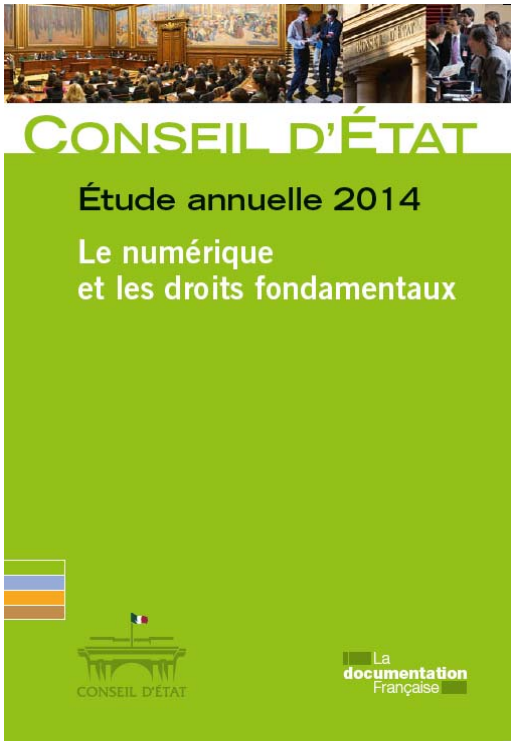
CONSEIL D'ÉTAT

Étude annuelle 2014

Le numérique et les droits fondamentaux



Dossier de presse

Conférence de presse - Mardi 9 septembre 2014

www.conseil-etat.fr

Suivez l'actualité du Conseil d'État sur Twitter : @Conseil_Etat

Retrouvez le live tweet :
#étudenumériqueCE

Sommaire

SYNTHESE

Le numérique, parce qu'il conduit à la mise en données et à la mise en réseau générale du monde, pose problème au regard des droits fondamentaux ; non qu'il serait un phénomène négatif en soi, mais parce qu'il met en question leur contenu et leur régime. En effet, il renforce la capacité des individus à jouir de certains droits, comme la liberté d'expression ou la liberté d'entreprendre ; il en fragilise d'autres comme le droit à la vie privée, la sûreté et le droit à la sécurité.

L'étude annuelle du Conseil d'État intervient alors que le phénomène prend une nouvelle dimension : un triple basculement se manifeste, dans les innovations techniques, dans l'économie et dans l'appréhension du numérique par la société, et renforce les interrogations sur les droits fondamentaux. Après avoir exposé comment l'essor du numérique a déjà suscité la reconnaissance de nouveaux droits et libertés fondamentaux et modifié leurs conditions d'exercice (1re partie), l'étude montre pourquoi l'ambivalence du numérique impose de repenser la protection de ces droits (2e partie). Elle fait en ce sens cinquante propositions pour mettre le numérique au service des droits individuels comme de l'intérêt général (3e partie).

1. – L'essor du numérique a suscité la reconnaissance de nouveaux droits fondamentaux et modifié leurs conditions d'exercice

1.1. L'essor du numérique entraîne des mutations techniques, économiques et sociales

Le numérique se définit comme la représentation de l'information ou de grandeurs physiques (images, sons) par un nombre fini de valeurs discrètes, le plus souvent représentées de manière binaire par une suite de 0 et de 1. Sa puissance transformatrice tient à sa capacité à exprimer des réalités disparates (sons, images, textes, comportements humains, processus industriels ...) dans un langage commun universel ouvrant la possibilité de les traiter de manière systématique et de les mettre en relation. Il en résulte des mutations techniques, économiques et sociales.

Les mutations techniques découlent de la mise en réseau des machines et de la mise en données du monde. La mise en réseau des machines a été rendue possible par les choix d'architecture qui ont présidé à la conception d'internet dans les années 1960 et 1970 : l'ouverture qui permet à tout réseau local d'être connecté à l'internet sans contrôle d'une autorité centrale ; la neutralité, les routeurs utilisés dans les nœuds d'interconnexion étant indifférents au contenu du message. Ces choix ont permis l'expansion mondiale d'internet, qui compte aujourd'hui près de 3 milliards d'utilisateurs. La mise en données du monde est permise par la croissance du nombre d'utilisateurs, la puissance de calcul des machines et la présence de plus en plus diffuse de capteurs connectés.

Définie strictement, l'économie numérique se compose de quelques secteurs spécialisés tels que les télécommunications, l'édition de logiciels ou les sociétés de services et d'ingénierie informatique (SS2I) ; mais elle se déploie aujourd'hui bien au-delà et tend à transformer la quasi-totalité des secteurs d'activité : industries culturelles, presse, commerce et distribution, hôtellerie, transport de personnes, services financiers, automobile, bâtiment... Dans tous ces secteurs, le numérique manifeste sa capacité à bouleverser les règles du jeu et les positions établies. Les modèles d'affaires des entreprises du numérique présentent des caractéristiques spécifiques : une orientation vers la croissance plutôt que la profitabilité à court terme, des stratégies de redéfinition des frontières des marchés dans lesquels elles opèrent, des stratégies de plateforme qui leur confèrent une position de porte d'accès aux

consommateurs et enfin une valorisation intensive des données, notamment des données personnelles. Les effets du numérique transforment aussi les relations sociales. Le numérique agit comme un multiplicateur de collaborations, qui se manifestent sous diverses formes : développement des services de partage, plateformes d'échanges de contenus, réseaux sociaux... Il favorise la participation et la transparence dans l'action des pouvoirs publics. Son impact sur les normes sociales fait débat, notamment en matière de vie privée. Aux tenants d'un dépassement de l'aspiration à la vie privée, en faveur d'un mouvement de « *publicisation de soi* », s'opposent ceux qui soutiennent que cette aspiration n'a pas disparu mais a seulement changé de contenu : il ne s'agit plus seulement d'être « laissé en paix », à l'abri des intrusions, mais aussi de maîtriser son image de soi et sa réputation.

1.2. Le numérique a suscité la reconnaissance de nouveaux droits fondamentaux : le droit à la protection des données personnelles et le droit d'accès à internet

Le droit à la protection des données personnelles (a) et le droit d'accès à internet (b) sont nés en réponse aux questions posées par l'essor du numérique. S'ils sont souvent présentés comme se rattachant respectivement au droit à la vie privée et à la liberté d'expression, leurs enjeux sont en réalité plus larges et peuvent être considérés comme des droits fondamentaux autonomes.

(a) Dans sa courte histoire, le droit à la protection des données personnelles aura connu un bouleversement complet des enjeux qui y sont associés : les auteurs du Rapport Tricot de juin 1975, dont les préoccupations principales portaient sur les conséquences de la constitution de grandes bases de données administratives, ne pouvaient envisager ni l'essor d'internet, ni la puissance de calcul dont disposeraient des terminaux mobiles, ni la valeur économique acquise par les données. Le cadre légal issu de ces réflexions s'est pourtant avéré d'une grande stabilité, ne donnant lieu qu'à une seule réforme importante, intervenue pour transposer la directive n° 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 et qui a notamment déplacé l'accent du secteur public vers le secteur privé.

Les différentes normes applicables en matière de protection des données personnelles (Constitution, convention n° 108 du Conseil de l'Europe du 28 janvier 1981, Charte des droits fondamentaux de l'Union européenne, directive n° 95/46/CE et loi du 6 janvier 1978 modifiée) convergent aujourd'hui quant aux principales garanties de la protection des données personnelles :
- principes relatifs à la qualité des données (loyauté de la collecte, finalités légitimes, proportionnalité, durée de conservation) ;
- exigence du consentement de la personne concernée ou d'un autre fondement légitime prévue par la loi ;
- interdiction de la collecte des données dites sensibles, sauf dans des cas particuliers prévus par la loi ;
- droits d'information, d'accès, de rectification et d'opposition;
- obligation de sécurité du responsable du traitement ;
- existence d'une autorité indépendante de contrôle.

Ces principes constituent le socle d'un droit européen des données personnelles, substantiellement différent du droit américain.

(b) La Cour suprême des États-Unis a été la première juridiction souveraine à être saisie des enjeux de l'accès à internet pour la liberté d'expression, dans un arrêt *Reno, Attorney general of the United States vs American Civil Liberties Union (ACLU)* du 26 juin 1997. En France, le Conseil constitutionnel s'est prononcé à l'occasion d'un recours contre la loi favorisant la diffusion et la protection de la création sur internet : il a jugé à cette occasion que la liberté de communication protégée par l'article 11 de la Déclaration des droits de l'homme et du citoyen « *implique la liberté d'accéder à ces services* » (décision n° 2009-580

DC du 10 juin 2009, §12). La reconnaissance de l'accès à internet comme un droit fondamental oblige à garantir l'égalité de traitement des particuliers et des entreprises dans cet accès : c'est l'enjeu des débats sur la « neutralité du net », concept formulé pour la première fois en 2003 par le juriste américain Tim Wu. La neutralité du net implique que tous les opérateurs de communications traitent de manière égale tous les flux de données quel que soit leur contenu. Elle correspond à l'architecture originelle d'internet, qui repose sur le principe du « meilleur effort » (« *best effort* ») : chaque opérateur fait de son mieux pour assurer la transmission de tous les paquets de données qui transitent par son réseau, sans garantie de résultat et sans discrimination. Plusieurs facteurs techniques, économiques et politiques conduisent cependant les opérateurs à différencier le traitement des paquets selon leur contenu. Les débats sur la neutralité du net ont pour objet de déterminer si ce principe doit être inscrit dans le droit positif afin de restreindre ces possibilités de différenciation. Ils revêtent un caractère à la fois technique, économique et politique.

1.3. Le numérique a entraîné de profondes modifications du régime juridique de plusieurs libertés fondamentales

L'essor du numérique favorise à l'évidence l'exercice de certains droits, tout en remettant en question certains aspects de leur régime juridique : c'est le cas de la liberté d'expression (a) et de la liberté d'entreprendre (b). Pour d'autres droits, comme le droit à la sécurité (c) et le droit de propriété intellectuelle (d), le numérique se présente davantage comme un risque, auquel le législateur doit parer.

(a) Si la **liberté d'expression** est le principe fondamental commun à tous les moyens de communication, le régime juridique qui en définit les conditions d'exercice n'est pas le même selon le *medium* employé. Jusqu'à l'émergence d'internet, il y avait une parfaite superposition entre la forme d'expression (presse, communication téléphonique et communication audiovisuelle), le moyen technique employé et le régime juridique. Internet met en question ces distinctions, puisqu'il permet de diffuser par le même *medium* des contenus relevant de la correspondance privée, de la presse et de l'audiovisuel, phénomène souvent qualifié de « convergence ».
Le régime juridique de la liberté d'expression sur internet est relativement stable depuis la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN). En cohérence avec l'architecture d'internet, il encadre de manière distincte la couche des infrastructures et la couche des contenus. Dans ce dernier cas, la LCEN a défini deux grandes catégories d'acteurs : les éditeurs d'une part, soumis à un régime très voisin de celui de la presse, les hébergeurs d'autre par, dont le régime de responsabilité civile et pénale est atténué par rapport à celui des éditeurs, puisqu'ils sont regardés comme n'exerçant pas de contrôle sur les contenus accessibles par leur site.
Le régime de la communication sur internet, qu'il s'agisse de celui des éditeurs ou *a fortiori* de celui des hébergeurs, est ainsi marqué par un grand libéralisme qui le distingue du régime de la communication audiovisuelle, lequel institue une autorisation préalable assortie d'obligations diverses pour les fournisseurs de contenus. Le développement de la consommation audiovisuelle sur internet, notamment de films et de séries télévisées, conduit à de nouvelles interrogations sur cet écart, qui peut constituer une distorsion de concurrence et fragiliser la politique française de soutien à la création et à la production de contenus culturels.

Internet soulève aussi de nouvelles questions quant aux limites de la liberté d'expression et à la lutte contre les contenus illicites. Les textes constitutionnels et conventionnels qui garantissent la liberté d'expression reconnaissent tous la possibilité de lui imposer certaines limites et, par lui-même, internet ne remet en cause ni l'existence de ces limites ni leur tracé. Toutefois, les spécificités d'internet conduisent à s'interroger sur l'efficacité des mesures prises par les pouvoirs publics à l'encontre des contenus illicites et sur le rôle reconnu aux

acteurs privés dans la lutte contre ces contenus. Si l'intervention des intermédiaires de l'internet peut apparaître salutaire pour assurer une protection efficace d'intérêts publics tels que la lutte contre la xénophobie ou la protection des mineurs, elle suscite des débats sur sa légitimité.

(b) Les bouleversements économiques suscités par le numérique ont une incidence sur le droit des activités économiques. La **liberté d'entreprendre** implique désormais le droit à une existence numérique. La loi et la jurisprudence garantissent aujourd'hui ce que l'on pourrait qualifier de « droit à une existence numérique » de l'entreprise, qui comporte plusieurs éléments : droit à un nom de domaine, droit à fournir des services sur internet, droit d'utiliser certains instruments tels que la publicité, la cryptographie ou les contrats conclus par voie électronique.
Les mutations associées au numérique compliquent la mise en œuvre des deux formes d'encadrement de la liberté d'entreprendre, la régulation générale de la concurrence et les réglementations sectorielles applicables à certaines activités. On observe d'abord dans de nombreux secteurs de l'économie numérique une progressive concentration du marché autour d'un ou plusieurs acteurs prééminents, qui est favorisée par les rendements d'échelle croissants, les effets de réseau et le rôle central des plateformes. Ces acteurs dominants sont conduits à étendre constamment leur activité à de nouveaux services et à racheter les opérateurs émergents susceptibles de leur faire concurrence.
L'économie numérique bouscule aussi de nombreuses réglementations sectorielles car elle confronte les acteurs établis avec de nouveaux intervenants qui contestent l'applicabilité de la règle sectorielle ou dont le modèle d'affaires repose sur une logique différente. C'est notamment le cas dans le domaine des télécommunications, du livre, de l'hôtellerie, des taxis et de l'assistance aux justiciables.

