



NUMÉRIQUE ET LIBERTÉS :  
**Un nouvel âge  
démocratique**

Rapport n° 3119

Présenté par  
**M. Christian PAUL  
et Mme Christiane FÉRAL-SCHUHL**  
Co-Présidents

XIV<sup>E</sup> LÉGISLATURE

COMMISSION DE RÉFLEXION ET DE PROPOSIT  
SUR LE DROIT ET LES LIBERTÉS À L'ÂGE DU NUMÉI



## Composition de la Commission

### *Co-présidents :*

**M. Christian Paul**, député de la Nièvre, Groupe Socialiste, républicain et citoyen ;  
**Mme Christiane Féral-Schuhl**, ancien bâtonnier de l'Ordre des avocats du barreau de Paris (2012-2014), avocate au barreau de Paris depuis 1981 spécialisée en droit de l'informatique et des nouvelles technologies, cofondatrice du cabinet Féral-Schuhl-Sainte-Marie, ancienne présidente du conseil d'administration de l'Association de droit de l'informatique juridique (2000-2010) ;

### *Députés :*

**M. Patrick Bloche**, député de Paris, Groupe Socialiste, républicain et citoyen ;  
**M. Sergio Coronado**, député des Français établis hors de France, Groupe Écologiste ;  
**M. Charles de Courson**, député de la Marne, Groupe Union des démocrates et indépendants ;  
**Mme Virginie Duby-Muller**, députée de Haute-Savoie, Groupe Les Républicains ;  
**Mme Laurence Dumont**, députée du Calvados, Groupe Socialiste, républicain et citoyen ;  
**Mme Corinne Erhel**, députée des Côtes-d'Armor, Groupe Socialiste, républicain et citoyen ;  
**Mme Gilda Hobert**, députée du Rhône, Groupe Radical, républicain, démocrate et progressiste ;  
**Mme Laure de La Raudière**, députée de l'Eure-et-Loir, Groupe Les Républicains ;  
**Mme Martine Martinel**, députée de Haute-Garonne, Groupe Socialiste, républicain et citoyen ;  
**M. Franck Riester**, député de Seine-et-Marne, Groupe Les Républicains ;  
**M. Gabriel Serville**, député de Guyane, Groupe Gauche démocrate et républicaine ;  
**M. Patrice Verchère**, député du Rhône, Groupe Les Républicains ;

### *Personnalités qualifiées :*

**M. Philippe Aigrain**, informaticien et chercheur, ancien directeur du secteur technique du logiciel à la Commission européenne (1996-2003), fondateur et président-directeur-général de Sopinspace, qui développe notamment des logiciels libres, co-fondateur de La Quadrature du net ;  
**M. Godefroy Beauvallet**, ingénieur en chef des télécommunications, directeur du fonds AXA pour la recherche, membre du Conseil national du numérique, maître de conférence associé à Télécom ParisTech ;  
**Mme Valérie-Laure Benabou**, professeur des universités, professeur agrégé de droit privé à l'Université de Versailles Saint-Quentin-en-Yvelines, personnalité qualifiée au Conseil supérieur de la propriété littéraire et artistique ;  
**M. Jean Dionis du Séjour**, maire d'Agen, ancien député, rapporteur au nom de la commission des affaires économiques de la loi pour la confiance dans l'économie numérique en 2003-2004 ;  
**M. Daniel Le Métayer**, directeur de recherche à l'INRIA, établissement public de recherche dédié aux sciences du numérique, au centre de recherche Grenoble – Rhône-Alpes à Lyon responsable de l'INRIA Project Lab CAPPRIS (Collaborative Action on the Protection of Privacy Rights in the Information Society) ;  
**M. Winston Maxwell**, avocat associé du cabinet Hogan Lovells, spécialiste des droits français et européen des communications, du droit des médias et de la neutralité du net, co-président du comité sur l'économie numérique de la chambre de commerce franco-américaine ;  
**Mme Francesca Musiani**, sociologue, chercheuse à MINES ParisTech, docteur en socio-économie de l'innovation (Thèse intitulée « Nains sans géants. Architecture décentralisée et services Internet », lauréate du prix de thèse « Informatique et Libertés » de la CNIL en 2014) ;  
**M. Edwy Plenel**, journaliste, président et directeur de la publication du site d'information en ligne Mediapart, ancien directeur de la rédaction du Monde, secrétaire général du Syndicat de la presse indépendante d'information en ligne (SPIIL) ;  
**Mme Myriam Quémener**, magistrate au parquet général de la cour d'appel de Versailles, précédemment sous-directrice de la justice pénale générale à la direction des affaires criminelles et des grâces au ministère de la Justice (2004-2007), substitue du procureur général près la cour d'appel de Versailles (2007-2012), procureur de la République adjoint près le tribunal de grande instance de Créteil (2012-2013) ;  
**Mme Thaima Samman**, avocate, membre des barreaux de Paris et Bruxelles, anciennement directrice du département juridique et affaires publiques à Microsoft France puis Associate General Counsel, Senior Director Corporate Affairs/CSR à Microsoft Europe, Moyen-Orient et Afrique ;  
**M. Henri Verdier**, directeur de la mission Etalab au secrétariat général pour la modernisation de l'action publique, entrepreneur numérique (associé et co-fondateur de la société MFG-R&D), personnalité qualifiée au sein du comité de prospective de l'ARCEP ;  
**M. Cyril Zimmermann**, fondateur et président-directeur-général de Hi-Media, entreprise française spécialisée dans la monétisation de l'audience, et de Hi-Cab, société de moto-taxi, président de l'Acsel, l'association de l'économie numérique.

