

L'évolution des droits du citoyen avec la communication numérique

22. L'individu est en constante évolution. Antoinette Rouvroy estime que nous aimons à nous penser, individus du XXI^{ème} siècle, comme des processus en constante évolution, non clôturés, peu définis, pour les possibilités de nouveautés que cette absence de définition rend possible plutôt que comme des êtres finis, achevés, définitivement rangés dans un statut social, une profession, une catégorie, raison pour laquelle on tient à garantir juridiquement, à travers le droit à la protection de la vie privée notamment, une forme d'immunité contre les contraintes déraisonnables dans la construction de sa propre identité⁶¹. Ce point de notre réflexion liminaire est central car les réalités sociales, humaines, économiques et juridiques impliquent une mise à jour permanente et continue du droit, notamment aujourd'hui avec les NTIC et le numérique. Parmi tous les domaines qui sont particulièrement transformés par le numérique, le domaine légal est sans doute celui qui est le plus compliqué à appréhender, notamment à cause de l'hétérogénéité des domaines qui doivent être maîtrisés : droit, technologie, philosophie...⁶².

23. Internet contient en lui-même les germes de la démocratie. Sa diffusion et son utilisation conduisent à une plus grande transparence et circulation de l'information dans tous les domaines de la vie économique, politique et sociale de notre époque, accélérant le processus de "démocratisation réelle" de la société. Le principe sur lequel repose Internet est la nécessité de décentraliser les centres de décision, permettant à plusieurs nœuds du réseau de communiquer entre eux par de multiples voies possibles, non préétablies. Ce moyen de communication avait été conçu pour une éventuelle guerre nucléaire, par le commandement militaire américain, pour augmenter les possibilités de défense en cas d'attaque nucléaire sur le Pentagone, décentralisant les centres de décision militaires américains sur de nombreux points du territoire, reliés entre eux dans un réseau non hiérarchique. Ce besoin militaire a en effet commencé à changer la structure du pouvoir du monde entier, basée sur des structures pyramidales et descendantes qui, principalement grâce à leur pouvoir, contrôlent

⁶¹ ROUVROY (A.), « La gouvernamentalité algorithmique : radicalisation et stratégie immunitaire du capitalisme et du néolibéralisme ? », *La deleuziana – Revue en ligne de philosophie* – ISSN 2421-3098 n. 3 / 2016 <http://www.ladeleuziana.org/wp-content/uploads/2016/12/Rouvroy2f.pdf>

⁶² AUGIER (M.), *La société numérique*, Paris, Éditions L'harmattan, 2016, 252 p.

les informations et les redistribuent en fonction de leur utilisation et de leur consommation par les citoyens.

24. La menace terroriste actuelle. La menace terroriste actuelle paraît être tellement présente que l'intérêt général et la protection de la sécurité publique semblent devoir primer malgré les traditionnelles garanties relatives notamment au nécessaire respect des textes constitutionnels. Le Conseil constitutionnel lors de son contrôle de la loi fonde ses raisonnements en grande partie sur le respect par la loi de la proportionnalité entre l'objectif sécuritaire à atteindre et la protection des droits et libertés fondamentaux⁶³. Ces propos peuvent s'appuyer sur un exemple d'inconstitutionnalité de dispositions visant à surveiller les communications⁶⁴. Il s'agit de celles qui figuraient à l'article L 811-5 du Code de la sécurité intérieure, reformulant le dispositif de surveillance et de contrôle des communications dont l'inconstitutionnalité et la violation du respect de la vie privée a été mise en évidence par Olivier Le Bot : « Pour être conformes à la Constitution, les atteintes à ce droit doivent être justifiées par un motif d'intérêt général et mises en œuvre de manière adéquate et proportionnée à cet objectif ». L'exigence de proportionnalité de la restriction fait défaut en l'absence de tout encadrement de celle-ci. La disposition en cause n'interdisait pas que les mesures qu'elle autorise puissent être utilisées "à des fins plus larges" que la mise en œuvre des seules exigences constitutionnelles inhérentes à la sauvegarde des intérêts fondamentaux de la nation. La loi ne définit pas « la nature » des mesures de surveillance et de contrôle que les pouvoirs publics sont autorisés à prendre. Et surtout, les dispositions en cause « ne soumettent le recours à ces mesures à aucune condition de fond ni de procédure et n'encadrent leur mise en œuvre d'aucune garantie⁶⁵. On peut moduler la garantie des droits en fonction de la nécessité de la société, et sous l'effet des attentats terroristes, l'attitude jurisprudentielle du Conseil constitutionnel a été en faveur de la protection de la sécurité⁶⁶.

