Le Conseil d'Etat, héraut de la révolution numérique ?

Protection des données personnelles (Conseil d'Etat)

Jean-Philippe Foegle

Édition électronique

URL : <http://journals.openedition.org/revdh/1038>

DOI : 10.4000/revdh.1038

ISSN : 2264-119X

Éditeur

Centre de recherches et d'études sur les droits fondamentaux

Référence électronique

Jean-Philippe Foegle, « Le Conseil d'Etat, héraut de la révolution numérique ? », *La Revue des droits de l'homme* [En ligne], Actualités Droits-Libertés, mis en ligne le 30 décembre 2014, consulté le 19 avril 2019. URL : <http://journals.openedition.org/revdh/1038> ; DOI : 10.4000/revdh.1038

Ce document a été généré automatiquement le 19 avril 2019.

Tous droits réservés

Le Conseil d'Etat, héraut de la révolution numérique ?

Protection des données personnelles (Conseil d'Etat)

Jean-Philippe Foegle

- 1 « Dans une période de transformations rapides, il est inévitable que le droit apparaisse comme « une force de contrainte, donc une influence négative dans un monde qui admire avant tout l'action positive » Ce constat d'une « crise dans la nature de la loi », dressé il y a un peu plus de 40 ans par le juriste Nord-Américain E. Levi¹, semble on ne peut mieux exprimer l'existence d'un « hiatus » persistant entre l'évolution des technologies et leur encadrement juridique. Le constat d'une inadaptation intrinsèque du droit aux évolutions technologiques s'est fait ressentir - loi de Moore² oblige - de manière particulièrement criante s'agissant des encadrements des technologies numériques. Les tentatives doctrinales de réconcilier droit et numérique, dont l'une des plus significative reste à ce jour celle entreprise par Lawrence Lessig³, ont conclu à un effacement du droit au profit de la technique, la régulation des comportements sur les réseaux numériques passant désormais moins par le biais du droit et de l'intervention des pouvoirs publics que par l'architecture technique du réseau internet lui-même, qui acquière « force de loi » (Code is law). Cette irrégularité apparente du numérique marque son ambivalence essentielle : elle fait du phénomène tout à la fois un facilitateur d'accès aux droits fondamentaux, et un nouveau facteur de risques pour ces mêmes droits.
- 2 En ce qu'il se défie largement de l'emprise des pouvoirs publics et conduit à une mise en réseau croissante du monde⁴, le numérique et en particulier le réseau internet constitue un puissant outil au service du renouvellement de la démocratie délibérative⁵ et de la citoyenneté participative⁶, et a conduit de facto à favoriser l'exercice d'un certain nombre de droits au nombre desquels le droit à la liberté d'expression⁷ et, de manière plus ambiguë, la liberté d'entreprendre⁸, ainsi que le droit à la vie privée⁹. L'émergence des technologies numériques a également suscité l'émergence de droits fondamentaux nouveaux tels que le droit à l'accès à internet désormais consacré à un rang supralégal¹⁰ et le droit à la protection des données personnelles, qui forme désormais

en Europe un corpus cohérent et bien distinct du droit Nord-Américain en la matière¹¹. Plus largement, comme le rappelle le rapporteur spécial de l'ONU sur la liberté d'expression Franck La Rue¹², internet, par son rôle catalyseur, « facilite aussi la réalisation d'une série d'autres droits de l'homme ».

- 3 Mais les technologies numériques sont également de nature à produire des risques supplémentaires pour les citoyens, comme le souligne longuement l'étude elle-même¹³. Outre la lutte contre les contenus illicites et attentatoires à la dignité humaine qui ont conduit à de vives controverses transatlantiques¹⁴, l'étude identifie quatre classes de risques distincts liés à un usage potentiellement indu des données personnelles dans un cadre technologique marqué tout à la fois par une profusion, une diversification et une agrégation croissante des données personnelles¹⁵. Ces risques – réels ou supposés – liés à l'expansion des usages du numérique apparaissent d'autant plus préoccupants que la structure même des réseaux numériques et leur nature extraterritoriale rend particulièrement difficile l'action des pouvoirs publics en la matière. En effet, s'il a été de longue date souligné que l'Internet n'échappe « ni en droit, ni en fait » à la puissance publique, la diversité et la complexité des intérêts en présence – et notamment les intérêts économiques de la filière numérique ainsi que les droits individuels des internautes – implique une réponse nuancée de la part de la puissance publique. La question de la régulation publique d'internet est, c'est désormais un fait établi, bien loin de se réduire à l'opposition binaire entre des Etats supposés hostiles aux libertés individuelles et un réseau par nature porteur de liberté tels que l'envisaient les fondateurs du réseau¹⁶.
- 4 Plus encore, la garantie des droits fondamentaux des internautes implique la mise en œuvre d'un certain nombre d'obligations de protéger (les usagers contre la voracité certains acteurs privés du numérique¹⁷) et d'obligations de réaliser (la liberté des internautes et l'égal accès au réseau). Les risques cités supra ont conduit dans un premier temps à une approche du sujet principalement répressive de la part des pouvoirs publics et des juridictions suprêmes, conduisant notamment, en France à la création de la très controversée Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet. La Cour européenne des droits de l'homme elle-même, si elle reconnaît et protège l'Internet en tant que vecteur de communication, tend néanmoins à faire de celui un « espace dangereux », justifiant des dérogations aux libertés plus larges que celles traditionnellement admises¹⁸. Au-delà de ce « tout répressif », la vision dominante de la gestion publique des réseaux numériques tend toutefois vers une approche décentralisatrice dite de « co-régulation »¹⁹ dans laquelle les pouvoirs publics se voient contraints de jouer à armes égales avec une multitude d'acteurs privés tels que l'IETF et l'ICANN²⁰, dont le rôle effectif est encore trop mal connu des juristes français. La rénovation de la régulation publique d'internet impliquait sans nul doute de repenser les fondements même de l'exercice de la puissance publique en la matière, le mode de gouvernance spécifique d'internet questionnant largement l'effectivité de l'intervention des Etats.
- 5 C'est donc au vu de ces enjeux multiples que le Conseil d'Etat a été conduit à mener la présente réflexion, et ce d'autant plus que le cadre politique et institutionnel semblait la rendre indispensable. La période récente a en effet été marquée sur le plan politique par les révélations de lanceurs d'alerte nord-américains sur les programmes de surveillance illégale de captation des métadonnées²¹ et des débats persistants sur la neutralité du net et ses remises en causes²² mais surtout, sur le plan juridique, par la discussion d'une

proposition de directive de la Commission Européenne destinée à remplacer le cadre juridique existant en matière de protection des données personnelles²³ et par deux décisions retentissantes²⁴ de la Cour de Justice de l'Union Européenne invalidant d'une part la directive n° 2006/24/CE autorisant la collecte de métadonnées à des fins de sécurité²⁵ et consacrant d'autre part un « droit à l'oubli » au profit des internautes²⁶.

