CNCDH

COMMISSION NATIONALE
CONSULTATIVE
DES DROITS DE L'HOMME

RÉPUBLIQUE FRANÇAISE

AVIS

# AVIS «PROTECTION DE LA VIE PRIVÉE À L'ÈRE NUMÉRIQUE »

22 MAI 2018

*L'Avis «Protection de la vie privée à l'ère numérique »*
*a été adopté à l'unanimité*
*lors de l'Assemblée plénière du 22 mai 2018.*

# Table des matières

Depuis 1995, date de l'entrée en vigueur de la directive européenne sur le traitement des données à caractère personnel[1] , les capacités de stockage, de traitement et de circulation des ordinateurs ont été multipliées par 1000. L'Internet, désormais à travers également les objets connectés, est devenu omniprésent. En 2025, on évalue à 4 800 par jour les connexions entre les personnes et les objets connectés[2]. L'évolution technologique elle-même connaît un décuplement sans précédent, à travers la combinaison des technologies et des nanotechnologies. Alors que l'audience des réseaux sociaux croît par ailleurs à un rythme considérable (2.9 milliards de personnes sont actives sur les réseaux sociaux, soit 39% de la population mondiale), force est de constater que le numérique, en investissant, pour un grand nombre de personnes, quasiment tous les champs de la vie sociale, transforme les grands équilibres classiques entre sphère privée et sphère publique.

S'il n'existe pas de définition formelle de la vie privée[3], le nombre d'instruments internationaux y faisant référence et l'abondance de la jurisprudence la concernant suffisent à l'élever au rang de droit fondamental. Le droit à la vie privée est notamment énoncé dans la Déclaration universelle des droits de l'homme (article 12), dans le Pacte international relatif aux droits civils et politiques (article 17), et dans la Convention de sauvegarde des droits de l'homme et des libertés fondamentales (article 8). Il est également garanti par l'article 7 de la Charte des droits fondamentaux de l'Union Européenne. Cette absence de contours stricts laisse une marge d'appréciation aux États pour en garantir la protection. En France, le droit au respect de la vie privé figure à l'article 9 du code civil[4]. Le droit au respect de la vie privée est absent des Constitutions de 1946 et de 1958, mais le Conseil constitutionnel lui reconnaît une valeur constitutionnelle, et ce, sur le fondement de l'article 2 de la Déclaration des droits de l'homme et du citoyen[5] ; le Conseil constitutionnel fait par ailleurs de la vie privée une composante de la liberté individuelle[6].

La notion de vie privée englobe à la fois la notion d'intimité et celle d'autonomie de la personne. Dans une perspective classique, la vie privée correspond à la « *sphère secrète de la vie d'où [l'individu] aura le pouvoir d'écarter les tiers* »[7]. Il s'agit d'abord de permettre à l'individu de s'opposer à toute intrusion non consentie dans sa sphère intime. Le droit au respect de la vie privée est donc un « droit de se masquer » qui vaut

1 Directive n° 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative *à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*.

2 Yves Poullet, « Règlement européen sur la protection des données : quels enjeux ? » Conférence à l'IEP de Paris le 9 mars 2018.

3 Le juge de la CEDH se serait gardé de la définir en termes stricts, précisément afin de tenir compte des évolutions sociales et technologiques : Ursula Kelly, *Le droit au respect de la vie privée et familiale : un guide de mise en œuvre de l'article 8 de la Convention européenne des droits de l'homme*, Conseil de l'Europe, 2003.

4 Code civil, article 9 : « *Chacun a droit au respect de sa vie privée* ».

5 Conseil constitutionnel, Décision n° 99-419 DC du 9 novembre 1999, considérant 73.

6 Conseil constitutionnel, Décision n° 94-352 DC du 18 janvier 1995, considérant 3.

7 Carbonnier, J., Droit civil, volume 1, Paris : PUF, 2004, p. 518.

pour tout individu[8], dans toutes les sphères de la vie sociale, y compris dans les relations de travail. La protection de l'intimité de la personne porte à la fois sur l'ensemble des éléments matériels (son patrimoine, son domicile, ses correspondances) et immatériels de la vie d'une personne (son image, son corps, sa vie amoureuse et spirituelle). Le droit au respect de l'intimité, pour fondamental qu'il soit, n'est pas cependant pas absolu. Ainsi, si les immixtions dans la vie privée d'autrui sont, en principe, illicites[9], il peut exister des ingérences étatiques légitimes, par exemple pour la protection de la liberté d'expression ou la lutte contre la criminalité[10]. Il convient alors de trouver un juste équilibre entre les différents intérêts fondamentaux en présence.

Plus récemment, sous l'influence de la jurisprudence de la Cour européenne des droits de l'homme, la notion de vie privée a évolué, pour englober la sphère au sein de laquelle toute personne peut librement se construire et s'épanouir dans ses relations avec autrui et le monde extérieur. Le droit au respect de la vie privée est donc également un « droit de se découvrir », que garantit le respect de l'identité de la personne. Ainsi, la Cour européenne des droits de l'homme fait de la vie privée « *une notion large qui englobe, entre autres, des aspects de l'identité physique et sociale d'un individu, notamment le droit à l'autonomie personnelle, le droit au développement personnel et le droit d'établir et entretenir des rapports avec d'autres êtres humains et le monde extérieur* »[11]. Bien plus, la Cour estime que la protection de la vie privée implique également la reconnaissance au profit de chaque individu d'une « *capacité à être soi-même* » : « *Sur le terrain de l'article 8 de la Convention en particulier, où la notion d'autonomie personnelle reflète un principe important qui sous-tend l'interprétation des garanties de cette disposition, la sphère personnelle de chaque individu est protégée, y compris le droit pour chacun d'établir les détails de son identité d'être humain* »[12]. Cette conception étendue de la vie privée, entendue comme une protection de l'autonomie de la personne et de son droit à l'autodétermination, a des répercussions en termes d'indisponibilité de l'état-civil des personnes (nom, sexe) et de protection des relations affectives (familiales, amoureuses et sexuelles).

Le droit au respect de la vie privée comporte donc deux composantes : un droit « interne » de préserver sa sphère d'intimité des intrusions extérieures, et un droit « externe » de déployer librement sa personnalité dans la vie sociale, notamment en communiquant ses informations personnelles selon sa convenance. L'extension croissante des domaines de la vie connectés soulève évidemment de nombreuses questions en matière de protection de la vie privée ; son régime juridique ne doit pas être moins exigeant dans la vie numérique que dans la réalité physique. En effet, compte tenu de leur maîtrise sur de nombreuses données personnelles numériques, les

8 1ère Civ. 23 octobre 1990, pourvoi n°89-13.163, Bulletin 1990 n°222 : « *Toute personne, quels que soient son rang, sa naissance, sa fortune, ses fonctions présentes ou à venir, a droit au respect de sa vie privée* ».
9 1ère Civ. 6 mars 1996, pourvoi n°94-11.273, Bulletin 1996 I n° 124.
10 Telles que la publication d'informations personnelles de personnalités politiques, susceptibles de jouer un rôle dans la formation de l'opinion publique.
11 CEDH, Pretty c/ Royaume-Uni, 29 avril 2002.
12 CEDH, Christine Goodwin c/ Royaume-Uni, Grande chambre, 11 juillet 2002, req. n°28957/95.

grands groupes internationaux, notamment les GAFAM[13], ont désormais une emprise considérable sur nos vies privées, dont les États et les sociétés civiles ne peuvent se désintéresser[14].

Les progrès numériques offrent aux individus, même très éloignés des centres d'activités, la possibilité d'un développement culturel et social, source d'enrichissement personnel. Cette richesse humaine, rendue possible par les progrès numériques, pour laquelle la CNCDH manifeste son enthousiasme, est toutefois susceptible de mettre en péril les droits humains. Au nombre de ceux-ci, on compte des atteintes croissantes à la vie privée, la marchandisation générale des données personnelles, le ciblage par des algorithmes, ainsi que la falsification d'informations ou encore la manipulation des faits[15]. De nombreux usagers exposent plus ou moins volontairement et de manière croissante leurs données à caractère personnel, sans nécessairement prendre conscience des risques pour le respect de leur vie privée. Certes, ces pratiques sont souvent la transposition numérique d'atteintes aux droits déjà anciennes, mais le développement de l'Internet leur donne une dimension nouvelle, qui appelle de nouvelles normes et de nouvelles actions. L'encadrement de ces pratiques s'avère donc nécessaire pour éviter toute intrusion abusive dans la vie privée des individus, et pour garantir le droit à connaître l'usage qui est fait des données personnelles collectées. Aussi, les progrès du numérique nécessitent de nouvelles règles, le renforcement de certains droits et donc une certaine révolution sociétale[16] et juridique, afin d'être en mesure de gérer toutes les problématiques que la déterritorialisation est susceptible de générer[17].

En qualité d'institution nationale de promotion et de protection des droits de l'homme, et afin d'éclairer les travaux des pouvoirs publics à l'heure de l'entrée en vigueur du Règlement général sur la protection des données (RGPD)[18], la Commission nationale consultative des droits de l'homme a souhaité s'autosaisir de ces enjeux. La CNCDH se fonde tout d'abord sur le postulat selon lequel les données produites et communiquées par une personne lors de son utilisation des outils numériques constituent le prolongement de cette personne[19]. De la même manière, les droits de la personne sur ses données relèvent des droits de la personnalité, et non de du droit

13 Ce sigle désigne les cinq grandes firmes américaines qui dominent le marché du numérique : Google, Apple, Facebook, Amazon, Microsoft.

14 Audition de Côme Berbain, conseiller au Secrétariat d'État au numérique, le 22 décembre 2017

15 Rendue possible par les pseudonymes ou la création de plusieurs adresses électroniques ou comptes sur les réseaux sociaux.

16 Dans le sens notamment d'une plus grande compréhension des enjeux, par un plus grand nombre de personnes.

17 La CNCDH se fait l'écho du Conseil national des politiques de lutte contre la pauvreté et l'exclusion sociale (CNLE), qui rapporte que « *le non-recours au droit est un phénomène majeur dans notre société. Il s'explique par un certain retrait du service public et particulièrement une réduction des fonctions d'accueil, d'orientation et d'assistance, au profit de procédures numérisées* » (Contribution au suivi du plan pluriannuel contre la pauvreté et pour l'inclusion sociale, mars 2017)

18 Règlement n° 2016/679 relatif *à la protection des données personnelles*.

19 Benjamin Bayart va même jusqu'à comparer nos données personnelles à notre ombre : audition de Benjamin Bayart, le 23 janvier 2018.

de propriété. La CNCDH critique toute patrimonialisation des données personnelles, même au nom d'une vie privée active.

L'application en mai 2018 du règlement européen entraînera en effet la modification du cadre juridique français et, en particulier, des dispositions de la loi fondatrice du 6 janvier 1978 dite « informatique et libertés » dont les intuitions sur la protection de la vie privée étaient prémonitoires. Ce règlement, qui remplacera la directive du 24 octobre 1995 est d'application directe. Mais, le RGPD laisse des marges significatives de liberté aux législateurs des États membres de l'Union européenne (UE) qui, si elles étaient pleinement exploitées, permettraient à ce nouveau cadre de mieux protéger les droits de l'homme en territoire numérique. La CNCDH regrette à ce titre que le projet de loi, auquel il appartenait de définir ces aménagements, soit conçu et présenté aux assemblées dans la précipitation. Procédure accélérée, habilitation à procéder par ordonnance, impréparation des administrations territoriales et centrales : l'engagement tardif du Gouvernement sur ce dossier n'a pas permis de conduire une réflexion approfondie, alors même que le règlement appelait à des arbitrages d'ordre éthique et philosophique. La nécessité d'une réflexion fondamentale dépasse le cadre du RGPD. Si le cadre juridique posé par la loi de 1978 était un outil robuste et précurseur, amélioré d'ailleurs à plusieurs reprises, à l'heure du « big data » et compte tenu de l'ampleur des progrès numériques, il apparaît toutefois dépassé.