⁶³ LE BOT (O.), « L'oubli d'intégrer les communications hertziennes dans le droit commun du renseignement », Paris, *Constitutions*, 2016, pp. 653-655.

⁶⁴ Cons. const., n° 2016-590 QPC du 21 octobre 2016, *La quadrature du Net et autres (surveillances et contrôle des transmissions empruntant la voie hertzienne)*.

⁶⁵ LE BOT (O.), « L'oubli d'intégrer les communications hertziennes dans le droit commun du renseignement », Paris, *Constitutions*, 2016, pp. 653-655.

⁶⁶ V. par ex. Cons. const., n° 2016-600 QPC du 2 décembre 2016, *M. Raïme A. [Perquisitions administratives dans le cadre de l'état d'urgence III]*.

La réforme pénale⁶⁷ est intervenue malgré le fait qu'aux États-Unis des dispositions similaires avaient déjà été adoptées sans pour autant aboutir à d'efficaces résultats. En tout état de cause, et malgré cette comparaison de cadres juridiques, un point commun intéressant rapproche ces systèmes, la volonté de la loi anti-terroriste d'accentuer la protection des citoyens, priorité qui reste l'un des objectifs principaux de l'État.

25. Les lois sur le renseignement ouvrent la possibilité d'une récolte massive et d'un traitement généralisé d'informations personnelles et privées. Ce type de moyens, dont l'inefficacité a été démontrée dans les États qui l'ont mis en place, ne sont, en l'état actuel, ni susceptibles d'un encadrement précis, ni une assurance absolue contre les attaques et attentats terroristes. Cela d'autant que les moyens humains des services de renseignement sont encore insuffisants en qualité et en quantité pour parvenir à éradiquer les racines djihadistes qui conduisent des dizaines d'hommes et femmes radicalisés à rejoindre les rangs de l'organisation terroriste ISIS ou agir, comme dans l'attentat de *Nice*, en « loups solitaires ». L'instauration de l'état d'urgence permet de contrôler les communications qui ne sont pas cryptées et qui ne sont pas effectuées à travers le *dark web*. Le terme *darkweb* définit non seulement le web non indexé et non accessible par des moyens standards mais aussi le web criminel ; il n'existe pas un terme pour différencier les deux, et dans l'imaginaire collectif, ce terme définit surtout le web criminel. L'utilisation du *dark web* permet en effet d'échapper à toute surveillance de la part des forces de l'ordre. Le contrôle du *dark web* est unanimement retenu par tous les spécialistes du numérique, comme impossible car les communications effectuées à travers le *dark web* sont anonymes et ne laissent aucune trace IP rendant impossible la localisation de leurs auteurs⁶⁸. En amont des questions relatives à « l'internet caché » et l'exception de l'état d'urgence, se pose celle de l'intérêt de l'exception de l'état d'urgence en matière numérique alors que les services de renseignement sont conscients de ne pas pouvoir avoir accès à de nombreuses communications secrètes effectuées à travers cet « internet caché ». Dans la situation actuelle où les terroristes cherchent précisément à

⁶⁷ Loi n° 2016-987 du 21 juillet 2016 prorogeant l'application de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence et portant mesures de renforcement de la lutte antiterroriste.