- 6 C'est à ces enjeux multiples et complexes que répond directement l'étude. Après avoir dans une première partie rappelé – de manière très complète – les bouleversements introduits par le numérique puis souligné dans une seconde partie les enjeux juridiques que suscite l'« ambivalence » du phénomène numérique, l'étude formule en troisième partie près de 50 propositions pour « mettre le numérique au service des droits individuels et de l'intérêt général ». Ces propositions, extrêmement nuancées et largement constituées de « droit mou » et de déclarations d'intention, forment néanmoins un ensemble cohérent et semblent s'articuler en deux axes distincts mais complémentaires.
- 7 Le **premier**, qui vise à favoriser une logique explicitement qualifiée d'« empowerment »²⁷, propose d'accroître le contrôle des individus et de leurs groupements sur leurs données personnelles et créant de nouveaux droits ou en favorisant l'exercice de droits existants (1°). Le **second**, partant du constat que les principes directeurs du droit à la protection des données personnelles restent pertinents dans leur ensemble, propose néanmoins, de rénover les instruments de protection des droits fondamentaux en la matière pour garantir leur effectivité. Les propositions formulées tendent alors vers une redéfinition des modes de régulation de l'usage du numérique par les acteurs privés du secteur (2°), et proposent d'assurer de manière plus effective le respect des droits fondamentaux dans l'utilisation du numérique par les personnes publiques elles-mêmes, notamment en matière de fichage policier et de rétention des métadonnées (3°).

1°/- Garantir l'« autodétermination informationnelle » des usagers du numérique : du jargon à la pratique

- 8 Partant du constat que les usagers du numérique n'ont d'autre alternative que de se voir confrontés à un choix binaire, à savoir accepter en bloc l'ensemble des services impliquant une captation de leurs données personnelles ou « rester à l'écart du traitement de leurs données personnelles », l'étude souhaite « accroître la capacité des individus à agir pour la défense de leurs droits » en consacrant le droit à l'« autodétermination informationnelle » (Informationnelle selbstbestimmung) des internautes. Ce concept, forgé par la Cour Constitutionnelle Allemande en 1970²⁸ et inconnu en nos contrées, consiste à garantir « la capacité de l'individu à décider de la communication et de l'utilisation de ses données personnelles ». Jugeant que la reconnaissance d'un tel droit conférerait un « contenu positif » à un droit à la protection des données personnelles actuellement essentiellement défensif et rejetant résolument la reconnaissance d'un droit à la propriété des individus sur leurs données personnelles²⁹, le Conseil d'Etat propose (Proposition n° 1, p. 29) d'inscrire cette conception dans un règlement de l'Union Européenne ou, dans l'attente, dans la loi du 6 janvier 1978 modifiée. Cette première proposition, qui constitue une grille de lecture nouvelle en France du droit à la protection des données personnelles, marque l'ensemble des autres qui consistent, dans leur ensemble, à offrir aux usagers du numérique les leviers d'action

individuels et collectifs nécessaires à l'effectivité de cette « autodétermination numérique ».

- 9 Le Conseil d'Etat propose ainsi, s'agissant de la mise en place de **leviers d'action individuelle** des usagers du numérique, d'offrir à la CNIL une « mission de promotion des technologies renforçant la maîtrise des personnes sur l'utilisation de leurs données », tels que les moyens de cryptologie (Proposition n° 4, p. 276). De manière bien plus concrète et bien plus intéressante, l'étude propose de « mettre en œuvre de manière efficace » le droit au déréférencement reconnu par la CJUE (Proposition n° 5, p. 278). Constatant qu'« entre l'arrêt de la CJUE et les procédures mises en place par les exploitants des moteurs de recherche, il y a place pour une intervention des pouvoirs publics », l'Etude propose que la doctrine de mise en œuvre de l'arrêt Google Spain soit explicitée par des lignes directrices du G29 et, sur le plan procédural, que les éditeurs de sites dont le déréférencement est demandé aient la possibilité de faire valoir leurs observations, notamment au sujet de l'intérêt du public à obtenir l'information en question³⁰. Une telle réforme permettrait, aux yeux des rédacteurs de l'étude, de répondre aux principales critiques formulées à l'encontre de la décision Google Spain, et notamment les accusations de « censure privée » du net par les moteurs de recherche³¹.
- 10 Est également proposé, de manière plus ambitieuse, d'organiser par le biais d'une loi les conditions d'une décision unique de déréférencement prises par les exploitants des moteurs de recherche, pour ne pas décourager les particuliers en leur imposant de saisir individuellement l'ensemble des exploitants détenant des données personnelles les concernant. Enfin, après avoir passé en revue de manière sommaire les différents mécanismes d'« alerte éthique » mis en place depuis 2007 (Voir ADL du 20 mai 2014) et souligné que le droit d'alerter sur des faits délictueux pourrait servir de droit d'alerte en matière de données personnelle dans la mesure où « la plupart des manquements à la législation sur les données personnelles font en France l'objet d'incriminations pénales », l'étude se prononce néanmoins en vue de l'institution d'un droit d'alerte spécifique portant sur les manquements à la législation sur les données personnelles. Celui-ci, qui aurait pour vecteur une action de la CNIL, s'exercerait devant le correspondant informatique et libertés de la CNIL, concomitamment ou préalablement à la saisine de cette autorité (Proposition n° 7, p. 283).
- 11 En dernier lieu, s'agissant de la mise en place de leviers **collectifs** d'action des usagers du numérique, l'étude propose de créer, par l'intervention d'une loi, une action collective distincte de l'action de groupe instituée par la loi du 17 mars 2014 relative à la consommation³², et destinée à faire cesser les violations de la législation sur les données personnelles. Cette action serait exercée devant le tribunal de grande instance par les associations agréées de protection de consommateurs ou de défense de la vie privée et des données personnelles (Proposition n° 8, p. 285). Est également envisagé d'accroître la visibilité des usagers du numérique sur la gestion de leurs données personnelles en mettant en Open Data l'ensemble des déclarations et autorisations de traitement de données détenus par la CNIL (Proposition n° 9, p. 287). Enfin, l'étude propose de définir de manière stricte les obligations auxquelles seraient soumises les « plateformes » (Voir II de la présente étude) à l'égard des utilisateurs. Dans ce cadre, la loyauté des plateformes à l'égard de leurs utilisateurs impliquerait quatre obligations distinctes dans le but d'assurer un service optimal à leurs utilisateurs. En premier lieu, cette obligation de loyauté obligerait les plateformes à élaborer des critères de classement et de référencement (des contenus proposés) pertinents au regard de l'objectif de meilleur