### III. CONTRIBUTIONS AU GROUPE DE TRAVAIL SUR LA VIE PRIVÉE

#### A. CONTRIBUTION DE M. WINSTON MAXWELL : LA NOTION DE CONSENTEMENT

Le consentement est l'un des fondements de la protection des données à caractère personnel. Reconnue comme un droit fondamental en Europe, la protection des données personnelles est un élément de la liberté individuelle : sans une certaine maîtrise de ce qui est divulgué à propos de soi, l'individu perd son autonomie par rapport aux autres. Le contrôle par chaque individu de ses données va donc au cœur de l'autodétermination informationnelle de l'individu <sup>(1)</sup>.

Traditionnellement, cette maîtrise sur les données à caractère personnel se manifeste à travers le consentement de l'individu. Si l'individu donne son consentement, il exprime sa liberté de choix par rapport à ses données à caractère personnel. Un consentement éclairé et librement consenti permet de procéder à la plupart des traitements de données à caractère personnel. L'autonomie de chacun est respectée.

Dans un environnement numérique, le consentement trouve néanmoins ses limites. Comme l'a exprimé la Présidente de la CNIL devant notre Commission, chaque individu est entouré d'une multitude de traitements par de nombreux réseaux et services numériques qui régissent une partie de nos vies en permanence. Dans ce contexte, l'idée que chaque individu peut donner son consentement pour chaque traitement est illusoire.

Selon le Conseil d'État :

*« 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 » <sup>(2)</sup>.*

La plupart des fournisseurs de services numériques s'appuient sur des conditions générales d'utilisation. Avant d'utiliser le service, le consommateur coche une case indiquant qu'il a lu les conditions et qu'il les accepte. Comme l'a souligné le Conseil d'État dans son étude de juillet 2014 <sup>(3)</sup>, même le consommateur le plus attentif ne pourra prendre le temps de lire ces conditions d'utilisation. Et même s'il prenait le temps, le consommateur ne serait pas en mesure d'apprécier les risques encourus par telle ou telle utilisation de ses données personnelles. Les risques sont abstraits, et les conditions d'utilisation ne permettent pas de les apprécier. Par ailleurs, les fournisseurs de service ne sont pas en mesure d'offrir une alternative au consommateur. Si le consommateur souhaite utiliser un service numérique, il doit accepter les conditions d'utilisation telles qu'elles. Un grand nombre de ces services sont fournis gratuitement, ce qui signifie que leur modèle économique peut s'appuyer sur la vente de publicités. La vente de publicités s'appuie à son tour sur l'analyse de données à caractère personnel. Si le consommateur souhaite bénéficier d'un service gratuit, il devra généralement accepter que le service utilise ses données.

Les conditions d'utilisation étant trop longues, le consentement de l'individu peut également être sollicité par des fenêtres *pop-up* que le consommateur accepte au fur et à

---

(1) Conseil d'État, op. cit., p. 268.

(2) Ibid, p. 18.

(3) Ibid., p. 176.

mesure de son utilisation du service. L'utilisation répétée de fenêtres *pop-up* peut agacer le consommateur au point où il ne regarde plus les messages et les accepte systématiquement.

Le consentement s'avère donc souvent inefficace. Ce constat est appuyé par de nombreuses études en psychologie et en économie comportementale. Acquisti *et al.* <sup>(1)</sup> ont démontré que la plupart des individus attachent une valeur faible à la protection de leurs données personnelles. Dans leur étude, 71 % des personnes ont accepté d'échanger leur mot de passe contre une barre de chocolat. Dans une autre étude, l'équipe d'Acquisti a démontré que les consommateurs qui bénéficient de mécanismes de contrôle de leurs données sur une plateforme numérique sont plus susceptibles de communiquer des données sensibles. Donner plus de moyens de contrôle aux consommateurs peut paradoxalement les inciter à être moins vigilantes <sup>(2)</sup>.