C'est ce que le règlement de 2018 tente d'appréhender. Aujourd'hui, la trajectoire mondiale de la donnée est délicate à cartographier et, précisément, il est difficile de savoir entre les mains de qui elle viendrait à tomber. Il est également devenu délicat d'anticiper quelles données permettront, par agglomérations et recoupements, de produire des renseignements permettant d'identifier ou cibler une personne. En d'autres termes, les barrières et sécurités que l'on dressait naguère entre la vie intime et la vie collective sont aujourd'hui fragilisées par les nouvelles potentialités des « data ». Pourtant, si l'on en croit les usages, notre société semble consentir peu ou prou à ce nouveau mode de vie, même si l'on peut s'interroger sur le caractère volontaire, effectif et éclairé de ce consentement. Et l'on peut, dès lors, questionner le sens que notre « société de l'information » donne à la notion de respect de la vie privée dans cet espace numérique.

Si dans certaines circonstances, les individus exposent volontairement leurs données personnelles (par exemple sur les réseaux sociaux), ils peuvent également être amenés à les céder du fait d'exigences sociales, par ailleurs raisonnées, légitimes et pertinentes : c'est le cas notamment du cadre scolaire. Dans ce type de situations, la collecte d'informations touchant à la vie privée des personnes s'impose à elles, mais semble relever de ce qu'on pourrait appeler une finalité d'intérêt public. Pour autant, il est nécessaire que leur utilisation se fasse de manière légitime, pertinente et proportionnée.

La CNCDH tient également à rappeler le caractère paradoxal des reproches adressés à l'Internet : d'un côté, la profusion d'informations plus ou moins exactes (parmi lesquelles les « fake news »), qui alimentent les propos extrémistes et les discours de haine ; de l'autre, et son corollaire : la dénonciation d'une trop grande intrusion des dispositifs de surveillance de ces discours dans les conversations et la vie privées. Ainsi, les réseaux sociaux sont présentés comme tantôt trop permissifs, tantôt trop répressifs, créant ainsi une certaine « schizophrénie » chez leurs usagers. Par ailleurs, le « big data » sur lequel repose le modèle économique des réseaux sociaux, qui donnent l'impression d'une omniscience de ceux-ci sur la vie des usagers, n'est possible que parce que ces derniers eux-mêmes l'alimentent[20].

La CNCDH soulignera d'abord la menace que fait peser le numérique sur le respect de la vie privée, cette menace devant toutefois être mesurée à l'aune des nouveaux visages de la vie privée (I). Elle recherchera, ensuite, les moyens les plus appropriés pour renforcer l'effectivité des garanties offertes (II). La Commission s'efforcera, enfin, de proposer des mesures permettant d'atteindre un équilibre protecteur et pérenne dans l'architecture des droits de l'homme (III).

20 Cela ne justifie toutefois en aucun cas leur ingérence dans la vie privée des personnes.

# I. Les transformations de la vie privée à l'âge de « l'homo numericus »

## A. Évolution du lien entre vie privée et données personnelles

La CNCDH réunit délibérément la question de la donnée personnelle à celle de la vie privée alors que les deux, *a priori*, ne se confondraient pas entièrement. Pourtant toute donnée connectée produite par une activité humaine, même prosaïque et impersonnelle, peut servir de fondement à la reconstitution d'informations plus précises et attentatoires à l'intimité de la personne.

Les nouvelles pratiques numériques tendent parfois à concevoir le traitement des données personnelles en dehors de la problématique de la vie privée, comme si un tel traitement ne constituait plus nécessairement une menace pour cette dernière. Tandis que la jurisprudence de la Cour européenne des droits de l'homme considère la protection des données personnelles comme une composante du droit à la vie privée[21], la Charte des droits fondamentaux de l'Union européenne consacre à ces droits deux chapitres distincts[22]. Or, contrairement à une opinion répandue, les utilisateurs continuent dans leur majorité à être attachés au principe de vie privée, y compris les jeunes générations[23]. En effet, l'exposition accrue de soi ne signifie pas une moindre volonté de contrôle sur les informations divulguées, et l'étendue du public auprès duquel elles sont rendues visibles. Il est frappant de constater que l'espace emblématique du « partage » d'éléments de sa vie privée, les réseaux sociaux, n'inspire pas confiance : ce sont les acteurs auxquels les Français accordent le moins de confiance en matière de protection de leurs informations personnelles[24]. Depuis 1978, la loi « informatique et libertés » régit pourtant le traitement des données personnelles afin que celui « *ne porte pas atteinte à la vie privée* »[25]. Cependant, malgré les garanties offertes par la loi de 1978 pour sa protection[26], la vie privée y reste encore principalement conçue comme un espace clos qu'il faudrait protéger contre des fichiers publics intrusifs[27]. La loi de 1978 ne pouvait bien sûr pas encore anticiper les nouveaux sens que la vie privée allait prendre, notamment comme droit à l'autonomie personnelle, qui tendent aujourd'hui à devenir « *ce qui va se dilater inéluctablement, notamment dans les réseaux sociaux, et*

21 CEDH, Grande chambre, S. et Marper c/ Royaume-Uni, 4 décembre 2008, req. n°30562/04 et 30566/04. La décision prend acte du fait que la Convention de sauvegarde ne consacrait pas d'article spécifique au traitement des données personnelles, et a donc fait découler celles-ci de l'article 8 relatif au droit à la vie privée.

22 L'article 7 de la Charte porte sur le droit à la vie privée et familiale, l'article 8 sur la protection des données à caractère personnel. Le paragraphe 93 de la jurisprudence Télé 2 Sverige AB, notamment, rappelle que la protection des données personnelles doit également être appréciée au regard d'un autre droit non moins fondamental, celui de la liberté d'expression (article 11 de la Charte).

23 Audition de Martin Untersigner, 13 février 2018.

24 Harris-Interactive, 2017, Baromètre 2017 de la confiance des Français dans le numérique.

25 Loi 78-17 du 6 janvier 1978, article 1.

26 Audition de Bernard Benhamou, le 23 janvier 2018.

27 Audition de Pierre-Olivier Gibert, le 29 janvier 2018.

*qui appelle un nouveau type de protections dans l'espace numérique* »[28].

Dans ce cadre légal, la CNIL entend donc, d'abord et avant tout, maintenir le cap d'une définition « traditionnelle » de la vie privée face à ce qui constitue le défi des prochaines années : le « privacy paradox », selon lequel les utilisateurs de l'Internet exposent plus volontiers leur intimité qu'autrefois tout en éprouvant, en même temps, une inquiétude croissante pour la protection de leur vie privée[29]. Les récentes actions de la CNIL en direction des jeunes internautes, pour les sensibiliser à la protection de leur vie privée en ligne, en attestent[30]. Or, ces efforts sont compliqués par la nouvelle dynamique des données : protéger sa vie privée ne tient plus seulement au tri attentif que l'internaute fera entre les données qu'il accepte de communiquer en ligne et celles qui lui paraîtraient trop personnelles, car les frontières entre donnée personnelle et impersonnelle, donnée privée et donnée publique, donnée anonyme et donnée permettant l'identification, sont devenues impossible à distinguer pour l'utilisateur, d'autant plus que le flou est savamment entretenu par les grands fournisseurs de services de l'Internet.

En effet, à l'heure du « big data », toutes les données sont potentiellement personnelles et font peser un risque sur la vie privée. Car, si le prélèvement de la donnée pris individuellement est théoriquement encadré par une finalité, la somme des données que l'on renseigne en ligne, par le biais de processus d'agrégation et de recoupements automatisés, peut produire des informations nouvelles, constituant parfois des renseignements très détaillés sur les caractéristiques de la vie privée d'une personne[31],[32]. Les algorithmes qui analysent le « big data » peuvent avoir pour fonction d'agréger et de recouper des données, afin de reconstituer les profils des utilisateurs, et donc de révéler l'intimité d'une personne à partir d'informations éparses que l'on pensait muettes. Ainsi, d'une part, toute donnée, même *a priori* anodine, est potentiellement un enjeu de vie privée et, d'autre part, consentir à verser des données à des services en ligne, au cas par cas et pour des finalités spécifiques et distinctes, ne permet pas forcément de contrôler les informations qui seront potentiellement produites par agrégation automatisée[33], via notamment des applications tierces.

28 Audition de Jean Lessi, le 29 janvier 2018.

29 On notera les termes sévères du Conseil économique, social et environnemental qui, en 2015, parlait de « schizophrénie » de notre société. Eric Peres, *Les données numériques : un enjeu d'éducation à la citoyenneté. Rapport du CESE*, janvier 2015, p. 46.

30 Voir notamment le film tourné par le blogueur « le Rire jaune » et produit par la CNIL et la MGEN : « Protéger sa vie privée! ». Accessible sur https://www.youtube.com/watch?v=U7xOBOnQoG4 (consulté le 3 mars 2018).

31Audition de deux inspecteurs du ministère de l'Education nationale représentant l'Inspection générale de l'administration de l'Éducation nationale et de la recherche, le 11 janvier 2018 ; audition de M. Bernard Benhamou, le 23 janvier 2018.

32 Voir à ce titre l'arrêt du Conseil d'État n°393714 du 8 février 2017. La décision concerne un traitement de données effectué au moyens de panneaux publicitaires numériques et dans le cadre duquel les informations recueillies étaient anonymisées : l'éventualité que des personnes puissent être identifiées grâce au recoupement de l'information relative aux déplacements des personnes d'un panneau à l'autre et de quelques chiffre de leur adresse MAC – le reste des chiffres étant masqués par souci d'anonymisation – avait conduit le juge administratif à interdire le traitement.

33 La CNIL, citant Henri Verdier écrivait déjà en 2010 que « *Si avec la naissance de la CNIL, les enjeux étaient le*

Les failles de sécurité des systèmes de stockage des données personnelles menacent également la vie privée des utilisateurs : comment choisir l'entreprise numérique la plus sûre, à l'heure où aucune organisation n'est parfaitement hermétique aux intrusions, comme le montre les cas Facebook[34] ou Equifax[35] ? L'affaire « Cambridge Analytica »[36] met en lumière la négligence dont les réseaux sociaux peuvent faire preuve en termes de protection des données de leurs utilisateurs[37]. Ces failles dans les systèmes de sécurité des réseaux sociaux semblent d'autant plus inquiétantes que la captation massive des données menace l'anonymat[38]. La popularité croissante des objets connectés tend à accroître ce risque : « *La sécurité de ces objets reste pour l'instant rudimentaire. De l'absence de mécanismes de cryptage pour la transmission des données, jusqu'à l'impossibilité d'intégrer des mises à jour de sécurité, la sécurité des objets connectés constitue aujourd'hui un des maillons les plus faibles des infrastructures de l'Internet*[39] ». Pour preuve : le 4 décembre 2017, la CNIL a ainsi mis en demeure[40] une compagnie de fabrication de jouets connectés de sécuriser ses produits qui avaient une fonction possible de micro « espion »[41].