⁶⁸ Notons que l'anonymat a déjà eu de graves conséquences dans le passé, et notamment l'envoi des lettres anonymes a permis la délation sous l'occupation pendant la Seconde Guerre mondiale. En France plus de 3 millions de lettres anonymes ont été envoyées dénonçant les voisins, les concurrents ou même des membres de la famille.

réduire les libertés fondamentales, il peut sembler paradoxal qu'on les restreint, sans privilégier d'autres voies moins coercitives.

26. La nécessité d'un droit d'accès à internet avec des droits corollaires protecteurs.

Un des grands risques relatifs à internet concerne la manipulation des communications, des informations et la possibilité de masquer la réalité. Cette réalité masquée est possible avec les « bulles de filtres »⁶⁹, la censure des informations et le contrôle des médias sociaux. Aujourd'hui le plus grand rempart contre ces agissements est le fait d'être conscients de ces pratiques douteuses et critiquables. D'emblée il est possible d'affirmer que les « bulles de filtres » peuvent porter atteinte et fausser la démocratie numérique. Repenser le domaine constitutionnel uniquement sous l'aspect de l'évolution des nouvelles technologies de la communication paraît ne pas être suffisant si une réflexion éthique et morale n'est pas menée parallèlement. Par conséquent dans notre recherche relative à l'essor de nouveaux droits fondamentaux constitutionnels liés au droit d'accès à internet et à la libre communication numérique il a été nécessaire de choisir de s'intéresser à certains des nombreux domaines issus de cette liberté protéiforme. Portant un grand intérêt au sujet, on a souvent été confrontés à l'apparition de nouveautés. On constate l'utilisation par les internautes d'un nouveau type d'internet, le *dark web* qui leur permet de naviguer de façon anonyme et cryptée afin d'éviter toute répercussion liée aux espionnages privés ou publics.

B – Un nouvel espace pour l'exercice de la démocratie

27. Le domaine des relations humaines a été profondément modifié par l'introduction du numérique et d'internet. Internet constitue un élément désormais incontournable de l'exercice de la liberté de communication et d'information, mais également un facteur de risque nouveau pour la protection de la vie privée et des données personnelles⁷⁰. On remarque que les débats relatifs au rôle d'internet dans la vie politique et dans la démocratie ont très rapidement laissé la place à la pratique elle-même, comme si on

⁶⁹ Elie Pariser souligne le fait que lorsqu'on effectue une recherche sur internet par mot clé, deux utilisateurs d'internet n'ont pas les mêmes résultats à leurs recherches. Avec les algorithmes ils auront des résultats qui correspondent à leurs idées et à leurs opinions. PARISER (E.), *The filter bubble, what the internet is hiding from you*, 2011, Éditeur Penguin, p. 55.

⁷⁰ FALQUE-PIERROTIN (I.), « La constitution et l'Internet », Paris, *Les Nouveaux cahiers du Conseil constitutionnel*, n°36, juin 2012, p. 9.

attendait depuis si longtemps cette nouvelle voie démocratique sans hiérarchie. Toute notre organisation sociale est basée sur des structures de pouvoir hiérarchiques. L'église est un exemple d'organisation hiérarchique par excellence, organisée de manière pyramidale du pape aux cardinaux en passant par les évêques jusqu'au curé de campagne. Une autre structure hiérarchique est la structure militaire, qui part des généraux en passant par les différents grades (major, capitaine, lieutenant...) jusqu'au simple soldat. L'État est également organisé de manière similaire, du Président de la République, aux Ministres, en passant par les différentes structures hiérarchiques territoriales (régions, provinces, communes). Le même constat est possible avec la plupart des organisations économiques et sociales, telles que les partis politiques, les syndicats, les chaînes de distribution, les entreprises nationales, diverses associations. Tous ont en commun des structures hautement hiérarchisées, avec des degrés de pouvoir précis et un échange d'informations et de décisions de haut en bas. Internet est un réseau non hiérarchique qui échange des informations de manière non traditionnelle, les informations ne sont pas médiatisées ou filtrées par les structures de pouvoir, il est libre de circuler sur le net à très faible coût, sans censure, avec le schéma de communication un par un, un à beaucoup, beaucoup à plusieurs.