D'autres tests confirment que les consommateurs ne lisent pas ce qu'ils acceptent : dans une expérimentation, 7 500 personnes ont donné leur accord pour céder leur âme pour l'éternité à un fournisseur de service :

*« Hardly anyone reads privacy policies. To give an example, an English company obtained the soul of 7500 people. According to its terms and conditions, customers granted "a non transferable option to claim, for now and for ever more, your immortal soul," unless they opted out. The company later said it wouldn't exercise its rights »* <sup>(3)</sup>.

Ces phénomènes commencent à être bien compris par les psychologues et les économistes.

Si le consentement est une fausse bonne idée, que proposer à sa place ?

Dans la législation actuelle, le consentement n'est pas le seul fondement pour un traitement. Il existe notamment la notion « d'intérêt légitime » accompagné de mesures destinées à protéger les individus. L'intérêt public peut également justifier, dans certains cas, un traitement sans le consentement de l'individu <sup>(4)</sup>.

Nissenbaum <sup>(5)</sup> propose d'imposer des règles de traitement qui varieraient selon le contexte dans lequel les données sont collectées. Cette approche reconnaît un consentement implicite pour tout traitement qui découlerait naturellement du contexte d'origine de la collecte de données. Un traitement qui sortirait de ce contexte nécessiterait un consentement explicite. Cette idée n'est pas loin de celle du groupe article 29 (G29), qui reconnaît la possibilité d'effectuer des traitements pour des finalités qui ne sont pas "incompatibles" avec la finalité d'origine <sup>(6)</sup>. Une finalité « incompatible » nécessiterait le recours à un consentement explicite. Une finalité « compatible » ne nécessiterait pas de consentement.

Le Forum économique mondial préconise la notion d'« empowerment » au lieu de la notion plus formaliste de consentement <sup>(7)</sup>.

---

(1) A. Acquisti, L. John, G. Loewenstein, « What is privacy worth ? », 2004.

(2) L. Brandimarte, A. Acquisti, G. Loewenstein, « Misplaced confidences : privacy and the control paradox », WEIS Working Paper, 2010.

(3) F. Z. Borgesius, « Consent to behavioural targeting in european law – What are the policy implications of insights from behavioural economics ? », Amsterdam Law School Legal Studies Research Paper, n° 2013-43, p. 31.

(4) Article 7 de la loi n° 17-78 du 6 janvier 1978 précitée.

(5) H. Nissenbaum, « Privacy as Contextual Integrity », Wash. L. Rev., 2004.

(6) Article 29 Working Party, « Opinion 03/2013 on Purpose Limitation », WP 203, 2 avril 2013.

(7) World Economic Forum, « Unlocking the value of personal data : from collection to usage », février 2013. Voir également Conseil d'État, op. cit., p. 170.

Constatant l'inefficacité du consentement dans un environnement numérique, Borgesius<sup>(1)</sup> propose que le législateur définisse une zone d'utilisations « normales » de données, par exemple en matière de publicité ciblée. À l'intérieur de cette zone de normalité, le consentement du consommateur ne serait pas nécessaire. En revanche, une utilisation qui sortirait de cette zone de normalité nécessiterait un consentement renforcé. Ce consentement renforcé se manifesterait par au moins 3 clics de souris, par exemple, ou par un appel téléphonique, ou par l'envoi d'une lettre... Pour certains types de traitement, le législateur pourrait imposer une interdiction totale. C'est le cas en France, par exemple, pour les traitements de données ADN en dehors de la recherche médicale.

La difficulté pour le législateur serait de définir ces « zones de normalité », qui peuvent évoluer avec le temps. La définition nécessiterait une étude d'impact, et la prise en compte d'aspects dynamiques, autant culturels et économiques. Ce travail pourrait être confié au régulateur, par exemple à la CNIL en France.

La CNIL effectue déjà ce genre d'évaluation lorsqu'elle élabore des normes simplifiées ou des autorisations uniques pour certains traitements. Ces normes simplifiées et autorisations uniques définissent une zone de traitement acceptable à l'intérieur de laquelle le consentement individuel n'est généralement pas nécessaire. Cette piste pourrait être privilégiée, le consentement étant réservé à des utilisations qui sortent de l'ordinaire et qui surprennent par rapport au contexte d'origine de la collecte<sup>(2)</sup>.

---

(1) F. Z. Borgesius, « Consent to behavioural targeting in european law – What are the policy implications of insights from behavioural economics? », Amsterdam Law School Legal Studies Research Paper, n° 2013-43.

(2) Selon le Conseil d'État, « collecter des données de manière déloyale, c'est surprendre la confiance de la personne concernée et commettre ainsi une faute à son égard » in *Conseil d'État*, op. cit., p. 173.