

A S S E M B L É E N A T I O N A L E

X I V ^e L É G I S L A T U R E

Compte rendu

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

Mercredi
8 octobre 2014
Séance de 10 heures

Compte rendu n° 3

SESSION ORDINAIRE DE 2014-2015

- Présentation par M. Jean-Marc Sauvé, vice-président du Conseil d'État, de l'étude annuelle 2014 du Conseil d'État, *Le numérique et les droits fondamentaux*..... 2
- Informations relatives à la Commission. 15

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



La séance est ouverte à 10 heures 15.

Présidence de M. Jean-Jacques Urvoas, président.

La Commission reçoit M. Jean-Marc Sauvé, vice-président du Conseil d'État, pour une présentation de l'étude annuelle 2014 du Conseil d'État, Le numérique et les droits fondamentaux. M. Jean-Marc Sauvé est accompagné de Mme Maryvonne de Saint-Pulgent, présidente de la section du rapport et des études, de M. Jacky Richard, rapporteur général et président adjoint de cette section, et de M. Laurent Cytermann, rapporteur général adjoint de cette section.

M. le président Jean-Jacques Urvoas. Nous accueillons aujourd'hui M. Jean-Marc Sauvé, vice-président du Conseil d'État, que je remercie d'avoir bien voulu accepter de venir nous présenter le rapport du Conseil d'État consacré au numérique et aux droits fondamentaux. Ce n'est pas un exercice si courant au sein de notre Commission, mais cette présentation se justifie par l'ampleur de l'étude qui a été menée et le fait qu'elle réponde à plusieurs de nos préoccupations constantes.

Nous avons eu ainsi l'occasion de travailler notamment sur la question des fichiers de police mais aussi de la protection des données personnelles au plan européen. Il y a un mois, nous avons d'ailleurs tenu une réunion interparlementaire en accueillant avec la commission des Affaires européennes des délégations de nombreux parlements d'États membres de l'Union européenne sur ce sujet.

Je voudrais rappeler aussi le rapport d'information sur les droits de l'individu dans la révolution numérique que Jean-Luc Warsmann, Patrice Verchère et Patrick Bloche ont publié lors de la précédente législature dans le cadre d'une mission commune à la commission des Lois et à la commission des Affaires culturelles. Les préoccupations qui étaient les nôtres à l'époque sont également celles que vous développez aujourd'hui dans ce rapport, qui constitue une réflexion utile, attendue et qui fait déjà l'objet de beaucoup de commentaires. J'ai notamment noté le jugement positif porté par le Défenseur des droits sur votre travail ces jours derniers.

La révolution numérique ne doit pas être perçue uniquement comme une menace pesant sur notre vie privée avec les fichiers qui se développent ou les réseaux sociaux. Elle est aussi un formidable vecteur de liberté qui, comme vous le notez, impose de repenser le régime juridique de plusieurs libertés fondamentales.

Monsieur le vice-président, je vous cède la parole en indiquant que vous êtes accompagné de Mme Maryvonne de Saint-Pulgent, qui préside la section du rapport et des études, ainsi que de M. Jacky Richard, rapporteur général et président adjoint de la même section, et de M. Laurent Cytermann, rapporteur général adjoint.

M. Jean-Marc Sauvé, vice-président du Conseil d'État. Monsieur le Président, merci de votre accueil au sein de la commission des Lois. Je présenterai à grands traits notre étude, puis Mme de Saint-Pulgent pourra justifier la nécessité de repenser la protection des droits fondamentaux dans le contexte d'internet avant que M. Jacky Richard n'expose de façon plus détaillée les propositions.

L'étude repose sur trois points principaux.

En premier lieu, les technologies numériques entretiennent des rapports ambivalents avec les droits fondamentaux. Elles favorisent l'exercice de ces droits, notamment la liberté d'expression et la liberté d'entreprendre ; elles ont aussi suscité la reconnaissance de nouveaux droits fondamentaux qui présentent un caractère autonome : le droit à la protection des données personnelles et le droit d'accès à internet. Mais elles exposent les individus à des risques inédits, en particulier dans le domaine des données personnelles, où l'on constate une diversification des sources et des moyens d'agrégation : l'accumulation des données et les possibilités de tri et de recomposition constituent en effet une menace pour la vie privée et les libertés. Ces technologies confrontent par ailleurs les pouvoirs publics à de nouvelles exigences de régulation, de conciliation entre libertés individuelles et sauvegarde de l'ordre public, et de lutte contre de nouvelles formes d'activités illicites ou criminelles, comme la cybercriminalité et le terrorisme mondialisé.

En deuxième lieu, face à cette ambivalence, le cadre juridique français et européen doit s'adapter afin de mettre davantage ces technologies au service des individus et de l'intérêt général. L'internet n'est pas un espace de non droit, contrairement à ce qui avait été prophétisé dans les années 1990, mais il soulève des difficultés juridiques inédites : une gouvernance assurée par différentes institutions, plus privées que publiques et plus étrangères que françaises, une incertitude quant à la loi applicable – le plus souvent celle du pays où est établi l'opérateur, qui est fréquemment hors de nos frontières – et la difficulté à garantir l'effectivité des décisions administratives ou juridictionnelles – problème rencontré quand il est apparu que Yahoo assurait la diffusion d'objets d'origine nazie, une décision française ne pouvant s'appliquer aux États-Unis. En outre, un excès de régulation aurait des effets négatifs sur le potentiel de croissance que représente l'internet à l'échelle de l'Europe.

Le droit existant comporte d'ores et déjà des principes fondateurs à conserver. Il est à cet égard satisfaisant de constater que des principes fixés au milieu des années 1970 par le rapport Tricot et la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés demeurent encore globalement pertinents. Il en est ainsi, dans le domaine des données personnelles, d'une définition large de cette notion ainsi que des principes de finalités déterminées, de proportionnalité, d'exactitude, de consentement informé dans la collecte et de conservation des données.

