviendront une arme de dissuasion massive, certaines autorités se limiteront à la sanction.

Mme Valérie-Laure Benabou. Pour revenir sur la possibilité ou non d'associer les individus à la valorisation de leurs données, je me demandais s'il s'agissait non pas d'une quadrature du Net mais bien d'une quadrature du cercle. En effet, il y a cette idée de récusation de la propriété de la donnée par celui qui en est à l'origine. J'aurai sur ce point un léger désaccord. Techniquement parlant, il n'y a pas de raison d'affirmer qu'on va perdre tout contrôle en cédant sa propriété et que ce serait une catastrophe. Des outils d'inaliénabilité existent. Le droit de la propriété intellectuelle prévoit une cession par laquelle on ne cède pas vraiment… Il y a des possibilités de licence. On pourrait émettre l'idée d'une propriété rendue partiellement indisponible à la personne. L'idée de propriété reste donc modulable plus qu'on ne le pense. Si l'on parle de contrôle, la propriété est un outil très connu, qui a le mérite d'être assez ancien et assez éprouvé. Aussi, récuser la propriété au simple motif qu'on la perdrait à l'occasion d'une cession, me paraît une justification un peu courte.

Plus généralement, peut-on vraiment penser que l'internaute, le sujet de la donnée, a vocation au partage de cette valeur économique ? Est-ce que cela a un sens étant donné l'asymétrie évidente entre le responsable de traitement et l'individu à l'origine d'un petit faisceau de données qui peut-être, en lui-même, n'a pas de valeur ? Comme c'est par l'agrégat que naît la valeur, quelle vocation a-t-on à partager des données si l'on n'est à l'origine que d'un micron de cet agrégat ?

Ensuite, à supposer que ce partage soit légitime, comment le rendre effectif ? Comment organiser des opérations de communication de données (*reporting*) permettant à la personne d'être associée à cette valorisation ?

Enfin, à supposer qu'on laisse tomber l'idée de la participation à la valorisation en amont, on continue de considérer que la personne doit conserver un contrôle, y compris un contrôle « filant », au fur et à mesure que ses données vont être transmises, aliénation qui, elle, repose souvent sur l'idée de propriété – d'où cette asymétrie qui me paraît quelque peu surprenante. Or, de par le contrôle, cette autodétermination informationnelle conduit forcément à une certaine précarisation des acteurs économiques situés en aval. En effet, s'ils transfèrent des données dont, à tout moment, une personne peut retirer, supprimer des éléments, quelle est la valeur économique transmise ?

Y a-t-il moyen d'opérer un partage de valeur entre l'individu et le responsable de traitement ? Est-ce que cela a un sens et, sinon, comment continuer à maintenir un contrôle de l'internaute sur ses propres données tout en permettant la circulation de la valeur économique liée aux données traitées ?

Mme Isabelle Falque-Pierrotin. À défaut d'une réponse complète à cette question très compliquée, je proposerai quelques pistes.

Le dispositif juridique actuel reconnaît la protection des données comme un droit fondamental et la concilie avec la logique économique telle qu'elle s'est développée. Est-il utile d'en changer et d'adopter celui de la propriété ? Je suis certes d'accord avec vous : on peut moduler la propriété ; mais le dispositif en vigueur fonctionne dans vingt-huit pays européens, il est imité dans toute une série de pays dans le monde – en Afrique francophone aussi bien qu'en Amérique du Sud –, et il reconnaît aux personnes des droits pour le moins puissants. Aussi, avant de lui substituer un droit de propriété dont on ne sait même pas de quelle manière il s'appliquera, je me montrerais très prudente, d'autant que dans cette notion de propriété, il y a une notion d'appropriation patrimoniale réductrice par rapport à l'approche consistant à considérer les données comme un droit fondamental et pas simplement comme un objet économique. A mon sens, aucune raison vraiment convaincante ne devrait nous pousser dans ce sens, au contraire.

Cela dit, comment l'individu peut-il bénéficier de la chaîne d'utilisation de sa donnée et cela a-t-il un sens ?

Il ne faut pas lancer des signaux contradictoires. Si l'on dispose d'un cadre de régulation qui considère la protection des données comme un droit fondamental, inaliénable et qui, bien sûr, prend en compte la logique économique, il ne faut pas, dans le même temps, par des incitations, envoyer le signal inverse selon lequel nous aurions intérêt à commercialiser au maximum nos propres données.

Je ne peux pas, en tant que présidente de la CNIL, me prononcer sur les dispositifs économiques permettant de faire ce que vous décrivez. En revanche, je peux affirmer que plus l'individu jouira de droits effectifs – tels qu'ils existent aujourd'hui et tels que le règlement pourra demain les lui reconnaître – sur sa donnée personnelle – accès, portabilité, transparence –, plus le rapport individu-prestataire sera équilibré. Quelle est la valorisation économique de ce rééquilibrage de pouvoirs, je suis bien incapable de vous le dire.

Mme Valérie-Laure Benabou. J'ai bien précisé que je n'étais pas forcément favorable au dispositif de la propriété mais l'argumentaire me paraissait un peu court.

Je souhaite revenir sur le paradoxe suivant : le renforcement à l'autodétermination informationnelle frappe de précarité le circuit aval. Si je fais abstraction de la protection de l'individu au profit de la protection de la valorisation des données, comment ceux qui traitent les données peuvent-ils se prémunir quand eux-mêmes sont en train de patrimonialiser leur traitement contre cette précarité « génétique » liée à la capacité permanente de la personne à soustraire une partie de cette valeur ?

Mme Isabelle Falque-Pierrotin. Nous ne parlons pas nécessairement des mêmes données. Il ne s'agit pas pour l'individu de récupérer toute la valeur ajoutée que l'entreprise aurait elle-même créée autour des données collectées auprès de ses clients. Toute l'intelligence que la société aura développée sur la segmentation, mais aussi sur la compréhension, l'enrichissement de sa base client, reste la propriété de la société et ne sera pas concernée par le droit à la portabilité.

Ce dernier, même si ses contours ne sont pas encore bien définis par le projet de règlement, concerne un nombre beaucoup plus limité de données que l'individu a lui-même déposées auprès de la société, et non les traitements de *back office* que la société a développés dans ses modèles économiques sur ledit individu. Aussi la chaîne de valeur de l'entreprise n'est-elle pas fragilisée. Le droit à la portabilité ne prévoit pas d'extraction, à l'initiative de

l'individu, de toute la connaissance acquise sur lui par la société pour ensuite la « porter » ailleurs.

M. Philippe Aigrain. Le fossé entre un droit fondamental attaché à la personne et un droit de propriété est assez considérable même si, dans l'histoire, ont existé ce qu'on a appelé des droits de propriété attachés à la personne. Pour combler ce fossé, certains ont suggéré une solution intermédiaire et considéré comme une sorte de droit corporel le lien qui unit l'individu aux données. Judith Rochfeld s'est ainsi inspirée du droit des parties du corps humain. Je considère que les individus d'aujourd'hui ont un corps numérique diffus et qu'on devrait prendre cette notion au sérieux. Ces solutions vous paraissent-elles intéressantes à explorer ?