(c) Le numérique permet ou favorise de nouveaux types d'atteintes à la sûreté et la sécurité, qui nécessitent des réponses juridiques. Il donne aussi à la police de nouveaux moyens qui appellent de nouvelles garanties pour préserver l'**équilibre entre sauvegarde de l'ordre public et liberté personnelle**.
Le numérique peut être la cible d'atteintes à la sécurité, ayant pour but d'accéder à des données confidentielles, de détruire ou d'altérer des données, d'entraver le bon fonctionnement du système ou d'utiliser des ressources informatiques à l'insu de leur détenteur. La loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique, dite « loi Godfrain », punit les faits d'accès frauduleux à un « *système de traitement automatisé de données* », d'entrave à leur fonctionnement ou encore de modification ou de suppression frauduleuse de données. L'État et les « opérateurs d'importance vitale » (OIV) n'échappent pas à la dépendance croissante de leur fonctionnement aux systèmes d'information. Pour faire face à ces attaques, ils ont complété les dispositifs existants de répression pénale en adaptant leurs moyens matériels (création en 2009 d'une agence spécialisée, l'Agence nationale de la sécurité des systèmes d'information (ANSSI)) et juridiques (pouvoir donné au Premier ministre par une loi de fixer des règles de sécurité des systèmes d'information qui s'imposent aux OIV). Le numérique peut aussi être utilisé pour porter atteinte à la sécurité : s'il n'est pas à l'origine de types de délinquance tels que la contrefaçon, l'escroquerie ou la pédophilie, il les facilite et en fait apparaître de nouvelles formes. En sens inverse, le numérique renforce l'efficacité tant de la police judiciaire que de la police administrative et du renseignement. Il renforce l'efficacité de leurs modes opératoires préexistants, tels que les fichiers, l'usage de données biométriques ou la vidéosurveillance. Il rend également possibles de nouveaux modes d'investigation, notamment par la surveillance des communications électroniques et le recours aux nouveaux modes d'exploitation des données associés au *Big Data*. Des garanties ont été instaurées par le législateur afin d'encadrer ces moyens nouveaux des services de police et de renseignement, notamment pour :
- la mise en œuvre des fichiers de sécurité, qui font l'objet d'un encadrement spécifique par la loi du 6 janvier 1978 modifiée ;

- la vidéosurveillance, soumise à un régime d'autorisation par la loi du 21 janvier 1995 ;
- l'interception des communications, la loi du 10 juillet 1991 ayant distingué les interceptions judiciaires des interceptions administratives de sécurité, et la loi du 23 janvier 2006 ayant complété ces régimes d'interception du contenu des communications par un régime de conservation et d'accès aux « métadonnées » (données sur les personnes participant à une communication, la durée de leur échange et leur localisation, également appelées données de connexion).

(d) Le **droit de la propriété intellectuelle** a été étendu à des objets issus des technologies numériques, les logiciels et les bases de données ; il joue ainsi dans l'économie numérique un rôle structurant. Prérogatives classiques du droit d'auteur, le droit de reproduction et le droit de représentation ont montré leur plasticité en s'appliquant à la numérisation et à la diffusion sur internet. Pour autant, internet fait largement abstraction du droit de propriété intellectuelle en facilitant de manière considérable la reproduction et la diffusion des œuvres en méconnaissance du droit d'auteur et des droits voisins.
Les pouvoirs publics ont réagi en combinant prévention (recours et protection juridique des « mesures techniques de protection » entravant la copie, notification des contenus illicites aux hébergeurs), répression (mise en place par les lois du 12 juin 2009 et du 28 octobre 2009 d'un dispositif de « réponse graduée ») et promotion des usages licites.

1.4. Internet n'échappe ni en fait, ni en droit à la puissance étatique, mais lui pose des défis inédits

Contrairement à ce qu'avaient espéré ses pionniers, internet n'est pas un espace hors du droit. Les deux postulats de cette approche libertaire, le défaut de légitimité des États à réglementer internet et leur incapacité à le faire, n'ont pas été vérifiés. **Les États ne sont pas moins légitimes à légiférer sur les réseaux numériques** que sur tout autre domaine d'activité humaine. La capacité des États à exercer leur pouvoir sur internet est désormais avérée. L'illustration la plus extrême en est donnée par les pratiques d'États non démocratiques, qui parviennent à entraver de manière significative l'accès de leurs ressortissants à internet. Les États de droit exercent également, dans des cadres définis par la loi et sous le contrôle du juge, un pouvoir de contrainte sur internet, par exemple lorsque des tribunaux ordonnent le retrait d'un nom de domaine ou le déréférencement d'un site.
Que la puissance de l'État parvienne à s'exercer sur internet ne signifie pas qu'elle n'y rencontre pas **des difficultés particulières**. Celles-ci tiennent notamment au mode de **gouvernance d'internet**, à la détermination de **la loi applicable** et à **l'effectivité** des interventions de l'État.

Alors que les précédentes innovations technologiques (télécommunications, aviation...) avaient suscité la création d'organisations intergouvernementales spécialisées, la gouvernance d'internet se distingue par l'absence d'autorité centrale et le rôle joué par plusieurs instances de droit privé, agissant notamment par la voie du droit souple et dans lesquelles la place des États- Unis est prépondérante : ICANN pour la gestion des noms de domaine, IETF et W3C pour la définition des standards techniques, *Internet Society* et Forum pour la gouvernance d'internet et pour le traitement des questions politiques, économiques et de société liées à internet. Dans ce modèle qualifié de « **multiacteurs** », les États ne sont que des parties prenantes parmi d'autres. En rendant accessibles aux internautes de chaque pays les contenus et les services proposés dans le monde entier, internet crée de très nombreux conflits entre les systèmes juridiques des différents États et les confronte ainsi à une double difficulté : d'une part, la complexité des règles de droit international privé, qui déterminent la loi applicable et la juridiction compétente, est source d'incertitudes ; d'autre part, ces règles peuvent désigner des juridictions et des lois étrangères. L'État est ainsi confronté à la possibilité que ses lois sur la protection des

données personnelles, la liberté d'expression ou la propriété intellectuelle ne soient en définitive pas applicables à toutes les situations qu'il entend régir. Internet pose enfin trois problèmes spécifiques pouvant amoindrir l'effectivité des interventions de l'État : la facilité de recréation d'un site internet ayant été convaincu d'activité illicite ; la nécessité d'obtenir l'exécution de décisions administratives ou juridictionnelles par des États étrangers ; le décalage entre la vitesse d'évolution de l'univers numérique et le temps des processus institutionnels et juridictionnels.

De ces multiples évolutions du droit du numérique se dégagent deux tendances qui déterminent la manière dont la protection des droits fondamentaux doit aujourd'hui être repensée : le numérique ouvre de nouveaux espaces aux libertés, notamment en matière d'expression, d'association, de sociabilité ; il est aussi un enjeu stratégique suscitant une vive compétition entre États et entre acteurs économiques.

2. – L'ambivalence du numérique nécessite de repenser la protection des droits fondamentaux

Face à l'explosion numérique, le droit s'est déjà beaucoup transformé. Il n'est pourtant pas parvenu à un point d'équilibre. Les interrogations sur la pertinence du régime juridique des droits fondamentaux se succèdent au même rythme que celui des innovations dont le numérique est porteur. La difficulté d'y répondre tient à **l'ambivalence intrinsèque** du phénomène numérique : il ouvre de nouveaux espaces de libertés, tout en étant porteur de risques pour celles-ci. Une intervention trop rigoureuse du législateur destinée à **prévenir les aspects négatifs** du numérique **risque**, du même mouvement, **d'en entraver le potentiel positif**. Pour surmonter cette difficulté, il faut repenser les modes de protection des droits fondamentaux pour les adapter à l'explosion des données, au rôle inédit des grandes « plateformes » et au caractère transnational d'internet.

2.1. L'explosion des usages des données personnelles et des risques associés conduit à en repenser la protection

• *Les risques liés à l'explosion des données personnelles*

Depuis l'adoption de la loi du 6 janvier 1978, les sources et les types de données personnelles en circulation se sont considérablement diversifiées. Les données ne sont plus seulement collectées par des entités organisées (administrations, entreprises, associations), mais aussi mises en ligne par les individus euxmêmes ou par des tiers ou recueillies de manière automatique. Elles ne correspondent plus seulement aux caractéristiques objectives de l'individu (âge, sexe, profession...) ; il peut s'agir d'informations sur ses goûts, ses opinions, ses relations, ses déplacements ou encore de signaux biologiques ou corporels.
Si toutes ces informations restaient disséminées auprès des personnes qui les ont recueillies, les risques pour la vie privée seraient sans doute limités. La dynamique de l'économie numérique pousse cependant à leur regroupement. Le numérique a suscité l'émergence d'acteurs nouveaux, tels les moteurs de recherche ou les réseaux sociaux, qui sont dépositaires, par leur fonction, de pans entiers de notre vie personnelle. La publicité joue en la matière un rôle particulier : plus le nombre d'informations détenues sur **le « profil»** d'une personne est grand, plus les publicités qui lui sont adressées seront potentiellement pertinentes. Les grandes entreprises du numérique sont engagées dans des stratégies de

diversification dont l'un des objectifs est de multiplier les données détenues sur chaque individu. Il existe aussi des acteurs spécialisés dans la collecte et la revente des données, les ***data brokers*** ; le plus important d'entre eux affirme détenir des données sur 700 millions de personnes dans l'ensemble du monde.
Cette diffusion généralisée des données personnelles et la tendance des acteurs économiques à les regrouper sont porteuses de **risques** pour les individus, que l'étude classe en **six catégories** : la diffusion de données personnelles en dehors de la volonté de l'individu concerné ; la réception de plus en plus fréquente de publicités de plus en plus ciblées et personnalisées ; le développement de pratiques commerciales abusives, consistant en une différenciation entre les clients à partir de l'exploitation de leurs données ; les risques de réputation, pouvant conduire à des restrictions dans l'accès à l'assurance, au crédit, à l'emploi ; les utilisations malveillantes, portant directement atteinte aux biens ou aux personnes ; l'utilisation des données personnelles par les pouvoirs publics à des fins de sauvegarde de l'ordre public et de la sécurité nationale, lorsqu'elle est excessive.

• *Un cadre juridique dont les principes fondamentaux demeurent pertinents, mais dont les instruments doivent être profondément transformés*

Les nouveaux risques liés au numérique suscitent des interrogations sur la pertinence du cadre juridique actuel de la protection des données personnelles.
Les principes fondamentaux de la protection des données résistent cependant à ces interrogations :
- **Une définition large des données à caractère personnel** (couvrant notamment l'adresse IP et les « profils » utilisés en matière de publicité en ligne), telle que la préconise le G29, est nécessaire pour assurer la protection des personnes et c'est bien celle que retient la jurisprudence française.
- **Le principe de finalités déterminées** est au cœur de la confiance que les personnes peuvent avoir dans les services de la société numérique. C'est grâce à ce principe que les données personnelles ne sont pas des marchandises comme les autres : elles peuvent être échangées, mais le droit de propriété de leur acquéreur reste limité par les droits de la personne sur ses données, qui impliquent que leur utilisation soit limitée aux finalités pour lesquelles elles ont été initialement collectées.
- **Les principes de proportionnalité et de limitation de la durée** de conservation découlent de ce premier principe.
- Quant aux principes de loyauté de la collecte et d'exactitude des données traitées, ils ne sont que l'expression des principes généraux de la responsabilité.
- **Le rôle du consentement** de la personne ne doit être ni surestimé (dans la législation actuelle, il n'est ni une condition nécessaire ni une condition suffisante de la licéité du traitement des données), ni méconnu, car il incarne la liberté de la personne en matière d'utilisation de ses données personnelles.
Ces principes ne sont **pas une entrave au développement du *Big Data***. En effet, nombre des usages du *Big Data* ne visent pas les personnes en tant que telles, mais **l'exploitation statistique** des données les concernant. Or le principe de finalités déterminées n'exclut pas la liberté de réutilisation statistique : dans le cadre juridique actuel, la finalité statistique est toujours présumée compatible avec la finalité initiale du traitement. Lorsque les usages du *Big Data* visent les personnes en tant que telles, par exemple pour établir un profil prédictif de leurs caractéristiques (solvabilité, dangerosité...), la pleine application des principes fondamentaux de la protection des données est en revanche requise.

Si les principes conservent leur pertinence, **les instruments de la protection des données doivent être adaptés et renouvelés**. Quatre voies complémentaires devraient être explorées : l'utilisation des technologies pour renforcer la capacité des personnes à contrôler l'utilisation de leurs données ; la définition d'une « chaîne de responsabilités », allant des concepteurs de logiciels et d'objets connectés aux utilisateurs finaux et complétant la

responsabilité du responsable de traitement ; une attention particulière portée à la circulation des données personnelles ; le passage d'une logique formelle de déclaration à une logique de respect en continu de la réglementation, assuré par des contrôles internes et externes.

Les évolutions en cours du droit de l'Union européenne s'engagent à juste titre dans la voie de la réaffirmation des principes et de la rénovation des instruments.
En premier lieu, l'arrêt *Google Spain c/ AEPD* de la Cour de justice de l'Union européenne, en date du 13 mai 2014, **qualifie les moteurs de recherche de responsables de traitement des données personnelles** qu'ils collectent lorsqu'ils sont saisis de requêtes concernant un individu. Il en déduit l'existence d'**un droit au déréférencement**, fondé sur le droit d'opposition de la personne au traitement de ses données personnelles et sur le droit à l'effacement des données dont le traitement n'est pas conforme à la directive n° 95/46/CE. En se fondant sur les principes de la directive de 1995, la CJUE a donc créé un nouvel instrument adapté au problème de « l'e-réputation » de la société numérique contemporaine, dont la mise en oeuvre devra toutefois veiller à une conciliation équilibrée avec la liberté d'expression (cf. *infra* **proposition n° 5**).
En second lieu, la Commission a adopté le 25 janvier 2012 **une proposition de règlement** relative aux données à caractère personnel, appelée à se substituer à la directive n° 95/46/CE. L'adoption de ce règlement par le Parlement européen et le Conseil permettrait de mettre en place un corps de règles uniques dans l'ensemble de l'Union européenne et de **placer ainsi la protection à un échelon continental** plus adapté au caractère transnational d'internet. Le règlement rénove nombre d'instruments, notamment en supprimant l'obligation de déclaration des traitements qui revêtait un caractère trop formaliste, en rendant obligatoire la désignation de « délégués à la protection des données » par les responsables de traitement, en introduisant le concept de protection de la vie privée dès la conception (« *privacy by design* ») et en instaurant des sanctions administratives dissuasives. Si ces évolutions sont bienvenues, d'autres innovations peuvent être encouragées, notamment les technologies de renforcement de la vie privée ou le développement de la certification et de la corégulation.

• *La surveillance des communications par les pouvoirs publics présente des enjeux spécifiques et appelle des réponses adaptées*

Les principes de la surveillance des communications par les pouvoirs publics ont été fixés par la loi du 10 juillet 1991. Celle-ci a réaffirmé le secret des communications et n'a permis d'y porter atteinte que dans deux hypothèses, sur décision de l'autorité judiciaire ou, « à titre exceptionnel » et pour des finalités définies par la loi, sur décision du Premier ministre et sous le contrôle de la Commission nationale de contrôle des interceptions de sécurité (CNCIS). Depuis lors cependant, les pratiques de surveillance des communications par les pouvoirs publics et leur contexte ont profondément évolué, suscitant d'importants débats sur leur place et les garanties qui doivent les entourer.
L'essor des communications électroniques et des capacités de stockage et d'analyse des données a démultiplié les possibilités d'interception. Les deux derniers livres blancs sur la défense ont fait de la collecte de renseignements par cette voie l'une des priorités de la politique de sécurité nationale de la France, qui s'est traduite par une forte augmentation des moyens matériels des services.