Pour autant, le cadre juridique doit être enrichi, notamment pour que soit définie une chaîne de responsabilité comprenant l'ensemble des acteurs : les éditeurs et les hébergeurs mais aussi les opérateurs des réseaux et les plateformes. Cette rénovation doit s'inscrire dans une dynamique européenne, en particulier dans le cadre de la proposition de règlement relative à la protection des personnes physiques à l'égard du traitement de données personnelles ou de directives dans le domaine numérique, notamment la révision de la directive relative aux droits d'auteur. De même, devons-nous tenir compte de la jurisprudence constructive de la Cour de justice de l'Union européenne (CJUE), qui s'est déjà traduite par deux grands arrêts en 2014 : l'arrêt *Google Spain* sur la question du déréférencement pour des données personnelles et l'arrêt *Digital Rights* sur la durée de conservation des métadonnées – ce qui implique de réfléchir aux données qui peuvent être conservées, aux durées de conservation et aux personnes justifiant un besoin de protection particulière.

En troisième lieu, dans cette perspective, l'étude annuelle du Conseil d'État propose cinq axes de rénovation de notre cadre juridique. D'abord, créer trois nouveaux principes transversaux : un droit à l'autodétermination informationnelle, à l'image de celui consacré par la Cour constitutionnelle allemande en 1983 – au lieu d'un droit à la propriété des données personnelles, qui ne nous paraît pas pertinent ; le principe de neutralité des réseaux ; le

principe de loyauté dans le traitement des données personnelles – qui s’appliquerait à d’autres acteurs que les éditeurs ou les hébergeurs, notamment les plateformes.

Il s’agit aussi de renforcer les pouvoirs des individus et de leurs groupements, en particulier en définissant les modalités de mise en œuvre du droit au déréférencement, en précisant les obligations concrètes découlant du principe de loyauté ou en envisageant une action collective, distincte de l’action de groupe, en cas de violation de la législation sur les données personnelles.

Troisième axe de réforme : repenser le rôle des autorités publiques à l’échelle de l’Union européenne, notamment sécuriser la liberté de réutilisation de données non personnelles, ou anonymisées, créer une procédure d’homologation des codes de conduite professionnelle, encadrer l’usage d’algorithmes dans le traitement des données numériques et le profilage des comportements, et renforcer les moyens de coordination et de lutte contre les contenus illicites et les contrefaçons – particulièrement dans le domaine des industries culturelles, en créant un régime spécifique de responsabilité pour les plateformes.

Quatrième axe : assurer le respect des droits fondamentaux dans l’utilisation du numérique par les personnes publiques, ce qui implique de poursuivre l’ouverture des données publiques tout en prévenant les risques d’atteinte excessive à la vie privée et de renforcer les garanties entourant la constitution et l’usage des fichiers de police judiciaire – dans le cadre de l’arrêt de la Cour européenne des droits de l’homme (CEDH) du 18 septembre 2009, *Brunet contre France*, qui a condamné notre pays en raison de l’insuffisance de la gestion du stock des données du fichier STIC (Système de traitement des infractions constatées). Il faut aussi tirer les conséquences de l’arrêt *Digital Rights* en matière d’accès et de conservation des métadonnées. Le Conseil d’État propose, dans ce contexte, de refondre la législation sur les interceptions de sécurité et de recréer une autorité publique indépendante dans ce domaine. Il conviendra alors de définir les données ou métadonnées qui pourront être conservées, la durée et les fins de cette conservation ainsi que les types de protection pour certaines catégories de personnes.

Enfin, il convient d’organiser la coopération européenne et internationale et, pour cela, de définir un socle de règles applicables à tous les prestataires de service exerçant leur activité dans l’Union européenne, quels que soient leurs lieux d’établissement. Il ne s’agit pas de remettre en cause le droit du pays d’établissement des opérateurs, mais d’avoir un ensemble de règles communes s’appliquant au pays de destination.

Pour chacune des 50 propositions avancées, l’étude précise le vecteur juridique le plus adapté, qu’il s’agisse du droit dérivé européen, d’une loi, d’un acte réglementaire ou de formes de droit souple. Dans cette perspective, un rôle moteur revient au législateur français, soit directement, soit indirectement par sa participation aux réflexions et aux propositions sur de nouveaux instruments de droit dérivé européen.

Mme Maryvonne de Saint-Pulgent, présidente de la section du rapport et des études du Conseil d’État. Quatre raisons conduisent à repenser les droits fondamentaux dans ce domaine.

D’abord, la transnationalité du numérique, qui pose des questions sur le droit applicable. Lorsque *Google* et *Facebook* inscrivent dans leurs conditions générales d’utilisation que le droit applicable est celui des États-Unis, quelle est la portée effective de la loi française ou européenne qui assure en principe la protection des citoyens ?

En deuxième lieu, l'ambivalence du numérique, qui ouvre de nouveaux espaces pour les libertés fondamentales en créant de nouvelles menaces. Il ne faut pas que les mesures prises pour conjurer les menaces étouffent le potentiel libérateur du numérique.

Troisièmement, celui-ci avive les tensions entre libertés fondamentales : droit à la vie privée contre droit à la sécurité – comme le montrent les questions posées par le renseignement et la surveillance des communications électroniques – ou contre la liberté d'expression – comme en témoigne l'arrêt *Google Spain*. Ce problème, qui est familier au juge, se pose dans ce domaine avec une acuité particulière.

Quatrièmement, le numérique est un enjeu de compétition et de lutte de pouvoir très violente entre États et acteurs économiques. Si on ne peut subordonner la protection des droits fondamentaux à des impératifs économiques, on ne peut ignorer le risque que l'Europe devienne une colonie du monde numérique.

Nous invitons donc le législateur national et européen à repenser en profondeur les modes de protection de plusieurs libertés fondamentales. Nous avons dû à cet égard prendre position sur plusieurs sujets médiatiques.

Le premier consistait à savoir s'il fallait reconnaître un droit de propriété sur les données personnelles. Le Conseil d'État a répondu par la négative : si l'individu est en théorie propriétaire de ses données, la propriété patrimoniale sur celles-ci poserait plus de problèmes qu'elle n'en résoudrait. D'ailleurs, pour l'instant, personne n'est propriétaire de ces données – les opérateurs sont propriétaires de bases de données ou de fichiers, et non des données elles-mêmes.