Mme Isabelle Falque-Pierrotin. Elles le sont en effet : si l'on est de plus en plus « instancié » par une sorte de double numérique, les données personnelles sont comme un élément de corps numérique. Le raisonnement que l'on a eu jusqu'à présent sur le corps – indisponibilité du corps, droits de l'individu sur son corps, protection du corps humain… – peut être pour partie réinterprétée, transposée dans le domaine de la protection des données personnelles. Je trouve une telle inspiration intellectuelle et juridique très forte ; elle correspond à la tradition humaniste française et européenne et me paraît pleine d'avenir.

M. Daniel Le Métayer. Deux questions – liées – me tiennent à cœur : celle de la certification et celle de l'analyse de risque. J'ai tendance à penser qu'il faut sortir de cette vision binaire : on ne coupera pas à une démarche d'analyse de risque. Ce qui compte est de savoir comment cette analyse est réalisée et de savoir si, dans la boucle, un tiers sera capable de la valider, de la justifier, voire de la « certifier ».

On sait que la CNIL décerne déjà des labels à des procédures d'audit, des formations. J'ai vu qu'un référentiel avait été publié pour des produits – mais à ma connaissance il n'y a pas eu encore de produit certifié. Peut-on vraiment espérer que le *privacy by design* que vous appelez de vos vœux, que la diffusion des techniques de protection de la vie privée prenne vraiment une certaine ampleur, tant qu'il n'y a pas vraiment d'éléments différenciateurs, tant qu'il n'y a pas, comme dans d'autres industries, des labels certifiant la bonne qualité d'un produit ? Jusqu'où la CNIL doit-t-elle aller et comment les rôles doivent-ils se répartir ? En matière de sécurité, il existe tout un écosystème autour de la certification : des sociétés conseillent, d'autres aident à certifier, d'autres encore sont accréditées pour certifier le compte de l'American National Standards Institute (ANSI). Que pensez-vous de cette démarche en matière de vie privée, étant bien entendu que les exigences sont ici plus difficiles à caractériser ? Faut-il aller dans cette direction ? La CNIL peut-elle être amenée à jouer un rôle similaire à celui de l'ANSI en publiant des référentiels, en accréditant des sociétés qui, elles, procéderaient aux évaluations qui conduiraient à la délivrance de labels ?

Mme Isabelle Falque-Pierrotin. Nous ne sommes pas opposés à l'analyse de risque. Le domaine de la sécurité, que vous avez mentionné, est l'un de ceux dans lequel la CNIL s'est montrée une autorité précurseur. On doit néanmoins faire attention à ce que l'on affirme : une protection limitée aux cas présentant un risque diffère du tout au tout avec le système actuel où l'individu a des droits indépendamment du risque encouru ou du mal subi du fait d'un traitement. J'ai aujourd'hui le droit d'accéder à mes données même pour un traitement très banal. L'analyse de risque est très utile lorsqu'elle permet de raisonner sur des allocations de ressources mais pas si elle conduit à conditionner des droits à l'existence du risque. C'est comme si j'avais une maison dans une zone dont l'environnement n'était pas

sûr : le risque y serait important et permettrait de déterminer le niveau des verrous de ma porte ; mais il reste que je garde un droit absolu, même dans cette zone, à ne pas être volé.

Nous essayons de faire passer l'idée, au niveau européen, que l'analyse de risque est utile dans certains cas mais ne peut conditionner l'exercice de droits qui, eux, sont des droits objectifs qui peuvent induire des obligations pour les responsables de traitement, des mesures à mettre en place, comme des mesures de sécurité ou des mesures d'*accountability* mais pas le droit des personnes.

La certification va-t-elle se développer ? La réponse est sûrement oui. Le rôle des certificateurs dans les questions de *privacy*, d'encadrement des flux internationaux de données, va s'accroître. Nous en sommes convaincus au point que nous nous essayons à ce métier nouveau, vous l'avez mentionné, à travers des labels. La question est de savoir quel est le rôle des acteurs privés et celui du régulateur dans ces nouvelles fonctions. Certains acteurs internationaux, au nom du réalisme et du pragmatisme, poussent au remplacement des régulateurs par les certificateurs. Or leur activité est complémentaire. Les régulateurs doivent fixer les crans de la certification, quitte à déléguer à des certificateurs l'application du référentiel.

M. Jean Dionis du Séjour. Je reviendrai sur la question très intéressante de Mme Benabou : faut-il valoriser l'information au stade où elle est une unité ou uniquement reconnaître qu'elle n'a de valeur qu'une fois traitée en tant qu'agrégat ? Ne doit-on pas reconnaître à l'information unitaire au moins une valeur de matière première ? On retrouvera dès lors la question du droit de propriété sur les données personnelles et la question de la capacité de la personne à les céder en tant que matière première, faute de quoi on risque de laisser se développer des trafics plus ou moins clandestins. On constate l'émergence d'un *business* de mégadonnées. On ne peut pas avancer que le traitement serait la seule valeur : la matière première a bien un prix économique qu'il me paraît difficile de nier à terme.

Mme Isabelle Falque-Pierrotin. Il ne s'agit pas de le nier mais de souligner que l'inspiration du droit de la protection des données personnelles est différente. Aujourd'hui, la protection des données personnelles existe depuis la collecte jusqu'à tous les usages qu'elle implique.

M. Jean Dionis du Séjour. Je suis tout à fait d'accord et reconnais que ce droit fonde la démarche de la CNIL. Mais surgit ce phénomène économique massif et je souhaite connaître la position de fond de la CNIL sur la question posée par Mme Benabou. L'information au niveau unitaire a-t-elle une valeur marchande en tant que matière première ? Cela me paraît difficilement niable et dès lors comment légiférer ?

Mme Isabelle Falque-Pierrotin. Encore une fois, il ne s'agit pas de le nier : nous sommes tous convaincus que l'information unitaire agrégée et traitée a une valeur économique. Seulement, la réponse à la question que vous posez ne se trouve pas, à ce stade, dans le droit à la protection des données personnelles. Il s'agit de questions adjacentes et le droit des données personnelles ne peut y apporter de réponse économique ; il n'a pas été construit dans l'objectif de valorisation d'une matière première.

M. le président Christian Paul. Dans de nombreux domaines, on peut créer de la valeur sans que la matière première soit appropriée.

Mme Isabelle Falque-Pierrotin. Je crois surtout que ce droit va avoir des incidences économiques. Lorsque vous renforcez le droit des personnes sur la chaîne de circulation de l'information les concernant, elles obtiennent en réalité un retour sur investissement sur l'utilisation de leurs données ; ce n'est pas une valorisation économique quantitative mais bien une action qui a une incidence économique sur la chaîne de valeur. Le droit à la protection des données personnelles n'a pas été constitué pour organiser la chaîne économique.