service rendu aux utilisateurs, qui devraient être informés de ces critères et, in fine, pouvoir les paramétrer pour ne pas être enfermés dans une personnalisation imposée « par le haut ». En second lieu, s'agissant de retraits de contenus illicites, les plateformes se verraient imposer l'obligation de définir de manière claire les critères de retrait de contenus illicites et mettre les utilisateurs ayant mis en ligne un contenu de cette nature en mesure de faire valoir ses observations en cas de retrait de celui-ci.

*

2°/- Réformer la régulation juridique du numérique pour garantir les « intérêts collectifs » de ses usagers

- 12 Au-delà de la logique d'« empowerment » favorisée dans une première partie de l'étude, le Conseil d'Etat propose un certain nombre de réformes de la régulation du numérique, réformes supposées garantir la nouvelle « autodétermination informationnelle » des usagers du numérique. L'étude souligne en effet que « la seule affirmation de ce droit [à l'autodétermination informationnelle] ne permet pas de le rendre effectif, et les instruments de la protection des données doivent être profondément transformés pour y parvenir ». Cette transformation des instruments de protection des données est ici envisagée dans deux directions distinctes.
- 13 La première concerne la protection des internautes et usagers du numérique contre les acteurs privés, et aborde directement la question de l'architecture d'internet. L'étude aborde en premier lieu la question de la neutralité du net : formulé pour la première fois par le juriste américain Tim Wu³³, celle-ci implique que tous les opérateurs traitent de manière égale tous les flux de données quel que soit leur contenu. C'est la neutralité du réseau entendue en ce sens qui permet de faire d'assurer l'accès non discriminatoire de tous les utilisateurs au réseau et de garantir ainsi tout à la fois la liberté d'expression, l'égalité d'accès au service et la liberté d'entreprendre. Or, ce principe lié à l'architecture originelle d'Internet basée sur la règle du best effort (obligation de moyen des opérateurs d'acheminer tous les contenus sans discrimination) apparaît aujourd'hui sérieusement menacé en raison de la puissance de marché de certains éditeurs de contenus, qui apparaissent en mesure d'accaparer, à terme, la bande passante d'Internet au détriment de la masse des utilisateurs. Après avoir lié le principe au droit fondamental d'accès à internet et rappelé la convergence croissante du droit positif en la matière, en France³⁴ comme au niveau de l'Union européenne³⁵, l'Etude propose de consacrer le principe de neutralité des opérateurs de communications électroniques dans les termes votés par le parlement européen le 3 avril 2014 dans le cadre du quatrième paquet télécom, qui définit la neutralité du net 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 » (Proposition n° 3, p. 274).
- 14 Toutefois, jugeant l'approche du Parlement européen « prématurément contraignante », le Conseil d'Etat propose de tempérer ce principe de neutralité en lui apportant une série de trois dérogations, qui vident en réalité en grande partie le principe de sa portée³⁶. La première tient aux mesures de gestion de trafic³⁷, à savoir les interventions des opérateurs sur les flux de données, réalisées dans des hypothèses de congestion du réseau

en vue d'offrir des garanties en terme de qualité de service, et d'économiser la bande passante, ce qui implique généralement de privilégier certains flux au détriment d'autres dont la qualité se trouvera dégradée : le Conseil d'Etat souhaite sur ce point revenir sur la formulation adoptée par le Parlement Européen, jugée plus restrictive que la formulation adoptée par la Commission européenne³⁸. De même, l'étude préconise de revenir à une définition plus large des « services spécialisés », définie dans le texte adopté par le parlement les services « offrant une fonctionnalité nécessitant une qualité supérieure de bout en bout » tels, par exemple, que la télévision à la demande sur internet. Sur ce point, le Conseil d'Etat estime souhaitable que, pour favoriser l'innovation, ce type de services se développent tout en y apportant des contreparties, à savoir une obligation d'information préalable de l'autorité de régulation concernée, qui obtiendrait tout à la fois un droit d'opposition a priori en cas de risque manifeste de dégradation de la qualité de l'internet, et a posteriori s'il s'avère que la qualité de l'internet est effectivement dégradée. Enfin, l'étude émet le souhait que les opérateurs de communication puissent exiger, de la part des fournisseurs de contenus représentant une part significative du trafic, un paiement en vue d'accéder aux utilisateurs, et ce en vue rééquilibrer la relation entre les opérateurs de communication et certains fournisseurs de contenus.