28. L'individu crée un réseau de contacts dans lequel il veut être le protagoniste. Par conséquent, le réseau social est né et se développe après le réseau traditionnel, qui est un élargissement participatif de l'ego individuel, qui place les petits ou les grands groupes dans un système dans lequel chaque individu peut s'exprimer et se rapporter à un groupe d'amis ou de connaissances. Facebook est l'un des exemples les plus réussis de ce phénomène qui met l'accent sur le désir de l'individu de créer un réseau de contacts humains autour de lui en grand nombre. Tout le monde veut être le protagoniste d'internet et mener à bien leurs idées et projets, en les communiquant au monde. De toute évidence, dans ce processus, ceux qui ont la plus grande capacité à adapter et à prévoir le système peuvent mieux mettre leurs compétences dans le système et peut-être utiliser des listes de diffusion, des groupes de discussion et d'autres outils numériques avec les nouvelles opportunités qu'offre le réseau. Cependant, on ne doit pas oublier les nouveaux et anciens protagonistes de la communication, qui continuent à avoir un rôle très important, notamment : la téléphonie mobile et la télévision.

29. Internet est un réseau non hiérarchique qui échange des informations de manière non traditionnelle. Les informations ne sont pas médiatisées ou filtrées par les

structures de pouvoir. Les informations sont libres de circuler sur le net à très faible coût, sans censure. Contrairement à la vision générale induite par les moyens de communication traditionnels (télévisions, journaux et magazines), Internet n'est pas seulement une bibliothèque universelle sur laquelle rechercher des informations, mais surtout un moyen très puissant de communiquer des informations, utilisant de nombreux outils qui s'intègrent les uns aux autres (services mail, mail, newsgroup, chat, téléconférence, vidéo à la demande, etc.), élargissant le même concept de communication dans l'espace et dans le temps. En fait, il est très facile et économique de contacter, au moment qui convient le mieux, des milliers de personnes n'importe où dans le monde en très peu de temps, avec des outils plus faciles et plus rapides que tout autre moyen. Cet ensemble d'outils augmente incroyablement nos « relations humaines », nous faisant connaître de nombreuses personnes, proches et lointaines, qui partagent avec nous des idées et des projets ou simplement des intérêts de toute nature. On pourrait penser que ces relations ne sont que virtuelles, donc de nature à ne pas modifier notre vie réelle, en fait l'être humain est amené à communiquer avec ses semblables et sa curiosité innée le conduit également à chercher d'effectuer des rencontres directes dans la vie réelle avec ces contacts pour établir de nouvelles relations, des relations d'amitié ou d'intérêt à des fins légaux ou illégaux. De nos jours ce phénomène a pris une ampleur qualifiable d'impressionnante, tant elle englobe pratiquement toutes les sphères de la société et tant elle continue et vraisemblablement continuera à se développer et à prendre de l'ampleur. Ce développement rapide en quelques décennies permet déjà d'analyser une situation actuelle bien évoluée. Tout comme dans le passé il a été nécessaire de dépasser d'éventuelles réticences dans son utilisation, et aujourd'hui conscients de ses apports on doit étudier comment mieux rénover le droit constitutionnel, afin de lui permettre de progresser, protéger et limiter. Aujourd'hui la pratique de l'utilisation d'internet n'est plus sans contrôle. En effet la réaction des pouvoirs publics face aux abus liés à internet est bien présente avec un important arsenal législatif notamment en période d'état d'urgence.