---

*recueil des données pour de mauvais usages, aujourd'hui, c'est l'interopérabilité qui est la nouvelle question centrale. Le traitement statistique permet de brasser des informations qui ne sont pas intrinsèquement personnelles : 'elles parlent des gens sans être nominatives'. Les sciences autour des données vont progresser et on ne fera plus le détour par l'identification ou par l'espionnage du sujet (comme connaître son orientation personnelle).* » CNIL, « La dictature de algorithmes », *Cahier IP* n°1, dossier « Vie prive à l'horizon 2020 », 2010, p. 20

34 L'entreprise Cambridge Analytica a profité d'une faille du système de sécurité de Facebook pour analyser en 2016 les données de millions d'utilisateurs à leur insu.

35 Cible d'une attaque informatique en 2017, la compagnie d'assurances Equifax a vu fuir les données personnelles de près de 150 millions de ses clients. La compagnie Uber également connu une brèche significative : les données personnelles de près de 60 millions d'utilisateurs ont été piratées.

36 Dans laquelle une société britannique aurait récupéré illégalement les données de 87 millions d'utilisateurs de Facebook.

37 La société Cambridge Analytica, spécialisée dans la vente d'outils d'influence, est accusée d'avoir recueilli les données d'environ 50 millions d'utilisateurs de Facebook sans leur consentement. Le 17 mars 2018, trois journaux américains ont révélé que la collecte de ces données avait été effectuée à l'insu des internautes concernés : elle revêtait la forme d'un exercice académique, alors qu'elle absorbait le données non seulement des participants, mais aussi de leurs contacts Facebook. Par ailleurs, l'audition de Marc Zuckerberg devant le Congrès américain, les 10 et 11 avril, a révélé que son réseau social collecte des données de personnes non inscrites lorsqu'elles naviguent sur Internet, par l'intermédiaire des boutons « J'aime » et « Partager ». Ces boutons permettent de se connecter à d'autres services via Facebook, et permet d'améliorer le profilage et le ciblage publicitaires.

38 La notion d'obscurité, défendue par Woodrow Hartzog, ne signifie pas l'inaccessibilité totale, mais le maintien d'une part d'ombre autour de la vie privée : pour cela, il est nécessaire de renforcer ses paramètres de confidentialité, utiliser des messageries cryptées, enclencher la touche « Avion » de son portable. Cette « *obscurité pratique* », estime-t-il, devrait être renforcée avec l'extension des nouvelles technologies biométriques, afin de « *favoriser l›autonomie, l›épanouissement personnel, la socialisation et la liberté face aux abus de pouvoir* ». Frédéric Joignot, « Comment nos visages sont traqués ? », *Le Monde*, 22 mars 2018.

39 Bernard Benhamou, *Données personnelles et objets connectés en Europe. Perspectives technologiques et enjeux de régulation*. Rapport du 18 avril 2017 pour l'Institut des Mines-Télécom.

40 Il s'agit d'une interpellation formelle faite par la CNIL au responsable de traitement qui ne s'est pas acquitté de ses obligations.

41 Il s'était avéré que les conversations entre la poupée et l'enfant, enregistrées par l'appareil, pouvaient être écoutées par quiconque était équipé d'un smartphone et de l'application permettant de se connecter au jouet, à condition de se trouver à moins de neuf mètres du jouet. Le secret des échanges entre l'enfant et le jouet, ainsi que toute conversation à proximité, n'étaient donc pas garantis.

Dans ce contexte, la stratégie de la CNIL ne consiste pas à redéfinir la notion de vie privée dans la vie numérique, au risque sinon de la fragiliser[42], mais plutôt à identifier les nouvelles manières dont le numérique y porte atteinte et à y répondre. Aussi, selon la CNIL, le besoin serait de repenser la définition de la vie privée à l'ère numérique plutôt que de multiplier et renforcer les champs d'interventions des acteurs de sa protection[43]. Si la CNCDH considère cette stratégie indispensable tant il convient, plus que jamais, dans ce contexte de circulation et d'exploitation générale des données personnelles, de protéger les personnes des intrusions dans la vie privée, elle considère aussi le droit au respect de la vie privée, comme un droit positif à l'autonomie et au développement de la personne dans l'espace numérique. A travers la maîtrise de ses données personnelles, l'homo numericus doit conserver sa « capacité à être lui-même » : sa vie privée ne doit pas être façonnée par un traitement incontrôlé de ses données aboutissant à un profilage limitant le droit à son développement personnel. Cette seconde composante de la vie privée suppose de consacrer un véritable droit à l'autodétermination informationnelle[44], qui comporte aussi le droit d'exposer publiquement ses données personnelles. Pour la CNCDH la protection de la vie privée, comme protection contre les intrusions, et comme droit à l'autonomie personnelle, ne s'opposent pas mais sont complémentaires.

## B. Exposition croissante de l'intimité

Dans ce contexte de numérisation croissante de nos sociétés, la vie privée fait l'objet d'une exposition sans précédent, notamment sur les réseaux sociaux. « *Nous partageons avec des cercles toujours plus larges nos photographies, notre localisation, les playlists que nous écoutons, nos avis sur tel service ou telle prestation. Nous partageons même avec de vastes communautés – pour les adeptes du « quantified self » – des données extrêmement intimes, que l'on ne murmurait autrefois qu'à son médecin, à son prêtre et à son banquier* »[45]. Ce phénomène de grande ampleur touche toutes les générations, notamment les plus jeunes, ce qui n'est pas sans décontenancer les pouvoirs publics[46]. Notons à ce sujet que la confidentialité que pouvait autrefois revêtir une pathologie est aujourd'hui davantage confiée en premier recours à un moteur de recherche plutôt qu'à un professionnel de santé, habilité au secret médical.

Une des caractéristiques majeures de l'exposition croissante de la vie privée est son « *décompartimentage* »[47]. Les moteurs de recherche permettent ainsi d'obtenir un aperçu structuré d'informations relatives à une personne sur l'Internet, qui touchent potentiellement à une multitude d'aspects de la vie privée[48]. Grâce aux interconnexions

42 Audition de M. Jean Lessi, le 29 janvier 2018.
43 *Ibid*.
44 Voir Conseil d'État, Etude annuelle 2014, *op. cit.*, p. 133
45 Isabelle Falque-Pierrotin, éditorial du dossier « Partage ! », *Cahier IP – Innovation et prospectives*, n° 4, 2015.
46 Audition de Jean-Marc Merriaux, le 11 janvier 2018.
47 Audition de Jean Lessi, le 29 janvier 2018.
48 CJUE, Grande Chambre, 13 mai 2014, Google Spain SL et Google Inc. c. l'Agencia Española de Protección de Datos et Mario Costeja Gonzalez, Aff. C-131/12.

d'informations réalisées par le moteur de recherche, il est possible d'établir un profil détaillé d'une personne. Autrefois, il était impossible de reconstituer le parcours d'achats d'une personne tant que le paiement s'effectuait en liquide et dans plusieurs établissements successifs. Le compartimentage de la vie privée était jadis immédiat et naturellement protecteur. Aujourd'hui, en raison des traces laissées par les opérations en ligne et l'historique de la navigation sur l'Internet[49], il devient tout à fait possible de reconstituer des parcours de choix, et partant, un certain profil des personnes. Cette interconnexion des contenus et ce pistage automatique des actions individuelles en ligne entraînent une exposition démultipliée de la vie privée, et constituent un défi majeur pour sa protection.

Le volume et la fréquence des informations collectées (« big data »), dus aux progrès numériques, accentuent donc nécessairement l'exposition de la vie privée. Le « big data » se caractérise en effet par les trois « v » : volume, vitesse, variété[50]. Il se nourrit des données relevant de la vie privée, données fournies par les individus eux-mêmes, notamment les réseaux sociaux, qui l'alimentent. Dans les ressources humaines, par exemple, le fichage et le repérage sur des réseaux professionnels permettent d'aspirer diverses données rendues, volontairement ou non, publiques par l'intéressé. On améliore ainsi la rencontre entre offres et demandes d'emplois - à travers un traitement affiné et rationalisé des profils de postes et des candidatures – et, ce faisant, la mobilité dans le monde du travail. Le risque de fonder une politique de ressources humaines sur un traitement général et automatique de nombreuses données personnelles est d'accroître les déterminismes sociaux, notamment par une surpondération du passé de la personne (données personnelles agrégées et traitées) par rapport à ses projets présents, et par des catégorisations discriminantes des profils de personnes. Le second impact du « big data » sur les données personnelles se caractérise par l'enrichissement de celui-ci par des données brutes. Cet enrichissement quantitatif et qualitatif permet un ciblage continu des individus et donc une amélioration du profilage, ce qui peut servir aussi bien l'employeur dans le cadre d'un recrutement que l'entreprise souhaitant proposer des offres commerciales ciblées. Si ce sont des outils d'aide à la décision, ces perfectionnements peuvent être utiles. En effet, les nouvelles opportunités d'agrégation, d'analyse et de corrélations statistiques au sein de quantités massives de données semblent permettre de mieux saisir la réalité sociale, de façon plus directe et immanente[51]. Toutefois, le traitement algorithmique des données personnelles, agrégées et recoupées à d'autres données, peut conduire à limiter mécaniquement ce qui est socialement, économiquement et culturellement offert et possible de faire, et en conséquence de limiter le droit fondamental au développement personnel.

La circulation accrue et massive des données à caractère personnel tend également à rendre poreuse la frontière entre vie privée et vie publique. Le partage de ces données sur les réseaux sociaux remet en question la frontière jusqu'alors plus claire entre les

49 Le numérique inclut aussi l'analyse des paiements par cartes accréditives « dans la vie réelle » : c'est une source importante du « big data ».
50 *Ibid.*
51 Antoinette Rouvroy, *Gouvernementalité algorithmique et perspectives d'émancipation*, Cairn, 2013.

deux. A titre d'exemple, lorsqu'une personne met en ligne des données personnelles sur un réseau de plusieurs centaines d'internautes « amis », cela relève-t-il de la sphère publique ou de la sphère privée ? Quand une personne communique sur sa messagerie électronique, cela relève-t-il du régime des correspondances privées dont le caractère secret est protégé par le droit pénal ? Cette question de la limite entre sphère privée et sphère publique est centrale dans la manière dont chacun exerce ses droits les plus fondamentaux. Elle l'est aussi dans la manière dont s'apprécient les équilibres auxquels se réfèrent les juges. Le temps où la personne pouvait, avant d'autoriser l'utilisation d'une donnée personnelle, identifier la destination de cette donnée est révolu. Désormais, une donnée peut être transmise dans ce qui paraît être un espace numérique privé, puis ensuite intégrée dans des bases de données qui, par leur ampleur, relèvent d'une sphère plus collective. Il s'agit donc, non pas de proposer une nouvelle définition de la vie privée, mais, pour chacun, de se réapproprier cette question en vue d'exercer utilement l'autonomie qui vient de lui être reconnue.