- 15 L'étude tend également de manière regrettable à restreindre la portée du principe de neutralité d'internet en n'exigeant des plateformes aucune forme de neutralité, à rebours de réflexions plus récentes tendant au contraire à inclure celles-ci dans le périmètre de la « neutralité d'internet »³⁹. En effet, celle-ci considère que les plateformes⁴⁰ telles qu'Amazon ou Ebay, détiennent une « liberté éditoriale » consistant à hiérarchiser, organiser ou personnaliser des divers contenus selon les modalités qui leur paraît la plus pertinente, et que cette liberté doit être respectée (Proposition n° 3, p. 273). L'étude propose donc de ne soumettre celles-ci qu'à une simple obligation de loyauté à l'égard de leurs utilisateurs, loyauté qui consisterait à assurer le service de classement des contenus « de bonne foi [...] sans chercher à l'altérer ou à le détourner à des fins étrangères à l'intérêt des utilisateurs » telles que la volonté de ne pas favoriser les contenus d'un concurrent. Cet encadrement de l'activité des plateformes impliquerait préalablement de définir une catégorie autonome des « plateformes » échappant à la *summa divisio* – introduite par la Loi pour la Confiance dans l'Economie Numérique (LCEN) – entre les intermédiaires techniques et les éditeurs de contenus⁴¹ – et qui inclurait de manière relativement large 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. Dans ce cadre, et dans le but de repenser les modalités de lutte contre les contenus illicites, le régime de responsabilité pénale et civile des plateformes serait calqué sur celui des hébergeurs, dont la responsabilité n'est engagée que s'ils ont connaissance du caractère manifestement illicite de certains contenus⁴² (Proposition n° 28, p. 304).
- 16 Enfin, l'étude propose de définir de manière claire un droit des algorithmes prédictifs en garantissant leur caractère transparent et non-discriminatoire. Les algorithmes, dont l'explosion des usages correspond à l'explosion parallèle du « Big Data », sont utilisés de manière croissante tant par les plateformes – dans le but de classer les contenus selon leur intérêt⁴³ – que par les pouvoirs publics en vue d'identifier des profils « à risques »⁴⁴, génèrent des dangers pour la sauvegarde des libertés individuelles, d'autant plus que la technicité de ces algorithmes et le fait que ceux-ci soient souvent couverts par le secret industriel rend leur contrôle particulièrement ardu. L'étude identifie plus spécifiquement trois risques liés à l'usage de ces algorithmes, à savoir d'une part un risque d'enfermer les

utilisateurs dans une « personnalisation » dont ils ne seraient pas maîtres⁴⁵ et d'autre part une confiance abusive dans les résultats d'algorithmes supposés infaillibles. Plus largement, le risque lié à l'usage de ces algorithmes tient également à la possible rupture d'égalité introduite par une exploitation de plus en plus fine des données personnelles, la personnalisation à outrance pouvant favoriser les discriminations.

- 17 Pour pallier ces risques, l'étude propose d'une part, pour écarter tout risque d'accorder une confiance aveugle en ces algorithmes, d'assurer l'effectivité de l'interdiction de fonder une décision sur la seule mise en œuvre d'un traitement automatisé – déjà prévue par l'article 10 de la loi du 6 janvier 1978 modifiée – en confirmant par un instrument de droit souple (recommandation de la CNIL ou avis du G29) la nécessité d'une intervention humaine (Proposition n° 23, p. 300). D'autre part, est proposé, pour garantir la transparence d'imposer une obligation de transparence sur les données personnelles utilisées aux auteurs de décisions fondées sur un algorithme (Proposition n° 24, p. 300). Enfin, est proposé, pour pallier la difficulté technique de contrôler ces techniques particulièrement complexes, de développer les moyens humains nécessaires à la CNIL pour contrôler et observer les résultats de ces algorithmes (Proposition n° 25, p. 301), notamment dans le but de détecter d'éventuelles discriminations ou pratiques commerciales déloyales (Proposition n° 26, p. 302).

*

3°/- Assurer le respect des droits fondamentaux dans l'usage des données personnelles par les pouvoirs publics : un aggiornamento forcé

- 18 Le deuxième axe visant à garantir l'autodétermination informationnelle des usagers du numérique cette fois-ci la protection de ceux-ci contre les ingérences des autorités publiques, et aborde l'épineuse question du fichage policier au regard des récentes condamnations de la France en ce domaine.⁴⁶
- 19 Ainsi, en matière de **fichiers de police judiciaire**, l'étude, rappelant la récente condamnation de la France en raison de règles relatives au fichier automatisé des empreintes digitales (FAED), estime que la conservation de données de personnes mises en causes mais n'ayant pas fait l'objet d'une condamnation définitive ne devraient pas être remise en cause, mais que les textes autorisant les fichiers devraient préciser les conséquences à tirer des décisions judiciaires (Proposition n° 34, p. 315). L'étude cite en exemple les dispositions encadrant le fonctionnement du TAJ - dont le fonctionnement est par ailleurs loin d'être à l'abri de toute critique, sans que cela n'ait plus ému le Conseil d'Etat par le passé⁴⁷ - où une décision de relaxe ou d'acquittement devenue définitive emporte (sauf opposition du procureur de la république- effacement du fichier., et souhaite que ce type de dispositions soient étendues au FAED (par décret) et au FNAEG (par l'intervention d'une loi). Dans la continuité de cette volonté d'« apurement » des fichiers de police judiciaire, l'étude préconise également de définir un plan d'apurement du TAJ, les rapports de contrôle rendus sur ce fichier ayant montré d'importantes difficultés dans la mise en œuvre effective des décisions de justice⁴⁸ (Proposition n° 35, p. 317). De la même manière l'étude souhaite que soit mises en œuvre la décision du

Conseil Constitutionnel concernant le FNAEG⁴⁹, en modulant la durée de conservation des données dans ledit fichier en fonction de la gravité de l'infraction commise et de la minorité de la personne au moment de l'enregistrement (Proposition n° 36, p. 318). Enfin, dans le but de prévenir en amont les dysfonctionnements désormais bien connus des fichiers de police, le Conseil d'Etat suggère de faciliter les expérimentations de fichiers en allégeant la procédure actuelle⁵⁰ dans le but d'en alléger le caractère jugé trop formaliste (Proposition n° 36, p. 318).