30. Le risque de transformer la démocratie en une société de surveillance. Un régime d'état d'urgence fait peser sur les droits fondamentaux et sur les démocraties des dangers. Ainsi, ce régime exceptionnel doit être constitutionnellement strictement limité et encadré. La Constitution française prévoit, dans son article 16 alinéa 1, la possibilité pour le Président de la République de disposer de pouvoirs exceptionnels permettant la mise en suspens du droit commun. L'état d'urgence présente la spécificité d'être une « mise entre parenthèses » du droit commun prévue par le droit du pays qui l'applique. L'état d'urgence a une double

application : temporelle⁷¹ et territoriale⁷². Les origines de la création de l'état d'urgence remontent au droit et à la civilisation romaine notamment avec la possible mise en place de politiques d'exception. En droit romain l'état d'urgence désignait un régime exceptionnel mis en place par un Gouvernement en cas d'atteinte grave à l'ordre public, de troubles graves ou de calamités nationales. Au XXI^{ème} siècle l'exceptionnalité de l'état d'urgence, son strict encadrement et à sa limitation de durée doivent être maintenus. Avec les NTIC, l'état d'urgence paraît ne plus avoir les mêmes résultats concrets et la même force d'impact immédiate. Une des causes de cette insuffisance est le *dark web*, qui est une véritable zone virtuelle de non-droit. Les attentats qui ont frappé les capitales européennes ont changé les logiques sécuritaires et conduisent vers une mise à jour contemporaine au XXI^{ème} siècle du droit. En tout état de cause le défi sécuritaire est international, dès lors il faut être dans l'exigence du respect et de l'exécution des décisions transfrontalières. L'encadrement d'internet doit permettre de réaliser les priorités de protection de la sécurité et des droits fondamentaux. Les sites et les communications numériques abjectes doivent être punis. Le domaine des droits fondamentaux numériques est actuellement pris en considération uniquement sur le plan législatif, ce qui paraît insuffisant à cause des motifs précédemment énoncés. L'état d'urgence doit être décidé pour des durées courtes, afin de pouvoir mobiliser en urgence des ressources de l'État sans que leurs actions ne soient entravées par les législations et longueurs administratives. Se pose la question de la rencontre et l'intégration des droits numériques aux droits fondamentaux, *quid* de la qualification des droits et libertés fondamentaux. À partir du moment où l'homme utilise le numérique il est nécessaire de créer le droit qui lui est applicable. C'est une situation qui nécessite d'apporter un regard juridique nouveau. La violence et la puissance possible par le numérique doit être encadrée. Il s'agit d'interpréter et d'imaginer. Le difficile lien entre les droits fondamentaux est établi par plusieurs motifs et intérêts individuels et généraux. Une des justifications possibles à ce constat alarmant est le fait qu'on n'a pas encore le recul et l'expertise adaptée. De plus, il est pour l'heure impossible de limiter les communications dans le *dark web*.

31. La législation contre le *dark web* à cause de la non-indexation des sites internet.

Les institutions étatiques essayent de trouver les moyens pour contrôler l'accès et le contenu

⁷¹ Suspension temporelle du droit commun : état de guerre, de catastrophe naturelle...

⁷² Suspension territoriale du droit commun dans une partie spécifique du territoire français.

du *dark web* qui est également utilisé par les terroristes. Ces contrôles paraissent matériellement impossibles à mettre en place et à faire respecter notamment à cause de la nature transfrontalière et complètement anonyme de ce réseau. Par conséquent il est très compliqué de constater les infractions et de le sanctionner. Les perturbateurs de la vie en société utilisent des technologies ultra modernes pour transmettre leurs idées maléfiques et rassembler de nouveaux adhérents. Il pourrait alors paraître inutile de restreindre ou surveiller l'exercice des libertés fondamentales des citoyens si certains de ces nouveaux moyens de communication numérique échappent à la forte surveillance de masse issue de l'établissement de l'état d'urgence. De plus, dans le *dark web*, on peut trouver des articles journalistiques, des livres, des images, des vidéos, mais aussi de nombreux contenus illégaux (armes, drogues...). Par conséquent sur le *dark web* on trouve tout type de personne, paradoxalement il n'est pas réservé aux personnes souhaitant enfreindre la loi. Un des grands avantages du *dark web* et qu'on va étudier est qu'il réussit à garantir l'anonymat total de ses utilisateurs par une technologie de plusieurs relais et de périphériques, le VPN⁷³.