Dans ce contexte d'exposition de sa vie privée, les cas de révélation de celle des autres, même de bonne foi, semblent voués à se multiplier. C'est au regard de cette éventualité que le Comité ad hoc pour la révision de la Convention 108 pour la protection des données du Conseil de l'Europe rappelle la responsabilité qui pèse sur les personnes physiques susceptibles d'avoir des usages du numérique à la frontière de la vie privée : « *le partage de données au sein de la « sphère privée » comprend notamment le partage fait au sein de la famille, d'un cercle restreint d'amis ou d'un cercle limité en taille, fondé une relation personnelle ou une relation de confiance particulière* »[52]. Sur la base de cette définition, le Comité souligne que cela exclut donc les cas où « *des données personnelles sont rendues accessibles à un grand nombre de personnes ou à des personnes manifestement étrangères à la sphère privée, par exemple sur un site web public* »[53]. Ce principe de construction et de prise en compte de l'altérité repose sur la responsabilisation des usagers, notamment la connaissance des implications des photos de groupe que l'on publie sur la toile. Ce manque de conscience des risques peut conduire à des dérives : certaines personnes ont eu la désagréable surprise de voir des articles de blog en ligne faire état d'informations sur leur passé (condamnations, photographies compromettantes…). Au Danemark, plus de 1000 jeunes sont également poursuivis pour avoir diffusé les vidéos, entre 2015 et 2017, des ébats de deux adolescents de 15 ans via la messagerie Facebook. L'exposition de la vie privée n'est certes pas nouvelle, mais elle était jadis plus restreinte[54].

Dans les relations de travail, le risque d'intrusion du numérique dans la vie privée est accru pour les salariés, dans la mesure où l'expression d'un consentement libre et éclairé n'y est pas aisée. Il se développe une véritable porosité entre les sphères privée et professionnelle des salariés, que ce soit par la possibilité de recevoir des ordres en tout lieu et à toute heure (question de la déconnexion), par la question du travail à

52 Conseil de l'Europe, 2017, *Projet de rapport explicatif relatif à la Convention 108 modernisée*, p.5 (https://rm.coe.int/16806b6ec3).
53 *Ibid*, p.5.
54 Audition de Jean Lessi, le 29 janvier 2018.

distance, par l'accès à des données personnelles du salarié, etc. En plus de l'atteinte à la vie privée des salariés, les risques sont multiples, notamment en termes de santé des salariés en cas d'absence de droit réel à la déconnexion (notamment burn-out suite à une augmentation du temps de travail ou une diminution du temps de repos), discrimination ou inégalité de traitements (face aux données à la disposition de l'employeur notamment traitées via des algorithmes), économiques (licenciements sans causes réelles et sérieuses pour de faux motifs dont la cause réelle serait la connaissance de la vie privée du salarié). Pour la CNCDH, les enjeux qui y sont liés doivent faire l'objet d'un cadre national réglementé plus protecteur au bénéfice de l'ensemble des salariés. La Commission rappelle que l'employeur a le devoir de faire respecter le droit à la santé et à la sécurité des salariés, et que la qualité de vie au travail ne doit pas être une variable économique d'ajustement.

L'enjeu de l'articulation entre exposition de la vie privée et sécurisation des usagers de l'Internet est donc celui de la responsabilisation. Il faut leur donner la possibilité de construire l'identité et les caractéristiques d'eux-mêmes qu'ils veulent diffuser sur Internet, c'est-à-dire leur apprendre à sélectionner avec discernement la part de leur vie privée qu'ils souhaitent exposer, et celle qu'ils préfèrent garder secrète. Il convient ainsi de prévenir le plus possible les risques d'abandon ou de perte de contrôle des données mises en ligne. La CNCDH se montre optimiste sur l'attention portée par les usagers, notamment les plus jeunes, au maintien du contrôle de leur vie privée. En effet, l'exposition accrue de soi qui s'accentue chez les jeunes générations, ne signifie pas nécessairement une moindre volonté de contrôle sur la divulgation des informations touchant à la vie privée et l'étendue de son audience.

Le problème actuel de la protection de la vie privée semble donc être la difficulté à la circonscrire avec précision, tant parce que la notion est devenue complexe à saisir pour le juge et le législateur, qu'en raison du potentiel démultiplié que chaque donnée isolée, personnelle ou non, acquiert à la faveur du « big data » : il est pratiquement impossible à l'heure actuelle de savoir de quelle donnée jugée impersonnelle et parfaitement anonyme émergera une information sur la vie intime. Le « big data » contribue donc à la perméabilisation de la frontière entre vie privée et publique et à une reconstitution de plus en plus aisée, par agrégation et recoupements de la première, dans des espaces qui ne sont pas privés.

## C. Nouvelles formes d'atteinte à la vie privée : sur les nouvelles pratiques des GAFAM et des entreprises ayant la vente des données personnelles pour modèle économique

Les données personnelles jouent un rôle de plus en plus important dans l'économie numérique actuelle , et sont même au fondement d'un nouveau modèle économique : les grands opérateurs offrent une multitude de services gratuits (réseau, moteur de recherche, messageries) moyennant la collecte massive d'une infinité d'informations personnelles exploitables : la valeur financière économique des réseaux sociaux

numériques et de nombreux services en ligne reposent sur leur capacité à capter des données personnelles traitables et utilisables. La gratuité d'accès à de nombreux services du web n'est pas réelle, mais conditionnée par l'échange, souvent inconscient sur sa portée, des données personnelles des utilisateurs. Tous les GAFAM ne recourent pas massivement aux données des personnes utilisatrices de leur service, au motif que le modèle économique d'Apple et Microsoft, notamment, repose sur la vente de matériel et de programmes, plutôt que sur la valorisation commerciale des données[55]. Facebook et Google, dont le ciblage publicitaire est la principale source de profits, se défendent, quant à elles, de faire circuler ces données auprès de leurs clients. Proposant de cibler des profits selon leurs sensibilités supposées, ces entreprises valorisent l'action publicitaire des annonceurs ; ceux-ci n'ont pas accès, en revanche, aux données relatives à ces profils[56].

La diversification des services en ligne s'est donc accompagnée d'une multiplication des techniques de collecte des informations relatives aux individus. Les grandes sociétés informatiques disposent de possibilités décuplées de recoupement des informations laissées sur la toile par les individus, et exploitent de manière stratégique ces recoupements, en particulier celles dont le modèle économique repose sur la cession ou le traitement de données au bénéfice de tiers. Elles ont en effet la capacité, grâce à la taille et à l'interconnexion croissantes des fichiers de données – le « big data » - et au développement d'algorithmes puissants, de faire parler des informations éparses (que l'on croyait muettes), révélant ainsi, parfois, l'intimité d'une infinité de personnes.

Si l'exploitation de ces ressources informationnelles par les entreprises est souvent présentée dans la littérature en économie et en marketing comme une source de bien-être pour les consommateurs, d'innovations et d'opportunités commerciales inédites, elle représente également une source de menaces pour la vie privée et d'externalités négatives pécuniaires. Les exploitants de données personnelles peuvent par exemple opérer des stratégies de discrimination par les prix sur les marchés de biens de consommation courants, de l'assurance, de la banque, du travail… en fonction du profilage des individus : les individus les moins riches, les moins solvables ou présentant des risques de santé paieront un prix plus élevé que les autres. Les entreprises, mais à terme aussi les services publics, collectent des données personnelles sur leurs clients ou usagers pour les exploiter selon des modalités variées : identifier ces derniers, communiquer ou interagir avec eux de façon plus ou moins ciblée, différencier leurs prix ou la qualité de leurs offres en fonction des profils identifiés, animer une communauté en ligne, faciliter l'appariement entre les utilisateurs de leurs services, revendre ces données à d'autres firmes. Les moyens de collecte et de production de ces informations sont eux-mêmes très diversifiés. Les individus peuvent ainsi divulguer volontairement leurs données par déclaration (formulaires d'abonnement et d'inscription, données de transaction, etc.), en acceptant que leurs données soient enregistrées (traces de navigation, localisation géographique, mots clés extraits de leurs commentaires

55 Audition de Bernard Benhamou, le 23 janvier 2018.

56 Audition d'Anton Battesti et Ophélie Gérulis, représentant Facebook France, le 11 janvier 2018. Audition d'Olivier Esper et Benjamin Duchaffaut, représentant Google France, le 5 février 2018.

et discussions en ligne, etc.), en les partageant au sein d'un réseau, et souvent à leur insu. Cette seconde forme d'exposition s'avère une source majeure d'informations sur l'Internet à travers la collecte massive de données enregistrées par des traceurs et traitées ensuite à l'aide d'algorithmes permettant de déduire des informations à valeur ajoutée à partir de données brutes très disparates.

Depuis la fin des années 1990, de nombreuses technologies ont été développées pour observer les comportements de navigation sur l'Internet et, corollairement, identifier de façon unique et systématique l'internaute[57]. Initialement, la volonté était d'offrir un meilleur service à l'internaute, mais au fil des ans, les technologies de suivi étant devenues plus intrusives, elles peuvent désormais servir à identifier de façon unique un internaute et à rassembler par la suite des traces de navigation. Ces informations brutes peuvent servir à produire des données individuelles (comportements, goûts, liens sociaux, etc.), lesquelles peuvent à leur tour générer des données personnelles lorsqu'elles sont associées à des données d'identification ou de contact des individus. De nombreuses données deviennent presque systématiquement personnelles, en fonction du traitement algorithmique dont elles font l'objet ; or, les utilisateurs ne maîtrisent par la création de ces profils qui pourtant sont constitués à partir de l'exploitation de leurs données. Peu de sites internet annoncent, via les chartes de vie privée, les conditions générales de ventes ou d'utilisation du site (CGV, CGU), qu'un comportement de diffusion potentielle de données personnelles à des acteurs tiers a lieu. La plupart des visiteurs estiment que leurs données personnelles restent dans le giron du site internet qu'ils visitent. Cette création d'une identité de nous-même, sans que nous en soyons acteurs, constitue un défi majeur pour l'autonomie informationnelle et l'auto-détermination sur l'Internet. La CNCDH, dans le prolongement du droit de l'Union, considère que ces processus d'interconnexion, d'agrégation et de traitement des données personnelles réalisés par les grands opérateurs doivent être considérés non comme des actions commerciales anodines, mais comme des ingérences dans la vie privée des personnes[58]. A ce titre, ils ne sauraient être justifiés par la seule existence d'un contrat passé entre l'opérateur et ses clients, ni a fortiori par les seuls intérêts économiques des opérateurs en présence[59]. Les intérêts et droits fondamentaux des personnes faisant l'objet de ce processus, notamment le droit au respect de leur vie privée, doit être au cœur du nouvel ordre numérique en construction.

57 La première de ces technologies est l'adresse IP.

58 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.

59 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.

# II. Les enjeux de la reconfiguration de la vie privée par le numérique

Sans protection juridique supplémentaire, le traitement massif des données par les acteurs de l'économie numérique est susceptible de compromettre le respect de la vie privée, d'autant que « *quantitativement et qualitativement, jamais aucun média n'avait été en capacité de disposer d'autant de données privées et intimes sur autant de personnes en temps réel et à flux constant* »[60]. Il convient donc de garantir aux citoyens une protection suffisante, notamment dans le cadre de la circulation des données et de leur commercialisation ; les données personnelles ne sont pas entièrement « disponibles », c'est-à-dire « dans le commerce », et ne relèvent pas d'une totale liberté contractuelle : elles sont soumises à des principes et droits fondamentaux, dont le droit au respect de la vie privée[61]. La protection des données personnelles résulte d'un lien de droit puissant qui est établi entre la personne et ses données personnelles. Le droit d'une personne sur ses données n'est pas un droit sur une chose (droit réel) mais un droit inhérent à la personne et protégeant sa personnalité (droit de la personnalité). Son exercice est fondé sur le consentement libre, éclairé et spécifique de son titulaire. La question se pose toutefois de savoir s'il n'existe pas des situations dans lesquelles il est légitime et licite de contraindre une personne à verser ses données à un tiers public ou même privé. Ainsi, selon le RGPD, si les données traitées peuvent avoir une « finalité d'intérêt public », y compris lorsqu'elles sont sensibles, elles peuvent bénéficier de certaines exceptions, notamment en ce qui concerne l'exigence de consentement. Cette articulation entre l'exigence centrale d'un consentement pour la communication et l'usage de ses données personnelles et l'existence d'obligations légales de transmission des données est au cœur de la protection de la vie privée numérique.