Si on créait un droit de propriété sur les données, cela voudrait dire qu'on pourrait le céder ; or un récent sondage indiquait que les Français, tout en étant inquiets sur l'utilisation de leurs données personnelles, étaient prêts à les vendre pour 500 euros par an. En outre, la capacité juridique des États à protéger les individus s'agissant de cette utilisation deviendrait une ingérence dans l'exercice du droit de propriété, dont on voit la montée dans l'échelle des principes garantis par la Constitution.

Le Conseil d'État a donc proposé de reconnaître, comme la Cour constitutionnelle allemande, un droit à l'autodétermination informationnelle, qui est un droit de la personne, et non patrimonial. Si ce n'est pas un droit nouveau, il est proposé de l'inscrire dans la loi nationale pour permettre de réinterpréter tous les droits sur les données personnelles à la lumière du principe fondamental selon lequel l'individu, sans être propriétaire de ses données, doit contrôler l'usage qui en est fait.

Le deuxième sujet concerne l'utilisation des données massives, ou *Big Data*, et pose la question de leur compatibilité avec la loi de 1978 dite « Informatique et libertés ». Le Conseil d'État y répond positivement : il n'y a pas lieu de revoir les principes de proportionnalité ou de finalité. Mais il propose de distinguer deux types d'usages : les usages à caractère statistique – dans lesquels on ne s'intéresse pas aux personnes en tant que telles mais à la masse des données –, qui doivent rester très libres – ce qui suppose que le projet de règlement européen ne contraigne pas trop de tels usages, comme c'est le cas dans la rédaction actuelle – ; les usages ciblant les personnes en tant que telles – notamment le profilage, évaluant par exemple la solvabilité d'un emprunteur ou recherchant des fraudeurs potentiels – qui doivent rester soumis aux principes de la loi de 1978.

Troisième question : y a-t-il un droit à l'oubli ? Je rappelle que l'arrêt *Google Spain* a reconnu seulement un droit au déréférencement : il ne s'agit pas du droit de la personne à voir effacer les informations la concernant sur les sites sources, mais de discuter de leur référencement sur les moteurs de recherche. Le Conseil préconise de mieux mettre en œuvre cet arrêt, en organisant notamment le débat sur le droit des sites qui ont produit les contenus à être informés des déréférencements envisagés, et de confier à la Commission nationale de l'informatique et des libertés (CNIL) et à ses homologues européennes le soin de définir les lignes directrices de ce droit au déréférencement.

Quatrième question, la neutralité, qui implique que les opérateurs de communication électronique traitent de manière égale toutes les communications, quel que soit leur contenu. Il s'agit d'une garantie fondamentale pour le bon fonctionnement d'internet, mais aussi pour les libertés d'expression et d'entreprendre. Le Conseil d'État préconise donc d'inscrire cette notion dans la loi nationale, sachant qu'elle ne peut s'appliquer à certains opérateurs, notamment les plateformes. Pour celles-ci, il est proposé que s'applique le principe de loyauté, qui fait appel à des notions bien connues du droit commercial et de la consommation.

Cela suppose la définition d'un nouveau régime juridique, les plateformes étant inconnues du droit positif, qui ne connaît que les éditeurs et les hébergeurs. Ce faisant, cette proposition met en cause les définitions de la directive de 2000.

Enfin, cinquième sujet : la gouvernance d'internet, qui est une question de droit international. Un arrêt récent de la CJUE a soulevé des interrogations très importantes sur les principes de collecte systématique des métadonnées chez les opérateurs de communication. Il faut en tirer toutes les conséquences : l'option choisie par le Conseil d'État est non de travailler sur la collecte elle-même – celle-ci étant indispensable à la prévention des actions contre la sûreté nationale –, mais de revoir les conditions d'accès à ces données, tant en ce qui concerne les personnes, les administrations, la durée pendant laquelle les données collectées peuvent être examinées, que la protection de certaines personnes dont on ne pourrait consulter toutes les données selon les mêmes principes que ceux s'appliquant pour la surveillance des communications électroniques. Actuellement, rien ne protège les élus ou les magistrats contre l'examen des métadonnées les concernant.

M. Jacky Richard, rapporteur général et président adjoint de la section du rapport et des études du Conseil d'État. Je vais regrouper les 50 propositions du rapport selon cinq axes principaux, en rappelant que chacune mentionne, à la fin de son énoncé, le vecteur juridique qui permet sa mise en œuvre.

Premier axe : les propositions visant à définir de nouveaux principes fondant la protection des droits fondamentaux à l'ère du numérique.

D'abord, concevoir le droit à la protection des données personnelles comme un droit à l'« autodétermination informationnelle » et non comme un droit de propriété. Il ne s'agit de fait pas d'un droit nouveau, mais d'un principe essentiel donnant son sens aux autres droits fondamentaux et les garantissant. La définition formulée dans l'étude pourrait être inscrite dans les considérants de la proposition de règlement européen relatif à la protection des données, ou par anticipation, dans la loi française relative à l'informatique, aux fichiers et aux libertés de 1978.

Deuxième proposition : consacrer le principe de neutralité du net et des opérateurs de communications électroniques. Il y a plusieurs conceptions à cet égard : le Conseil d'État

propose la sienne, qui n'est pas très éloignée de celle de l'Autorité de régulation des communications électroniques et des postes (ARCEP) et assez proche de celle votée par le Parlement européen le 3 avril 2014, mais avec des nuances liées à une définition plus large des « services spécialisés » et à un droit de suspension ou d'opposition si les risques touchant la neutralité de gestion du trafic sont manifestes ou s'il y a une forte dégradation possible de cette neutralité. Nous avons cherché en effet un équilibre entre la protection des droits fondamentaux, d'une part, et le maintien du droit de l'entreprise et le développement économique, d'autre part.

Troisième proposition : définir une nouvelle catégorie juridique pour les plateformes, distincte à la fois de celle des hébergeurs et des éditeurs de contenus, ce qui suppose une modification de la loi pour la confiance dans l'économie numérique (LCEN).