- 20 Plus intéressant, l'étude propose de revoir le cadre de la surveillance des communications électroniques à des fins de prévention des atteintes à la sécurité nationale. Jugeant que le principe même de cette surveillance ne saurait être remis en cause, les rédacteurs de l'étude souhaitent toutefois, **en matière de conservation des métadonnées**, « tirer les conséquences » de l'arrêt Digital Rights Ireland⁵¹ de la CJUE (Proposition n° 38, p. 320), qui avait invalidé la directive n° 2006/24/CE permettant la rétention des métadonnées à des fins de sécurité, la jugeant, pour trois motifs distincts, contraire aux articles 7 et 8 de la Charte des Droits Fondamentaux de l'Union Européenne. La première tenait à ce que la directive couvrait « de manière généralisée toute personne et tous les moyens de communication électronique ainsi que l'ensemble des données relatives au trafic sans qu'aucune différenciation, limitation ni exception soient opérées en fonction de l'objectif de lutte contre les infractions graves » (§ 57). La deuxième tenait à ce que celle-ci ne prévoyait « aucun critère objectif permettant de délimiter l'accès des autorités nationales compétentes aux données et leur utilisation ultérieure » (§ 60). La troisième tenait enfin à ce que la durée de conservation avait été fixée sans tenir compte de l'utilité de la conservation au regard des finalités poursuivies (§ 63-64). S'interrogeant longuement sur la portée exacte de l'arrêt de la CJUE (V. Etude citée, p. 200-201), l'étude souligne que celui-ci peut faire l'objet d'une interprétation étroite ou large, étant entendu qu'une interprétation « large » de l'arrêt invaliderait d'office tout système de conservation systématique des métadonnées, et devrait conduire à réformer la législation Française en la matière⁵². Dans le but de prévenir toute invalidation ultérieure de la législation française, les rédacteurs de l'étude proposent, en premier lieu et compte tenu des termes de l'arrêt Digital Rights Ireland, qui ne retient comme finalité d'intérêt général justifiant l'accès aux données que la lutte contre la criminalité grave, de réserver l'accès aux métadonnées à des fins de police judiciaire et aux délits d'une gravité suffisante. Le Conseil d'Etat propose également de moduler la période accessible lors de la consultation de métadonnées « en fonction de la finalité et de la gravité des infractions » tout en étendant les règles spécifiques de protection qui bénéficient à certaines catégories de personnes (Parlementaires, avocats, magistrats).
- 21 Enfin, en lien avec l'épineuse question du contrôle des interceptions de sécurité, l'étude propose de préciser le cadre juridique des interceptions opérées à l'étranger et de l'utilisation de certains moyens d'investigation spéciaux prenant appui sur des technologies numériques telles que la géolocalisation (Propositions n° 39 et 40, pp. 321 et 322). Dans ce cadre, la loi devrait rappeler les finalités de l'interception des communications à l'étranger, qui devraient être calquées sur celles définies par l'article L 241-3 du Code de la Sécurité Intérieure. Dans cette hypothèse et dans le but de renforcer le contrôle des interceptions de sécurité, est proposé de faire de la Commission Nationale de Contrôle des Interceptions de Sécurité (CNCIS) une Autorité de contrôle des services de renseignement, dotée de moyens et de prérogatives renforcées (Proposition n° 41, p. 323). Et, notamment, la future autorité devrait être dotée de prérogatives de contrôle sur

pièces et sur place, et son champ d'action s'étendrait aux interceptions opérées à l'étranger. Enfin, prenant pour modèle les préconisations du rapport rendu par la commission mandatée par le président des Etats-Unis sur la réforme des services de renseignement⁵³, l'étude préconise de reconnaître aux agents du renseignement le droit de signaler l'existence de programmes illégaux de collectes de données, et ce selon des « modalités sécurisées » (Proposition n° 42, p. 324).

*

* *

- 22 Much ado about nothing ? Largement attendue par les acteurs du numérique et par les défenseurs des droits fondamentaux des internautes, la présente – ne boudons pas notre plaisir – répond largement aux attentes suscitées. Celle-ci aborde en effet de front, dans un contexte juridique particulièrement complexe et évolutif, un nombre important de questions en suspens, telles que les conséquences à tirer des récentes décisions de la CJUE, tout en portant des propositions qui, comme celle d'imposer aux opérateurs une obligation de neutralité, ont été de longue date portées par la société civile (qui a, par ailleurs, été largement consultée préalablement à la publication du rapport). Celui-ci marque une progression exponentielle – loi de Moore oblige ? – de la réflexion du Conseil d'Etat sur ces questions, l'approche adoptée apparaissant bien plus équilibrée que lors du précédent rapport sur ce thème, qui restait encore largement marqué par une obsession de lutte contre les contenus illicites⁵⁴.
- 23 Soulignons toutefois que la présente étude – dont nous n'avons par ailleurs réalisé qu'une présentation incomplète au regard de la densité de celle-ci – n'est pas exempte d'ambiguïtés. Si celle-ci ne peut que rassurer sur l'étendue annoncée du « droit à l'oubli » – qui ne concernera en aucune façon les sites tels que Wikipédia –, elle laisse néanmoins perplexe sur un certain nombre de points. Ainsi, la neutralité d'Internet, introduite par la grande porte tel un « produit d'appel », semble immédiatement évacuée par la porte de service tant les possibilités de dérogations envisagées sont larges et concernent des pans entiers de l'économie numérique, la volonté de préserver les intérêts économiques des plateformes ayant, de toute évidence, prévalu sur les considérations de protection de droits fondamentaux des internautes. De la même manière, bien qu'elles soient les bienvenues, les propositions de refonte du droit applicable aux interceptions de sécurité et à la rétention de métadonnées restent extrêmement évasives et prudentes, et contrastent avec les positions prises en la matière dans le cadre de l'Union européenne. Quand à la protection des lanceurs d'alerte dans le domaine du renseignement, celle-ci reste inexistante, faute de droit individuel à lancer l'alerte en la matière. Ici également, la simple évocation de la « sécurité nationale » semble, d'emblée, neutraliser la possibilité ne serait-ce que d'envisager des réformes pourtant rendues nécessaires par l'ampleur des programmes révélés par le lanceur d'alerte Edward Snowden.
- 24 Surtout, l'ensemble des propositions ne semblent relever, au final, que d'un simple aggiornamento aux évolutions juridiques en provenance du droit de l'Union européenne, ou à une simple prise de position à l'égard des réformes initiées par la Commission européenne, bien loin de la redéfinition annoncée des modes de protection des droits fondamentaux des usagers du numérique.⁵⁵ Et lorsque les propositions énoncées ne se limitent pas à une simple adaptation à des contraintes externes, celles-ci, constituées de

« droit souple », ne semblent que peu susceptibles d'être effectives. La portée limitée des propositions formulées dans l'étude ainsi que le recours au concept quelque peu jargonnant d'« empowerment » ne serait-elle pas, au fond, le marqueur d'une impuissance constatée – mais non avouée – en la matière ?