## A. Droit de la personnalité et protection de l'autonomie de la personne

### 1. Non patrimonialisation des données personnelles

Pour lutter contre les formes nouvelles d'exploitation des données personnelles, certains avancent que la solution la plus efficace consisterait à instaurer un droit de propriété sur les données personnelles au profit des individus, afin de leur permettre de mieux les contrôler et éventuellement de les monétiser pour organiser un retour de la valeur vers ceux qui en sont la source. L'idée, *a priori* séduisante, serait de faire de chaque individu le véritable maître de son identité numérique. Chacun pourrait gérer ses données en les louant, prêtant, récupérant, etc. Toutefois, l'application du concept de propriété est contestable philosophiquement et juridiquement, et n'apporte pas de réponses adéquates.

60 Olivier Ertzscheid, « Le scandale Facebook pose avant tout une question politique », *Libération*, 23 mars 2018.
61 Auditions de Marylou le Roy et Yann Bonnet, équipe permanente du Conseil national du Numérique.

Dans le but d'obtenir un niveau de protection élevé le législateur français a, dans la loi Informatique et liberté de 1978, placé le droit de la protection des données personnelles dans la catégorie des droits dits extrapatrimoniaux. En effet, dans la conception française, et même dans la conception européenne, les informations relatives aux personnes relèvent des droits de la personnalité, c'est à dire des droits inhérents à la personne humaine. Ce droit est tellement consubstantiel à la personne que celle-ci ne peut pas choisir d'en disposer totalement librement. Ces droits extrapatrimoniaux formant le prolongement de la personne elle-même, ils ne relèvent pas de la qualification de bien et sont, par principe, hors du commerce. Ces droits sont incessibles, imprescriptibles et perpétuels. Ainsi le Conseil d'État rappelle-t-il qu'« *en l'état du droit, il n'existe pas de droit de propriété de l'individu sur ses données personnelles. […] la protection des données personnelles, telle qu'elle est conçue par la loi du 6 janvier 1978, la Convention n° 108 du Conseil de l'Europe ou la directive n°95/46/CE, ne repose pas sur une logique patrimoniale mais sur une logique de droits attachés à la personne […] ; il n'existe pas de droit de propriété sur les données brutes* »[62].

La CNCDH soutient la pleine consécration, en droit français, du droit à l'autodétermination informationnelle reconnu par le Conseil d'État. La cour constitutionnelle allemande a reconnu ce droit, dans un arrêt du 15 décembre 1983[63]. Il permet de donner à l'individu les moyens de demeurer libre de conduire son existence, dans une société où le numérique prend une place croissante, qui l'amène à laisser, de plus en plus souvent, trace de ses données personnelles. Le Conseil d'État précise également qu' « *alors que le droit à la protection des données peut être perçu comme un concept défensif, le droit à l'autodétermination lui donne un contenu positif : il ne s'agit plus seulement de protéger le droit au respect de la vie privée, mais d'affirmer la primauté de la personne qui doit être en mesure d'exercer sa liberté (…) En ce sens, le droit à l'autodétermination répond d'avantage à l'aspiration croissante des individus à l'autonomie de la décision* »[64]. Cette aspiration au contrôle de ses données, que l'idée de leur patrimonialisation essaye de saisir, s'avère tout à fait garantie mais avec une plus grande souplesse par la notion d'autonomie informationnelle et personnelle. La portée exacte du principe d'autonomie est consacrée par la loi du 7 octobre 2016 : « t*oute personne dispose du droit de décider et de contrôler les usages qui sont faits des données personnelles la concernant* » (article 54). Le droit à l'autodétermination informationnelle fait pleinement partie des droits de la personnalité.

Le concept de propriété heurte également notre conception de la vie privée qui place sa protection sur le terrain de la dignité humaine. En se référant au concept de propriété, le risque de marchandisation de ses données personnelles est évident. La propriété comprend aussi le droit de céder la chose. Or, comment pourrait-on céder une donnée qui est aussi un attribut de sa personnalité ? Faut-il imaginer des droits d'exclusivité ? Mais ce régime juridique est inadapté aux enjeux d'Internet. Comment y faire valoir ses droits de propriété quand on a soi-même diffusé une donnée personnelle?

62 *Ibid*., p. 264.
63 Que la CEDH a abondamment cité dans sa propre jurisprudence.
64 Etude annuelle du Conseil d'État, « Le numérique et les droits fondamentaux », 2014, p.267-268

Quant aux informations relatives à sa vie publique, il ne peut être question d'un droit de propriété à moins de remettre en cause fondamentalement la liberté d'expression.

Ensuite, le Conseil d'État relève que deux arguments s'opposent à l'idée d'une patrimonialisation des données. D'abord, le maintien d'un déséquilibre structurel entre les individus pris isolément et les entreprises : les données des utilisateurs ne commencent à être véritablement utiles, et avoir une valeur économique pour les entreprises que lorsqu'elles sont agrégées (c'est le « big data ») : les données d'une seule personne ne valent que quelques dizaines de centimes. Les entreprises n'auraient qu'à formuler leur contrat sous forme de cession de droits d'utilisation de données, ce dont nombre de conditions générales d'utilisation se rapprochent déjà beaucoup[65]. Dès lors, lorsque le rapport de force entre des contractants est inégal, quelle valeur donner au consentement à contracter ?

### 2. Fragilité du consentement

Les différentes normes applicables en France en matière de protection des données personnelles (loi Informatique et Libertés, Convention n° 108 du Conseil de l'Europe, Charte des droits fondamentaux de l'Union européenne, le règlement général n° 2016/679 sur la protection des données) convergent aujourd'hui quant aux principales garanties de la protection des données personnelles : principes relatifs à la qualité des données, exigence du consentement, interdiction de la collecte de données sensibles, droits d'information, d'accès, de rectification et d'opposition, obligation de sécurité du responsable de traitement. Au cœur de ces garanties figure assurément le consentement, qui suppose que toute personne connaissant l'utilisation possible de ses données, consente effectivement à cette utilisation. Le consentement est souvent présenté comme la pierre angulaire du procédé de traitement des données des individus : son absence ne devrait pas permettre l'utilisation des données personnelles. Récemment, la législation européenne a entendu faire du consentement le socle de la protection des données à caractère personnel : « *le consentement devrait demeurer l'élément clé de l'approche de la protection des données de l'Union européenne, puisqu'il s'agit du meilleur moyen pour que les personnes puissent contrôler les activités de traitement des données, […] il devrait être aussi simple de retirer son consentement que de le donner* »[66]. Par ailleurs, la CNCDH considère que le refus d'autoriser le prélèvement des données formulé par la personne, ne doit pas fermer l'accès aux techniques numériques auxquelles l'individu souhaite avoir accès.

Si la CNCDH approuve totalement la philosophie de la législation européenne qui place le consentement au cœur du droit au respect de la vie privée numérique, elle constate que son rôle, aujourd'hui, ne doit pas être surestimé : dans la législation

65 *Ibid.*

66 Parlement européen, Commission des libertés civiles, de la justice et des affaires intérieures, *Projet de rapport sur la proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données* (règlement général sur la protection des données), 16 janvier 2013.

actuelle, en fonction de la nature de la collecte de données, il n'est une condition ni systématique ni toujours suffisante de la licéité du traitement des données. En outre, l'exigence d'un consentement, s'il ne s'inscrit pas dans un dispositif s'assurant de son caractère libre, spécifique et éclairé, n'est pas de nature à garantir à la personne une réelle maîtrise de sa vie privée et ses données personnelles. Face à l'utilisation toujours plus massive des réseaux internet et des objets connectés, les individus peinent à faire valoir leur consentement. La plupart ignorent même comment se protéger[67].

Dès lors pour certains, le recueil du consentement est une fiction, d'autant plus que les utilisateurs ne peuvent négocier les conditions d'utilisation de leurs données et que la plupart des fournisseurs de services de la société numérique – auquel il est très difficile de ne pas avoir recours – appliquent quasiment tous les mêmes procédés. Il n'existe pas alors de réelle liberté de choix. Seule marge de liberté qui tend à se développer, le choix entre une version gratuite du service, en échange de l'utilisation des données personnelles, et une version payante (souvent de qualité supérieure) sans intrusion supposée dans la vie privée. Cette liberté induit néanmoins une inégalité entre les utilisateurs en fonction de leurs moyens financiers.

Il apparaît par ailleurs que dans le monde numérique, le recueil du consentement n'implique la personne que de manière formelle, sans réellement lui donner les moyens de comprendre l'utilisation de ses données ou d'agir sur celle-ci. On peut alors se demander si le principe du consentement informé est réellement adapté à un modèle dans lequel la plus grande part de la collecte des données se fait de manière automatisée.

En tout état de cause, la CNCDH regrette les termes du débat parlementaire relatifs au consentement. Elle s'inquiète notamment qu'il n'ait pas été question de préciser ce qui constituait un consentement « valide » : la définition du RGPD, selon laquelle donner son consentement consiste à « manifester son accord de façon libre, spécifique, éclairée et univoque » (considérant 32), ne semble pas opérationnelle tant que chaque terme de cette formule n'est pas circonstancié. « *Cela ressemble à un vœu pieux tant il est difficile d'imaginer les entreprises scier la branche sur laquelle elles sont assises en demandant à leurs internautes de cocher la case : 'oui, j'accepte que mes données soient collectées et exploitées à des fins commerciales'. (D'ailleurs), l'internaute lui-même a du mal à prendre la mesure du problème* »[68].

67 Ainsi, 90% des Français se disent préoccupés pour leurs données mises en lignes (Sondage CSA, « Les Français et la protection de leur données personnelles », septembre 2017), mais ils sont 89% à affirmer ne pas lire ou lire partiellement les informations relatives aux politiques de confidentialité. Parmi eux, 80 % les considèrent comme trop longues, 54 % non modulables, et 42 % peu claires (Julie Lallouët-Geoffroy, « Ruses numériques : nos vies privées menacées par des Etats paranoïaques et les géants du Web », Chronique d'Amnesty International, n°376, mars 2018).

68 Amnesty International, « Gaffe aux Gafa », Julie Lallouët-Geffroy 27 mars 2018.

Rappelons que l'article 4-11 du RGPD reprend la définition qui fait du consentement la « manifestation de la volonté ». Comme le rappelait la CNCDH en 2015[69], la volonté doit être comprise comme le résultat d'une délibération en le for intérieur, le consentement étant la formulation publique des conclusions de cette délibération. Or, sur l'Internet, cette délibération interne est particulièrement difficile à informer, compte tenu des ramifications infinies de la toile. Comment, dans ces conditions, fixer dans le droit des critères d'accessibilité et de clarté propres à protéger l'usager ? Il faudrait commencer par établir une typologie des utilisateurs en fonction de leur capacité à exprimer un consentement éclairé sur la toile. Il convient de ne pas oublier qu'en fonction de l'âge, des caractéristiques cognitives, voire de la condition sociale, l'agilité numérique varie, si bien que les notions « d'accessibilité » et de « clarté des termes » doivent être adaptées. En la matière, la CNCDH se montre préoccupée par la vulnérabilité spécifique des enfants: dans le RDGP, la référence aux enfants est ainsi insuffisante et relève d'une vision stéréotypée de la capacité. Pour sa part, la CNCDH estime que, compte-tenu de l'importante intrusion dans la vie privée que peut constituer la collecte des données à caractère personnel sur l'Internet, il est raisonnable de fixer à 15 ans l'âge à partir duquel un mineur peut « *consentir seul à un traitement de données à caractère personnel* »[70], et ainsi s'inscrire sur une plateforme numérique ou un réseau social. Les dispositions prévues par le projet de loi relatif à la protection des données personnelles, amendé par l'assemblée nationale[71], lui semblent à ce titre répondre à un équilibre entre protection des mineurs et émancipation numérique des jeunes.