Deuxième famille de propositions : celles qui visent à renforcer les pouvoirs des individus et de leurs groupements. Elles constituent une bonne manière de mettre en œuvre l'autodétermination informationnelle et font beaucoup appel au droit souple.

Il s'agit de l'attribution à la CNIL d'une mission de promotion des technologies renforçant la maîtrise par les individus de leurs données personnelles, d'un droit d'alerte pour les salariés des organismes traitant de telles données, de la mise en place d'une action collective – distincte de l'action de groupe, destinée à faire cesser les violations de la législation sur ces données – ou de l'engagement d'une réflexion sur les enjeux éthiques liés au numérique, confiée à la CNIL et au Conseil national du numérique (CNN). Enfin, il est proposé de mettre en œuvre un droit au déréférencement, à la suite de l'arrêt *Google Spain*. Cette proposition prévoit les conditions d'application d'une décision unique de déréférencement. Alors que *Google* a engagé toute une série d'initiatives, dont la mise en place d'un comité consultatif, le rapport propose aux autorités publiques de reprendre la main. La question est notamment de savoir si le déréférencement ne concerne que *Google.fr* ou également *Google.com*.

Troisième famille de propositions : celles qui visent à redéfinir les instruments de la protection des droits. Il s'agit d'abord de sécuriser le développement des *Big Data*, qui permet la valorisation du numérique à des fins économiques, pour la réutilisation statistique des données personnelles, quelle que soit la finalité initiale de leur traitement – proposition n° 12. Nous proposons aussi de créer une procédure d'homologation des codes de conduite professionnels élaborés au niveau national ou européen – proposition n° 16 –, de développer la normalisation en matière de sécurité des traitements de données personnelles – proposition n° 17 –, de mettre à l'étude la création d'un numéro national unique d'identification (NIR, numéro d'inscription au répertoire) non signifiant et permettre le recours au NIR pour les traitements de données personnelles ayant pour fin la recherche et les politiques publiques dans le domaine de la santé. L'utilisation restreinte du NIR constitue en effet un frein important : on a dit, par exemple, qu'on aurait pu prévoir les graves dysfonctionnements récents liés à un médicament n'ayant pas été fait pour ce pour quoi il avait été initialement conçu si on avait pu davantage utiliser les bases de données.

Nous suggérons également de définir un droit des algorithmes prédictifs, qui doivent toujours réserver une part d'intervention humaine, aucune décision touchant les individus ne devant intervenir par la simple application d'un algorithme.

La quatrième famille de propositions concerne l'État, qui doit être exemplaire dans l'utilisation des données personnelles. Le Conseil d'État propose que l'État amplifie sa

politique *d'open data* pour que les données soient utilisables tout en prévenant les risques pour la vie privée, en évitant notamment les risques de réidentification grâce à des standards d'anonymisation. Il propose aussi de renforcer les garanties entourant l'usage des fichiers de police – TAJ (traitement d'antécédents judiciaires), FAED (fichier automatisé des empreintes digitales) ou FNAEG (fichier national des empreintes génétiques) – pour que les classements sans suite, relaxes, acquittements et non-lieux puissent être pris en compte, de manière à éviter les condamnations dont nous avons fait l'objet.

En matière de renseignement, le Conseil d'État propose deux lectures de l'arrêt *Digital Rights* : une lecture très stricte, qui semble avoir été celle des juges, et une lecture plus ouverte. Il suggère de retenir cette dernière, notamment en réservant l'accès aux métadonnées à des fins de police judiciaire aux crimes et délits d'une gravité suffisante et en réexaminant les régimes prévoyant l'accès de diverses autorités administratives – par exemple, la Haute autorité pour la diffusion des œuvres et la protection des droits sur internet (HADOPI), l'Autorité des marchés financiers (AMF) ou l'administration fiscale – à des fins autres que la sécurité intérieure.

Nous proposons également de moduler la période d'accessibilité des données en fonction de la gravité et d'étendre aux procédures d'accès aux métadonnées les garanties prévues en faveur des parlementaires, avocats, magistrats et journalistes pour les interceptions judiciaires.

De même, le Conseil d'État propose de définir par la loi le régime de l'interception des communications à l'étranger, en fixant les finalités de ces interceptions et en prévoyant leur contrôle par une autorité administrative indépendante. La Commission nationale de contrôle des interceptions de sécurité (CNCIS), créée par la loi de 1991, serait en outre transformée en une « Autorité de contrôle des services de renseignements » dotée de moyens renforcés, plutôt que de confier ces prérogatives à une autorité généraliste.

Enfin, la cinquième famille de propositions traite du champ d'application territorial de la règle de droit en matière de numérique et de gouvernance d'internet.

Le Conseil d'État prend position sur la territorialité du droit en préconisant de desserrer la contrainte de l'application du droit du pays d'origine et de renforcer, dans le cadre des règles européennes, celui du pays de l'internaute. Mais cette proposition n'est pas générale : cela n'aurait pas de sens de dire que c'est systématiquement ce dernier droit qui prévaut ; ce serait aussi nous tirer une balle dans le pied, car nous avons d'excellentes entreprises irriguant les réseaux étrangers. Reste que dans des domaines bien précis, que nous avons qualifiés de « loi de police » au sens du droit international privé, la loi du pays de l'internaute s'appliquerait.

De plus, nous recommandons de donner une plus grande place aux États dans les instances de gouvernance d'internet comme l'ICANN – la Société pour l'attribution des noms de domaine et des numéros sur internet. Mais il ne s'agit pas de modifier les règles de fonctionnement de cette instance : la conférence de São Paulo sur le net numérique d'avril dernier a tracé des voies très intéressantes et je crois que les autorités américaines sont prêtes à évoluer. Il est en outre possible de lier des alliances avec des pays tels que le Brésil et la Corée du Sud.

Enfin, nous préconisons l'adoption d'une convention internationale relative aux libertés fondamentales et aux principes de la gouvernance d'internet qui engagerait ses signataires en faveur de la promotion des droits fondamentaux sur le net.

M. le président Jean-Jacques Urvoas. Monsieur le vice-président, Madame, Messieurs, merci pour cette présentation. Quelle différence faites-vous entre l'action collective et l'action de groupe ?