- 25 Malgré la volonté affichée d'organiser la coopération européenne et internationale en la matière, la « colonisation numérique » de l'Union européenne par les entreprises nord-américaines rend largement illusoire, en l'absence de coordination des efforts entrepris à l'échelon continental les velléités de retrouver une souveraineté en matière informationnelle, souveraineté qui conditionne pourtant la capacité des Etats européens à garantir la protection des données de leurs citoyens. Et à cet égard, certaines évolutions esquissées sur le plan international, tel que l'accord TISA dont le contenu a été révélé par le site Wikileaks⁵⁶, ne peuvent que rendre pessimiste quand à l'avenir de concepts tels que la « neutralité » du net. Malgré l'intérêt et le caractère novateur des propositions formulées dans la présente étude, celle-ci reste encore, malheureusement bien loin d'annoncer le « grand soir » en matière de protection des droits fondamentaux à l'ère numérique.

*

- 26 **Conseil d'Etat, Etude annuelle 2014, *Le numérique et les droits fondamentaux*, adoptée le 17 juillet 2014 par l'assemblée générale du Conseil d'Etat, publiée le 9 septembre 2014.**

*

Les Lettres « Actualités Droits-Libertés » (ADL) du CREDOF (pour s'y abonner) sont accessibles sur le site de la Revue des Droits de l'Homme (RevDH) – Contact

NOTES

1. LEVI (E.), "The crisis in the nature of law", dans *The Record of the Association of the Bar of the City of New-York*
2. Les lois de Moore sont des lois empiriques qui ont trait à l'évolution constante de la puissance des ordinateurs et de la complexité du matériel informatique. L'Etude rappelle que l'évolution des capacités de calcul et de stockage des ordinateurs a, en pratique, suivi cette loi. V. Etude commentée, pp. 43-44.
3. Lawrence Lessig, "Code is law." *The Industry Standard*, 1999, p.18. V., pour une traduction en langue Française de cet article : <http://www.framablog.org/index.php/post/2010/05/22/code-is-law-lessig>

4. L'étude rappelle l'évolution du nombre d'utilisateurs du réseau, qui devrait atteindre 4 milliards d'ici 2017, engendrant de nouveaux enjeux en matière de protection des données personnelles. V. Etude commentée, p. 44
5. Le Comité des Ministres du Conseil de l'Europe rappelle ainsi que l'internet « *Dournit des outils essentiels pour la participation aux activités politiques ainsi qu'à d'autres activités d'intérêt public, et aux délibérations sur ces questions.* ». V. Comité des ministres, 21 septembre 2011, recommandation sur la protection et la promotion de l'universalité, de l'intégrité et de l'ouverture de l'internet, §3
6. L'étude rappelle les différents modes de participation et de co-création que suscite internet et souligne leur potentiel en matière de promotion de la transparence de l'Etat et de la participation du public. V. Etude commentée, pp. 63-67
7. L'Assemblée Parlementaire du Conseil de l'Europe s'est ainsi félicitée de « *la rapide croissance de l'accès du grand public en général aux services médiatiques fondés sur les TIC* » qui rend, « *beaucoup plus difficile pour les régimes non démocratiques de priver leur population de l'information et de l'échange de points de vue nécessaires à tout contrôle du gouvernement par le peuple* » (V. Assemblée parlementaire, 25 avril 2012, recommandation sur la protection de la liberté d'expression et d'information sur l'Internet et les médias en ligne, § 3).
8. Le Conseil Constitutionnel, saisi d'une QPC sur l'article 45 du Code des postes et télécommunications électroniques, a ainsi créé un « droit à l'existence numérique » au profit des entreprises, en jugeant, *l'encadrement, tant pour les particuliers que pour les entreprises, du choix et de l'usage des noms de domaine sur internet affecte la liberté de communication et la liberté d'entreprendre* ». V. CC, QPC n° 2010-45 du 06 octobre 2010, M. Mathieu P., §16.
9. En effet, comme le rappelle l'étude commentée, le lien entre le droit à la vie privée et le numérique est souvent envisagé sous l'angle unique des atteintes du second au premier, alors que les réseaux permettent également de rendre plus effectif une autre facette du droit à la vie privée entendu comme « le droit pour l'individu de nouer et de développer des relations avec ses semblables (Cour EDH, 16 décembre 1992, Niemetz c. Allemagne, n° 13710/88) ». V. Etude commentée, p. 146
10. Le Conseil Constitutionnel a ainsi consacré un « droit » d'accès à internet en jugeant « *qu'en l'état actuel des moyens de communication et eu égard au développement généralisé des services [Internet] ainsi qu'à l'importance prise par ces services pour la participation à la vie démocratique et l'expression des idées et des opinions, ce droit implique la liberté d'accéder à ces services* ». V. CC, DC n° 2009-580 du 10 juin 2009, Loi favorisant la diffusion et la protection de la création sur internet, §5
11. L'étude rappelle que les différentes normes applicables en la matière (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 quand aux principales garanties en matière de protection des données personnelles : Qualité des données ; exigence du consentement de la personne concernée ; interdiction de la collecte de données sensibles ; droits d'information, d'accès et de rectification ; obligations de sécurité du responsable du traitement ; existence d'une autorité indépendante de contrôle. V. Etude commentée, p. 9.
12. Frank La Rue, *Report of the Special Rapporteur on the promotion of the right to freedom of opinion and expression*, Nations Unies, mai 2011.
13. Etude commentée, Partie II ; « *L'ambivalence du numérique nécessite de repenser la protection des droits fondamentaux* ».
14. V., sur ces questions : Amélie Robitaille-Froidure, *La liberté d'expression face au racisme : étude de droit comparé franco-américain*. Editions L'Harmattan, 2011 ; *Liberté d'expression et protection du mineur sur Internet : étude comparée des droits français et américain à l'aune du droit européen et international*, LGDJ, 2013.