M. Jean Dionis du Séjour. C'est tout de même la question du moment.

Mme Isabelle Falque-Pierrotin. Certes. Vous posez en fait la question des mégadonnées (*bigdata*), que nous avons examinée sous tous ses aspects. Le *bigdata* ne pose pas un problème de principe quant à la protection des données personnelles. Pas un exemple précis ne nous a été soumis montrant que la protection des données personnelles aurait interdit à des applications *bigdata* d'être mises en place.

Vous mettez également en avant le fait que, les acteurs du *bigdata* ayant une dimension internationale, la manne économique qui lui est liée nous échappe. Cela n'a rien à voir : le problème est de disposer d'acteurs économiques compétitifs par rapport aux acteurs internationaux. Et ce n'est pas, j'y insiste, le droit de la protection des données personnelles qui apportera la réponse. Il faut faire attention, par conséquent, à ne pas chercher à faire jouer à ce droit un rôle qu'il ne peut pas avoir : il ne créera pas les acteurs internationaux du *bigdata*. Il peut apporter une arme de régulation supplémentaire en soumettant les acteurs internationaux du *bigdata* à des règles européennes lorsqu'ils traitent des données européennes. C'est bien du reste ce qui va se passer avec le projet de règlement qui prévoit, pour la première fois, que les acteurs internationaux, s'ils utilisent des données de citoyens européens, seront soumis au droit européen. Ils sont ainsi replacés au même niveau de concurrence que les acteurs européens. Cette action économique est indirecte.

Mme Valérie-Laure Benabou. Qu'en est-il de votre proposition concernant des dispositions internationales d'ordre public ? Quel en serait le « socle » ?

Mme Isabelle Falque-Pierrotin. Il s'agirait des principes généraux du règlement que nous voudrions voir reconnus comme une loi de police pour éviter qu'ils soient contournés par des lois étrangères qui s'appliquent aujourd'hui sans contrepartie sur le territoire européen. Le fait de reconnaître ces dispositions comme des lois de police permettrait de créer un conflit de loi pour l'heure inexistant et de mieux résister aux lois internationales.

Mme Valérie-Laure Benabou. Quel serait le fait générateur : la localisation finale de l'internaute, sa nationalité ? Car dans le cas du *Cloud*, si l'hébergement se situe à Pétaouchnok, qu'en sera-t-il ?

Mme Isabelle Falque-Pierrotin. Vous êtes beaucoup plus compétente que moi sur les questions de droit international privé pour que je me hasarde à un débat trop sophistiqué sur ce sujet. Au stade présent de notre réflexion, nous retiendrions le critère de résidence.

M. le coprésident Christian Paul. En ce qui concerne les algorithmes, sur quelles missions de la CNIL vous appuyez-vous pour aller plus loin ? La lutte contre les discriminations ? Par ailleurs, quels sont vos moyens juridiques, quelle est votre stratégie ?

Sur quelles autres juridictions éventuelles s'appuyer pour assurer la neutralité des plateformes et, plus précisément, la loyauté des algorithmes ?

Mme Isabelle Falque-Pierrotin. Ce n'est pas une revendication de la CNIL mais une proposition du Conseil d'État à laquelle nous souscrivons et qui correspond déjà à notre mission. Lorsque nous contrôlons des traitements, nous vérifions leur loyauté. Il s'agit donc d'aller un cran plus loin pour offrir à l'individu concerné par ce traitement des indications sur ce qui en résulte.

Il existe une forte pression pour nous inciter à investir dans ce domaine. Nous avons un département d'experts composé d'une quinzaine de personnes très compétentes sur lesquelles nous nous appuierions et nous travaillerions avec d'autres autorités comme l'ANSI pour disposer de la plus grande expertise technique possible sur le sujet.

M. le coprésident Christian Paul. Et sur le plan juridique, les textes qui régissent l'activité de la CNIL le permettent-ils ?

Mme Isabelle Falque-Pierrotin. C'est le cas. Nous devons nous assurer que la collecte est loyale, que les données sont pertinentes. On sait que votre donnée est collectée, dans quelles conditions et pour quelle finalité. Si un algorithme opaque croise votre donnée avec des tas d'autres à partir de raisonnements qui ne sont pas connus de vous, la loyauté du traitement n'est dès lors probablement pas assurée.

M. Philippe Aigrain. Quand Maryvonne de Saint-Pulgent nous a présenté le rapport du Conseil d'État, elle avait particulièrement insisté sur l'obligation de transparence et d'information. Dans certains cas, l'obligation de justifier les conclusions auxquelles on est parvenu ne suffit pas mais si on l'appliquait par exemple aux décisions prises au titre de la récente loi sur le terrorisme, elle aurait un effet fortement dissuasif.

Mme Isabelle Falque-Pierrotin. J'ajouterai que si un algorithme conduisait à exclure une personne du bénéfice d'un droit ou d'une prestation, on disposerait d'une autre base légale pour intervenir et il ne s'agit pas là d'une hypothèse relevant de la science-fiction.

M. Winston Maxwell. Notre commission se met en ordre de bataille pour examiner un futur projet de loi sur le numérique. Votre position, sur tous ces sujets, est-elle d'attendre le règlement ou bien, au contraire, recommanderiez-vous au législateur de devancer le cours des choses ?

Mme Isabelle Falque-Pierrotin. Nous avons fait des propositions à Fleur Pellerin et à Axelle Lemaire qui lui a succédé pour compléter, le cas échéant, un projet de loi. Il est évident que la capacité à légiférer sera tempérée par le règlement européen à venir. Aussi n'est-il sans doute pas opportun de légiférer sur certains sujets. En revanche, sur d'autres, on peut proposer certaines dispositions allant dans le sens général du règlement. Ainsi, nous avons proposé l'ajustement de notre niveau de sanction qui nous paraît trop faible.

M. Daniel Le Métayer. J'aurai une dernière question sur l'*accountability* que vous avez évoqué à plusieurs reprises. Il s'agit à mon avis d'une dimension essentielle pour l'avenir, notamment dans le cadre du projet de règlement. Si on déplace le curseur des contrôles *a priori* vers les contrôles *a posteriori*, il va falloir que ces derniers soient très sérieux. Pensez-vous que le projet de règlement va suffisamment loin sur ce plan ? Ne peut-on imaginer, à terme, si l'on prend vraiment le mot *accountability* au sens propre de « rendre des

comptes » et si l'on songe aux pratiques des entreprises en matière de comptes financiers, qu'une entreprise rende régulièrement des comptes sur la manière dont elle utilise les données personnelles, et des comptes certifiés par une entité indépendante ?

Mme Isabelle Falque-Pierrotin. La question de l'*accountability* n'est pas définitivement tranchée dans les négociations sur le règlement. Nous craignons que l'approche par le risque ne vide une partie des obligations de l'*accountability* de leur contenu puisque ces obligations pourraient être limitées aux traitements à haut risque. L'*accountability* est une chance pour la protection des données si cette approche est substantielle, c'est-à-dire si elle correspond vraiment à des outils nouveaux mis en place au sein de l'entreprise pour que la protection des données soit effective à travers des processus de formation, des dispositifs d'audit, un correspondant informatique et liberté, à savoir si elle correspond à toute une gouvernance interne au sein des entreprises. La CNIL est très intéressée par la mise en place d'une « *accountability* » effective. Reste que dans les négociations finales sur le règlement, nous allons nous montrer très vigilants car nous avons le sentiment qu'il ne va peut-être pas rester grand-chose de ces obligations d' *« accountability »* ce qui serait un peu embêtant.