Pouvez-vous nous préciser le contenu du droit à l'autodétermination informationnelle ?

Enfin, s'agissant du contrôle exercé par ce que vous appelez « l'Autorité de contrôle des services de renseignements », est-ce-que ce sont bien les techniques spéciales soumises à autorisation administrative que vous visez et non l'exercice d'un contrôle sur les services de renseignement eux-mêmes ?

Mme Marietta Karamanli. Le droit au déréférencement pourrait se heurter à plusieurs obstacles techniques et à la garantie de la liberté d'expression. D'autres pistes ont été envisagées comme l'effacement par principe des données d'un profil d'utilisateur après un certain délai ou la possibilité pour les utilisateurs de définir une date de péremption de leurs publications : qu'en pensez-vous ?

Quel est par ailleurs votre avis sur la proposition de règlement de la Commission européenne prévoyant d'alléger les obligations des entreprises en supprimant l'obligation systématique de déclaration préalable à la mise en œuvre d'un traitement automatisé des données personnelles en contrepartie du fait que les responsables du traitement soient soumis à des exigences de sécurité accrues ? Quels devraient être les principes gouvernant cette responsabilisation ?

Mme Laurence Dumont. Je voudrais saluer le travail considérable mené par le Conseil d'État et le pragmatisme de sa démarche. Beaucoup de propositions reposent finalement sur du droit souple, sachant que le calendrier est long, nombre de ces propositions étant liés au règlement européen, dont l'adoption interviendra au mieux d'ici deux ans.

Le droit de propriété peut en effet conduire à limiter la protection des données personnelles et à une relation déséquilibrée entre l'individu et l'acheteur, car une fois qu'on a vendu quelque chose, on n'a plus la main dessus : pouvez-vous nous en dire plus sur ce droit à l'autodétermination, qui suppose que les personnes concernées soient réellement capables d'être autonomes dans leurs décisions ?

Une constitutionnalisation de cette protection avait par ailleurs été envisagée : je pourrais y être favorable, compte tenu des déséquilibres que l'étude met en avant dans la relation entre l'individu et les organismes collectant et traitant les données.

Enfin, la proposition n° 4 envisage de donner à la CNIL et aux autorités de protection une mission explicite de promotion des technologies renforçant la maîtrise des personnes sur l'utilisation de leurs données personnelles : or, cette instance joue déjà pour partie ce rôle grâce notamment au laboratoire qu'elle a créé récemment et est à l'origine d'un collectif d'une soixantaine d'acteurs pour défendre l'idée de l'éducation numérique comme grande cause nationale. Sauf à sous-entendre une augmentation substantielle des moyens affectés à

cette nouvelle mission de la CNIL, je vois donc mal en quoi cette proposition renforcerait effectivement la protection des données personnelles.

M. Luc Belot. Merci de cette initiative nous permettant d'évoquer les droits fondamentaux à l'heure du numérique, qui fait l'objet d'une actualité régulière, que ce soit dans le domaine du vin, des taxis et des voitures de tourisme avec chauffeur (VTC), ou qu'il s'agisse du partage de logement ou de l'arrivée de *Netflix* dans le marché de la vidéo à la demande sur nos ondes et, depuis aujourd'hui, sur nos box.

La présentation de votre rapport devant les membres du CNN a suscité chez eux beaucoup d'intérêt.

Mais je regrette qu'on soit trop souvent sur ces questions sur un registre défensif, alors que, comme le souligne votre rapport, le système européen est robuste, notamment sur les données personnelles.

Il faut retenir à cet égard des éléments liés à la neutralité du net, la réforme du « *Safe Harbour* » – ou sphère de sécurité –, ce qui a trait aux fichiers de police ou aux services de renseignement et ce qui devra relever d'une loi spécifique autour du numérique, qui traitera l'ensemble des sujets évoqués dans le rapport en les approfondissant : l'évolution de la CNIL, le cadrage des autres tiers de confiance ou le principe d'autodétermination.

Il convient de faire évoluer l'application du droit en clarifiant l'obligation de coopération des hébergeurs et des plateformes – qui doivent avoir une dénomination spécifique.

Le statut des données servant un intérêt public, comme une interface de programmation (API) des taxis ou les données de santé ou de transport nécessite selon moi des précisions législatives : pourquoi ne pas l'avoir abordé ? Pensez-vous qu'il n'y a pas lieu de légiférer sur ce point ?

M. Guillaume Garrot. Je remercie moi aussi le Conseil d'État pour cette étude.

Pouvez-vous préciser la notion d'autodétermination informationnelle ? Quels en seraient les avantages pour le citoyen et le fonctionnement pratique ?

M. Patrick Mennucci. Je m'associe à ces remerciements.

Avez-vous abordé la question de la possibilité pour un État de couper l'accès à des sites internet qu'il jugerait dangereux ? Prévoyez-vous une évolution dans ce domaine ? Il s'agit d'une question essentielle dans la lutte contre le terrorisme.

M. Philippe Gosselin. Je m'associe aussi aux remerciements au sujet de ce rapport, qui tombe à point nommé et souligne bien l'ambivalence du numérique, laquelle appelle de nouveaux principes régulateurs.

Sans doute le cadre européen est-il le bon : on le voit s'agissant du projet de règlement sur la protection des données personnelles, que nous avons tenté d'améliorer. Mais il ne faut pas oublier pour autant le cadre national : le travail de la CNIL a fait ses preuves et la France préside le G29, ce groupe des CNIL européennes. Il y a à cet égard une lutte entre la *common law* et le droit continental, qui sous-tend des enjeux économiques importants. Cela renvoie à l'articulation entre droit européen et droit interne : les autorités nationales doivent

défendre un certain nombre de messages et de pouvoirs en la matière. Si vous le mettez en avant, il faudrait peut-être amplifier le mouvement : nous aurons sans doute l'occasion d'y revenir avec une loi sur le numérique qui modifierait substantiellement la loi de 1978.

Il faudrait aussi réfléchir davantage à la transformation du droit de propriété, le Conseil constitutionnel retenant davantage la notion d'*usus* que d'*abusus*. Quelle est votre position sur ce point ?