Pus récemment, l'arrêt *Digital Rights Ireland* du 8 avril 2014 de la CJUE a remis en cause le cadre européen de la conservation des données et les révélations de ce qu'il est convenu d'appeler « l'affaire Prism » ont, partout dans le monde, porté ces sujets au premier plan du débat public. Alors que depuis la loi du 10 juillet 1991, le législateur a procédé en la matière par extensions successives du champ de la collecte de renseignement, il apparaît nécessaire aujourd'hui de procéder à un réexamen global du cadre juridique de la surveillance des communications, dans le but de **préserver la capacité de notre pays à**

protéger sa sécurité nationale tout en apportant l'ensemble des garanties nécessaires à la protection des droits fondamentaux, et notamment de la sûreté.

Par son arrêt *Digital Rights Ireland*, la CJUE a déclaré invalide la directive n° 2006/24/CE du 15 mars 2006, qui prévoyait que les États devaient imposer aux opérateurs de communications de conserver pendant une durée comprise entre six mois et deux ans l'ensemble des données de connexion de leurs utilisateurs, en vue de garantir la disponibilité de ces données à des fins de recherche, de détection et de poursuite d'infractions graves. Elle a jugé que cette obligation générale de conservation constituait une ingérence particulièrement grave dans les droits à la vie privée et à la protection des données personnelles garantis par les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne ; si elle admet que cette ingérence est justifiée par des buts d'intérêt général tels que la lutte contre le terrorisme et la criminalité organisée, elle considère qu'elle n'est pas proportionnée, dès lors que la directive couvre les données de toute personne, ne prévoit aucune garantie concernant l'accès aux données conservées et fixe la durée de conservation sans tenir compte de l'utilité de la conservation par rapport aux objectifs poursuivis. L'arrêt de la CJUE soulève la question de la conformité au droit de l'Union européenne des législations nationales, telles que la législation française, qui prévoient une telle obligation de conservation générale des données de connexion.
Compte tenu des enjeux de la surveillance des communications pour la protection de la sécurité nationale, l'étude du Conseil d'État ne propose pas de supprimer cette obligation mais préconise de renforcer les garanties concernant l'accès et l'utilisation de ces données.

2.2. Promouvoir les libertés à l'ère des « plateformes »

Le numérique favorise à l'évidence l'exercice de la liberté d'expression, de la liberté d'entreprendre et de la liberté d'association. Cependant il favorise aussi les comportements illicites, tels que les abus de la liberté d'expression et la contrefaçon. Par ailleurs, les situations d'inégalité de puissance et d'allocation de ressources rares peuvent justifier, comme dans d'autres domaines de la vie économique et sociale, l'intervention des pouvoirs publics pour promouvoir la plus grande liberté possible pour chacun.

• *Neutralité des réseaux, loyauté des plateformes et lutte contre les contenus illicites*

L'étude du Conseil d'État propose de **consacrer dans le droit positif** le principe de **neutralité du *net***, car il constitue une garantie fondamentale des libertés énumérées ci-dessus, en permettant à toute entreprise, toute association ou tout particulier de bénéficier d'un égal accès à tous les internautes. Les menaces qui pèsent aujourd'hui sur le respect de ce principe sont en outre plus consistantes qu'aux débuts d'internet, en raison de la position dominante de certains fournisseurs de contenus et de la part du trafic représentée par quelques grands sites de diffusion de vidéos. Il importe cependant, dans le cadre de la proposition de règlement de l'Union européenne (« quatrième paquet télécoms »), de prévoir une définition suffisamment large des « services spécialisés », dans le cadre desquels les opérateurs peuvent proposer un niveau de qualité garanti et supérieur à celui de l'internet généraliste. Le développement de ces services spécialisés est en effet nécessaire pour proposer des usages innovants tels que, par exemple, la télémédecine. En contrepartie de cette définition large, les autorités de régulation des communications électroniques devraient disposer de prérogatives suffisantes pour empêcher les services spécialisés de nuire à la qualité de l'internet généraliste.

Les opérateurs de communications électroniques ne sont pas les seuls acteurs à jouer un rôle déterminant dans l'exercice des libertés sur internet : la situation des « **plateformes** » doit également être traitée. Cette expression désigne usuellement les sites qui permettent à

des tiers de proposer des contenus, des services ou des biens ou qui donnent accès à de tels contenus : magasins d'applications, sites de partage de contenus, places de marché, moteurs de recherche... Le rôle d'intermédiation confère aux plateformes un pouvoir, à la fois économique et de prescription, qui a une forte incidence sur l'exercice par les tiers de leurs libertés et pose aux pouvoirs publics des questions inédites.

L'étude du Conseil d'État relève d'abord que la *summa divisio* prévue par l'article 6 de la LCEN, qui transpose la directive « commerce électronique » de 2000, entre les intermédiaires techniques, dont la responsabilité civile et pénale est limitée, et les éditeurs de site, n'est plus adaptée face au rôle croissant des plateformes. En effet, nombre de plateformes ne se contentent pas de stocker passivement les offres des sociétés tierces ou les contenus mis en ligne, elles les organisent en les indexant et en faisant, le cas échéant, des recommandations personnalisées aux internautes. Plusieurs arrêts de la CJUE et de la Cour de cassation ont montré qu'une place de marché ou un moteur de recherche ne répondaient pas à la condition de rôle purement technique et passif prévue par la directive de 2000 pour bénéficier de la qualité d'hébergeur et du régime de responsabilité limitée qui lui est associé. La responsabilité limitée joue pourtant un rôle essentiel dans l'exercice des libertés sur internet, en évitant aux plateformes de procéder à une censure préventive des contenus mis en ligne pour ne pas voir leur responsabilité engagée. Il apparaît donc nécessaire de créer **une nouvelle catégorie juridique, celle des plateformes**, dont la définition ne reposerait plus sur le caractère technique et passif de leur rôle, mais sur le fait qu'**elles proposent des services de classement ou de référencement de contenus, biens ou services mis en ligne par des tiers**.

Les plateformes ne peuvent être soumises à la même obligation de neutralité que les opérateurs de communications électroniques, car leur rôle est de fournir un accès organisé, hiérarchisé ou personnalisé aux contenus mis à disposition sur leur site ou auxquels elles donnent accès : un traitement égalitaire ne peut être demandé à un moteur de recherche, puisque l'objet même d'un moteur de recherche est de hiérarchiser les sites internet. En revanche, **les plateformes devraient être soumises à une obligation de loyauté envers leurs utilisateurs**, tant les utilisateurs non professionnels **dans le cadre du droit de la consommation** que les utilisateurs professionnels dans le cadre **du droit de la concurrence**. Parce qu'elles jouent un rôle de porte d'entrée pour la diffusion ou pour l'accès, aux contenus sur internet, les plateformes sont impliquées dans les débats concernant la lutte contre les contenus illicites. Outre leurs obligations légales lorsqu'elles sont saisies de signalements de tels contenus, elles mettent aussi en place des **démarches volontaires dans le cadre de « politiques » relatives aux contenus** qu'elles acceptent ou d'outils de détection des contrefaçons qu'elles mettent à la disposition des ayants droit. Ce rôle est l'objet de controverses, certains acteurs le qualifiant de « police privée ». Le Conseil d'État considère qu'il ne serait pas réaliste de dénier aux acteurs privés le droit de décider du retrait d'un contenu et de réserver ce droit au juge. En revanche, il importe de mieux garantir les droits des personnes faisant l'objet d'une mesure de retrait, qui ne disposent souvent pas de possibilités de faire valoir leurs observations. En outre, le pouvoir de fait considérable associé à la définition des « politiques » relatives aux contenus devrait s'exercer dans des conditions plus grandes de transparence et de concertation avec les parties prenantes.

• *La nécessité de doter la régulation audiovisuelle d'instruments adaptés à l'environnement numérique*

Deux des fondements théoriques de la régulation audiovisuelle, l'occupation du domaine public et la nécessité de réglementer des programmes « linéaires », ne peuvent être transposés aux services audiovisuels accessibles par internet. Le premier est tiré des règles générales de la domanialité publique qui permettent à la personne publique d'imposer des obligations d'intérêt général aux occupants et ne peuvent s'appliquer aux services

audiovisuels diffusés par internet, lesquels ne passent pas par l'utilisation privative du domaine public hertzien. Le second fondement tient à ce qu'il est convenu d'appeler le caractère « linéaire » des services audiovisuels classiques. Sur internet, l'utilisateur peut passer comme il le souhaite d'un site à un autre et dispose donc d'une plus grande liberté de choix. En revanche, un troisième fondement théorique est aussi pertinent sur internet que sur les moyens de communication audiovisuels classiques : celui des objectifs de valeur constitutionnelle que sont la sauvegarde de l'ordre public, le respect de la liberté d'autrui et la préservation du caractère pluraliste des courants d'expression socioculturels, ainsi que de l'intérêt général qui s'attache à la promotion de la diversité culturelle.
Afin de ne pas porter atteinte à la neutralité du net, l'étude propose de ne pas imposer aux opérateurs de communications de procéder à une différenciation entre des contenus licites dans le cadre de l'internet généraliste. En revanche, de telles obligations sont envisageables dans le cadre de la distribution de services spécialisés.

• *Prendre la mesure du rôle joué par les algorithmes et concevoir l'encadrement de leur utilisation*

L'algorithme est au cœur du rôle d'intermédiation joué par les plateformes. L'usage des algorithmes n'est cependant pas réservé aux plateformes et le développement du *Big Data* conduit à les appliquer dans de très nombreux domaines. L'utilité des algorithmes pour optimiser le fonctionnement d'un certain nombre de services n'est pas discutable. Ils présentent cependant trois sources de risques pour l'exercice des libertés : l'enfermement de l'internaute dans une « personnalisation » dont il n'est pas maître ; la confiance abusive dans les résultats d'algorithmes perçus comme objectifs et infaillibles ; de nouveaux problèmes d'équité du fait de l'exploitation toujours plus fine des données personnelles.
L'encadrement de l'utilisation des algorithmes est un domaine nouveau pour les pouvoirs publics, mais devenu nécessaire en raison du rôle grandissant de ces mécanismes et des risques qu'ils présentent pour l'exercice des libertés. L'étude du Conseil d'État préconise trois méthodes d'encadrement : assurer l'effectivité de l'intervention humaine dans la prise de décision au moyen d'algorithmes ; mettre en place des garanties de procédure et de transparence lorsque les algorithmes sont utilisés pour prendre des décisions à l'égard d'une personne ; développer le contrôle des résultats produits par les algorithmes, notamment pour détecter l'existence de discriminations Illicites.

2.3. Rendre applicable un socle de règles impératives pour tous les acteurs du numérique, quel que soit leur lieu d'établissement

La question du droit territorialement applicable sur internet constitue un enjeu de simplification et d'accessibilité du droit, mais également un enjeu stratégique, car elle met en cause la capacité des États à assurer la protection des libertés fondamentales de leurs citoyens ainsi que le droit au recours de ceux-ci. Les implications pour la concurrence entre entreprises numériques sont significatives.

• *Définir un socle de règles impératives applicables à tous les acteurs quel que soit leur lieu d'établissement*

La plupart des grandes entreprises du *net* étant établies aux États-Unis, la grande masse **des particuliers et des entreprises européennes se voient opposer la compétence juridictionnelle et la législation des différents États américains**, prévues par les conditions générales d'utilisation de ces services.

Il serait cependant hâtif d'en déduire que les États européens ont intérêt à réclamer l'application systématique à leurs internautes de leurs règles de droit, quel que soit le pays d'origine du site internet. Il est en effet difficilement envisageable que le principe du pays de l'internaute devienne une règle générale et absolue de détermination de la loi applicable sur internet, car il ne peut être raisonnablement demandé à un site de se conformer à toutes les règles de droit de tous les pays du monde, ne serait-ce que parce qu'elles sont sur bien des points contradictoires entre elles, et que se conformer à certaines d'entre elles pourrait le mettre en infraction avec les règles de son propre État. Une telle orientation postulerait en outre que les acteurs français ou européens sont toujours voués à être sur internet en tant que consommateurs et non en tant que producteurs de services. Le Conseil d'État préconise donc de **promouvoir le principe du pays de destination, non pour l'ensemble des règles juridiques applicables aux acteurs d'internet, mais pour un socle de règles** choisies en raison de leur importance particulière dans la protection des droits fondamentaux ou de l'ordre public.
Les règles du socle seraient applicables à tous les sites dirigeant leur activité vers la France ou l'Union européenne (selon que la règle est de niveau national ou européen), la notion d'activité dirigée vers un pays ayant le sens qui lui a été donné par la jurisprudence.

Selon les sujets, trois méthodes peuvent faire prévaloir le principe du pays de destination :
- l'application des règles de droit commun du droit international privé, qui permet notamment d'aboutir au résultat recherché en matière pénale ;
- **la qualification de « loi de police »** au sens du droit international privé, qui devrait être retenue **en matière de protection des données personnelles** et **d'obligations de coopération des acteurs privés** avec les autorités judiciaires et administratives agissant **à des fins de sécurité nationale** ;
- la coordination des législations nationales par un traité ou un acte de droit dérivé de l'Union européenne, qui pourrait être envisagée pour faire prévaloir le principe du pays de destination en matière d'audiovisuel.

• *Assurer une coopération efficace dans l'application, au sein de l'Union européenne et avec les autres systèmes juridiques*

Il revient aux États ou à l'Union européenne de fixer le champ d'application de leurs règles de droit. L'exécution de ces règles par des acteurs issus d'autres États implique en revanche une bonne coopération avec ces derniers. Trois types de relations sont abordés par l'étude : les relations entre États de l'Union européenne, dans la perspective de l'entrée en vigueur de la proposition de règlement relatif à la protection des données personnelles ; les relations entre l'Union européenne et les États-Unis ; les relations avec les autres systèmes juridiques. **Au sein de l'Union européenne**, la désignation d'une **« autorité chef de file »** pour les responsables de traitement établis dans plusieurs États membres est nécessaire pour assurer l'efficacité de la régulation. Elle doit **cependant s'accompagner de mécanismes efficaces de coordination entre autorités** afin de prévenir les risques de « *forum shopping* » ainsi que de garanties du droit au recours des particuliers.
S'agissant des relations **avec les États-Unis**, le mécanisme du « ***Safe Harbour*** » devrait **être profondément réformé**. Sa renégociation avec le gouvernement américain doit porter sur deux questions : le passage d'une logique de déclaration d'engagements et d'autocertification à une logique de réglementation contraignante pour les entreprises adhérentes, assortie d'une intensification des contrôles par les autorités ; l'évolution du contenu des obligations contenues dans le *Safe Harbour*, les obligations actuelles étant souvent floues et éloignées du niveau de protection garanti en Europe.