15. Il s'agit des risques suivants : Captation des données personnelles sans consentement ; ciblage de données personnelles pour des pratiques commerciales non consenties ; utilisation disproportionnée des données personnelles ; utilisation détournée, abusive ou malveillante des données personnelles. V. Etude citée, p. 164
16. L'étude cite ici les propos d'un des fondateurs du réseau, David Clark : « *We reject kings, presidents and voting. We believe in : rough consensus and running code* ». Etude commentée, p. 133
17. L' Etude cite ainsi l'exemple des « *Data Brokers* », nouveaux acteurs du numérique dont le modèle économique est basé sur la captation et la revente des données personnelles, avec un risque d'agrégation des données particulièrement risqué pour les internautes. V. Etude citée, p. 158.
18. V. TRÉGUER, Félix, 2013, « Internet dans la jurisprudence de la Cour européenne des droits de l'Homme », *Revue des droits et libertés fondamentaux* , 20 mai 2013.
19. Cette approche, également qualifiée de paradigme multistakeholder, a été mentionnée pour la première fois dans le rapport du Conseil d'Etat "Internet et les réseaux numériques" et apparaît également dominante dans la déclaration (non contraignante) de la Réunion Mondiale Multipartite sur l'Avenir de la Gouvernance de l'Internet.
20. L'ICANN joue un rôle de coordination des noms de domaine tandis que l'IETF définit, par des règles de droit souple, les standards techniques appliqués à l'Internet. La forte influence des Etats-Unis sur ces instances et le fonctionnement opaque de ces institutions a été maintes fois dénoncée. V notamment Rolf Weber, Shawn Gunnarson. "A constitutional solution for internet governance." *Colum. Sci. & Tech. L. Rev*, vol XII. Cité dans Etude commentée, p. 135-136.
21. Il s'agit principalement du programme PRISM. V, sur les aspects juridiques de ce programme : Résolution du Parlement Européen du 12 mars 2014 sur le programme de surveillance de la NSA, les organismes de surveillance dans divers Etats-Membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique et matière de justice et d'affaires intérieures, n° 2013/2188(INI) ; G29, Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes, avril 2014, WP 215.V. également Cour EDH, 4^e Sect. Décision de communication du 17 janvier 2014, Big Brother Watch et autres c. Royaume-Uni, Req. n° 58170/13 ; v. aussi la récente annonce de l'introduction d'une nouvelle requête : Aimee Hamilton, « Application filed with ECHR to protect UK investigative journalism from surveillance », in Index, 15 septembre 2014.
22. Voir notamment l'avis de la Quadrature du Net sur cette question.
23. (COM(2012)0010 – C7-0024/2012 – 2012/0010(COD)
24. Certains membres de la doctrine ont parlé de « Révolution numérique » du juge de l'Union. V Denys Simon « La révolution numérique du juge de l'union – les premiers pas de la cybercitoyenneté », *Revue Europe*, vol. 24, N° 7, 2014 , pages. 4-9
25. CJUE, Grande Chambre, 8 avril 2014, Digital Rights Ireland Ltd & Michael Seitlinger e.a. , affaires jointes C-293/12 & C-594/12. Pour un commentaire éclairant de cette affaire la lettre ADL du 14 mai 2014 de Marie-Laure Basilien-Gainche.
26. CJUE, Grande Chambre, 13 mai 2014, Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos et Mario Costeja González, Aff. C-131/12 – ADL du 16 juin 2014
27. L'empowerment désigne l'octroi de plus de pouvoir aux individus ou aux groupes pour agir sur les conditions sociales, économiques, politiques ou écologiques qu'ils subissent.
28. BverfG, 1 BvR 518/02, 4 avril 2006
29. Cette solution avait été proposée par de nombreux auteurs français (Alain Bensoussan, « Vie privée à l'horizon 2010. Paroles d'experts » *Cahier IP Innovation et prospective*) et Nord-américains (Lawrence Lessig dans la première édition de « code is law »). Le conseil d'Etat rejette cette solution en relevant d'une part que cette solution ne parviendrait pas à rééquilibrer la relation

entre les usagers et les éditeurs de services numériques en raison de la valeur marchande individuelle faible des données personnelles des internautes et d'autre part qu'une telle solution supprimerait la possibilité pour les pouvoirs publics d'imposer des limites à la capacité des individus de décider de l'utilisation de leurs données personnelles. Etude commentée, pp. 454-455.

30. Dans l'arrêt Google Spain, la CJUE avait précisé que la Cour précise que le droit au déréférencement ne pourrait être exercé si « *pour des raisons particulières, telles que le rôle joué par ladite personne dans la vie publique, que l'ingérence dans ses droits fondamentaux est **justifiée par l'intérêt prépondérant dudit public à avoir, du fait de cette inclusion, accès à l'information en question*** » (CJUE, Grande Chambre, 13 mai 2014, Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos et Mario Costeja González, Aff. C-131/12, § 97 – ADL du 16 juin 2014)

31. V. sur ce point la position de la Quadrature du Net : « Droit à l'oubli » : la CNIL s'adoue censeur du net.

32. L'Etude souligne que l'action de groupe instaurée par cette loi ne s'applique que difficilement en matière de protection des données personnelles, puisque celle-ci ne concerne que la réparation des préjudices patrimoniaux alors que le préjudice subi en raison d'un usage indu des données personnelles est en général un préjudice d'ordre moral. Etude commentée p. 283-284.

33. Tim Wu, "Network neutrality, broadband discrimination." *J. on Telecomm. & High Tech. L.* 2, 2003, p. 141.

34. L'ARCEP a formulé en 2010 un instrument de droit souple énonçant quatre principes non-contraignants en matière d'accès à internet, et qui apparaissent très proches des réflexions européennes en la matière. V. ARCEP, « Neutralité de l'internet et des réseaux. Propositions et recommandations », Septembre 2010.

35. La proposition de règlement dite « quatrième paquet télécom » (2013/0309(COD)) reconnaît à son article 23 le principe de neutralité du net dans des termes très proches des recommandations de l'ARCEP.

36. V. sur ce point la critique radicale mais non dénuée de fondement de Guillaume Champeau.

37. Définie par l'ARCEP comme « *toutes les formes d'intervention sur les flux de données mises en oeuvre et prenant en compte la nature du trafic, ou encore l'identité et la qualité de son émetteur et de son destinataire* ». V. ARCEP, « Neutralité de l'internet et des réseaux. Propositions et recommandations », Septembre 2010.