Mme Sandrine Mazetier. Merci pour ce rapport et les prises de position très nettes du Conseil.

Mais je m'interroge sur le débat entre droit de propriété et autodétermination informationnelle : ne faudrait-il pas un échelon de droit de propriété intermédiaire à l'échelle européenne ou nationale pour respecter l'équilibre entre libertés individuelles et protection des États ? On laisse en effet relativement seuls des individus qui, en acceptant des conditions générales de vente, autorisent des opérateurs extérieurs à exploiter ou à vendre des données personnelles, sachant qu'en cas de litige, celui-ci se déroule souvent à l'étranger. Ne devrait-on pas avoir une forme de droit de propriété des données personnelles des ressortissants des États membres de l'Union européenne, que celle-ci défendrait vis-à-vis d'opérateurs internationaux qui n'ont de compte à rendre devant aucun État ?

Par ailleurs, ne faudrait-il pas avoir une réflexion européenne sur les interceptions de sécurité à l'étranger ?

Mme Marie-Françoise Bechtel. Je m'associe aussi aux remerciements. Ce rapport, qui est une mine pour le législateur, porte sur un domaine sensible et d'actualité : à l'occasion du débat en première lecture sur le projet de loi de lutte contre le terrorisme, nous avons soulevé des interrogations recoupant certaines de celles du rapport, notamment s'agissant de l'équilibre entre les libertés dans le domaine du numérique et la possibilité de prendre des mesures de police administrative de blocage des sites.

Si un droit de propriété présenterait en effet plus d'inconvénients que d'avantages, quel serait le contenu du droit d'autodétermination informationnelle ? Comment est-il dénommé en Allemagne et s'applique-t-il dans ce pays ? Comment pourrions-nous l'appliquer dans notre droit latin ?

Quant au principe de loyauté, il s'applique au contenu : comment l'articulez-vous avec les obligations de surveillance des opérateurs, en vigueur depuis la directive européenne de 2004 ?

M. François Vannson. Ce rapport constitue un travail remarquable.

Serait-il souhaitable d'avoir une véritable politique européenne concernant les hébergeurs ?

Certaines personnes créent des sites internet et discréditent par leur action des entreprises, des institutions ou des hommes ou femmes publics en toute impunité, car elles sont toujours à la limite de la diffamation. De plus, les magistrats estiment généralement qu'un homme public, en s'exposant, doit accepter ce type de situation. Cela me paraît très grave pour notre démocratie : ne pourrait-on réfléchir également à ce sujet ?

M. Patrice Verchère. S'agissant de la proposition n° 39, comment définir par la loi le régime de l'interception des communications à l'étranger pour nos services de renseignement quand les trois quarts du temps ils agissent dans l'illégalité la plus complète ?

M. Lionel Tardy. Je salue cette étude large et ambitieuse. Mettre en œuvre une partie de ses propositions demanderait beaucoup de temps et plusieurs projets de loi. On voit bien l'importance du numérique au regard des droits fondamentaux.

L'étude fait souvent référence à juste titre à des textes de niveau européen, notamment au règlement sur les données personnelles. Pouvez-vous nous en dire plus sur l'importante proposition n° 18, visant à anticiper et organiser la transition vers le nouveau cadre juridique issu de ce règlement ? Cette nécessaire transition a-t-elle déjà été amorcée ?

M. Olivier Marleix. Je suis frappé par l'écart entre l'intelligence que le législateur français met à contrôler ce que fait l'État en matière de protection des données et l'incapacité à avoir la même exigence à l'égard d'opérateurs privés – je pense notamment au décalage entre l'énergie mise à empêcher le déploiement de l'utilisation d'une carte d'identité électronique comportant des empreintes digitales et le peu de moyens de droit et techniques dont nous disposons pour savoir ce qu'*Apple* fait par exemple des empreintes collectées.

Au regard de l'espoir fondé sur une réglementation européenne dans ce domaine, ne pourrait-on pas s'appuyer davantage sur la notion d'ordre public international ?

M. Jean-Marc Sauvé, vice-président du Conseil d'État. Merci de vos appréciations sur notre travail.

Je rappelle que sur ce sujet, nous ne partons pas de rien : nous nous sommes appuyés sur la réflexion procurée par les travaux parlementaires ou des institutions européennes et internationales, auxquels je tiens à rendre hommage. D'ores et déjà, certaines autorités, comme le Défenseur des droits, ont indiqué que de nouvelles propositions seraient faites, ce dont nous nous réjouissons.

S'agissant de l'autorité de contrôle des services de renseignement, nous ne visons que les moyens d'investigation spéciale dont ils disposent et n'entendons pas traiter le sujet plus vaste du contrôle de ces services, qui relève du Parlement.

Quant à l'autodétermination informationnelle, qui est une traduction littérale d'« *Informationnelle Selbstbestimmung* », elle doit permettre aux personnes de disposer des informations nominatives qui les concernent. Ce droit est seul de nature à garantir la protection de la vie privée. Car si nous patrimonialisons ces données, elles pourraient se céder et la personne n'en disposerait plus. Reste qu'un travail d'approfondissement complémentaire mérite d'être conduit : le rapport ne peut tout dire.

Par ailleurs, quand on parle d'action de groupe, en règle générale, on fait référence à la réparation de préjudices et à des enjeux patrimoniaux et financiers. Cette action débouche sur un jugement déclaratoire de responsabilité, alors que l'action collective aurait un champ d'application plus vaste : il s'agit de réparer des préjudices variés, qui peuvent être patrimoniaux mais aussi moraux.

Concernant le déréférencement, il s'oppose au droit à l'effacement. Nous considérons que le risque actuel est d'atteindre à la vie privée : il faut protéger les citoyens contre le risque procédant d'un référencement ainsi que d'une mémorisation et d'une

diffusion perpétuelles de liens permettant de se connecter à des données qui devraient rester privées. Mais il convient là encore de trouver un juste équilibre entre la liberté d'expression et la protection de la vie privée. Or, si nous allions trop vite vers l'effacement des données, cela pourrait être assimilé à une censure et constituer une atteinte grave à la liberté d'expression. L'enjeu est d'arriver à un déréférencement effectif : ce n'est pas une mince affaire d'être déréférencé dans *Google.com* et non, seulement, dans *Google.fr*.