M. le coprésident Christian Paul. On peut l'améliorer dans le droit français.

Mme Isabelle Falque-Pierrotin. La négociation est de niveau européen.

M. le coprésident Christian Paul. Il nous reste à vous remercier et à tirer le meilleur parti de vos recommandations ainsi que de la lecture régulière des rapports de la CNIL.

La Commission en vient à l'audition de M. Marc Robert, procureur général près la cour d'appel de Versailles, auteur du rapport Protéger les internautes *sur la cybercriminalité.*

M .le coprésident Christian Paul. Vous voudrez bien, monsieur le procureur général, dresser un état des lieux des menaces lourdes et des nouveaux risques en matière de cybercriminalité et nous faire part des principales propositions qui peuvent être faites au Gouvernement et au législateur afin d'améliorer la lutte contre les cybercriminalités.

M. Marc Robert, procureur général près la cour d'appel de Versailles, auteur du rapport *Protéger les internautes* relatif à la cybercriminalité. Précision liminaire sans doute utile, madame la présidente, monsieur le président, je ne suis un spécialiste ni du numérique ni de la cybercriminalité. Le Gouvernement a souhaité placer un généraliste de la procédure pénale et du droit conventionnel à la tête d'un groupe interministériel chargé de faire des propositions en matière de lutte contre la cybercriminalité.

Représentants de la police, de la gendarmerie, de la justice, des douanes, de l'économie numérique, de la consommation, nous sommes parvenus à nous mettre d'accord – le fait est assez rare pour être souligné – sur un constat et sur des propositions, tout en laissant volontairement de côté des sujets relevant d'autres instances. Nous n'avons notamment pas voulu aller sur les brisées de la Commission nationale de l'informatique et des libertés (CNIL).

Notre mission, très précise, dictée par les enjeux européens, consistait à élaborer une stratégie d'ensemble de lutte contre la cybercriminalité.

J’ai voulu que nous partions non des attentes des administrations centrales mais des attentes de catégories d’acteurs qui m’apparaissaient plus pertinentes en la matière – victimes individuelles, associations de consommateurs, entreprises, barreaux, acteurs répressifs dans leur pluralité – afin d’avoir un constat plus indépendant.

D’autre part, j’ai souhaité que nous ayons en permanence en ligne de mire l’ensemble des exigences relevant des droits fondamentaux que sont la liberté d’expression et la protection de la vie privée. Nous avons ainsi consacré un chapitre spécial de notre rapport à la jurisprudence en ce domaine – article 8 et article 10 de la Convention européenne des droits de l’homme, décisions principales du Conseil constitutionnel.

Un premier constat s’impose : il est très difficile d’appréhender la cybercriminalité. Tout d’abord, nous avons eu beaucoup de mal à la définir, en cela, nous n’avons pas été les seuls puisqu’aucun système juridique dans le monde n’est parvenu à le faire, si ce n’est sous forme de litote. En outre, elle n’a pas de frontière matérielle : elle concerne tous les pans de la délinquance et a tendance à s’étendre, par scissiparité, à toutes ses formes.

La principale conclusion que nous avons tirée de nos travaux va peut-être vous surprendre : le défi auquel nous sommes confrontés en France comme ailleurs relève moins de solutions juridiques que d’une stratégie globale mettant l’accent sur des points sur lesquels les juristes ont moins tendance à insister habituellement.

Premier point fondamental : la prise de conscience du phénomène nous paraît devoir être encore approfondie. Cela est particulièrement vrai pour les menaces touchant les entreprises, non pas seulement les 150 organisations d’importance vitale auxquelles on pense toujours, mais tout le tissu économique jusqu’aux plus petites PME.

Le deuxième point fondamental sur lequel nous souhaitons insister est l’exigence de la prévention. Le groupe de travail, composé en grande majorité d’acteurs de la répression, s’est mis d’accord pour considérer que la sensibilisation des internautes était la priorité des priorités car ils constituent le premier point d’appui de la cybercriminalité comme le montrent les atteintes à la vie privée ou les escroqueries de masse. Or la prévention paraît actuellement totalement éclatée, inorganisée et très peu soutenue par l’État.

Le troisième point est la formation des acteurs répressifs et, de manière générale, de tous ceux dont la vocation est de faciliter le contact avec Internet. Il y a encore un travail important à accomplir d’autant que nous constatons chez bon nombre de magistrats une ignorance des mécanismes et des caractéristiques techniques de la cybercriminalité.

Le quatrième point renvoie à l’absence de pilotage centralisé de la lutte contre la cybercriminalité au niveau de l’État. Il s’explique par des raisons historiques : la prise de conscience est récente. Dans un ordre dispersé, chaque administration a créé des instances spécifiques et le nombre des autorités administratives indépendantes s’est multiplié, à chaque fois pour prendre en compte un aspect seulement de cette forme de criminalité.

Par comparaison, des secteurs connexes ont donné lieu à une coordination poussée : il en va ainsi pour l’économie numérique, pour la cyberdéfense, qui fait l’objet d’une forte structuration de l’État autour du Secrétariat général de la défense placé sous la responsabilité du Premier ministre, ou encore pour les cyberattaques, à travers le rôle joué par l’Agence nationale de la sécurité informatique (ANSI), dotée de moyens importants et elle aussi placée sous la responsabilité du Premier ministre.

À l'étranger, certains États se sont dotés d'un pilotage unique regroupant les différents secteurs du numérique quand d'autres ont procédé à une distinction entre cyberdéfense, cybersécurité et cybercriminalité tout en en mettant en place des structures organisées et coordonnées, je pense notamment à l'Allemagne.

En France, la lutte contre la cybercriminalité ne fait l'objet d'aucune organisation de ce genre alors qu'elle requiert une synergie, une mise en cohérence, une planification des priorités. Pour combler cette lacune, nous avons proposé la création d'un organisme interministériel.

Une autre carence de l'organisation de l'État se manifeste sur le plan judiciaire. Non seulement la prise de conscience est limitée à quelques individus, mais il n'existe aucune structure dédiée tant au niveau central que territorial, exception faite de Paris. Il est normal sans doute que la justice soit moins réactive que les services d'enquête de la police ou de la gendarmerie mais cette situation ne doit pas perdurer. Nous préconisons donc la création d'une instance pluridisciplinaire au sein de l'administration centrale et la reconnaissance de compétences préférentielles pour Paris et pour les juridictions interrégionales spécialisées.