32. L'anonymat permet d'échanger des communications sur des forums, sur des réseaux sociaux, tout en protégeant sa vie privée. À cet égard, les associations de protection de l'enfance et la CNIL conseillent en particulier aux enfants et aux adolescents de ne pas utiliser leur véritable identité sur les réseaux sociaux. À l'ère du numérique l'anonymat est pour certaines internautes une méthode indispensable à l'exercice de la liberté d'expression et du droit à l'information, comme pour les lanceurs d'alerte, mais aussi à la protection de la vie privée. Afin de permettre le maintien de l'utilisation des pseudonymes tout en garantissant la lutte contre les abus et de pallier aux risques accrus de cybercriminalité, des propositions de solutions ont tenté de voir le jour et de devenir obligatoires en France. La signature numérique et par corrélation l'identité numérique sont des moyens efficaces, néanmoins elles exposent les citoyens à des risques de piratage, de vol et d'usurpation d'identité. Internet est apparu propice à l'usurpation d'identité, il avait été initialement projeté d'incriminer l'usurpation d'identité seulement lorsqu'elle était numérique. Une telle restriction pourtant ne se justifiait nullement en droit⁷⁴. C'est ainsi que

⁷³ Le Virtual private network.

⁷⁴ LEPAGE (A.), « Usurpation d'identité caractérisée par la création d'un faux site internet », Paris, *Revue mensuelle LexisNexis Comm. Com. Élect.*, janvier 2017, pp. 46-47.

la loi du 14 mars 2011⁷⁵ a incriminé sans exclusivité l'usurpation d'identité. En droit l'incrimination est donc totalement indifférente à internet, et ce à un double regard : le fait que l'usurpation d'identité soit commise sur internet n'est pas un élément constitutif de l'infraction et il n'en constitue pas davantage une circonstance aggravante⁷⁶. Si, en droit, le recours à internet n'est donc pas nécessaire à la caractérisation de cette infraction, il n'en demeure pas moins qu'en fait celle-ci trouve un terrain propice sur internet, en particulier dans les réseaux sociaux⁷⁷. Certains systèmes actuels d'authentification reposent sur des concepts datant du début des années 90. Concepts qui ont démontré leurs faiblesses technologiques et qui contiennent des failles exploitables par les *hackers*. Il faut encourager l'introduction d'un titre d'identité utilisant des technologies numériques, notamment si dans le futur les risques de piratages seront réduits à leur plus bas niveau. L'obligation d'utilisation de la signature numérique pourrait être une solution aux problèmes liés à l'impossible traçabilité des adresses IP par les utilisateurs du *dark web*.

33. L'identité numérique découle de notre activité en ligne. On peut se demander pourquoi il est nécessaire de maîtriser correctement son identité numérique. Ceci permettrait par exemple aux internautes de ne pas confondre son interlocuteur avec quelqu'un d'autre, de mieux le cerner, et de mieux comprendre les remarques, commentaires ou publications émis. De plus, si notre identité est clairement établie, il sera plus facile de faire des liens entre nos activités, la pertinence de ce qu'on publie et le poids que l'on peut porter à notre production numérique. Quand on désire intégrer un nouveau réseau, un groupe ou un collectif sur le web, notre identité peut devenir un atout ou un inconvénient pour notre intégration. Les autres personnes, membres de ces ensembles n'auront pas besoin de cerner qui on est et elles pourront se concentrer sur ce qui concerne la finalité du groupe ou du collectif. Pareillement, aujourd'hui, lorsqu'on est sur un réseau ou un groupe sur le web il est plus facile de répartir le travail si les autres personnes peuvent se fier aux données nous concernant. L'identité numérique permet d'avoir une réputation sur le web, d'être considéré par nos pairs, voire être reconnu comme un expert sur certains sujets. Les autres membres

⁷⁵ Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure.