Madame Dumont, nous ne proposons pas de constitutionnalisation des droits liés à la protection des données. Notre démarche s'inscrit dans celle du Conseil constitutionnel, qui, à partir du corpus de la Déclaration des droits de l'homme et des principes constitutionnels, peut assurer un contrôle effectif de la législation sur les fichiers et la protection des données.

En revanche, il nous paraît important de donner à la CNIL un pouvoir de promotion des technologies de protection : les autorités indépendantes sont régies par un principe de spécialité et elles ne peuvent pas, sans habilitation du législateur, se donner des pouvoirs qui ne leur ont pas été reconnus.

Monsieur Belot, il faut que nous arrivions à un nouvel équilibre dans les relations transatlantiques. Le « *Safe Harbour* » présente deux limites : les recommandations des normes de droit souple qu'il comporte apparaissent comme d'un niveau généralement regardé comme insuffisamment protecteur de la vie privée et des données personnelles et il repose trop exclusivement sur l'autocontrôle. Il faudrait progresser sur ces deux points.

Enfin, nous proposons d'agir dans le cadre de l'Union européenne pour définir un corpus de règles sur la protection des libertés et la garantie de la sécurité, opposables aux opérateurs, quelle que soit la loi du pays d'établissement de ceux-ci. On ne peut y parvenir qu'en promouvant la notion de « loi de police », qui s'applique dans un cadre territorial déterminé. Mais nous n'entendons pas substituer la loi du pays de destination à celle du pays d'origine.

Mme Maryvonne de Saint-Pulgent, présidente de la section du rapport et des études du Conseil d'État. Il faut en effet approfondir la portée pratique du droit à l'autodétermination informationnelle. Le Conseil d'État va d'ailleurs organiser en février prochain une journée d'étude sur ce sujet, notamment sur des applications concrètes de ce droit dans les domaines de la santé et du travail.

S'il y a une analogie entre ce droit et le droit moral sur la propriété intellectuelle, qui est incessible et perpétuel et permet de s'opposer à certains usages excessifs, ce dernier constitue un facteur d'incertitude dans les relations économiques puisque, comme il ne se négocie pas, il plane comme une menace sur les utilisations des œuvres qu'il protège.

M. Laurent Cytermann, rapporteur général adjoint de la section du rapport et des études du Conseil d'État. Nous entendons ce droit à l'autodétermination informationnelle comme un horizon et un aiguillon. Il a vocation à donner du sens au droit à la protection des données personnelles tel qu'il existe aujourd'hui, en permettant à l'individu de décider de la communication et de l'utilisation de celles-ci. L'enjeu est la liberté de ce dernier dans une société numérique où l'usage des données est de plus en plus massif. Or, on en est très loin. S'il existe les droits d'opposition, d'accès ou de rectification, l'individu n'a pas concrètement les moyens de les exercer. Il faut davantage de traçabilité de l'utilisation des données, notamment par les grands acteurs du numérique, et que les technologies de protection se développent beaucoup plus : le jour où il pourra savoir où sont ces données et

exercer facilement un droit de retrait à l'égard de tel ou tel acteur, on aura franchi un pas important dans cette autodétermination.

M. Jacky Richard, rapporteur général et président adjoint de la section du rapport et des études du Conseil d'État. Madame Bechtel, le concept d'autodétermination informationnelle a été inventé par la Cour de Karlsruhe en 1983 à propos d'une loi importante sur le recensement. Il s'applique en Allemagne à beaucoup de sujets, notamment en matière de police et de lutte contre le terrorisme. La note n° 457 de notre étude donne quelques références de décisions de justice dans ce pays, où cette notion, *a priori* très générale et floue, a été retenue dans des affaires juridiques précises.

M. Laurent Cytermann, rapporteur général adjoint de la section du rapport et des études du Conseil d'État. Madame Karamanli, nous voyons comme un progrès la suppression de l'obligation de déclaration systématique de traitement de données figurant dans la proposition de règlement. En effet, cette déclaration est trop légère pour certains, car ce n'est qu'une déclaration, et trop lourde pour d'autres, comme par exemple des *startups* à la recherche de leur modèle d'affaires et d'utilisation des données. Il faut donc établir une proportionnalité de l'encadrement en fonction du risque que présente le traitement et, pour celui comportant un risque important, prévoir des obligations plus lourdes – nous proposons une certification en continu de la mise en œuvre du traitement et une plus grande traçabilité de l'utilisation des données, afin qu'elles puissent être contrôlées.

Concernant les interceptions des données à l'étranger, évoquées par M. Verchère, on envisage l'application de la loi française, car il s'agit d'un acte de puissance publique comportant une responsabilité de l'État d'origine. D'ailleurs, aux États-Unis, prévaut la section 702 du *Foreign Intelligence surveillance Act* (FISA) encadrant les interceptions à l'étranger, même si elle est critiquée dans la mesure où elle permet une collecte trop massive. Or il nous a semblé qu'en France, le cadre juridique ne répondait pas à l'exigence de la CEDH affirmée dans l'arrêt de 2008 *Liberty contre Royaume-Uni*, qui est celle de la prévisibilité de la loi. Celle-ci doit préciser les finalités et les cas justifiant de telles interceptions, même si ce n'est pas facile.

M. Jean-Marc Sauvé, vice-président du Conseil d'État. Il ne nous est pas venu à l'idée de mettre en place une autorité indépendante de contrôle de l'action des services de renseignement à l'étranger. Mais lorsque sont opérées sur le territoire national des interceptions sur des communications à l'étranger, le législateur national a son mot à dire. Si nous avons retenu la proposition n° 39, c'est parce que nous devons tenir compte d'un certain nombre d'arrêts des juridictions européennes.

Au sujet de l'arrêt *Digital Rights*, nous réfléchissons à deux interprétations possibles : le débat reste ouvert et les autorités nationales ont leur propre espace de décision pour permettre à la CJUE de dire son interprétation.