Pour autant, le principe selon lequel les données personnelles ne peuvent être traitées qu'avec le consentement de la personne (sauf autre fondement légitime expressément prévu par la loi) touche au sens même de la protection de la vie privée et doit être maintenu, dans la mesure où cette obligation tend à reconnaître la liberté de la personne en matière d'utilisation de ses données personnelles. Aucune des approches qui nieraient cette liberté en lui préférant la liberté de réutilisation des données personnelles indépendamment de la volonté de l'individu, ou encore qui affirmeraient à l'excès la nécessité d'une intervention tutélaire de la puissance publique, postulant que l'individu dans le monde du « big data » serait incapable de veiller à ses données, ne saurait être suivie. Ne pourrait-on pas substituer à ces approches et dans le cadre du droit à l'autodétermination informationnelle, une démarche dite d' « empowerment » des individus, en développant leur capacité à appréhender l'utilisation de leurs données

69 CNCDH, *Avis sur le consentement des personnes vulnérables*, 16 avril 2015.

70 Article 14 A du Projet de loi relatif *à la protection des données personnelles*, n° 490, déposé le 13 décembre 2017 (voir ci-dessous).

71 Projet de loi relatif à la protection des données personnelles, n° 490, déposé le 13 décembre 2017, Article 14 A : La section 1 du chapitre II de la loi n° 78-17 du 6 janvier 1978 précitée est complétée par un article 7-1 ainsi rédigé : « *Art. 7-1. – En application du 1 de l'article 8 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, un mineur peut consentir seul à un traitement de données à caractère personnel en ce qui concerne l'offre directe de services de la société de l'information à compter de l'âge de quinze ans.*
*« Lorsque le mineur est âgé de moins de quinze ans, le traitement n'est licite que si le consentement est donné conjointement par le mineur concerné et le ou les titulaires de l'autorité parentale à l'égard de ce mineur.*
*« Le responsable de traitement rédige en des termes clairs et simples, aisément compréhensibles par le mineur, les informations et communications relatives au traitement qui le concerne.* »

personnelles et à la paramétrer par des outils adaptés ?

Il s'agirait alors d'utiliser les technologies pour renforcer la capacité des personnes à contrôler l'utilisation de leurs données. Si les technologies numériques conduisent à une dissémination toujours plus importante des données personnelles, elles peuvent aussi être utilisées pour protéger la vie privée (Privacy Enhancing Technologies) afin de rendre les données moins accessibles à des tiers (moyens de cryptage, réseaux privés virtuels…), ou pour renforcer la maîtrise de l'individu sur l'utilisation de ses données personnelles par des tiers (bloqueurs de « cookies », solution de gestion des données personnelles, plateformes d'accès à l'ensemble des données personnelles détenues par un ensemble de partenaires…).

### 3. Maîtrise des données transmises : conservation des données, droit à l'oubli, droit à la portabilité

Le droit de l'Union européenne, à travers le RGPD mais également la jurisprudence de la Cour de justice, renforce la maîtrise des individus sur leurs données personnelles en ligne. Ainsi, dans l'arrêt Google c/Spain, le juge européen a consacré le droit au déréférencement. Outre la question du champ d'application territorial des législations nationales relatives à la protection des données personnelles, cet arrêt est de première importance : il définit pour la première fois les responsabilités en matière de protection des données personnelles d'une catégorie d'acteurs numériques, les moteurs de recherche.

Autre possibilité offerte pour la maîtrise des données transmises, le droit à la portabilité, dont la CNCDH souhaite qu'il puisse s'appliquer sans restriction. Le RGPD semble l'avoir conditionné de manière excessive, et subordonné à des intérêts d'ordre économique[72]. En effet, le droit à la portabilité tel qu'il est défini à l'article 20 du RGPD ne s'applique pas aux données personnelles traitées sur une autre base légale que celle du consentement ou de l'exécution d'un contrat[73]. Or, le caractère fragile du consentement et les limites de la liberté contractuelle[74] sont susceptibles d'en limiter la portée. De plus, les établissements financiers ont toute latitude pour prélever les données personnelles traitées dans le cadre de leur activité de lutte contre le blanchiment. La CNCDH plaide au contraire pour une application intégrale du droit à la portabilité, c'est-à-dire la possibilité pour un usager de demander au responsable de traitement le retrait de l'ensemble des données, personnelles ou non personnelles (la frontière entre les deux se révélant de plus en plus ténue), et leur réutilisation, à son initiative. Cette compréhension exhaustive du droit à la portabilité a été envisagée par la loi pour une République numérique, bien que celle-ci en ait retardé l'application[75]. Pourtant, la

72 Audition de Benjamin Bayart, le 23 janvier 2018.
73 https://www.cnil.fr/en/node/23625.
74 (Voir paragraphes sur les limites de la liberté contractuelle).
75 Bien que promulguée en octobre 2016, la loi laisse en suspens la question du droit à la portabilité afin de mettre en conformité cette conception avec celle du règlement européen dont l'entrée en vigueur est prévue pour mai 2018.

CNCDH estime cette orientation plus protectrice et rejoint entièrement, sur ce point, les observations du rapporteur de la Commission des lois au Sénat, M. Christophe-André Frassadu : « *il s'agit moins d'anticiper le droit à la portabilité des données personnelles prévu par le futur règlement européen que d'assurer la régulation d'un secteur économique au bénéfice du consommateur et de la concurrence. [La portabilité des données non personnelles] est une chance de briser le quasi-monopole des grands opérateurs sur la concentration des données des utilisateurs des services en ligne, en permettant à des entreprises innovantes de proposer à ces derniers des services plus adaptés, exploitant directement la masse des données transférées* ». Cette déclaration est d'autant plus pertinente après les révélations du PDG de Facebook sur le laxisme dont l'entreprise a fait preuve dans la protection des données de certains de ses usagers[76]. Compte tenu des observations faites précédemment sur la perméabilisation croissante de la frontière entre vie privée et vie publique, la CNCDH déplore que cette orientation n'ait pas été retenue par l'assemblée nationale[77].

## B. Diversité et pluralité des intérêts légitimes sur la toile

### 1. Impératifs de lutte contre la criminalité

La vie privée peut légitimement connaître certaines restrictions, voire certaines ingérences de la part des États, notamment lorsqu'elles sont effectuées dans le cadre de missions d'intérêt public comme la lutte contre la criminalité[78]. Ceux-ci peuvent notamment mettre en place, dans le cadre de procédures administratives et pénales, des dispositifs pour recueillir des données, indépendamment de tout consentement. Dans ce cadre, le recueil des données doit être légitime, légal, nécessaire et proportionné conformément au standard du droit européen des droits de l'homme, ce qui pose notamment la question de la manière dont les opérateurs privés conservent les données pour les autorités judiciaires et administratives, et notamment la durée légale de leur conservation.

Le droit de l'Union européenne, dans l'arrêt Télé 2 Sverige AB rendu par la Cour de justice, limite le pouvoir des États d'exiger des opérateurs qu'ils conservent les métadonnées de leurs utilisateurs en vue d'être exploitées par les autorités publiques. Les États européens se sont logiquement montrés hostiles à cette décision et les législations relatives à la conservation des données qui limitent leurs capacités d'investigations. Certains magistrats plaident pour leur maintien[79], en ce qu'elles permettraient une lutte plus efficace contre la criminalité et le terrorisme. Si l'étude des métadonnées s'avère efficace pour lutter contre le terrorisme, elle peut également

76 A la suite de l'affaire Cambridge Analytica, Marc Zuckerberg a reconnu que la quasi-totalité de ses 2 milliards d'utilisateurs était de fait exposée au vol de leurs données.

77 En mars 2018, l'assemblée nationale a ainsi décidé d'abroger l'article 48 de la loi Numérique – applicable à partir du 25 mai 2018, comme le prévoit le RGPD.

78 Voir paragraphes 29 et 34.

79 Audition de Mme Charlotte Huet, représentant la Direction des affaires criminelles et des grâces, le 13 février 2018.

être utilisée pour des infractions de moindre intensité, même pour celles qui ne sont pas de l'ordre de la criminalité ou du terrorisme : toutes celles commises au moyen des télécommunications. Il est vrai que les métadonnées permettent d'éprouver de manière objective les allégations et les alibis sans porter atteinte au secret des correspondances et sans recourir à l'aveu. Mais l'accès aux données personnelles par le juge, ainsi que leur conservation systématique, peuvent constituer une menace pour la vie privée. Ainsi, quand il s'agit d'estimer le caractère proportionné ou non de la collecte généralisée de métadonnées, il faut concilier le droit au respect de la vie privée avec les objectifs de sécurité, ce qui suppose un accès aux données numériques conservées par les opérateurs.

La CJUE, dans l'arrêt précité Télé 2 Sverige AB, n'a toutefois pas retenu cet argument, au motif que le recueil et la conservation généralisée des données menaçaient de créer une société de surveillance généralisée et de porter atteinte à la vie privée. Saisie de deux affaires portant sur l'obligation générale imposée, en Suède et au Royaume-Uni, aux fournisseurs de services de communications électroniques de conserver les données relatives à ces communications, la Cour de Luxembourg a restreint l'accès aux données[80] aux seules fins de criminalité grave, excluant par conséquent le champ délictuel[81]. L'arrêt Télé 2 Sverige AB précise également qu'il ne peut être autorisé que pour les personnes soupçonnées de projeter, commettre ou avoir commis une infraction grave ou d'être impliquées, d'une manière ou d'une autre, dans la réalisation d'une telle infraction. Il n'est possible que lorsque « *les intérêts vitaux de la sécurité nationale, de la défense ou de la sécurité publique sont menacés par des activités de terrorisme et que l'accès aux données d'autres personnes permette de faire face à la menace* »[82]. Outre ces conditions exceptionnelles, la Cour de Luxembourg précise que l'accès aux données dans le cadre d'une procédure pénale doit faire l'objet d'un contrôle *a priori*, soit par une juridiction, soit par une entité administrative indépendante. Dans le même arrêt, dès lors que le recoupement des données « *est susceptible de permettre de tirer des conclusions très précises concernant la vie privée* »[83], la CJUE soumet également leur conservation à la seule finalité de lutte contre la criminalité grave (paragraphe 100). Ainsi s'impose le principe de proportionnalité, en vertu duquel les dérogations à la protection des données doivent être uniquement admises dans des cas de force majeure menaçant directement la sécurité des citoyens. Ce principe est clairement exprimé par le juge européen qui précise que, même si les circonstances s'y prêtent, « *la conservation des données n'en doit pas moins toujours répondre à des critères objectifs, établissant un rapport entre les données à conserver et l'objectif poursuivi* » (paragraphe 110). À ce titre, et conformément à cet arrêt, la CNCDH considère que

80 En particulier les données relatives au trafic et les données de localisation des abonnés à un fournisseur d'accès.

81 C'est tout le sens de l'arrêt Télé 2 Sverige AB. Dans cet arrêt, la Cour de Luxembourg tirant les conclusions de la directive de 2002 sur la protection des données et de la jurisprudence Digital Rights, condamne la collecte généralisée des données personnelles, au nom du respect de la vie privée.