S'agissant des relations **avec les autres systèmes juridiques**, la **convergence sur les valeurs** avec certains États, comme le Brésil et la Corée du sud, **permet d'envisager une politique plus ambitieuse** de reconnaissance mutuelle et d'actions conjointes de contrôle. La coopération en matière de lutte contre la cybercriminalité devrait être intensifiée, par exemple par la mise en place d'un groupe d'action interétatique qui définirait des recommandations détaillées sur les pratiques de coopération à mettre en place et qui publierait des listes d'États non coopératifs.

3. – Mettre le numérique au service des droits individuels et de l'intérêt général

Aujourd'hui, les droits reconnus aux individus se limitent, pour l'essentiel, à leur permettre de rester à l'écart du traitement de leurs données (choix qui n'est presque jamais fait), sans leur donner de réel pouvoir sur le contenu du service et la manière dont leurs données sont traitées. Mettre le numérique au service des droits individuels, tel devrait être le premier principe directeur de la protection des droits fondamentaux dans les usages numériques. Par cette logique d'« *empowerment* », « d'autonomisation » des individus, l'intervention publique peut accroître la capacité des individus à agir pour la défense de leurs droits et à amplifier ainsi les possibilités d'action des pouvoirs publics eux-mêmes. Face à des acteurs du numérique dont le succès passe par leur relation privilégiée avec leurs utilisateurs, les pouvoirs publics doivent eux aussi savoir « s'allier avec la multitude ».

Le second principe directeur des propositions formulées dans cette troisième partie tend à mettre le numérique au service de l'intérêt général. Le numérique peut bénéficier de manière considérable à l'efficacité des politiques de santé, d'éducation, de culture, de sécurité ou de lutte contre la fraude, ainsi qu'à la simplification des démarches administratives ; encore faut-il que les personnes publiques disposent de cadres et d'instruments juridiques appropriés pour saisir ces opportunités, tout en assurant le respect des droits individuels. Il s'agit pour elles de concilier des droits fondamentaux entre eux ou des libertés avec des objectifs de valeur constitutionnelle : ainsi la sûreté à laquelle concourent la prévention et la répression des infractions les plus graves. Même s'il reste un espace d'action autonome pour le droit interne, soit par la norme législative ou réglementaire, soit par le droit souple, nombre des propositions de cette étude relèvent de la compétence des institutions de l'Union européenne, soit parce qu'elles nécessitent une modification du droit de l'Union existant, soit parce que l'Union européenne constitue le niveau pertinent d'action.

3.1. Définir les principes fondant la protection des droits fondamentaux à l'ère du numérique

Il est parfois proposé de reconnaître aux individus un véritable droit de propriété sur leurs données, en pariant sur leur plus grande implication du fait qu'ils deviendraient financièrement intéressés à une bonne gestion de leurs données. Le Conseil d'État ne recommande pas une telle orientation. S'il préconise de renforcer la dimension de l'individu acteur dans le droit à la protection des données, c'est en envisageant celui-ci comme un **droit à l'autodétermination** plutôt que comme un droit de propriété (**proposition n° 1**). La reconnaissance du droit de propriété ne permettrait pas en effet de rééquilibrer la relation entre les individus et les acteurs économiques et compliquerait l'exercice de la régulation par les pouvoirs publics. Le droit à « l'autodétermination informationnelle », concept dégagé par

la Cour constitutionnelle allemande en 1983, est à la différence du droit de propriété un droit attaché à la personne, tendant à « garantir en principe la capacité de l'individu à décider de la communication et de l'utilisation de ses données à caractère personnel ». Ce droit ne devrait pas être défini comme un droit supplémentaire s'ajoutant aux autres droits (droit d'information, droit d'accès...), mais comme un principe donnant sens à tous ces droits, ceux-ci tendant à le garantir et devant être interprétés et mis en œuvre à la lumière de cette finalité.

Le principe de **neutralité des opérateurs de communications** électroniques doit être inscrit dans le droit positif, en prévoyant une définition large des services spécialisés assortie de pouvoirs importants des autorités de régulation pour veiller au maintien de la qualité générale d'internet (**proposition n° 2**). Les plateformes, qui constitueraient une nouvelle catégorie juridique, seraient quant à elles soumises à une obligation de loyauté, consistant à assurer de bonne foi le service de classement ou de référencement, sans chercher à l'altérer ou à le détourner à des fins étrangères à l'intérêt des utilisateurs (**proposition n° 3**).

3.2. Renforcer les pouvoirs des individus et de leurs groupements

Le renforcement des capacités d'action des individus doit intervenir à deux niveaux, individuel et collectif.
Au niveau individuel, l'étude du Conseil d'État préconise :
- de donner à la **CNIL** et à l'ensemble des autorités de protection des données européennes une mission explicite de **promotion des technologies** renforçant la **maîtrise des personnes** sur l'utilisation de leurs données (**proposition n° 4**) ;
- de mettre en œuvre de manière efficace le **droit au déréférencement** reconnu par la CJUE dans son arrêt *Google Spain,* notamment en donnant aux éditeurs des sites dont le déréférencement est demandé la possibilité de faire valoir leurs observations et en explicitant par des lignes directrices des autorités de protection des données leur doctrine de mise en œuvre de l'arrêt (**proposition n° 5**) ;
- de **définir les obligations des plateformes envers leurs utilisateurs** qui découlent du principe de loyauté : notamment, pertinence des critères de classement et de référencement mis en œuvre par la plateforme au regard de l'objectif de meilleur service rendu à l'utilisateur, définition des critères de retrait de contenus licites en termes clairs, accessibles à tous et non discriminatoires (**proposition n° 6**) ;
- d'organiser un **droit d'alerte** en matière de protection des données personnelles, sur le fondement du droit d'alerte « généraliste » reconnu par la loi du 6 décembre 2013 pour tout crime ou délit (**proposition n° 7**).

Les propositions portant sur les actions collectives sont les suivantes :
- création d'une **action collective** en matière de protection des données personnelles, permettant à certaines personnes morales agréées d'obtenir du juge une injonction de faire cesser des violations de la législation (**proposition n° 8**) ;
- mise en ***Open Data*** par la CNIL de toutes les **déclarations et autorisations** de traitements de données (**proposition n° 9**) ;
- développement de la **participation des utilisateurs** des plateformes **à l'élaboration des règles** définissant les contenus pouvant être mis en ligne sur leur site (**proposition n° 10**) ;
- attribution à la CNIL ou au Conseil national du numérique une mission permanente d'animation de la délibération collective sur les **enjeux éthiques** liés au numérique (**proposition n° 11**).

3.3. Redéfinir les instruments de la protection des droits fondamentaux et repenser le rôle des autorités publiques

• *En matière de protection des données personnelles*

Le cadre juridique de la protection des données personnelles a été défini alors que la circulation des données et leur valeur économique restaient limitées. L'intervention publique doit aujourd'hui assurer d'une part, la sécurisation juridique des usages des données, car c'est un facteur de développement de l'économie numérique, et d'autre part, un encadrement plus étroit des traitements présentant les risques les plus importants.
Afin de sécuriser juridiquement les usages présentant des risques limités pour les droits fondamentaux, les actions suivantes sont préconisées :
- maintenir sans ambiguïté dans la proposition de règlement européen la **liberté de réutilisation statistique des données personnelles**, quelle que soit la finalité initiale de leur traitement, en prévoyant pour seule condition que cette réutilisation soit entourée de garanties d'anonymat appropriées (**proposition n° 12**) ;
- renforcer le rôle de **conseil et d'accompagnement des responsables de traitement** par la CNIL et créer auprès d'elle une procédure de « rescrit données personnelles » (**propositions n° 13 et 14**) ;
- développer la corégulation avec les acteurs professionnels, en prévoyant une procédure d'homologation des codes de conduite, le respect d'un code homologué devant être l'un des critères retenus par l'autorité de contrôle pour ses décisions d'autorisation ou de sanction (**propositions n° 16, 17 et 18**).

Afin de proportionner l'encadrement au degré de risque du traitement, il convient de :
- créer pour les catégories de traitements présentant **les risques les plus importants** une **obligation de certification** périodique (complétant l'examen *a priori* par l'autorité de contrôle dans le cadre de la procédure de consultation préalable) par un organisme tiers indépendant et accrédité par l'autorité de contrôle (**proposition n° 19**) ;
- porter une attention particulière aux **transmissions de données personnelles d'une entité à une autre**, notamment en **codifiant dans la loi la jurisprudence** relative à la nullité des transactions portant sur des fichiers non autorisés ou non déclarés à la CNIL (**proposition n° 20**).
Le régime juridique des numéros d'identification devrait être revu, en mettant à l'étude la création d'un numéro national non signifiant (**proposition n° 21**) et dans l'immédiat, en élargissant les possibilités de recours au NIR dans le domaine de la santé et pour les autres usages (**proposition n° 22**).

Enfin, la protection des droits fondamentaux nécessite la mise en place d'outils de régulation de l'utilisation des algorithmes, notamment par l'exigence d'effectivité de **l'intervention humaine** dans le traitement des données (**proposition n° 23**) ou par l'observation de leurs résultats, notamment pour détecter des discriminations illicites, en renforçant à cette fin les moyens humains dont dispose la CNIL (**proposition n° 25**).

• *En matière de liberté d'expression*

Il conviendrait de prévoir une obligation pour les hébergeurs et les plateformes d'empêcher, durant un délai déterminé, la réapparition des contenus ayant fait précédemment l'objet de retrait ; cette obligation serait prononcée par l'autorité administrative (**proposition n° 28**).
L'existence de modalités spécifiques de contrôle des concentrations, qui complètent le contrôle général opéré par l'Autorité de la concurrence, est une garantie importante du pluralisme des médias. Cependant, en raison de la surabondance des contenus, les principales menaces pesant sur le libre choix des destinataires ne tiennent plus seulement à

une concentration excessive, mais aussi à la fragilisation du modèle économique de la presse, alors que celle-ci demeure une source essentielle d'information de qualité. Il conviendrait de **revoir le contrôle de la concentration** dans les médias, et notamment les quotas et la mesure des bassins d'audience utilisés pour la limiter, propre à mieux garantir le pluralisme en tenant compte de la multiplicité des supports d'information (**proposition n° 30**).

• *Par le développement de la médiation*

Nombre de litiges liés à l'utilisation des technologies numériques, qu'ils portent sur les données personnelles, les atteintes à la réputation sur internet ou le retrait de contenus mis en ligne, peuvent être qualifiés de « petits litiges » : leurs enjeux sont parfois significatifs pour les personnes concernées, mais les intérêts pécuniaires en cause sont le plus souvent limités. Les procédures juridictionnelles classiques sont peu adaptées au traitement de ces petits litiges, ce qui conduit nombre de personnes à renoncer à faire valoir leurs droits ; la médiation serait dans bien des cas plus adaptée (**proposition n° 31**).

3.4. Assurer le respect des droits fondamentaux dans l'utilisation du numérique par les personnes publiques

• *En matière d'ouverture des données publiques*

L'ouverture des données publiques, ou « *Open Data* », fait l'objet depuis 2011 d'une politique volontariste du gouvernement. Ce volontarisme politique, qui se traduit par l'affichage d'un principe d'ouverture par défaut aujourd'hui inscrit dans un instrument de droit souple, contraste avec la faiblesse des obligations prévues par le droit dur. L'inscription dans la loi d'une obligation de mise en ligne progressive de l'ensemble des bases de données détenues par l'administration présenterait plusieurs avantages, notamment celui d'étendre la politique d'*Open Data* aux collectivités territoriales, dont l'action en la matière est aujourd'hui inégale. Toutefois, la voie du droit souple apparaît plus appropriée pour promouvoir le développement de l'***Open Data***, notamment auprès de ces dernières. Une **charte d'engagements et de bonnes pratiques** pourrait donc être élaborée par l'État, les associations de **collectivités territoriales** et les représentants des utilisateurs des données, qui engagerait chaque organisme public adhérent à définir un programme d'ouverture de ses données publiques, à respecter des standards de qualité et à veiller à limiter les risques de réidentification (**proposition n° 32**). Ces risques seraient circonscrits par la définition de **bonnes pratiques d'anonymisation** et par la constitution au sein de chaque ministère un pôle d'expertise en matière d'anonymisation, *a priori* au sein du service statistique ministériel (**proposition n° 33**).

• *En matière de fichiers de police judiciaire*

Les fichiers de police judiciaire ont connu au cours des quinze dernières années une forte expansion liée notamment à l'allongement de la liste des infractions donnant lieu à enregistrement. Sans remettre en cause leur utilité pour les services de police, il apparaît souhaitable de renforcer les garanties entourant leur utilisation et de corriger certaines fragilités juridiques :
- Pour le fichier automatisé des empreintes digitales (FAED) et le fichier national automatisé des empreintes génétiques (FNAEG), il conviendrait de préciser les conséquences à tirer des décisions judiciaires (acquittement, non-lieu, relaxe, classement sans suite)

(**proposition n° 34**). Pour le fichier « Traitement des antécédents judiciaires », il s'agit d'assurer la mise en œuvre effective des dispositions qui le régissent (**proposition n° 35**), les contrôles successifs de la CNIL ayant montré un taux très élevé d'erreurs et d'absence de prise en compte des suites judiciaires.
- La décision n° 2010-25 QPC du 16 septembre 2010 du Conseil constitutionnel devrait être mise en oeuvre, en modulant la durée de conservation des données dans le FNAEG en fonction de la gravité de l'infraction et de l'âge de la personne au moment de l'enregistrement (**proposition n° 36**).

• *En matière de prévention des atteintes à la sécurité nationale*

Les **conséquences de l'arrêt *Digital Rights Ireland*** doivent être tirées en ce qui concerne **l'accès aux données de connexion collectées au titre de l'obligation de conservation systématique prévue par notre législation**, notamment en réservant l'accès à des fins de police judiciaire aux crimes et aux délits d'une gravité suffisante, en réexaminant les régimes prévoyant l'accès de certaines autorités administratives pour des finalités autres que la sécurité intérieure (notamment la HADOPI, l'ANSSI, l'administration fiscale, l'AMF) et en étendant, pour l'accès aux données de connexion, les règles spécifiques de protection qui bénéficient aux parlementaires, aux avocats, aux magistrats et aux journalistes en matière d'interceptions du contenu des communications (**proposition n° 38**).

Afin de satisfaire à l'exigence de prévisibilité de la loi issue de la jurisprudence de la CEDH, il conviendrait de définir par la loi le régime de l'interception des **communications à l'étranger,** en prévoyant les finalités de ces interceptions les garanties spécifiques bénéficiant aux résidents français et l'existence d'un contrôle d'une autorité administrative indépendante (**proposition n° 39**). Il conviendrait également de définir le régime juridique de l'utilisation par les services de renseignement, sur autorisation administrative, de certains moyens d'investigation spéciaux utilisant les techniques numériques aujourd'hui encadrés uniquement dans le cadre de la procédure judiciaire (déchiffrement, captation de données informatiques...) (**proposition n° 40**).