Autre constat qui nous a marqués : l'inefficacité du traitement des contentieux de masse, essentiellement les escroqueries et toutes les fraudes à la carte bleue commises *via* Internet. Pour la cyberescroquerie, qui fait potentiellement des centaines de milliers de victimes, cela tient au fait que ce traitement repose sur le recueil de plaintes individuelles, éclaté localement, sans qu'aucune synergie ne soit mise en œuvre. Ajoutons à cela les difficultés liées à l'identification et aux remontées des adresses IP et vous comprendrez pourquoi le nombre de classements sans suite est aussi important. Autrement dit, il y a une inadéquation totale du mode de traitement à la spécificité de ce contentieux, qui est insuffisamment prise en compte. S'agissant des fraudes à la carte bleue, le problème de la captation des données s'est trouvé réduit à un traitement indemnitaire *via* les organismes bancaires alors qu'il faudrait organiser entre les banques et l'État une obligation de transferts de données pour que nous puissions reprendre la main sur ce genre de fraudes qui relèvent de bandes organisées.

Nous avons également formulé des propositions importantes à propos des prestataires de l'Internet et sur le droit des victimes.

Je vous rassure tout de même, le questionnement juridique n'est pas tout à fait absent de notre analyse. Il a porté non pas tant sur le droit pénal de fond, qui nous paraît suffisant de manière générale, mais surtout sur la question de l'adaptation des moyens procéduraux à la spécificité de la cybercriminalité, compte tenu des difficultés très particulières que rencontrent les services d'enquête – je veux parler des services de droit commun et non des services spécialisés. Sur le terrain, ceux-ci se disent démotivés car ils considèrent n'avoir pas de prise sur ces types de délinquance, du fait de l'anonymisation, de la rapidité de flux et de l'extranéité.

In fine, nous avons dû aborder la question des moyens à mettre en œuvre pour lutter contre la cybercriminalité car jusqu'à présent, il n'y a eu aucune planification de cette nature.

J'en viens enfin aux changements intervenus depuis le dépôt du rapport. La loi sur le terrorisme a repris certaines de nos propositions mais en a écarté d'autres, le ministère de l'intérieur et le ministère de la justice ont procédé à certaines réorganisations. Toutefois, c'est surtout la loi sur le numérique qui devrait permettre d'avancer sur certaines questions.

Mme la coprésidente Christiane Féral-Schuhl. La lecture de votre rapport, monsieur le procureur général, montre bien que la sensibilisation et la formation sont avec l'organisation les dominantes de votre problématique.

J'aimerais vous interroger sur deux points spécifiques. Le premier, dont nous avons déjà débattu dans le cadre de notre commission, concerne la circonstance aggravante que pourrait constituer le recours à Internet. Quelle est votre position ?

M. Marc Robert. Nous n'avons pas pris de position doctrinale sur la question.

Le droit pénal de fond, comme je l'ai dit, nous paraît bien armé en France, notamment par rapport aux normes européennes proposées par l'Union ou par le Conseil de l'Europe et par rapport aux normes en vigueur dans les pays comparables au nôtre. Toutefois, il semble souvent hermétique pour les acteurs de terrain, si bien que certaines dispositions, relevant notamment de la loi de 2004, sont sous-utilisées. Il y aurait donc un important effort à faire en matière de pédagogie et de formation. Par ailleurs, il y aurait peut-être aussi à mener un travail de toilettage et d'harmonisation, ne serait-ce qu'au niveau terminologique.

En matière de circonstance aggravante, nous n'avons pas de religion déterminée car il me paraîtrait dangereux d'y associer un mode de communication ou d'expression. La circonstance aggravante me semble surtout liée au danger spécifique que représente tel ou tel type de support. Les difficultés que nous avons en matière de droit de la preuve ne doivent pas pousser à y recourir. On ne peut, à mon sens, l'appliquer de manière générale mais seulement si l'usage du moyen en question entraîne une dangerosité voire des effets spécifiques. Nous n'avons pas spécifiquement étudié les circonstances déjà existantes pour savoir si elles répondaient à cette définition.

Mme la coprésidente Christiane Féral-Schuhl. Le deuxième point est l'anonymat, sujet incontournable en matière de criminalité. Pourriez-vous partager avec nous les réflexions de votre groupe de travail ou celles qui vous sont propres ?

M. Marc Robert. Quand vous rencontrez les enquêteurs de terrain, la première chose dont ils vous parlent est l'anonymat. Dans les enquêtes classiques, ils doivent faire face à des problèmes d'identification mais le plus souvent le problème de l'anonymat organisé ne se pose pas. D'où leur désarroi quand ils y sont confrontés, d'autant que, comme ils le soulignent, la collaboration incertaine d'un certain nombre de prestataires Internet accroît leurs difficultés à remonter les adresses IP.

Cela signifie-t-il qu'il faille mettre fin d'une façon ou d'une autre à l'anonymat sur Internet ? Nul ne songe, me semble-t-il, à remettre en cause le droit à s'exprimer de manière anonyme, cela serait même contraire au mode d'organisation de l'ensemble des réseaux sociaux. Le droit de la presse a même consacré jurisprudentiellement cet anonymat. Je verrai donc très mal la mise en place d'un passeport numérique qui obligerait l'utilisateur à montrer patte blanche pour travailler sur tel ou tel outil. Plus raisonnablement, notre objectif consiste à faire en sorte que l'anonymat puisse être levé plus aisément lorsqu'il sert à couvrir une infraction. On sait combien les victimes sont traumatisées par la facilité avec laquelle certains se cachent derrière l'anonymat pour avilir et humilier. La réponse passe pour moi par une collaboration avec les prestataires, sinon par une obligation pour eux de collaborer.

M .le coprésident Christian Paul . Je souhaiterais vous poser une question, monsieur le procureur général, qui relève à la fois du principe et de la stratégie.

Deux doctrines prévalent en matière de cybercriminalité : la première consiste à intervenir sur les phénomènes de criminalité eux-mêmes en lançant des enquêtes et en mettant en œuvre des dispositifs répressifs ; la deuxième privilégie un blocage rapide, avec le risque de voir se développer des instruments cryptés et de nouveaux paravents pour occulter les formes de cybercriminalité.

Avez-vous constaté, notamment pour la pédophilie ou la pédopornographie, des phénomènes de migration vers d'autres réseaux moins accessibles pour les enquêtes judiciaires ?

M. Marc Robert. Je ne crois pas que ces formes de criminalité provoquent le plus de migrations. Elles font l'objet d'un consensus international en matière de blocages.

M. le coprésident Christian Paul. Entre services de police ?

M. Marc Robert. Pas simplement, il concerne aussi les États et les systèmes juridiques. Vous pourrez le constater dans maintes directives ou recommandations européennes qui insistent sur la nécessité de mettre fin à la pédopornographie, notamment grâce aux blocages. Et vous le retrouverez outre-Atlantique alors que nous savons que nos amis américains sont beaucoup plus prudents en ce qui concerne la protection de la vie privée et l'atteinte à la liberté d'expression.

En matière de blocage, vous connaissez notre position. Nous sommes bien obligés de constater qu'en France, depuis dix ans, les techniques qui y sont associées ont subi de multiples allers et retours. Tout a été essayé dans les normes françaises – blocage administratif, blocage civil, blocage pénal – et de nombreuses législations n'ont pas reçu d'application depuis dix ans, sans compter celles qui ont été abrogées avant même d'être mises en œuvre, notamment dans le domaine réglementaire.