⁷⁶ Les dispositions de l'alinéa 2 de l'article 226-4-1 énonçant que « cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne ».

⁷⁷ Par exemple avec la création d'un faux profil Facebook.

sauront qui on est. On pourrait de ce fait devenir une personne qui est contactée en cas de besoin ou afin de connaître notre avis. Sur internet il est fréquent que certains internautes mélangent leur identité numérique privée avec celle professionnelle mais il est préférable d'établir une différence entre le profil personnel et le profil professionnel notamment afin de ne pas subir des répercussions hiérarchiques. Lorsqu'on respecte certains principes de confidentialité de base on a déjà fait un grand pas en avant vers la maîtrise de notre identité numérique.

34. Internet peut aussi être utilisé pour nuire gravement à la société et à la sécurité publique. François Pellegrini souligne que : « l'ouverture des espaces numériques a naturellement conduit le législateur à y étendre son pouvoir de régulation. La loi pénale étant d'interprétation stricte, il a fallu définir de nouvelles incriminations pour les délits spécifiques au monde numérique »⁷⁸. En effet, en permettant la liberté d'accès et (éventuellement) la possibilité de se connecter sous la protection de l'anonymat⁷⁹, internet peut devenir un moyen pour commettre des infractions aux législations, telle la pédopornographie, l'apologie du terrorisme, la piraterie informatique, la violation du droit à la vie privée, etc.⁸⁰. Sans étudier toutes les facettes préoccupantes du numérique, il n'est pas inutile d'en pointer certaines qui se trouvent amplifiées par le réseau. Parmi les idéologies qui sont dangereuses sur internet, on trouve l'apologie du terrorisme djihadiste. De ce fait on devrait parvenir à réduire les risques liés à la liberté de communication et trouver les solutions juridiques les moins restrictives. En effet, les utilisations illicites d'internet ne justifieraient pas le blocage complet du réseau, notamment si l'on tient compte des innombrables bénéfices apportés pour la majorité des utilisateurs. Dans ce contexte le plus grand défi est celui de « mesurer » les droits fondamentaux, les intérêts généraux en friction ; d'un côté la protection des utilisateurs internautes, de l'autre, l'obligation de respecter la

⁷⁸ PELLEGRINI (F.), « La liberté à l'ère numérique », *Politeia* - Les Cahiers de l'Association Française des Auditeurs de l'Académie Internationale de Droit constitutionnel, Association française des auditeurs de l'Académie internationale de droit constitutionnel, 2017, Les métamorphoses des droits fondamentaux à l'ère du numérique, 31, p.161.

⁷⁹ Par un arrêt du 8 février 2017, le Conseil d'État donne raison à la CNIL d'avoir refusé d'autoriser le dispositif d'analyse des parcours de piétons de la société JC Decaux à partir de la captation de l'adresse MAC des terminaux mobiles. L'objectif de suivi individuel des flux piétons serait incompatible avec l'anonymisation. DEBET (A.), METALLINOS (N.), « Anonymisation et pseudonymisation », Paris, *Comm. Com. Électr.*, avril 2017, pp. 37-41.

⁸⁰ HALPERIN (J.-L.), « Protection de la vie privée et privacy : deux traditions juridiques différentes ? », Paris, *Les Nouveaux Cahiers du Conseil constitutionnel*, 2015, pp. 59-68.

liberté protéiforme conquise avec ce moyen de communication sans avoir recours à des restrictions disproportionnées par rapport aux objectifs à atteindre. Limiter totalement l'accès à internet signifierait violer des droits fondamentaux tels que la liberté d'expression et de communication des opinions, le droit à l'information, le droit à l'instruction et à la culture...