Il est proposé de faire de la CNCIS une autorité de contrôle des services de renseignement, dotée de moyens humains renforcés sur le plan quantitatif et qualitatif, avec des compétences de haut niveau en matière d'ingénierie des communications électroniques, d'informatique et d'analyse des données. Ses prérogatives devraient aussi être renforcées, par l'attribution de pouvoirs de contrôle sur pièces et sur place et d'un champ de compétences étendu aux interceptions opérées à l'étranger ainsi qu'à l'emploi des moyens d'investigations spéciaux (**proposition n° 41**). Les agents impliqués dans la mise en œuvre des programmes de renseignement auraient **un droit de signalement** à cette autorité administrative indépendante des pratiques manifestement contraires au cadre légal, selon des modalités sécurisées assurant la protection du secret de la défense nationale (**proposition n° 42**).

3.5. Organiser la coopération européenne et internationale

Un **socle de règles** applicables à tous les services dirigés vers l'Union européenne ou la France (selon que la règle est européenne ou nationale), quel que soit leur lieu d'établissement comprendrait (**proposition n° 43**) :
- la législation européenne relative à la protection des données personnelles, qui serait qualifiée à cette fin de « **loi de police** » au sens du droit international privé ;
- l'obligation de coopération des hébergeurs et des plateformes avec les autorités administratives et judiciaires, prévue par l'article 6 de la LCEN, dont le champ d'application territorial serait explicité ;
- le droit pénal, notamment les abus de la liberté d'expression, qui est déjà applicable à l'ensemble des sites, même établis à l'étranger mais destinés au public français.

En matière de protection des données personnelles, le *Safe Harbor* négocié avec les autorités américaines, devrait être réformé, en prévoyant un droit de regard des autorités européennes sur les contrôles et en renforçant les obligations de fond (**proposition n° 44**).
En matière de lutte contre la cybercriminalité, un groupe d'action interétatique devrait être créé pour définir des recommandations et publier une liste d'États non coopératifs (**proposition n° 47**).

L'annonce de la fin du lien contractuel entre l'ICANN et le gouvernement américain ouvre des perspectives de réforme de la gouvernance d'internet, pour l'ICANN mais aussi pour les autres instances qui doivent être investies d'une mission d'intérêt général guidée par un « mandat » international. Le processus de réforme en cours doit être l'occasion de donner une traduction concrète à ces exigences. Il conviendrait de promouvoir la démocratisation de l'ICANN, notamment en créant une assemblée générale rassemblant l'ensemble des parties prenantes et pouvant mettre en cause la responsabilité du conseil d'administration. Le rôle des États devrait être renforcé, en permettant au comité représentant les gouvernements (GAC) d'adopter des résolutions contraignantes (**proposition n° 48**). Pour l'ensemble des instances, il conviendrait de diversifier la composition des organes de gouvernance d'internet, par des critères de sélection imposant une réelle diversité linguistique et géographique et la mise en place de stratégies d'influence de la France et de l'Union européenne (**proposition n° 49**). Une convention internationale relative aux libertés fondamentales et aux principes de la gouvernance d'internet devrait notamment énoncer les principes que s'imposeraient les signataires (**proposition n° 50**).

****

Lorsqu'il s'est engagé dans cette étude, le Conseil d'État savait qu'il était attendu sur le terrain de la défense des droits fondamentaux. Il savait aussi qu'il ne devait pas se borner à la seule position – au demeurant fort légitime – de gardien des droits des individus. Il a souhaité prendre en considération toutes les potentialités du numérique, tout particulièrement celles qui en font le vecteur d'une économie qui favorise l'innovation, la croissance et l'emploi. Le Conseil d'État aurait manqué à son office et son étude annuelle, à son objectif, si n'avaient pas été concomitamment traités les deux aspects d'une même réalité : l'innovation numérique et le respect des droits fondamentaux des citoyens.

16 QUESTIONS/REPONSES

1. **Pourquoi le Conseil d'État a t-il décidé de consacrer son étude annuelle 2014 au sujet « *Le numérique et les droits fondamentaux » ?* Les deux décisions de la CJUE - *Digital Rights* Ireland du 8 avril 2014 sur la conservation des données de connexion de communication et *Google Spain* du 13 mai 2014 sur le « droit à l'oubli », ont- elles conforté ou infléchi les orientations du Conseil d'État dans sa réflexion générale sur le sujet ?**

Le choix du sujet de l'étude annuelle est à la fois **évident** et **audacieux** : évident parce que le Conseil d'Etat a toujours été un gardien des droits et libertés fondamentaux ; audacieux parce que le phénomène du numérique revêt des dimensions techniques, économiques et de société qui bouleversent complètement les repères juridiques habituellement reconnus. Le numérique qui conduit à une mise en données et à une mise en réseau générale, pose, en cela, problème aux droits fondamentaux ; non qu'il serait, en soi, un phénomène négatif, mais parce qu'il met en question leur contenu et leur régime.

Le choix du sujet s'inscrit **dans la continuité d'une réflexion** ancienne du Conseil d'Etat sur des questions fondamentales de droit et de société. Les auteurs du « *rapport Tricot* »[1] de juin 1975 dont les recommandations ont servi de base à la loi « Informatique et Libertés » du 6 janvier 1978, se prononçaient déjà sur les conséquences prévisibles de la constitution d'importantes bases de données par l'administration. En 1998, une étude thématique commandée par le Gouvernement au Conseil d'Etat sur « *Internet et les réseaux numériques »* répondait aux nouvelles questions liées aux enjeux juridiques du spectaculaire essor d'internet.
Quinze ans plus tard, il était nécessaire que le Conseil d'Etat revienne sur ces questions et y consacre son étude annuelle 2014 en raison des considérables évolutions techniques, économiques et sociales à l'œuvre.

Au moment où le Conseil d'Etat menait son étude, **deux décisions de la Cour de justice de l'Union européenne (CJUE) sont intervenues**. Elles ont permis au Conseil d'Etat d'approfondir sa réflexion en mettant à l'épreuve les orientations qu'il s'apprêtait à retenir et ont finalement conforté ses recommandations. La proposition n° 38 de l'étude tire un certain nombre de conséquences de l'arrêt *Digital Rights Ireland* du 8 avril 2014 qui **remet en cause le cadre européen de la conservation des données** par les opérateurs de télécommunications. L'arrêt *Google Spain c/ AEPD* du 13 mai 2014, quant à lui, a conforté le Conseil d'Etat dans sa recommandation **d'une conciliation entre le « droit à l'oubli » et la liberté d'expression** garantie par l'article 10 de la Convention européenne des droits de l'homme. La proposition n° 5 de l'étude énonce les conditions d'une mise en œuvre équilibrée du droit au « déréférencement » consacré par l'arrêt *Google Spain*.

D'une manière plus générale, l'étude du Conseil d'Etat n'entend pas se substituer aux nombreux travaux sectoriels très approfondis qui ont été conduits ces dernières années. Elle consiste plutôt à proposer **une approche globale** et répondre à la question suivante : face aux bouleversements suscités par le numérique, **dans quelle mesure la protection des droits fondamentaux doit-elle être repensée ?** Elle apporte également des réponses aux **nombreuses questions actuellement en débat** telles que la **neutralité d'internet**, sa **gouvernance**, le **« droit à l'oubli »**, **la propriété des données**, leur exploitation et agrégation en **méga-données** (*Big Data*), le rôle inédit des **« plateformes »** ...

[1] Du nom du conseiller d'Etat Bernard Tricot, rapporteur général de la « Commission informatique et libertés » constituée en novembre 1974 auprès du Garde des Sceaux et présidée par Bernard Chenot, vice-président du Conseil d'Etat et Maurice Aydalot, premier président de la Cour de cassation

L’étude a été attentive aux **risques** que présente le numérique mais n’a pas entendu méconnaître le rôle positif de ce dernier dans l’exercice des libertés ni sa contribution à la réforme des politiques publiques, à **l’innovation** et à la croissance. Son but n’est pas de proposer des protections supplémentaires contre le numérique, mais de faire en sorte que les risques dont il est porteur ne remettent pas en cause son potentiel.

2. Quel rôle doit jouer l'État pour protéger les droits fondamentaux dans un contexte de développement du numérique? Quels sont les objectifs de l'action des pouvoirs publics ? Quels en sont les moyens ?

Les pionniers d'internet ont conçu et présenté la communication numérique comme un espace échappant à tout contrôle des pouvoirs publics : autonome, décentralisé, transfrontalier et participatif. Pourtant, les deux postulats de cette approche « libertaire », le défaut de légitimité des États sur internet et leur incapacité à intervenir, n'ont en réalité jamais été vérifiés. **Les États ne sont pas moins légitimes à légiférer sur les réseaux numériques que sur tout autre domaine** d'activité humaine. Ils parviennent à y exercer leur pouvoir de contrainte : les pratiques de censure des Etats non démocratiques en donnent une illustration extrême ; mais c'est aussi le cas dans les Etats de droit, des tribunaux ordonnent le déréférencement de certains sites, tranchent des différends sur des noms de domaine ou encore enjoignent de publier une condamnation sur la page d'accueil d'un site.

Pour autant, si l'État n'est pas « hors-jeu » sur internet, son action se heurte à des limites :

- le mode de gouvernance d'internet, dans lequel les Etats ne sont que des parties prenantes parmi d'autres ;
- la détermination de la loi applicable, qui résulte du jeu, parfois complexe, des règles de droit international privé ;
- l'effectivité de l'intervention étatique, mise à mal par la facilité de recréation des sites convaincus d'activités illicites, la nécessité d'obtenir la coopération d'Etats étrangers pour faire exécuter les décisions de justice et la vitesse d'évolution des processus numériques.

Cependant, l'action de la puissance publique, nationale ou internationale, est, à l'ère numérique, plus que jamais nécessaire pour garantir les droits fondamentaux et valoriser le potentiel que recèle le numérique pour l'intérêt général. Pour être efficace, elle doit cependant s'appuyer sur des instruments profondément rénovés. C'est pourquoi le Conseil d'Etat préconise **la mise en place d'une « chaîne de responsabilités » dont l'État est, dans certains cas, le pilote** et qui inclut l'ensemble des acteurs concernés.

Comme dans d'autres domaines de la vie économique et sociale, les situations d'inégalité de position et d'allocation de ressources rares, fréquentes dans le monde du numérique, justifient aussi pleinement l'intervention des pouvoirs publics. Pour protéger les droits fondamentaux, l'Etat doit pouvoir, selon les cas, assurer une **meilleure régulation** ou favoriser l'émergence **de larges espaces de libertés** pour les citoyens, usagers ou non d'internet.

L'étude du Conseil d'Etat propose donc un ensemble de mesures adaptées à la spécificité du rôle des acteurs en jeu et aux multiples, et souvent contradictoires, intérêts en cause. On ne traite pas de la même façon les risques de contrefaçon d'un produit numérique et les menaces à l'ordre public ou à la sécurité nationale.

Plusieurs exemples de la diversité des interventions des pouvoirs publics peuvent être donnés. L'étude propose ainsi que :

- soient **renforcés les pouvoirs des personnes** et de leurs groupements (droit au déréférencement, droit d'alerte, action collective, homologation des codes de bonne conduite, médiation) ;

- soit instituée, par une directive européenne, une **nouvelle catégorie juridique, celle des « plateformes numériques »**. En effet les opérateurs de communications électroniques ne

sont pas les seuls acteurs à jouer un rôle déterminant dans l'exercice des libertés sur internet et la situation des « plateformes numériques » ne peut plus rester dans l'ambigüité actuelle. La définition des plateformes ne doit plus reposer sur le postulat du caractère technique et passif de leur rôle mais sur le fait qu'elles proposent des services de classement ou de référencement de contenus, biens ou services mis en ligne par des tiers. Les plateformes doivent donc être soumises à une obligation de loyauté envers leurs utilisateurs, tant les utilisateurs non professionnels dans le cadre du droit de la consommation que les utilisateurs professionnels dans le cadre du droit de la concurrence ;

- soit organisée une **régulation des contenus licites**, notamment des contenus audiovisuels, reposant sur des instruments adaptés à l'environnement numérique où la ressource n'est plus rare ;

- soit assurée, dans la **lutte contre les contenus numériques illicites**, une répartition appropriée des rôles entre l'administration et les plateformes, sous le contrôle du juge ;

- soit décidée la transformation de la Commission nationale de contrôle des interceptions de sécurité (CNCIS) en autorité de contrôle des services de renseignement, dotée de moyens humains renforcés avec des compétences en matière d'ingénierie des communications électroniques, d'informatique et d'analyse des données ;

- soit défini un socle de règles impératives applicables à tous les acteurs proposant des services aux internautes français ou européens, si besoin en passant par la qualification de **loi de police**, quel que soit leur lieu d'établissement. Serait retenu le **principe du pays de destination**, non pour l'ensemble des règles juridiques applicables aux acteurs d'internet, mais pour un socle de règles choisies en raison de leur importance particulière dans la protection des droits fondamentaux ou de l'ordre public. En effet, **la question du droit territorialement applicable** sur internet constitue un enjeu d'accessibilité du droit, et également un **enjeu stratégique**. Elle met en cause la capacité de la puissance publique à assurer la protection des libertés fondamentales de leurs citoyens ainsi que le droit au recours de ceux-ci. Les implications pour la concurrence entre entreprises numériques sont significatives ;

- soit donnée une plus grande place aux Etats dans les instances de gouvernance d'internet comme ICANN, qui leur permette de peser en faveur de résolutions plus conformes à l'intérêt général. Des alliances avec d'autres Etats tels que le Brésil et la Corée du Sud sont possibles sur ce point et bien d'autres.

* * *

Les caractéristiques propres au numérique (caractère transfrontalier, participatif et en mutation permanente) ne justifient évidemment pas une intervention exclusive de la puissance publique dans le domaine du numérique et de la protection des droits fondamentaux. Un partage concerté des rôles avec les autres acteurs : autorités européennes, autorités de régulation, plateformes, internautes eux-mêmes est préférable et plus réaliste, sans que cela n'exclue une régulation par les pouvoirs publics, y compris européens, dont le domaine d'action est adapté aux enjeux d'internet. Cette régulation doit être organisée afin de pouvoir proposer une réponse globale et un **cadre juridique d'ampleur continentale** à la collecte et au traitement de données par des opérateurs extra-européens.

3. Pourquoi le Conseil d'État soutient-il que la protection des droits fondamentaux dans les usages du numérique passe, à la fois, par l'accroissement des capacités d'action des individus et par la mobilisation des outils et des usages du numérique au service de l'intérêt général ?

Deux principes directeurs président aux orientations et propositions de l'étude du Conseil d'Etat.