Pour nous, le blocage doit être la réponse ultime : on ne doit y avoir recours que lorsque toutes les autres possibilités ont été épuisées. Ce principe de subsidiarité nous paraît extrêmement important. Le déréférencement, autrement dit l'obligation faite aux moteurs de recherche de déréférencer certains sites, nous paraît plus simple et plus efficace, même si la loi ne le permet pas encore. Nous considérons que même s'il y a lieu à blocage, il faut laisser à l'hébergeur ou au fournisseur d'accès le soin de trouver d'autres solutions qui aient la même efficacité afin de véritablement encourager cette subsidiarité.

Enfin, selon nous, le blocage doit être judiciaire, exclusivement judiciaire. La seule exception est la pédopornographie, compte tenu du consensus international, de la loi française et de la décision du Conseil constitutionnel.

L'intérêt du blocage est en réalité relatif : il permet d'éviter que le plus grand nombre puisse facilement accéder à des données illicites mais il ne constitue qu'un outil parmi d'autres. Le débat de nature technique sur ses modalités me dépasse très nettement. Beaucoup de pays ont choisi la voie de la facilité qui consiste à laisser au prestataire lui-même le choix du mode de blocage qui lui paraît le plus efficace. Dans certains cas, il est gratuit, y compris lorsqu'il est mis en œuvre sur décision judiciaire – je vous renvoie à la loi HADOPI.

Bref, ma préférence va aux solutions portant sur les outils de recherche.

M. Philippe Aigrain. Le consensus a toujours ses exceptions. L'article 4 de la loi d'orientation et de programmation pour la sécurité intérieure ou LOPPSI avait rencontré

beaucoup d'oppositions, y compris de part de représentants du parti aujourd'hui au gouvernement. Par ailleurs, à travers le dialogue que mon association, La Quadrature du Net, a noué avec des associations de lutte contre la pédopornographie, j'ai pu me rendre compte que les services d'enquête n'étaient pas unanimement favorables aux mesures de blocage de crainte qu'elles n'aboutissent à une clandestinisation accrue des sites et donc à une moindre détectabilité.

M. Marc Robert. Sur ce point, vous avez parfaitement raison, monsieur Aigrain. Les services d'enquête, notamment les services d'enquête anti-terroristes, considèrent certains sites comme des mines d'informations et souhaitent pouvoir les exploiter avant que les données ne soient supprimées.

M. Philippe Aigrain. Pour les acteurs sensibles au respect des libertés sur Internet, certaines mesures proposées par votre groupe de travail constituent des signaux d'alerte. Nous nous attendions à certaines, comme la responsabilisation des intermédiaires sous une forme qui remet en cause l'équilibre de la directive de 2000. Mais je dois dire que le retour à la suspension de l'accès à Internet a été pour nous une surprise. Nous pensions que la vigueur des débats entourant la loi HADOPI et la décision du 10 juin 2009 du Conseil constitutionnel avait assez souligné les problèmes que cette mesure posait, même si je suis bien conscient que vous préconisez son application à des victimes ayant subi un plus grand préjudice.

Les mesures que vous avez recommandées en matière de responsabilisation des intermédiaires supposent-elles, selon vous, de rouvrir le champ de la directive européenne de 2000 ou de sa transposition dans la loi pour la confiance dans l'économie numérique ou bien n'appellent-elles que de simples ajustements ?

M. Marc Robert. S'agissant de l'interdiction d'accès, je crois que la France a été traumatisée par les débats sur la loi HADOPI. Nous n'avons pas eu de chance que ce problème du droit d'accès soit uniquement envisagé sous l'angle du droit d'auteur. Il nous a semblé que pour les atteintes les plus graves aux mineurs, commises *via* Internet, il n'était pas choquant d'interdire à la personne concernée d'avoir accès à Internet pendant une période déterminée. Le système pénologique est très large et comporte des sanctions bien plus graves que celle-là. Pourquoi sanctuariser pour ce type de crime ce qui constituerait une peine judiciaire et non pas administrative ? Il faut raisonner aussi par rapport à la nature des crimes et aux intérêts supérieurs de protection des enfants.

S'agissant des mesures de responsabilisation des intermédiaires, nous avons beaucoup réfléchi au rôle des prestataires et avons fait deux constats.

Premièrement, les quinze dernières années ont été marquées par des valses-hésitations dans la politique de l'État à leur égard : dans un premier temps, on a cherché à appuyer la police du net sur l'autodiscipline des professionnels ; ensuite, on a tenté la corégulation ; puis, on a mis en œuvre des dispositifs de contrôle-sanction relevant d'autorités administratives indépendantes ou pas ; enfin, cerise sur le gâteau, on a instauré une réponse judiciaire, tantôt civile, tantôt pénale, sans que le partage soit extrêmement net.

Deuxièmement, nous avons fait figure de pionnier avec la loi de 2004 sur l'économie numérique, qui a connu quelques aménagements sans que l'architecture des sacro-saints articles 6 et 7 n'en soit affectée – je dis « sacro-saints » car dès que j'évoquais devant les représentants du ministère de l'économie numérique l'éventualité d'une réécriture, je sentais se manifester une sensibilité à fleur de peau, un peu comme pour la loi sur la presse. Lorsque

l'on fait le bilan de ces articles, on se rend compte qu'ils ne peuvent s'adapter ni à l'évolution des techniques ni à la diversification des prestataires. De surcroît, une bonne partie de leurs dispositions, qui prévoient des obligations à la charge des prestataires, n'est ni contrôlée ni respectée. Bref, en forçant le trait, je dirai que la loi de 2004 est en partie une coque vide. Demandez aux juges des référés, demandez à certaines victimes ce qu'ils pensent de l'effectivité de ses normes.

Bien sûr, il était hors de question pour nous de remettre en cause le principe de l'irresponsabilité des prestataires, gravé dans le marbre européen. Il n'était pas non plus envisageable de mettre en cause le principe de partenariat avec ces mêmes prestataires. Il doit être au contraire activement recherché. Nous appelons toutefois de nos vœux une clarification.

Nous souhaitons, tout d'abord, que leurs obligations sur le plan normatif soient précisées. Que peut-on leur demander ? La question se pose car la loi de 2004 est souvent relativement sibylline. Il nous paraît possible de charger fournisseurs et hébergeurs de détecter certaines infractions graves lorsqu'elles s'y prêtent. Certains d'entre eux s'y livrent déjà. Cependant, les mécanismes d'information de l'autorité publique ne sont pas toujours pertinents et quand je vois les chiffres qu'annoncent les intéressés, je pense que sommes assez loin de couvrir l'ensemble des infractions graves concernées.

Quant à la procédure de notification-action sur laquelle l'Europe fonde beaucoup d'espoir, je crois que si nous voulons la rendre effective, il faut renforcer les obligations qu'elle impose aux fournisseurs comme aux hébergeurs, notamment lorsque les signalements viennent des personnes lésées. Celles-ci ne font pas le poids vis-à-vis de ces prestataires, lesquels n'hésitent pas à les renvoyer d'un revers de main tout simplement parce qu'ils ont le pouvoir : face à eux, les individus sont des fétus de paille.