82 Jean-Philippe Foegle, « L'État de surveillance au régime sec : la CJUE renforce la prohibition de la surveillance de masse », *Revue des Droits de l'Homme*, 2017, p.27.

83 CJUE, Téléz Sverige AB, Paragraphe 99, 21 décembre 2016.

l'argument qui consisterait à légitimer la conservation préventive de l'ensemble des données d'une population à des fins sécuritaires, est disproportionné eu égard au droit qu'a chaque individu au respect de sa vie privée, à la libre expression et à la possibilité de vivre sans qu'un enregistrement de ses moindres faits et gestes entretienne en lui l'inquiétude d'une surveillance constante. Dans la continuité de la CJUE, la CNCDH appelle à baisser la durée légale pendant laquelle les responsables de traitement ont pour obligation de conserver toutes les métadonnées des utilisateurs. Considérant en effet la conservation généralisée des métadonnées comme procédant d'une forme de surveillance de masse incompatible avec l'idéal démocratique, et tenant compte d'autre part des besoins d'efficacité de la justice, la CNCDH plaide pour une possibilité de captation et de rétention des données personnelles circonscrite et limitée dans le temps, sous contrôle d'une Autorité Administrative Indépendante.

### 2. Liberté d'expression et accès à l'information

Les réseaux sociaux permettent une démultiplication des possibilités de s'exprimer et de s'informer. La circulation des données, et notamment des données personnelles, participent de ce développement de la société de la connaissance. Sous cet angle de partage du savoir, la CNCDH n'est donc pas favorable à un régime juridique qui restreindrait et compartimenterait systématiquement les données personnelles au détriment de la circulation d'information d'intérêt public de nature politique, économique, sociale, culturelle ou judiciaire.

L'émergence d'un nouveau droit à l'oubli numérique, qui peut être considéré comme une composante du droit à l'autodétermination informationnelle, est ainsi susceptible de porter atteinte à la liberté d'information et d'expression. Ce droit à l'oubli, consacré dans le droit de l'Union, notamment par l'arrêt Google Spain du 13 mai 2014[84], permet à une personne de demander que, dans le fonctionnement d'un moteur de recherche, des liens vers des pages web puissent être supprimés d'une telle liste de résultats au motif qu'elle souhaiterait que les informations y figurant et la concernant soient « oubliées » après un certain temps[85]. Ce droit au « déréférencement » permet donc, à certaines conditions, de supprimer certains résultats de recherche associés à une personne, mais il ne permet pas l'effacement de l'information sur le site internet source. Pour la Cour, il convient de rechercher un équilibre entre le droit de la personne sur ses données et le droit du public d'avoir accès à ses données. Cet équilibre met en balance la nature de l'information en question et sa sensibilité pour la vie privée de la personne concernée ainsi que l'intérêt du public à recevoir cette information, lequel peut varier, notamment, en fonction de la nature générale de l'information et du rôle joué par cette personne dans la vie publique[86]. En démocratie, le citoyen peut avoir un intérêt légitime à avoir

84 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.
85 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.
86 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.

connaissance d'une donnée personnelle relevant du droit au respect la vie privée. La CNCDH approuve le point d'équilibre fixé par la Cour européenne des droits de l'homme[87] entre liberté d'information et droit au respect de la vie privée autour de la notion de question d'intérêt public : là où aucune question de cette nature n'est en jeu, les impératifs du respect de la vie privée l'emportent[88]. Mais lorsqu'une question d'intérêt public est en débat, la vie privée est mise au second plan[89].

La CNCDH se prononce pour un service public du numérique afin de lutter contre la fracture du numérique et permettre un égal accès.

### 3. Données personnelles et éducation

La Commission entend soulever la question des données collectées en milieu scolaire, qui devraient relever de la notion de « mission d'intérêt public ». Si la captation et la conservation des données à caractère personnel peuvent en effet se révéler utiles dans le cadre éducatif[90], certaines « données scolaires » sont susceptibles de révéler de vastes pans de la vie privée des élèves, en particulier à la suite d'opération de recoupement : en agrégeant les données relatives aux absences et celle relatives à la fréquentation de la cantine, on peut, par exemple, déduire la confession d'un élève. De même, le handicap ou les troubles de santé peuvent apparaître dans le bulletin scolaire conservé en format numérique. On comprend que des parents puissent être réticents à renseigner les informations relatives à leurs enfants ou de consentir au traitement numérique de ces informations par les services scolaires. Pourtant, aujourd'hui, un enfant ne peut recevoir une éducation de qualité qu'à la condition que soient consentis la cession et le traitement de ces données. Du reste, sans collecte et traitement de données, il n'est pas envisageable de se projeter dans l'avenir promis par l' « e-learning » et l' « adaptive learning ».

Or, s'il fallait contraindre les services scolaires à une consultation de chaque parent afin de recueillir leur consentement au traitement des données de leur enfant, l'Éducation nationale se verrait contrainte d'offrir des services d'enseignement différenciés selon la sensibilité particulière de chaque parent. Les craintes pour le respect de la vie privée sauraient-elles justifier une rupture d'égalité entre les élèves en matière d'éducation ? La CNCDH estime qu'il est urgent d'intégrer les données collectées dans le contexte scolaire au champ des traitements relevant d'une « mission d'intérêt public » et d'appliquer les principes de contournement du consentement, de

87 C'est notamment l'objet de la jurisprudence Fuchsmann contre Allemagne de 2017. Les juridictions allemandes ayant refusé de supprimer un article de presse contenant des déclarations compromettantes sur un homme d'affaires, la Cour Européenne a dû vérifier que cette décision mettait correctement en balance des intérêts en cause. En l'espèce, le droit à la vie privée du justiciable (article 8 de la convention) et le droit à la liberté d'expression (article 10 de la convention) étaient en jeu. En confirmant la décision rendue par les juridictions internes, la CEDH donne plus d'importance à la liberté d'expression, par rapport au droit à la vie privée, au nom du droit à recevoir une information d'intérêt public.
88 CEDH, 24 juin 2004, von Hannover c/ Allemagne.
89 CEDH, 18 mai 2004, Sté Plon c/ France.
90 *Ibid*.

consultation préalable de la CNIL et de conduite obligatoire d'une étude d'impact lors de l'élaboration de tout nouveau traitement. Cette double exception aux dispositions générale du règlement – mais permise par celui-ci – permettrait de garantir le traitement à parité des enfants dans le cadre scolaire. D'ailleurs, et bien que toute anticipation soit délicate en la matière, on ne peut exclure qu'en contrôlant plus strictement les finalités des traitements, on réduise les risques de divulgation d'éléments de la vie privée des enfants auprès de tiers non fondés à la connaître[91].

La CNCDH recommande donc que le traitement de données collectées en milieu scolaire relève d'une « mission d'intérêt public ». Ces dispositions doivent spécifier que la collecte et le traitement de ces données : i) ignorent partiellement le consentement conformément à l'article 6 du RGPD ; ii) sont précédés d'une étude d'impact telle que le dispose l'article 35 du règlement ; iii) donnent lieu à une consultation préalable de la CNIL conformément à l'article 36-5 du règlement.

Par ailleurs, la recherche de systèmes d'information performants ne doit pas conduire à céder les données personnelles des élèves en contrepartie d'une offre de services gratuites des GAFAM. L'impératif pédagogique, s'il est légitime, ne doit pas rimer avec dépendance numérique à l'égard des géants de l'Internet[92]. La CNCDH recommande à cet égard l'utilisation de logiciels dit « open source », la conservation de données pour une durée strictement limitée au projet pédagogique et à l'intérieur de l'établissement scolaire.

Pour la CNCDH, les résultats scolaires des élèves sont des données privées qui doivent être protégées. Ainsi, la CNCDH s'inscrit contre toute possibilité d'accès public aux résultats scolaires. Dans la même logique, la CNCDH s'inscrit contre tout tri des élèves / candidats à un emploi indépendamment des décisions d'orientation des conseils d'orientation (pour les élèves) ou des diplômes.

### 4. Santé

Les données personnelles doivent également pouvoir être davantage exploitées pour des raisons de santé, comme il est écrit dans la loi de 1978[93]. La problématique est déjà tangible dans le champ des politiques de santé et le gouvernement a veillé particulièrement à détailler les conditions d'utilisation des données de santé[94]. Le projet

91 À l'heure actuelle, les enseignants utilisent, de fait, des applications numériques dans leurs classes. Il est difficile de contrôler ces usages et d'en anticiper les conséquences en matière de mise en danger de l'intimité des élèves. Audition de MM. Jean-Marc Merriaux, Inspecteur général de l'Administration, de l'Enseignement et de la Recherche et M. Gilles Braun, Inspecteur général de l'Éducation nationale, le 11 janvier 2018.

92 La CNCDH déplore la lettre du Directeur numérique du ministère de l'Education nationale, qui laissait entendre la possibilité d'une coopération –et donc, de confier et partager des données) des établissements scolaires français avec les GAFAM.

93 Loi n° 78-17 du 6 janvier 1978 relative *à l'informatique, aux fichiers et aux libertés*. Chapitre IX : « Traitements de données à caractère personnel à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé ». Le traitement des données dans ce contexte est tout de même réglementé (voir l'article 53 de la loi).

94 Audition de M. Anthony Duplan, Chef du bureau du droit constitutionnel et du droit public général, le 22

de loi relatif à la protection des données personnelles, dont l'article 13 est consacré aux données de santé, ne révolutionne certes pas l'esprit de la loi de 1978, mais va plus loin en établissant que certains traitements de données de santé peuvent relever d'une « finalité d'intérêt public ». Cette formule renvoie directement à la « mission d'intérêt public » contenue dans le RGPD, selon laquelle les données traitées dans ce cadre, y compris sensibles, peuvent bénéficier de certaines exceptions : si la collecte et le traitement de la donnée sont jugés nécessaires à la conduite d'une « mission d'intérêt public », le responsable de traitement peut notamment être dispensé de solliciter le consentement de la personne concernée (art. 6-e). Le RGPD prévoit des dispositions particulières pour les traitements, référentiels et règlements-types à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé, pouvant être établis par la CNIL, en concertation avec l'Institut national des données de santé. Le ministère de la Santé fait d'ailleurs de la simplification effective du partage des informations de santé entre tous les professionnels du soin un de ses trois objectifs stratégiques. Compte tenu de l'extrême confidentialité des données de santé, la CNCDH incite fortement à ce que le partage de ses données se fasse à travers un cryptage de qualité et des mesures drastiques de conservation.

L'exploitation de ces données ne doit pas aboutir à mettre un terme à l'universalité des systèmes de santé.

décembre 2017.

# III. L'effectivité des dispositifs de protection de la vie privée par le numérique

## A. Renforcer les garants de la protection des données

La protection de la vie privée à l'ère du numérique repose également sur un régime juridique exigeant applicable aux gestionnaires de données personnelles, qui doit continuellement être adapté et renforcé. Le RGPD marque le passage d'un mécanisme de formalités préalables (auprès d'une autorité de contrôle – en France, la CNIL) à un mécanisme d'autocontrôle : les gestionnaires des données sont érigés en « responsables de traitement ». Cette nouvelle approche, fondée sur la responsabilisation des acteurs des données, répond certes à la saturation des autorités de contrôle les rendant incapables de faire face à l'augmentation croissante des demandes d'autorisation, mais traduit aussi une nouvelle philosophie de l'action publique fondée sur l'autonomie et la responsabilité, dans le cadre d'objectifs. En optant pour ce nouveau mode de régulation, le législateur européen s'attache d'abord à garantir le bon fonctionnement du marché intérieur et à faciliter le libre flux des données au sein de ce marché. Le règlement, soucieux toutefois de garantir dans le même temps le respect de la vie privée des personnes, met donc en place un mécanisme destiné à pallier l'absence d'intervention de l'autorité de protection des données en mettant les responsables de traitement à contribution. Toutefois, le garant d'une régulation respectueuse des droits fondamentaux demeurant la CNIL, il est nécessaire qu'elle dispose des moyens de jouer ce rôle.