Le premier principe concerne la capacité d'action des individus. Les habitudes de consentement passif des individus sont l'un des principaux obstacles à une protection effective des droits fondamentaux dans les usages du numérique. Aussi, les conditions générales d'utilisation sont invariablement acceptées sans être lues. Aujourd'hui, les droits reconnus aux individus se limitent, pour l'essentiel, à leur permettre de rester à l'écart du traitement de leurs données, sans leur conférer de réels pouvoirs sur le contenu du service et la manière dont leurs données sont traitées. Il faut renforcer le pouvoir des individus et de leurs groupements pour rééquilibrer leurs relations avec les fournisseurs de services.

Les propositions formulées sont fondées sur une logique de **« responsabilisation » des individus,** puisqu'elles ont pour objet d'accroître leurs capacités d'action (par exemple en promouvant les technologies de protection de la vie privée, en accroissant la transparence sur les classements proposés par les plateformes, en donnant le droit de faire valoir ses observations sur l'application d'un algorithme prédictif…). Conforter les droits des individus passe également par le renforcement de leurs groupements (par exemple, en créant une action collective en matière de protection des données personnelles, en mettant en *open data* l'ensemble des déclarations de traitement transmises à la CNIL ou encore en favorisant les délibérations des politiques de contenu des plateformes). Le Conseil d'État préconise ainsi que les pouvoirs publics renforcent la capacité des personnes physiques à agir, de manière individuelle ou collective, afin d'en faire des gardiens efficaces de leurs propres libertés.

Dans cette perspective, il convient de donner à la CNIL et à l'ensemble des autorités de protection des données européennes une mission explicite de promotion des technologies renforçant la maîtrise des personnes quant à l'utilisation de leurs données (émergence de solutions technologiques en termes de renforcement de la vie privée, diffusion gratuite d'outils de protection de la vie privée par les FAI). Cela peut se faire dans un cadre volontaire ou en l'imposant par la loi, comme c'est le cas pour les logiciels de contrôle parental.

Le second principe directeur est de mettre le numérique au service de l'intérêt général. Le numérique peut contribuer de manière considérable à l'efficacité des politiques de santé, d'éducation, de sécurité, de lutte contre la fraude ou de promotion de la culture, ainsi qu'à la simplification des démarches administratives. Le Conseil d'État propose en ce sens de mieux affirmer la liberté de **réutilisation statistique des données personnelles**, d'ouvrir de manière maîtrisée l'utilisation des numéros d'identification et de renouveler la conception des garanties du pluralisme dans les médias. Cela signifie aussi que l'Etat s'impose à lui-même, lorsqu'il utilise le numérique, un haut niveau d'exigence dans le respect des droits fondamentaux : le Conseil d'Etat propose ainsi de poursuivre **l'ouverture des données publiques** tout en prévenant les risques pour la vie privée, de renforcer les garanties entourant l'usage des fichiers de police et de conjuguer le plein respect des droits fondamentaux et la prévention des atteintes à la sécurité nationale.

Les deux principes directeurs sont mis en œuvre dans le respect des règles fondamentales de la protection des données : finalité déterminée des traitements, loyauté et proportionnalité de leur collecte et conservation, usage statistique encadré des méga-données. De plus, ils justifient, l'un et l'autre, la nécessité de mettre en place des instruments nouveaux adaptés à la puissance du numérique. Les outils et usages du numérique que l'étude propose ont l'ambition de relever le défi permanent de la protection des droits fondamentaux, tout en assurant la sécurité nationale et en définissant une stratégie économique pertinente pour la prospérité de la France au sein de l'Europe.

4. Pourquoi le Conseil d'État ne consacre-t-il pas un droit de propriété des personnes sur leurs données ? Que représente la notion d'« autodétermination informationnelle » qu'il avance à la place ?

Face aux limites actuelles de la protection des données à caractère personnel, il est parfois proposé de donner aux individus un véritable droit de propriété sur leurs données ; le but recherché est notamment de susciter une implication plus active, les individus devenant financièrement intéressés à une bonne gestion de leurs données.
Le Conseil d'État ne recommande pas d'emprunter cette voie en dépit de son attrait apparent. S'il convient en effet de renforcer la dimension de l'individu acteur dans le droit à la protection des données, c'est en envisageant ce dernier comme un droit à l'autodétermination plutôt que comme un droit de propriété.
En l'état du droit, il n'existe pas de droit de propriété de l'individu sur ses données personnelles mais un dispositif juridique de droits attachés à la personne. Il convient d'**écarter l'introduction d'une logique patrimoniale** dans la protection des données personnelles, car il n'est certainement pas souhaitable que l'individu, par l'exercice du droit d'aliénation attaché au droit de propriété, renonce à toute protection de ses données personnelles.

C'est dans cette mesure que le Conseil d'État envisage le droit à la protection des données personnelles comme **un droit à l'autodétermination informationnelle**, plutôt que comme un droit de propriété (proposition n°1), c'est-à-dire *« le droit de l'individu de décider de la communication et de l'utilisation de ses données à caractère personnel ».*

Le Conseil d'État propose ce concept d'« autodétermination informationnelle », dans une logique proche de celle consacrée par la Cour constitutionnelle fédérale de l'Allemagne. Celle-ci, dans un arrêt du 15 décembre 1983 relatif à une loi sur le recensement, a établi sur le fondement des articles 1er (dignité de l'homme) et 2 (droit au libre développement de sa personnalité) de la Loi fondamentale allemande, que *« la Constitution garantit en principe la capacité de l'individu à décider de la communication et de l'utilisation de ses données à caractère personnel »*. Alors que le droit à la protection des données peut être perçu comme un concept défensif, le droit à l'autodétermination lui donne un contenu positif. Il ne s'agit plus seulement de protéger le droit au respect de la vie privée, mais d'affirmer la primauté de la personne qui doit être en mesure d'exercer sa liberté.

Dans cette perspective, la notion d'autodétermination informationnelle servirait à fonder **non pas un droit supplémentaire**, comme le droit d'information, le droit d'accès, le droit de rectification, mais un **principe essentiel donnant sens à d'autres droits fondamentaux**, afin de mieux les garantir.

Afin de doter cette notion d'une portée étendue à l'ensemble des États membres de l'Union européenne, la définition proposée 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.

5. **Quelle conception de la neutralité du net le Conseil d'État retient-il ? En quoi le choix qu'il fait est déterminant au regard de ses propositions concernant la protection des droits et libertés ?**

Le principe de « neutralité du Net » est né avec Internet ; il repose sur une idée simple à laquelle les concepteurs d'internet sont restés attachés : **les opérateurs de réseaux doivent traiter de manière égale l'ensemble du trafic qu'ils acheminent.** Il permet à chaque utilisateur d'accéder aux contenus de son choix dans des conditions identiques et, réciproquement, à chaque fournisseur de contenus d'accéder à tous les utilisateurs dans les mêmes conditions. Il est ainsi une garantie de la liberté de communication, de la liberté d'entreprendre et de la liberté d'association, ce qui justifie qu'il soit protégé par la loi.
La consécration du principe de neutralité apparaît **particulièrement nécessaire aujourd'hui.** En effet, la part et le poids du trafic représentés par les flux de vidéo diffusés par quelques sites et la puissance de marché acquise par leurs éditeurs rendent crédible le scénario d'un accaparement par quelques acteurs dominants de la bande passante et de la qualité de diffusion.

Le principe de neutralité du net, tel qu'il est mentionné à l'article 2 de la proposition de règlement européen votée par le Parlement le 3 avril 2014, est défini comme « *le principe selon lequel l'ensemble du trafic Internet est traité de façon égale, sans discrimination, limitation ni interférence, indépendamment de l'expéditeur, du destinataire, du type, du contenu, de l'appareil, du service ou de l'application* ». Ce principe permet à chacun d'émettre et de recevoir des contenus dans les mêmes conditions.

Toutefois, tout comme le principe d'égalité, qui admet des différences de traitement lorsqu'elles sont justifiées par des différences de situation ou par un motif d'intérêt général, **le principe de neutralité du Net doit laisser aux opérateurs de communications des espaces de différenciation**.
Le Conseil d'État propose ainsi de garder la définition retenue par le Parlement européen dans la version de la proposition de règlement sur la protection des données personnelles telle qu'elle a été votée le 3 avril 2014.
Quelques corrections devraient cependant être apportées à l'approche trop restrictive du Parlement européen afin de revenir à la définition plus souple de la neutralité du Net proposée par la Commission.

- Le Conseil d'État préconise de retenir une définition plus large des « *services spécialisés* » qui nécessitent une qualité de flux supérieure et qui échappent au principe de neutralité du net. Parmi ces « *services spécialisés* », devenus incontournables, figurent notamment les services de téléphonie ou de télévision sur internet. Cette définition plus large doit, en contrepartie, s'accompagner de garanties d'absence de dégradation de la qualité générale d'internet. L'autorité de régulation compétente serait chargée de donner un avis avant tout accord entre un opérateur de communications et un fournisseur de contenus portant sur la fourniture d'une qualité de service supérieure pour les « *services spécialisés* ». L'autorité de régulation aurait aussi le pouvoir de contrôler la qualité de l'accès à internet et de rompre l'accord, si le service spécialisé provoque une dégradation générale de la qualité d'internet.

- Le Conseil d'État n'est pas favorable à une facturation généralisée des fournisseurs de contenus par les opérateurs de communications électroniques afin de leur donner accès aux utilisateurs finaux. Il préconise une facturation asymétrique qui ne s'appliquerait qu'aux plus gros fournisseurs de contenus, qui représentent une part significative du trafic, non pour qu'ils bénéficient d'une qualité supérieure mais simplement afin de ne pas voir leur qualité d'accès dégradée. Il n'y aurait ainsi pas d'atteinte à la liberté de communication des acteurs de petite et moyenne taille.

La conception du principe de neutralité du Net choisie par le Conseil d'État est donc un **équilibre entre la nécessité pour certains « *services spécialisés* » de pouvoir bénéficier d'une qualité de service supérieure, l'obligation de respecter le libre accès aux utilisateurs finaux et les libertés d'entreprendre, de communication et d'association** qui en découlent. Cette conception s'inscrit pleinement dans la cohérence des propositions du Conseil d'État qui veulent sauvegarder le potentiel de développement de l'économie numérique tout en apportant des garanties supplémentaires pour la protection des droits fondamentaux, notamment le principe de non discrimination.

6. **Pourquoi la reconnaissance du rôle des prestataires que sont les « plateformes numériques» nécessite-t-elle l'expression d'un droit spécifique des plateformes ? Pourquoi le Conseil d'État parle-t-il, à leur propos, de « loyauté » plutôt que de « neutralité » ?**

Le Conseil d'État propose la **création d'une nouvelle catégorie juridique de « prestataires intermédiaires »** au sens de la directive n° 2000/31/CE du 8 juin 2000 sur le commerce électronique, distincte à la fois des éditeurs de contenus et des hébergeurs, et **qui serait intitulée « plateforme ».**

Seraient ainsi qualifiés les services de référencement ou de classement de contenus, biens ou services édités ou fournis par des tiers et partagés sur le site de la plateforme. Une telle définition couvrirait l'ensemble des acteurs tels que : moteurs de recherche, réseaux sociaux, sites de partage de contenus (vidéos, musique, photos, documents …), places de marché, magasins d'applications, agrégateurs de contenus ou comparateurs de prix. Par son caractère générique, elle pourrait également couvrir à l'avenir de nouveaux types de services encore peu développés ou inexistants. Cette définition cherche à cerner ce qui caractérise la plateforme, c'est-à-dire son rôle d'intermédiaire actif dans l'accès à des contenus, des biens ou des services qui ne sont pas produits par elle.

C'est ce rôle d'intermédiaire qui justifie un régime de responsabilité spécifique. En effet, l'article 6 de la loi pour la confiance dans l'économique numérique (LCEN) de 2004[2] distingue les hébergeurs, dont la responsabilité civile et pénale est limitée, des éditeurs, qui sont soumis à un régime de responsabilité similaire à celui de la presse écrite. Cette distinction est aujourd'hui discutée: la jurisprudence a défini l'hébergeur comme l'intermédiaire technique ne jouant pas de rôle actif qui lui permette d'avoir connaissance ou de contrôler les données stockées. Le cas des moteurs de recherche fait aujourd'hui particulièrement question. Ce ne sont pas des éditeurs de données, mais ils jouent un rôle actif dans le stockage et le référencement de celles-ci en agissant sur leur présentation à l'utilisateur. A moyen terme, tous les grands services d'intermédiation utilisés sur Internet pourraient ainsi perdre la qualification d'hébergeur, avec un impact sur leur régime de responsabilité civile et pénale. En revanche, la catégorie des plateformes n'inclurait pas ceux des acteurs ayant une responsabilité directe dans la mise en ligne des contenus, tels les sites de musique en ligne ou de vidéo à la demande, considérés comme des éditeurs. La définition d'une nouvelle catégorie juridique a donc semblé nécessaire.

Du fait de leur nature et de leur liberté éditoriale, le principe de neutralité ne peut s'appliquer aux plateformes. L'étude annuelle du Conseil d'État propose donc de soumettre cette nouvelle catégorie juridique à une **exigence de loyauté.** Celle-ci consiste à **assurer de bonne foi le service de classement ou de référencement proposé**, sans chercher à le détourner à des fins contraires à l'intérêt des utilisateurs.

La reconnaissance d'un devoir de loyauté pour cette nouvelle catégorie juridique ne change rien aux limites posées à la responsabilité de la plateforme, visant à éviter une trop grande censure sur leurs auteurs. En revanche, elle implique l'émergence d'un nouveau droit spécifique des plateformes. Déjà soumises à des obligations particulières en droit de la concurrence et en droit de la consommation, les plateformes seraient, au titre de l'exigence de loyauté, tenues à **quatre nouvelles obligations** (proposition n°6) :

- Une obligation de pertinence des critères de classement et de référencement ;
- Une obligation d'information sur ces critères ;

[2] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

- Un encadrement des retraits de contenus par la plateforme ;
- Une obligation de notification préalable des changements de politiques relatives aux contenus (pour les utilisateurs commerciaux).

Enfin, le Conseil d'État propose également de développer la participation des utilisateurs des plateformes à l'élaboration des règles éditoriales (proposition n°10).