Mme Laure de La Raudière. Pourriez-vous nous donner des exemples ?

M. Marc Robert. Nous avons rencontré certaines associations de consommateurs qui ont essayé en vain de demander aux hébergeurs de retirer certains contenus totalement illicites et qui ont ensuite engagé des actions civiles – on sait les obstacles auxquels elles se heurtent et le coût qu'elles représentent. Certaines victimes individuelles d'infractions de presse se sont vu opposer des fins de non-recevoir à leurs demandes de retrait, du moins lorsque les prestataires ont pris la peine de leur répondre.

La notification par les autorités publiques est une procédure que nous n'avons pas assez développée en France contrairement à d'autres États. Il faudrait mieux l'organiser.

Quant aux obligations judiciaires, il conviendrait d'établir une liste beaucoup plus précise.

Enfin, il faudrait un système de contrôle et de sanction. Certaines sanctions prévues par la loi de 2004, comme la consultation du casier judiciaire, n'ont jamais été appliquées. Personne ne se sent responsable quand il s'agit de sanctionner les fournisseurs ou les hébergeurs qui ne jouent pas le jeu.

À cela s'ajoutent deux problèmes particuliers.

Le premier porte sur les fournisseurs de moteurs de recherche, qui ne sont pas concernés par la loi, ce qui est une lacune particulièrement importante.

Le deuxième concerne les prestataires de droit américain. Nous avons entendu les représentants de tous les prestataires principaux, qui sont à 90 % des prestataires de droit américain. Dès lors que les sociétés les plus importantes revendiquent en permanence l'extranéité juridique, estiment qu'elles ne peuvent pas être requises par les autorités françaises, et contestent l'applicabilité de la loi de 2004 en ce qui les concerne, que reste-t-il de cette loi ? L'un des enjeux cruciaux pour que les services d'enquête et les juges des référés puissent véritablement jouer leur rôle est de faire en sorte de contraindre les services dits de droit américain à appliquer la législation française.

Nous nous sommes penchés sur le problème de la faisabilité de cette proposition de droit interne. Vous savez très bien qu'aussi bien le Conseil de l'Europe que l'Union européenne travaillent sur ces questions. *Google* a déjà fait assez parler de lui pour qu'on ne l'ignore pas. Nous avons considéré tout simplement qu'il était inadmissible que des sociétés étrangères ayant des milliers d'abonnés ou d'utilisateurs en France, engrangeant des bénéfices très substantiels liés à l'utilisation des données privatives à des fins publicitaires, refusent délibérément d'appliquer certaines obligations légales indispensables à la lutte contre la cybercriminalité. Nous recommandons de prévoir que les obligations normatives, tant civiles que pénales et administratives, imposées aux prestataires concernent non seulement les prestataires français mais aussi les prestataires étrangers exerçant une activité économique sur notre territoire, fût-elle accessoire, ou qui offrent des biens et des services, même à titre gratuit à des personnes domiciliées sur le territoire national et cela, indépendamment du lieu d'implantation du siège social ou du stockage des données. *Exit* le problème américain ou irlandais. Faisons en sorte que le droit soit égal entre tous : c'est la seule façon d'introduire un système équitable de concurrence entre prestataires.

À ces différentes conditions, la loi de 2004 pourra être effective.

Mme la coprésidente Christiane Féral-Schuhl. Je vous rejoins, monsieur le procureur général, sur les problèmes que pose la loi de 2004. L'une des difficultés est liée à l'évolution des prestataires. Le web 2.0 a émergé au moment de la publication de cette loi et a créé une zone de flou, qui ne permettait plus de déterminer qui était hébergeur ou fournisseur d'accès puisque certaines sociétés revendiquaient l'un ou l'autre statut selon les moments.

Votre proposition consiste-t-elle en une adaptation de la loi à cette catégorie de prestataires intermédiaires ? L'expérience a montré que chaque fois que le législateur tente de s'adapter à un état technologique donné, la loi était vite dépassée. Vous avez d'ailleurs parlé de coquille vide à propos de la loi de 2004.

Par ailleurs, j'ai une question plus technique concernant la conservation des données. Pour aider les services d'enquête à identifier les cybercriminels, il est demandé aux entreprises et grandes institutions de conserver les données pendant un an. Or elles sont systématiquement confrontées à une difficulté dont personne ne parle : le format de conservation, qui implique pour elles un coût important et monopolise un grand espace de stockage.

Enfin, vous avez évoqué le rôle que peuvent jouer les prestataires dans la procédure de blocage. J'ai le souvenir d'avoir participé à une expertise qui a conclu que selon la technique utilisée par l'opérateur, le fournisseur d'accès voire l'hébergeur, les difficultés rencontrées et les coûts à supporter étaient très différents. Je ne suis pas certaine que l'on puisse dire que blocage n'a pas de coût, en tout cas pas pour les fournisseurs d'accès. Selon

que le blocage intervient en amont ou en aval, l'efficacité est différente et les incidences économiques varient.

Ces questions sont techniques mais elles méritent d'être posées car elles renvoient au risque de rupture d'égalité entre les différents acteurs.

M. Marc Robert. S'agissant de l'adaptation de la loi de 2004, vous avez pu constater que nous avions été très prudents. Autant nous avons avancé des propositions pour accroître l'effectivité de certaines de ses procédures, notamment de contrôle-sanction, autant nous n'avons sollicité qu'un seul élargissement, aux moteurs de recherche.

Mme Christiane Féral-Schuhl, coprésidente. Ils étaient exclus de la loi.

M. Marc Robert. En effet et nous n'avons vu que des avantages à les intégrer dans son champ.

S'agissant des réseaux sociaux, nous avons été tellement prudents que nous ne nous sommes pas prononcés sur leur place faute de visibilité suffisante. Le Conseil d'État va peut-être plus loin que nous en la matière.

S'agissant de la conservation, je ne me méconnais pas du tout l'importance du choix technique, ni en termes d'effets, ni en termes de coût économique. Mais notre inquiétude première concerne une possible remise en cause sinon du principe du moins de la durée de conservation. C'est une menace que les services spécialisés prennent au sérieux, eu égard notamment aux documents européens en préparation et à la pression qu'exercent certains États membres – nous savons les problèmes de constitutionnalité rencontrés par l'Allemagne et dont elle n'est toujours pas sortie.

À propos des techniques de blocage, nous avons pris acte de la position du Conseil constitutionnel. Toutefois, il nous est apparu que les prestataires mettaient déjà en œuvre des méthodes de blocage, notamment à la demande des États-Unis, s'agissant de données à connotation pédopornographique ou pédophile : ils sont donc dotés d'un savoir-faire en la matière. Or dans toutes les négociations pré-réglementaires concernant le coût de ces procédures, les prestataires ont avancé des demandes exorbitantes, tout simplement pour échapper à l'application de la loi, raison pour laquelle certaines dispositions réglementaires n'ont pu entrer en vigueur. Nous ne sommes pas allés plus loin dans le choix des techniques car la composition essentiellement juridique de notre groupe de travail ne lui donnait aucune compétence pour ce faire. Qu'il y ait un coût, nous en convenons, mais il doit être évalué de manière sérieuse et tarifé – nous y tenons –, d'autant que des frais de justice s'imposent souvent. Les prestataires ne doivent pas masquer leur savoir-faire : qu'ils ne nous racontent pas qu'ils découvrent la technique du blocage, ils l'appliquent depuis quinze ans !