Monsieur Gosselin, il ne s'agit pas d'un débat entre le droit continental et la « *common law* ». Quand on parle à des juristes de cette notion, ils ont tendance à considérer que les concepts du droit continental s'imposent à eux d'une manière excessive et trop rigoureuse. La vraie question est celle de la puissance des différents opérateurs. Or le problème auquel nous sommes confrontés est que les principaux opérateurs se situent dans les pays de « *common law* ».

M. Philippe Gosselin. Je ne suis pas tout à fait convaincu.

M. Jean-Marc Sauvé, vice-président du Conseil d'État. Monsieur Mennucci, la possibilité de couper l'accès à des services véhiculant des contenus illicites est un enjeu fondamental en termes de respect de la loi, de prévention contre le terrorisme et de liberté d'expression. Dès maintenant, la législation permet aux éditeurs et aux hébergeurs de procéder au retrait de ces contenus, faute de quoi il est possible de bloquer l'accès aux sites en question. Quelles que soient la localisation de l'opérateur et la loi qui lui est applicable, il est évident que, dans le cadre des législations dont nous avons la maîtrise, nous avons la possibilité de faire prévaloir nos intérêts vitaux sur ces questions majeures.

Mme Maryvonne de Saint-Pulgent, présidente de la section du rapport et des études du Conseil d'État. Madame Bechtel, le Conseil d'État propose de ne pas modifier le régime de responsabilité des plateformes, qui reste celui de responsabilité limitée prévu pour les hébergeurs : comme elles ne produisent pas les contenus qu'elles référencent, elles n'ont pas à avoir un régime de responsabilité aligné sur celui des éditeurs. Mais elles restent soumises aux obligations s'imposant aux hébergeurs de retirer les contenus illicites.

L'obligation de loyauté porte sur toutes les autres activités des plateformes. Il s'agit de ne pas mélanger les genres, c'est-à-dire de ne pas, sous prétexte de donner des conseils avisés aux utilisateurs, promouvoir des contenus dans lesquels elles ont des parts financières. Cela oblige à être transparent sur les critères de référencement et de rendre un meilleur service à l'utilisateur.

Il s'agit aussi d'informer sur les retraits de contenus licites, les plateformes ayant leur propre politique éditoriale. L'obligation de loyauté est en effet d'informer les fournisseurs de contenu des règles de retrait et d'en discuter avec les intéressés, car cela porte atteinte aux droits des producteurs de contenu.

Enfin, quand changent les politiques de classement des algorithmes, il faut aussi afficher ce changement, les conséquences et ouvrir un espace de dialogue avec les fournisseurs, dont les intérêts économiques sont en cause. Nous sommes ici dans le droit de la consommation et le droit civil. Mais cette obligation n'existe nulle part actuellement puisque la catégorie juridique des plateformes ne figure pas dans la directive.

M. le président Jean-Jacques Urvoas. Monsieur le vice-président, Madame, Messieurs, je vous remercie : cette audition nous ouvre de nombreuses perspectives.

*

* *

Informations relatives à la Commission

La Commission a désigné :

– *Mme Christine Pires-Beaune*, rapporteure sur la proposition de loi de M. Bruno Le Roux et sur la proposition de loi de M. Jacques Pélissard relatives à l'amélioration du régime de la commune nouvelle, pour des communes fortes et vivantes (n° 2241 et n° 2244).

– *M. Jacques Pélissard*, co-rapporteur sur la mise en application de la loi qui serait issue de l'adoption définitive de la proposition de loi de M. Bruno Le Roux et de la proposition de loi de M. Jacques Pélissard relatives à l'amélioration du régime de la commune nouvelle, pour des communes fortes et vivantes (n° 2241 et n° 2244).

La séance est levée à 12 heures.



Membres présents ou excusés

Présents. - Mme Nathalie Appéré, M. Christian Assaf, Mme Marie-Françoise Bechtel, M. Erwann Binet, M. Gilles Bourdouleix, Mme Colette Capdevielle, Mme Marie-Anne Chapdelaine, M. Éric Ciotti, M. Jean-Michel Clément, M. Gilbert Collard, M. Sergio Coronado, Mme Pascale Crozon, M. Carlos Da Silva, M. Marc-Philippe Daubresse, M. Jean-Pierre Decool, M. Sébastien Denaja, Mme Françoise Descamps-Crosnier, M. Patrick Devedjian, M. Marc Dolez, M. Philippe Doucet, Mme Laurence Dumont, M. Olivier Dussopt, M. Georges Fenech, M. Hugues Fourage, M. Guillaume Garot, M. Bernard Gérard, M. Yves Goasdoué, M. Philippe Gosselin, M. Philippe Goujon, Mme Françoise Guégot, M. Philippe Houillon, M. Sébastien Huyghe, Mme Marietta Karamanli, Mme Nathalie Kosciusko-Morizet, M. Jean-Yves Le Bouillonnet, Mme Anne-Yvonne Le Dain, M. Bernard Lesterlin, M. Olivier Marleix, Mme Sandrine Mazetier, M. Patrick Mennucci, M. Paul Molac, M. Pierre Morel-A-L'Huissier, Mme Nathalie Nieson, M. Jacques Pélissard, M. Sébastien Pietrasanta, Mme Christine Pires Beaune, Mme Elisabeth Pochon, M. Jean-Frédéric Poisson, M. Pascal Popelin, M. Dominique Raimbourg, M. Bernard Roman, Mme Maina Sage, Mme Cécile Untermaier, M. Jean-Jacques Urvoas, M. Daniel Vaillant, M. Jacques Valax, M. François Vannson, M. Patrice Verchère, M. François-Xavier Villain, M. Jean-Luc Warsmann, Mme Marie-Jo Zimmermann, M. Michel Zumkeller

Excusés. - M. Frédéric Cuvillier, M. Guy Geoffroy, M. Daniel Gibbes, M. Guillaume Larrivé, M. Alfred Marie-Jeanne, M. Edouard Philippe, M. Roger-Gérard Schwartzenberg

Assistaient également à la réunion. - M. Luc Belot, M. Lionel Tardy