7. Pourquoi le Conseil d'État préfère t-il parler de droit au déréférencement plutôt que de droit à l'oubli ?

L'expression « droit à l'oubli » a l'avantage d'être très explicite mais rend mal compte de réalités complexes. La décision *Google Spain c/ AEPD* du 13 mai 2014 de la Cour de Justice de l'Union Européenne (CJUE) a **consacré un droit au « déréférencement »** plutôt qu'un « droit à l'oubli ». Depuis cette décision, **toute personne a en principe le droit d'obtenir d'un moteur de recherche qu'il n'affiche pas certaines informations la concernant**, même si ces informations ne lui sont pas préjudiciables. Par cet arrêt qui témoigne de la force des principes fondamentaux de la directive de 1995, la CJUE a donc créé un nouvel instrument de nature à peser sur le fonctionnement des moteurs de recherche, qualifiés de responsables de traitement. Elle apporte ainsi un élément de réponse à la **question, sensible dans la société numérique contemporaine, de « *l'e-reputation* ».**
Si l'arrêt *Google Spain* est très protecteur de la vie privée des particuliers, ses conséquences sur la liberté d'expression sont en revanche contestées. Jimmy Wales, le fondateur de l'encyclopédie en ligne *Wikipedia* a dénoncé l'arrêt comme instaurant *« l'une des censures les plus étendues jamais vues sur internet »*[3] et s'est inquiété de ses conséquences pour son propre site. Pourtant ce site ou les autres encyclopédies en ligne ne sont pas des moteurs de recherche.

Avant même l'arrêt de la CJUE, le concept de « droit à l'oubli » ne faisait pas l'objet d'un consensus ; des archivistes et des historiens s'étaient notamment inquiétés des risques pour la recherche historique et la mémoire collective que comportaient certaines dispositions de la proposition de règlement.
La question de la conciliation entre droit à la vie privée et liberté d'expression n'est pas neuve. Les juges judiciaires français, sur le fondement de l'article 9 du code civil et la CEDH, sur le fondement des articles 8 et 10 de la convention, ont développé une jurisprudence abondante sur ce sujet, qui cherche le juste équilibre entre le droit de chacun au respect de sa vie privée et la liberté d'informer.

L'arrêt *Google Spain* s'inscrit dans cette **recherche d'équilibre entre liberté d'expression et droit à la vie privée** qui prévalait avant l'essor d'internet et des moteurs de recherche, mais en déplace le curseur. Certes, il ne concerne que les moteurs de recherche et non les sites qui publient initialement ces informations. Cependant on sait à quel point l'abondance d'informations disponibles sur les réseaux a rendu indispensable la visibilité de ces informations et, par suite, donné un rôle décisif à leur « fléchage » par le référencement sur une plateforme.

D'autres inquiétudes quant au « droit à l'oubli » paraissent moins fondées. Il est ainsi parfois avancé que l'arrêt *Google Spain* donne aux moteurs de recherche un pouvoir trop important dans la sélection des informations devant être ou non effacées. Mais ce pouvoir s'exerce dans le cadre défini par l'arrêt de la CJUE et il est susceptible de recours devant l'autorité de contrôle ou la juridiction nationale compétente.
On ne peut enfin exclure que la jurisprudence Google Spain soit étendue aux réseaux sociaux et que sa portée en soit ainsi accrue. Un réseau social est en effet un traitement de données personnelles et on peut considérer l'exploitant du réseau social comme le responsable du traitement, dans la mesure où il en détermine « les finalités et les moyens ». Les droits d'effacement et d'opposition pourraient être exercés à son encontre dès lors que le consentement à un traitement de données peut être retiré.

A ce stade, le Conseil d'Etat propose de mettre en œuvre le « droit au déréférencement » qui découle des principes consacrés par l'arrêt *Google Spain* (proposition n°5) :

[3] "One of the most wide-sweeping internet censorship rulings that I've ever seen" ; interview à la BBC le 14 mai 2014.

- en donnant aux éditeurs des sites dont le déréférencement est demandé la **possibilité de faire valoir leurs observations** ;

- en explicitant par **des lignes directrices la doctrine** de mise en œuvre de *Google Spain* par les autorités de protection des données. L'adoption de ces lignes directrices par les autorités compétentes permettrait de répondre à l'argument selon lequel l'arrêt *Google Spain* conférerait aux moteurs de recherche un trop grand pouvoir d'appréciation ;

- en organisant les **conditions d'une décision unique de déréférencement** qui faciliterait les recours pour les particuliers. Cette décision de déréférencement pourrait prendre la forme d'une reconnaissance mutuelle des décisions prises par chaque exploitant sur la base d'un accord volontaire entre ceux-ci. La loi pourrait également prévoir la possibilité d'étendre à tous les exploitants une décision de déréférencement prise par l'un d'entre eux, sous réserve de son homologation par le juge.

8. **Quelle est la position du Conseil d'État sur les *Big Data* (méga-données) ? Qu'attend-t-on de la possibilité de réutilisation statistique des données personnelles ?**

Le Conseil d'État estime que le *Big Data* (méga données) **ouvre un considérable potentiel de développement du numérique.** L'expression « Big Data » désigne ainsi non seulement l'expansion du volume des données, mais aussi celle de la capacité à les utiliser. En effet, ce n'est que très récemment que des solutions permettant d'exploiter des données hétérogènes (textes, images, données de connexion, données de localisation....) et non structurées sous forme de base de données ont été développées. Le Big Data permet de faire des progrès substantiels dans de nombreux domaines, que ce soit pour **améliorer les politiques publiques, évaluer plus facilement les risques sanitaires ou encore optimiser les performances des entreprises.**

Les exemples d'utilisation des *Big data* qui servent l'intérêt général sont nombreux. Ce fut le cas au moment de l'affaire du Mediator dont les méfaits sur la santé ont été détectés par le biais d'une étude de la Caisse nationale de l'assurance maladie des travailleurs salariés (CNAMTS) sur la base du répertoire des actes de soins prodigués à chaque assuré social. En matière de contrôle des flux d'énergie, le *Big Data* permet la mise en place de réseaux intelligents s'appuyant sur les données collectées par des compteurs communicants. Cette mise en réseau pourrait mener à des économies d'énergie substantielles et à la réduction des émissions de gaz à effet de serre.

Le Conseil d'État est donc favorable à l'extension des usages des *Big data* à des fins d'intérêt général. Toutefois, ces usages doivent s'accompagner de garanties supplémentaires de protection de la vie privée des usagers.

L'article 6 de la directive n° 95/46/CE du 24 octobre 1995 prévoit qu'un « *traitement ultérieur à des fins statistiques, historiques ou scientifiques* » n'est pas réputé incompatible avec les finalités initiales du traitement de données, pour autant que les États membres prévoient des garanties appropriées, notamment en empêchant « *l'utilisation des données à l'appui de mesures ou de décisions prises à l'encontre d'une personne* ». Dans l'ordre interne, ces dispositions figurent dans la loi *Informatique et libertés* du 6 janvier 1978 modifiée en 2004. Elles permettent une **libre réutilisation statistique des données sans qu'y fasse obstacle la finalité initiale du traitement.** L'adoption de ce principe dans le projet de règlement européen permettrait de l'élever dans la hiérarchie des normes.

La position du Conseil d'État vise à introduire dans la proposition de règlement européen la **présomption de compatibilité de la réutilisation statistique des données,** qui n'y figure pas. Bien entendu, cette liberté de réutilisation statistique des données doit être accompagnée des garanties d'anonymat appropriées.

9. **Quel est l'intérêt de la mise en place d'un numéro d'identification unique non signifiant ? Pourquoi le Conseil d'État propose-t-il de d'élargir le domaine d'utilisation du numéro d'inscription répertoire (NIR) au secteur de la santé et de la recherche médicale ?**

La mise en place d'un numéro d'identification unique non signifiant en complément ou en substitut au numéro d'inscription répertoire (NIR) utilisé pour les traitements de données relatifs à la sécurité sociale permettrait de **lever certaines appréhensions concernant le respect de la vie privée.** En effet, le NIR est un numéro signifiant qui fournit des informations sur le sexe, l'année, le mois ainsi que le lieu de naissance. Le Conseil d'État préconise de mettre à l'étude la création de ce numéro national non signifiant et d'évaluer son intérêt pour la conduite des politiques publiques et la simplification des démarches administratives. Le numéro national non signifiant serait généré de manière aléatoire (proposition 21)

Le Conseil d'État propose, en outre, de **faciliter l'utilisation du NIR au secteur de la santé et de la recherche médicale afin de favoriser les politiques publiques de recherche et de prévention.** Or actuellement, l'utilisation du NIR est fortement encadrée par la loi, car c'est un numéro d'identification signifiant. Cet encadrement est susceptible de constituer un obstacle à des traitements d'utilité publique ne présentant pas de risques pour la vie privée. L'étude annuelle préconise ainsi de supprimer l'obligation de passer par un décret en Conseil d'Etat pour autoriser les traitements effectués à des fins de recherche dans le domaine de la santé ; seul l'avis rendu par la CNIL en vertu du chapitre IX de la loi du 6 janvier 1978 serait nécessaire pour mener à bien l'utilisation du NIR pour les traitements de données à des fins de recherche médicale (proposition 22).

Cette proposition du Conseil d'État va dans le même sens que le changement de doctrine d'utilisation du NIR annoncé par la CNIL dans son rapport d'activité pour 2013. La CNIL admet désormais que le NIR soit utilisé comme identifiant national pour les données de santé, alors qu'elle avait jusqu'ici toujours affirmé la nécessité d'un « cantonnement » au domaine de la sécurité sociale.

10. Pourquoi le Conseil d'État accorde-t-il autant d'importance aux algorithmes, au regard de la protection des droits fondamentaux ?

Les algorithmes sont au cœur du rôle d'intermédiation joué par les plateformes. Pivots du fonctionnement des moteurs de recherche, leur modification peut entraîner la rétrogradation de plusieurs pages d'un site commercial et ainsi engendrer des pertes financières considérables. Le développement des méga-données (*Big Data)* a conduit à leur expansion dans de très nombreux domaines : présélection des candidats à un emploi par des services de ressources humaines, identification de « profils » parmi les passagers d'un transport aérien ou encore mise en relation des utilisateurs d'un site de rencontre. Leur utilité pour optimiser le fonctionnement d'un certain nombre de services est indiscutable.

Toutefois, les algorithmes présentent **trois sources de risques** pour l'exercice des droits fondamentaux, auxquelles le Conseil d'État porte une attention particulière : **l'enfermement de l'internaute dans une « personnalisation »** dont il n'est pas maître ; la **confiance abusive dans les résultats d'algorithmes** perçus comme objectifs et infaillibles ; **de nouveaux problèmes d'équité du fait de l'exploitation des données personnelles** (en matière d'accès à l'emploi, au crédit, à l'assurance).

L'encadrement de l'utilisation des algorithmes est certes un domaine nouveau d'action pour les pouvoirs publics, mais devenu nécessaire en raison du rôle grandissant de ces mécanismes. Face aux risques qu'ils présentent, il convient de définir un véritable droit des algorithmes prédictifs. L'étude du Conseil d'État propose de concevoir trois méthodes d'encadrement :

- Assurer **l'effectivité de l'intervention humaine** dans toute prise de décision produisant des effets juridiques à l'égard d'un individu et fondée sur l'utilisation d'algorithmes (proposition n°23) ;

- Mettre en place des **garanties de procédure et de transparence,** lorsque des données personnelles sont utilisées par l'algorithme (proposition n°24) ;

- Développer le contrôle des résultats produits par les algorithmes, notamment pour **détecter des discriminations illicites**, en renforçant les moyens dont dispose la CNIL (proposition n°25).

11. Comment le Conseil d'État concilie t-il la protection de la vie privée avec les impératifs de la sécurité nationale ?

Le numérique a renforcé les moyens d'action de la police et des services de renseignement. Les fichiers de police ont grandement bénéficié de l'essor du numérique ; les services de renseignement ont, quant à eux, de plus en plus recours à la surveillance des communications électroniques. L'affaire « *Prism* »[4] de 2013 a fait de la question un élément clé du débat public. Le Conseil d'État préconise de **mieux assurer le respect des droits fondamentaux** dans l'utilisation du numérique par les personnes publiques, **tout en conciliant cet objectif avec les impératifs de la sécurité nationale.**

Si l'usage de fichiers par la police est ancien, le numérique a changé la nature de leur utilisation par les facilités de recherche et de conservation qu'il procure. En 2013, le fichier « traitement d'antécédents judiciaires » (TAJ) comptait ainsi plus de 12 millions de fiches[5]. La conservation des empreintes et l'usage des données biométriques ont également bénéficié du développement numérique : en témoignent l'essor du fichier national automatisé des empreintes digitales (FNAED) ou génétiques (FNAEG). Face à cette situation, le Conseil d'État juge souhaitable de **renforcer les garanties entourant l'utilisation de ces fichiers.** Sans remettre en cause leur utilité pour les services de police, il propose de mieux tirer les conséquences des décisions judiciaires (classement sans suite, non-lieu, relaxe et acquittement) et de définir concernant le TAJ un plan d'apurement des erreurs (propositions n°34 et 35).

En ce qui concerne la prévention des atteintes à la sécurité nationale, il convient de la concilier avec le respect des droits fondamentaux. La collecte de renseignement par la surveillance des communications électroniques est un élément essentiel de la stratégie de défense et de sécurité de la France. Les deux livres blancs de 2008[6] et de 2013[7] en ont fait une priorité, en prévoyant une augmentation des moyens alloués aux services de renseignement afin de mieux faire face aux nouvelles menaces contre la sécurité nationale, notamment celles liées au terrorisme.

Les principes encadrant la surveillance des communications par les pouvoirs publics en France ont été fixés par la loi du 10 juillet 1991[8]. Toutefois, l'essor du numérique a, depuis lors, démultiplié les capacités d'interception et d'analyse des données. Au niveau européen, le cadre juridique de la conservation des données de communication a été remis en cause par l'arrêt *Digital Rights Ireland* de la CJUE. Ce dernier invalide la directive du 15 mars 2006 relative à la conservation des données par les opérateurs de télécommunication, en estimant que l'atteinte à la vie privée commise lors de leur interception et de leur stockage ne doit pas être disproportionnée par rapport aux objectifs poursuivis par les pouvoirs publics.

Compte tenu des termes de l'arrêt *Digital Rights Ireland*, deux interprétations sont possibles : l'une, stricte, condamnant par principe tout système de conservation générale des

---

[4] Programme américain de surveillance des communications électroniques dont l'existence a été révélée le 6 juin 2013.

[5] Ce chiffre recouvre cependant des « doubles comptes » (la même personne peut être comptée deux fois), en raison de la fusion des fichiers d'antécédents de la police nationale (STIC) et de la gendarmerie nationale (JUDEX) qui a donné lieu au TAJ.

[6] *Livre blanc sur la défense et la sécurité nationale*, 17 juin 2008, La documentation Française, Paris

[7] *Livre blanc sur la défense et la sécurité nationale*, 19 avril 2013, La documentation Française, Paris

[8] Loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques.

« métadonnées » [9] ; l'autre, plus ouverte, permettant le maintien d'un tel système mais avec des garanties plus fortes que celles prévues par la directive du 15 mars 2006. Le Conseil d'Etat considère que **la remise en cause**, par principe, **de la conservation générale des métadonnées poserait d'importantes difficultés pour l'efficacité du renseignement et de la police judiciaire.** La portée de l'arrêt *Digital Rights Ireland* pourrait être précisée par la CJUE à l'occasion d'un nouveau renvoi préjudiciel d'une juridiction nationale.