Mme Valérie-Laure Benabou. Monsieur le procureur général, je tiens à vous féliciter ainsi que les membres de votre commission pour le travail colossal que vous avez effectué, à la mesure de l'objet polymorphe que vous avez étudié.

Parmi les différents moyens de lutte contre la cybercriminalité, il y a la nécessité pour l'internaute de sécuriser sa connexion mise en avant par la loi relative au droit d'auteur et aux droits voisins dans la société de l'information, dite loi DADVSI, et par la loi HADOPI. Que pensez-vous de cette piste, eu égard aux difficultés technologiques auxquelles se heurte l'individu lambda pour maîtriser sa connexion, notamment à l'ère des *hotspots* ?

M. Marc Robert. Cette question, nous ne l'avons pas abordée directement, mais indirectement à travers nos propositions en matière de prévention, inspirées de diverses préconisations d'associations de consommateurs qui ont souligné que les fournisseurs font tout pour priver de leurs moyens de maîtrise les utilisateurs. En réalité, cette sécurisation relève moins de moyens techniques disponibles que d'une éducation.

Nous avons été très frappées par la césure générationnelle qui sépare les internautes qui savent se défendre, protéger leurs données en utilisant au mieux les possibilités offertes par le net, des utilisateurs qui ne sont pas nés avec Internet et qui constituent une cible privilégiée pour les escroqueries. Je pense aux personnes d'un certain âge qui sont avec les entreprises – dont la situation est véritablement inquiétante – les premières victimes des atteintes économiques. À cet égard, permettez-moi d'évoquer une anecdote personnelle : le jour même où j'ai été nommé président du groupe de travail, ma carte bleue a été piratée sur le net !

Il serait bon de former ces personnes qui se sentent particulièrement désarmées à quelques moyens techniques permettant d'avoir une maîtrise sur leur connexion. Sur un plan technique, nous devrions pouvoir formaliser le consentement, élément fondamental pour déterminer s'il y a eu pénétration dans un ordinateur et manipulation. Les prestataires évitent soigneusement cette question. Il y aurait peut-être à la traiter dans une loi sur la consommation.

Mme Myriam Quéméner. Outre les moteurs de recherche et les réseaux sociaux, nous pourrions aussi évoquer les plateformes. L'étude annuelle du Conseil d'État a récemment souligné la nécessité de renforcer leurs responsabilités car elles sont le support de nombreuses infractions.

Certaines associations luttant contre les contenus racistes et antisémites sur Internet s'interrogent sur la possibilité d'utiliser davantage le droit de réponse prévu par la loi de 2004, disposition jamais utilisée qu'elles proposent éventuellement de réécrire. Il y a une grande attente des victimes en ce domaine.

S'agissant de la cyberpédophilie, nous sommes saisis de beaucoup d'affaires. La cour d'appel Versailles a développé une politique pénale de fermeté en appel. Le taux d'appel est en effet assez élevé, car certaines personnes estiment qu'elles n'ont pas directement touché des mineurs et que les faits qui leur sont reprochés ne sont pas graves. Nous connaissons aussi une hausse de procédures touchant au racisme, compte tenu du contexte international.

Nous revenons toujours à la nécessité de la mise en œuvre d'une stratégie globale. Certes, on observe une montée en puissance de la lutte contre la cybercriminalité. Le ministère de l'intérieur a ainsi créé une sous-direction qui lui est consacrée. Pour ce qui est de la justice, il reste encore beaucoup de chemin à parcourir. Je soulignerai l'indispensable mise en place de référents au niveau du siège car certains magistrats ne connaissent pas encore les modes opératoires et la nécessaire globalisation de la politique pénale. Pour l'heure, celle-ci revêt un caractère trop ponctuel : des commentaires sont faits à la publication de nouvelles lois et de nouveaux textes réglementaires. Il faudrait aussi mieux organiser les relations avec les autorités administratives indépendantes, notamment les plus récentes, comme l'Autorité de régulation des jeux en ligne (ARJEL). Je pense également au rôle que pourrait jouer le Défenseur des droits en matière de protection des victimes mineures.

Certes, il importe de modifier à la marge certains textes, mais il faut surtout encourager entre institutions des relations qui ne reposent pas uniquement sur des contacts personnels.

Mme Valérie-Laure Benabou. Vous soulignez avec raison que les fournisseurs de moteurs de recherche ne font pas l'objet de régime juridique particulier et vous préconisez à tout le moins un élargissement du statut du fournisseur d'hébergement. Pensez-vous que les statuts des fournisseurs de moteurs de recherche et des fournisseurs d'hébergement peuvent reposer sur un même modèle ? En réalité, leur position me semble différer : les fournisseurs de moteurs de recherche choisissent les liens qu'ils architecturent à travers un algorithme tandis que l'hébergeur ne choisit pas forcément les contenus qu'il héberge, caractéristique qui a servi de fondement à son régime de responsabilité.

M. Marc Robert. Nous n'avons pas défini dans le détail jusqu'à quel niveau les moteurs de recherche devaient s'intégrer à la loi de 2004. Il y a des débats très contradictoires, aussi bien au niveau de la Cour de Justice européenne que de la cour d'appel de Paris, sur la responsabilité des fournisseurs de moteurs de recherche et ils me semblent loin d'être clos.

Ce qui m'intéresse, au-delà du régime de responsabilité, ce sont les obligations positives qui pourraient leur être données. Cela me paraît constituer un moyen très souple et pour les individus et pour les institutions de mettre un terme à la diffusion de masse et c'est surtout cela qui m'intéresse. Cet objectif totalement pragmatique nous permettrait une plus grande efficacité et éviterait pour une bonne partie les débats sur le blocage.

M. Christian Paul, coprésident. Nous n'avons bien sûr pas évoqué tous les sujets liés à la cybercriminalité. Il en est cependant un que je vois monter dans les médias en ce moment sur lequel j'aimerais avoir votre position, monsieur le procureur général, ce sont les objets connectés.

M. Marc Robert. Je serai prudent. Je considère que nous devrions accompagner l'évolution technologique des objets connectés – domaine dans lequel la France est en pointe –, du fait des risques qu'elle peut générer. Mais, à titre personnel, je n'y vois pas assez clair pour affirmer qu'il faut encadrer leur utilisation sur le plan juridique, voire sur le plan pénal. À mon avis, il est beaucoup trop tôt pour le faire.

M. Christian Paul, coprésident. Je remercie M. le procureur général ainsi que les membres de la commission.

La séance est levée à vingt heures vingt-cinq.