38. La position du parlement européen supprime la possibilité de mesures de gestion du trafic destinées à prévenir les communications non sollicitées et exige que la congestion du réseau soit « *temporaire et exceptionnelle* », à l'inverse de la Commission Européenne qui exigeait que celle-ci soit temporaire **ou** exceptionnelle.

39. V. Conseil National du Numérique, « Neutralité des plateformes : réunir les conditions d'un environnement numérique ouvert et soutenable », 26 juin 2014.

40. L'expression désignant ici tous les sites servant de portail d'accès à des contenus de sites tiers, et recouvre notamment les moteurs de recherche, les réseaux sociaux, les sites de partage de contenus et les « magasins d'application » des téléphones mobiles. Etude commentée, p. 97.

41. L'article 6 de la loi prévoit cette division, qui se fonde sur l'idée selon laquelle les intermédiaires techniques tels que les hébergeurs n'ont qu'un rôle « passif », n'ayant pas connaissance des informations qu'ils stockent. Or, nombre de plateformes ne se contentent pas de ce rôle passif et ne peuvent bénéficier du régime de responsabilité limitée accordé aux intermédiaires techniques. De nombreux arrêts ont ainsi refusé la qualification d'hébergeur (l'hébergeur étant un intermédiaire technique selon l'article 2. du II de la LCEN) à des

plateformes telles qu'Ebay (V. par ex CJUE, Grande Chambre, L'Oreal e.a, 12 juillet 2011, Aff. C-324/09). Etude citée, p. 219

42. CC, DC n° 2003-496 du 10 juin 2004, §9.

43. L'étude cite l'exemple du « Newsfeed » de Facebook.

44. L'étude cite l'exemple du fichier « PNR » prévu par l'article 17 de la loi de programmation militaire du 18 décembre 2013, qui permet d'identifier les passagers aériens « à risques ».

45. V. Michael Fertik, « The Rich See a Different Internet Than the Poor », *Scientific American*, vol. 308, 15 janvier 2013.

46. V. Nicolas Hervieu, « Le fichage policier sous les fourches caudines européennes », *La Revue des droits de l'homme*, Actualités Droits-Libertés, mis en ligne le 19 septembre 2014

47. V. Marc Duranton et Jean-Philippe Foegle, « Fichage partout, oubli nulle part ? Le Conseil d'Etat ouvre un boulevard au fichier « TAJ » », *La Revue des droits de l'homme*, Actualités Droits-Libertés, mis en ligne le 16 juillet 2014

48. V. CNIL, Conclusions du contrôle des fichiers d'antécédents du ministère de l'intérieur, Juin 2013.

49. Dans sa décision n° 2010-25 QPC du 16 septembre 2010, le Conseil Constitutionnel avait, par une réserve d'interprétation, rappelé (§18) qu'il incombe au pouvoir réglementaire « de proportionner la durée de conservation des données personnelles, compte tenu de l'objet du fichier, à la nature ou à la gravité des infractions concernées tout en adaptant ces modalités aux spécificités de la délinquance des mineurs ». V. pour un commentaire de cette affaire : Conseil constitutionnel, Décision 2010-25 QPC, 16 septembre 2010, M. Jean-Victor C. [PDF] - Actualités droits-libertés du 18 septembre 2010 par Cédric ROULHAC

50. Les articles 26 et 27 de la loi du 6 janvier 1978 modifiée subordonnent l'autorisation d'un fichier de police) un arrêté ministériel pris après avis de la CNIL ou en décret en Conseil d'Etat pris après avis de la CNIL.

51. CJUE, Grande Chambre, 8 avril 2014, Digital Rights Ireland Ltd & Michael Seitlinger e.a. , affaires jointes C-293/12 & C-594/12.

52. Outre l'accès aux métadonnées à des fins de sécurité intérieure (article L 241-2 du code de la sécurité intérieure), des organismes non-juridictionnels ont également accès aux métadonnées à des fins de lutte contre la contrefaçon (HADOPI) ou de sécurité des systèmes d'information (ANSSI).

53. V. Liberty and Security in a Changing World, décembre 2013.

54. Conseil d'Etat, "Internet et les réseaux numériques", 1998.

55. Pour un constat similaire, v. Roseline Letteron, Le numérique et les droits fondamentaux : le rapport du Conseil d'Etat, 16 septembre 2014.

56. V. sur ce point : Tisa, l'accord qui menace données personnelles, neutralité du net et exception culturelle, Nextimpact, 18 décembre 2014.

RÉSUMÉS

Le 17 juillet 2014, l'assemblée générale du Conseil d'Etat a adopté son rapport annuel, intitulé « Le numérique et les droits fondamentaux » et publié le 9 septembre 2014. Premier du genre au Palais-Royal depuis l'étude thématique de 1998 intitulée « Internet et les réseaux numériques », celui-ci suscitait de fortes attentes de la part des acteurs de l'économie numérique et des défenseurs des droits de l'homme. Bien

que relativement timide sur certains points, le rapport introduit de nombreuses propositions que l'on pourrait qualifier d' « innovantes ». Identifiant un certain nombre de risques liés à l'usage des technologies numériques et partant du postulat que celles-ci ont opéré une profonde transformation du contenu et du mode d'exercice des droits fondamentaux, le rapport propose de refonder la protection des droits fondamentaux dans le cadre des technologies numériques dans deux directions distinctes. La première, qui vise à favoriser une logique explicitement qualifiée d'« empowerment », propose d'ouvrir aux usagers du numérique de nouveaux droits et de mettre en place les conditions nécessaires à la garantie de l'effectivité des droits existants. La seconde, partant du constat que les principes directeurs du droit à la protection des données personnelles restent pertinents dans leur ensemble, propose néanmoins, de rénover les instruments de protection des droits fondamentaux en la matière pour garantir leur effectivité.

AUTEUR

JEAN-PHILIPPE FOEGLE

Doctorant en droit public (CREDOF - Université Paris Ouest Nanterre) et allocataire doctoral (Conseil régional d'Ile de France)