Le Conseil d'État propose de prendre dès à présent les mesures qu'impose l'arrêt *Digital Rights Ireland*, au moins dans son interprétation ouverte. Il préconise notamment de **réserver l'accès aux « métadonnées » à des fins de police judiciaire aux crimes et délits d'une gravité suffisante et de réexaminer les régimes prévoyant l'accès de diverses autorités administratives** (par exemple la HADOPI, l'AMF ou l'administration fiscale) à des fins autres que la sécurité intérieure.
Il propose aussi d'étendre aux procédures d'accès aux métadonnées les garanties prévues **en faveur des membres du Parlement, avocats, magistrats et journalistes** en ce qui concerne les interceptions judiciaires (proposition n°38).

Le Conseil d'État propose par ailleurs 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 publique indépendante (proposition n°39).

[9] Les « métadonnées » sont les données relatives à une communication électronique autre que son contenu : elles recouvrent notamment les informations permettant d'identifier les personnes ayant communiqué (numéro de téléphone, adresse électronique, etc), la durée de leur communication et leur localisation.

12. Pourquoi le Conseil d'État propose t-il de créer une Autorité de contrôle des services de renseignements dotée de moyens et de prérogatives renforcées par rapport à ceux de la CNCIS ?

La loi du 10 juillet 1991, qui fixe les principes de surveillance des communications par les pouvoirs publics, est à l'origine de la création de la Commission nationale de contrôle des interceptions de sécurité (CNCIS), autorité administrative indépendante.

Compte tenu de l'essor considérable des communications électroniques, les moyens dont dispose la CNCIS, qui n'ont pas évolué depuis 1991, ne sont pas suffisants pour assurer un contrôle pleinement satisfaisant de l'action des services de renseignement en la matière. Des compétences de haut niveau en matière d'ingénierie des communications électroniques, d'informatique et d'analyse des données sont notamment requises. Mais surtout les prérogatives légales de la CNCIS n'apparaissent pas suffisantes. Celle-ci ne peut contrôler que des interceptions dont elle est informée. L'Autorité indépendante chargée du contrôle devrait être dotée de prérogatives de contrôle sur pièces et sur place : **elle aurait le droit d'obtenir communication de tout document et de contrôler les installations et moyens techniques employés dans le cadre de la collecte de renseignement.** L'extension de son champ de compétences, de ses prérogatives, et de ses moyens juridiques justifie la reconfiguration de la CNCIS.
La forte spécialité de ces missions conduit à proposer le principe du **maintien d'une autorité spécialisée, qui pourrait être dénommée « Autorité de contrôle des services de renseignements »**, plutôt que de confier ces prérogatives à une autorité généraliste**.** Son collège pourrait être composé de parlementaires et de magistrats des deux hautes juridictions, judiciaire et administrative. (proposition n° 41).

13. Quelles sont les propositions particulières du Conseil d'État dans le domaine des médias et de la culture ?

Le Conseil d'État estime nécessaire d'adapter la législation dans les domaines des médias et de la culture, afin de **mieux garantir à l'ère numérique l'exigence constitutionnelle de pluralisme considérée comme *« une des conditions de la démocratie »*** dans la jurisprudence du Conseil constitutionnel[10]*.*

Le domaine des médias est marqué, du fait du numérique, par la **surabondance des contenus.** Dorénavant, les principales menaces qui pèsent sur le libre choix des personnes ne tiennent plus seulement aux problématiques de concentrations excessives, mais aussi à la **fragilisation du modèle économique de la presse,** alors que celle-ci demeure une source essentielle d'information de qualité. La législation actuelle sur les concentrations dans les médias, conçue dans les années 1980, ne se fonde que sur la diffusion imprimée et ignore la diffusion numérique de la presse. Elle ne saisit pas le rôle croissant de prescription joué par les distributeurs de contenus audiovisuels numériques et les plateformes et elle encadre de façon rigide la concentration des groupes plurimédias. Le Conseil d'Etat propose **d'ouvrir une concertation en vue d'aboutir à une nouvelle loi tendant à mieux garantir le pluralisme au regard de l'ensemble des modes de diffusion contemporains (**proposition n° 30).

Le Conseil d'État propose également **d'encourager la prise en compte de la diversité culturelle dans les algorithmes de recommandation utilisés par les sites internet diffusant des contenus audiovisuels ou musicaux** (proposition n°27), en ayant recours au droit souple ou à la contractualisation, par une concertation avec les sites concernés sur des engagements volontaires en matière de soutien à la diversité culturelle.

[10] Décision n° 86-217 DC du 18 septembre 1986, *Loi relative à la liberté de communication,* §11.

14. Quelle est la position de l'Europe sur la protection des données personnelles ? Qu'est-ce qui relève encore du droit interne des États ? Qu'est-ce qui relève du droit de l'Union ? Quelle est la marge de manœuvre de la France pour faire évoluer le droit de l'Union ?

Le droit européen des données personnelles repose sur une pluralité de textes (Charte des droits fondamentaux de l'Union européenne, directive de l'Union européenne du 24 octobre 1995, convention n° 108 du Conseil de l'Europe du 28 janvier 1981) qui définissent plusieurs grands principes : **collecte des données loyale**, répondant à des **finalités déterminées et proportionnée** à ces finalités ; exigence du **consentement** de la personne ou d'un autre principe prévu par la loi ; **droits d'information, d'accès, de rectification et d'opposition** de la personne ; existence d'une **autorité indépendante de contrôle**.

L'ensemble constitue un **corpus juridique cohérent et protecteur, qui diffère** de manière substantielle **du droit des Etats-Unis d'Amérique**, dans lequel il n'existe pas de cadre général du traitement des données personnelles et qui retient une approche subjective, centrée sur la réparation du préjudice subi. En revanche, d'autres espaces juridiques sont plus proches du droit européen : des pays tels que le **Brésil** ou la **Corée du Sud** ont adopté au cours de ces dernières années **une législation protectrice.**

La proposition de règlement relative à la protection des données personnelles, soumise en 2012 au Conseil et au Parlement européen, a pour but de **substituer un régime harmonisé de protection des données aux différentes lois nationales transposant la directive de 1995.** La nature de la règle juridique concernant la protection des données serait ainsi modifiée : elle ne serait plus nationale, mais européenne. Ce **renforcement de l'intégration juridique** (accru par le passage du niveau de la directive à celui du règlement) apparaît nécessaire compte tenu du caractère transnational du fonctionnement d'internet et de la dimension des grandes entreprises du numérique.

Dès lors, l'échelon européen revêt aujourd'hui un caractère pertinent. Nombre des propositions de l'étude du Conseil d'Etat relèvent de la compétence de l'Union européenne, soit parce qu'elles impliquent une modification du droit de l'Union, soit parce que **l'Union européenne constitue, en opportunité, le cadre pertinent d'action.** La France peut bien sûr contribuer de manière importante à l'action européenne.

Toutefois, il est apparu au Conseil d'État qu'un nombre, certes limité, de propositions pouvaient être portées en priorité par les autorités nationales. Les délais de mise au point des directives ou règlements peuvent être longs et impliquer, par conséquent, **des initiatives des autorités françaises en matière, par exemple, de protection des données personnelles, de garantie en faveur des organes de presse ou encore de réglementation de la responsabilité des plateformes numériques.** D'autres sujets touchent aux intérêts fondamentaux de notre pays : il en est ainsi des modalités de conservation des données de communication à des fins de prévention ou de répression.

15. Quelle est la position du Conseil d'État sur l'application territoriale du droit de l'internet ? Comment et dans quels cas doit-on renforcer la règle du pays de destination des contenus numériques au détriment de la règle du pays d'origine de l'établissement émetteur ?

La fréquente confrontation de systèmes juridiques différents qu'occasionne internet est source d'une double difficulté pour les États : d'une part, la complexité des règles de droit international privé, qui déterminent la loi applicable et la juridiction compétente, est source d'incertitudes ; d'autre part, ces règles peuvent désigner des juridictions et des lois étrangères. L'État est ainsi confronté à la possibilité que ses lois sur la protection des données personnelles, la liberté d'expression ou la propriété ne soient en définitive pas applicables à toutes les situations qu'il entend encadrer.

La territorialité sur internet représente des enjeux de simplification et d'accessibilité du droit, mais aussi et surtout des **enjeux stratégiques.** L'objectif est de **trouver le bon équilibre entre le droit du pays de l'internaute et le droit du pays du site internet.** Si le droit du pays où est installé le site prévaut, alors internet est un facteur de mise en concurrence des systèmes juridiques et les entreprises dont les systèmes juridiques sont les moins protecteurs peuvent en retirer un avantage concurrentiel ; en revanche, si le droit du pays de l'internaute s'applique, alors le lieu d'établissement de l'entreprise est sans incidence.

Il est **difficilement envisageable que le principe « du pays de l'internaute »** (application du droit de l'internaute qui utilise un service sur internet) **devienne une règle générale et absolue** de détermination de la loi applicable sur internet. Il y a un risque de « fragmentation d'internet », c'est-à-dire de différenciation des contenus accessibles selon les pays. Une telle orientation postulerait en outre que les acteurs français ou européens soient toujours voués à être sur internet en situation de consommateurs et jamais de producteurs de services. Or, la France compte aussi des entreprises du numérique cherchant à développer leurs services à l'échelle mondiale ; pour elles, la sécurité juridique consiste à se voir appliquer les règles françaises partout dans le monde.

Le Conseil d'État préconise de **promouvoir le principe du droit du pays de l'internaute** non pour l'ensemble des règles juridiques applicables aux acteurs d'internet, mais **pour un socle de règles choisies en raison de leur importance particulière dans la protection des droits fondamentaux ou de l'ordre public.** Les règles du socle seraient applicables à tous les sites dirigeant leur activité vers la France ou l'Union européenne. Ce socle comprendrait notamment les catégories de règles suivantes :

- la législation européenne relative à la protection des données personnelles, qui serait **qualifiée à cette fin de « loi de police »** au sens du droit international privé ;
- **l'obligation de coopération des hébergeurs et des plateformes avec les autorités administratives et judiciaires**, prévue par l'article 6 de la loi pour la confiance dans l'économie numérique du 21 juin 2004, dont le champ d'application territoriale serait explicité ;
- **le droit pénal**, qui est déjà applicable à l'ensemble des sites destinés au public français. (Proposition n° 43)

16. Pourquoi faut-il une gouvernance mondiale d'internet ? Pourquoi est-elle aujourd'hui déséquilibrée ? A quels enjeux répondent les mesures préconisées par le Conseil d'État pour rééquilibrer la gouvernance d'internet ?

Par opposition au modèle intergouvernemental qui avait prévalu pour la gestion internationale d'autres moyens de communication, la gouvernance d'internet s'appuie sur plusieurs instances de droit privé chargées de traiter différents aspects de son fonctionnement (ICANN pour la coordination du système des noms de domaine, IETF et 3WC pour la définition des standards techniques, Internet Society et « Forum pour la gouvernance d'internet » pour le traitement des questions politiques, économiques et sociétales). On parle de « modèle multi-acteurs » pour désigner ce système dans lequel les Etats ne sont que des parties prenantes parmi d'autres, au côté des entreprises, des ONG ou des experts.

Le déséquilibre de la gouvernance d'internet provient du rôle historiquement prééminent des États-Unis dans la conception, puis dans la gestion d'internet. Les autorités américaines maintiennent à ce jour une tutelle sur l'ICANN, organisme de droit américain. Par ailleurs, si le « Forum pour la gouvernance d'internet » présente un caractère plus équilibré, il se borne à être un lieu de discussion entre acteurs sans élaboration d'une position commune.

Ce mode de gouvernance ne fait pas consensus.

Certains États, comme la Russie et la Chine, critiquent par principe l'inclusion d'acteurs non étatiques. D'autres États, issus notamment de l'Union européenne, critiquent **le caractère insuffisamment démocratique du « modèle multi-acteurs », qui doit être modifié pour assurer une meilleure prise en compte de l'ensemble des parties prenantes et de l'intérêt général**. Ainsi, la Commission européenne plaide pour une gouvernance plus transparente, fondée sur un **rééquilibrage des acteurs et sur une responsabilisation accrue des organes de décision actuels, notamment en les contraignant à rendre des comptes aux États.** Cette critique est plus aiguë à l'égard de l'ICANN et de sa subordination aux autorités américaines. La croissance du nombre d'internautes dans les pays émergents, ainsi que les révélations sur les programmes de surveillance de la NSA conduit la communauté internationale à remettre en cause la tutelle américaine.

Une gouvernance plus ouverte est également nécessaire pour des raisons techniques. Par exemple, la croissance du nombre d'adresses nécessite la migration des utilisateurs du protocole internet IPv4 vers la sixième version (IPv6). Or, malgré l'accord de principe de l'ensemble des parties prenantes, l'absence de moyens juridiques contraignants retarde ce processus, ce qui montre les limites du droit souple et invite à édicter des normes de droit dur dans le cadre d'une gouvernance globale.

Le Conseil d'État propose **plusieurs axes de réforme** de la gouvernance d'internet, répondant respectivement aux enjeux de gouvernance, de promotion de la diversité culturelle et de garanties des droits fondamentaux.

Sur le plan de la gouvernance, le « modèle multi-acteurs » ne doit pas être remis en cause, mais le **fonctionnement de ses instances doit être réformé**. L'abandon annoncé de la tutelle américaine sur l'ICANN ne doit pas conduire à ce que celle-ci ne rende compte qu'à elle-même, eu égard à sa mission d'intérêt général. L'étude annuelle du Conseil d'État préconise donc deux orientations. En premier lieu, une **responsabilisation accrue par la création de voies de recours contraignantes et d'une assemblée générale où siègeraient les différentes parties et devant laquelle le conseil d'administration serait responsable.** En second lieu, les intérêts défendus par les États, garants de l'intérêt général

et non simples « parties prenantes », doivent être mieux défendus. Cela suppose de **donner au comité représentant les gouvernements (le GAC) la possibilité de s'opposer aux décisions du conseil d'administration.**

Enfin, un dernier axe de réforme de la gouvernance d'internet, qui s'inscrit dans une perspective de plus long terme, concerne la protection des droits fondamentaux. Si la gouvernance d'internet a toujours reposé jusqu'ici sur le droit souple, ce modèle rencontre cependant certaines limites. Souvent présenté comme une manière de limiter le rôle des gouvernements, il ne crée en réalité aucune obligation pour les États de respecter les libertés fondamentales. **Une convention internationale** qui énoncerait les grands principes devant être respectés par les États serait plus protectrice des libertés. Sans entrer dans les modalités de la gouvernance, une convention internationale **pourrait énoncer les grands principes des libertés sur internet (liberté d'expression, vie privée et protection des données personnelles, neutralité et ouverture d'internet, transparence de la gouvernance)** et en rendrait la garantie plus effective.