### 1. Les responsables de traitement au cœur de la nouvelle approche

Les responsables de traitement, c'est-à-dire les personnes privées ou publiques qui déterminent les finalités et les moyens d'un traitement de données, sont placées par le RGPD en première ligne pour garantir le respect de la protection des données : en contrepartie, le règlement fait peser sur les responsables de traitement toute une série d'obligations tant opérationnelles qu'informationnelles. D'abord, ils doivent prendre en compte la protection des données dès la conception d'un service ou d'un produit et par défaut, en réalisant le cas échéant une étude d'impact. Ensuite, ils doivent documenter cette prise en compte afin de pouvoir rendre des comptes à ce sujet, le cas échéant, auprès de l'autorité de contrôle.

Toutefois, si une analyse d'impact pointe le risque élevé attaché à un traitement de données pour la protection de celles-ci, la CNIL devra néanmoins faire l'objet d'une consultation. A cet égard, la CNCDH s'interroge sur l'appréciation laissée aux responsables de traitement de mener une étude d'impact. Si le RGPD indique en effet quelques types de traitement les plus susceptibles de faire peser un risque sur la protection des données, et par conséquent soumis à une étude d'impact (art.35), il laisse aux autorités de contrôle le soin d'indiquer, éventuellement, soit une liste de traitement dispensés de faire l'objet d'une étude d'impact soit une liste des types de

traitement soumis à une telle obligation. La CNCDH salue les efforts fournis par la CNIL pour indiquer aux responsables de traitement dans quel cas une telle analyse s'impose : selon elle, les traitements qui remplissent au moins deux des critères suivants doivent faire l'objet d'une analyse d'impact[95] :

- évaluation (y compris le profilage) ;
- décision automatique avec effet légal ou similaire ;
- surveillance systématique ;
- collecte de données sensibles ;
- collecte de données personnelles à large échelle ;
- croisement de données ;
- personnes vulnérables (patients, personnes âgées, enfants, etc.) ;
- usage innovant (utilisation d'une nouvelle technologie) ;
- exclusion du bénéfice d'un droit/contrat.

Il n'en reste pas moins que les entreprises sur lesquelles pèse l'obligation de mener une étude d'impact ne sont pas clairement identifiées à l'heure actuelle.

Si le responsable de traitement n'est pas le mieux placé pour apprécier l'opportunité et, surtout, la nécessité d'une étude d'impact, le RGPD prévoit pour certains responsables de traitement l'obligation de désigner un expert délégué à la protection des données. D'après l'article 37 du RGPD, cette obligation est valable pour : les autorités ou les organismes publics ; les organismes que leurs activités de base amènent à réaliser un suivi régulier et systématique des personnes à grande échelle ; les organismes que leurs activités de base amènent à traiter à grande échelle des données dites « sensibles » ou relatives à des condamnations pénales et infractions. Ce délégué, qui apportera son analyse pour l'identification et la coordination des actions à mener en matière de protection des données personnelles, se trouve donc appelé à jouer un rôle essentiel pour garantir le respect de la réglementation, tant nationale qu'européenne.

Dans la mesure où ses missions peuvent conduire le délégué à émettre des avis défavorables à certains traitements ou à certaines options envisagées par son employeur et qu'en ce sens, il se doit de pouvoir exercer ses missions de manière indépendante[96], le règlement européen précise les conditions propre à garantir cette indépendance : le responsable de traitement ne doit pas donner d'instruction au délégué ni pouvoir le relever ou encore le sanctionner pour l'exercice de ses missions[97]. Mais, le règlement ne détaille pas les garanties statutaires propres à assurer l'indépendance du délégué à la

95 Voir le site de la CNIL : « Ce qu'il faut savoir sur l'analyse d'impact relative à la protection des données (DPIA) », 19 février 2018, disponible à : https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-lanalyse-dimpact-relative-la-protection-des-donnees-dpia.

96 Audition de M. Pierre-Olivier Gibert, président de l'Association française des correspondants aux données personnelles, le 29 janvier 2018.

97 Art. 38, al. 3 du RGPD.

protection des données. Aussi la CNCDH estime-t-elle important que le droit national comprenne un régime de protection particulier pour les délégués, à l'instar des autres statuts de salarié protégé.

## 2. La CNIL, clef de voûte du nouveau régime

L'effectivité de ce nouveau régime « a posteriori » de protection des données, implique l'existence d'une autorité de contrôle susceptible d'assurer pleinement sa mission d'encadrement et de conseil aux responsables de traitement, d'une part, et de disposer d'un pouvoir de sanction véritablement dissuasif, d'autre part.

Sous le régime d'encadrement antérieur au RGPD, la CNIL disposait d'un pouvoir de sanction pécuniaire relativement limité. Au point que la sanction de 150 000 euros – le montant maximum à l'époque pour un premier manquement – infligée en 2013 à Google, au motif que la formulation et la présentation des règles de confidentialité de l'entreprise ne permettaient pas à l'utilisateur « *de prendre conscience des finalités réelles, et par conséquent de l'ampleur de la collecte des données le concernant* »[98], paraissait dérisoire au regard des capacités financières de cette dernière. Conscient de ce déséquilibre des forces, le gouvernement avait augmenté, dans la loi du 7 octobre 2016 pour une République numérique[99], le plafond des sanctions susceptibles d'être prononcées, le portant à 3 millions d'euros. Le RGPD va encore plus loin dans ce sens puisque, désormais, l'amende administrative peut s'élever à 20 millions d'euros ou, dans le cas d›une entreprise, à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent. La CNCDH approuve cette aggravation des sanctions, car elle constitue un élément essentiel pour assurer la crédibilité et l'effectivité de l'encadrement des responsables de traitement, en particulier s'agissant des grosses structures, tels que les GAFAM.

Les inquiétudes exprimées par les administrations compétentes à l'occasion des auditions, s'agissant de la protection des droits numériques, concernaient d'ailleurs principalement les moyens humains nécessaires à la mise en œuvre du nouveau cadre légal. Si le RGPD allège la charge des autorités de contrôle en mettant fin à la plupart des contrôles *a priori* des traitements, il laisse entrevoir un alourdissement considérable de la charge contentieuse qu'aura à traiter la CNIL, en raison de la multiplication des types de traitement et de la massification des données, combinées à la mise en place et la promotion de nouveaux droits. En outre, la CNIL sera appelée à concevoir des référentiels de certification et des codes de conduite, afin d'aider les responsables de traitement à s'approprier les dispositions du RGPD, et elle contrôlera également les organismes de certification chargés d'attester la conformité des traitements de données à ces référentiels. La CNCDH a été alertée au sujet des moyens humains insuffisants dont disposait aujourd'hui la CNIL[100]. À titre de comparaison, alors que la CNIL s'appuie sur un

98 Délibération n°2013-420 de la formation restreinte prononçant une sanction pécuniaire à l'encontre de la société X, 3 janvier 2014.
99 Article 65.
100 Audition de M. Jean Lessi, le 29 janvier 2018.

effectif de 200 agents, l'autorité de contrôle britannique, l'Information Commissioner's Office, en compte environ 700. C'est pourquoi il est indispensable que les pouvoirs publics renforcent les moyens de l'autorité de surveillance nationale, afin qu'elle puisse disposer des ressources humaines lui permettant sa mission de contrôle dans de bonnes conditions. Il est également indispensable qu'elle-même et ses homologues européens voient leurs prérogatives renforcées pour être à même de remplir leur mission.

Enfin, s'agissant d'une procédure administrative de nature punitive, la CNCDH recommande la clarification et la précision du régime procédural, notamment la pleine application des garanties du procès équitable.

### 3. Mettre fin au quasi-monopole des GAFAM

L'affaire Cambridge Analytica a mis en lumière la trop grande confiance que pouvaient accorder les citoyens aux réseaux sociaux du point de vue de leur intégrité. Si le PDG de Facebook, au cours de son audition devant le Congrès américain le 10 décembre 2018, a lui-même admis « *ne pas avoir suffisamment réfléchi à la manière d'éviter les abus* », force est d'admettre que l'affaire Cambridge Analytica a mis fin à un climat de relative insouciance à propos de la capacité des réseaux sociaux à conserver pour eux les données confiées par les utilisateurs.

Une des questions centrales de la protection des données personnelles est en effet celle du quasi-monopole exercé par les GAFAM sur l'Internet. Le contrôle de ces géants économiques sur les données des personnes est devenu permanent, à tel point qu'il est difficile d'envisager l'internet sans eux. A ce titre, la CNCDH émet l'idée d'une plus grande souveraineté numérique de l'Union européenne, qui permettrait d'imposer des droits fondamentaux et un ordre public numérique à ces opérateurs qui se jouent des différences entre les systèmes juridiques. La fin du quasi-monopole se traduirait par une plus grande pluralité des acteurs du web et favoriserait la démocratie numérique. Pourquoi ne pas encourager le développement de l'open source via des filières technologiques d'apprentissage adaptée et par la même occasion le développement d'acteurs européen du numérique.

Les menaces qui pèsent aujourd'hui sur la neutralité du Net inquiètent la CNCDH. Cette neutralité doit permettre à un internaute, quelles que soient ses ressources financières, de pouvoir accéder à l'ensemble des données et des informations disponibles sur le web. Aujourd'hui, non seulement des États mais aussi des entreprises veulent mettre fin à cette neutralité (blocage de site de partage de musique, de films, d'accès à des plateformes de communication…). Il s'agit là d'une atteinte à la liberté d'expression et d'innovation[101]. Dans cette entreprise de défense, la CNCDH encourage les initiatives d'organisations associatives d'éducation populaire qui militent pour la neutralité du Net. Pour autant, elle appelle également les pouvoirs publics à poursuivre

101 Benjamin Bayart, « L'Europe doit défendre la «neutralité du Net », *Libération*, 2017.

la défense de cette neutralité. A ce propos, la Commission se réjouit de la déclaration du président de l'assemblée Nationale, qui, dans ses derniers vœux à la presse, propose d'inscrire dans la Constitution[102] un « *droit fondamental promouvant un accès libre, égal et universel aux réseaux numériques* » pour les citoyens. Il se fait ainsi l'écho du travail du groupe parlementaire chargé de réfléchir à la « démocratie numérique »[103].

La cryptographie, dont la CNCDH constate à la fois l'importance comme application du « Privacy by design » et la carence dans la fabrication des objets connectés[104], s'avère être un outil efficace pour renforcer la protection de la vie privée[105]. Partant du principe que chaque individu souhaite toujours garder pour lui seul au moins une partie des informations en lien avec sa vie privée, l'Observatoire des libertés et du numérique[106] remarque que « *le cryptage permet de protéger des données et échanges pour les soustraire aux regards indiscrets, qu'ils soient ceux d'individus malveillants, de régimes autoritaires, etc* »[107]. A ce titre, l'Observatoire des libertés et du numérique ajoute que le cryptage est indispensable pour rendre ces échanges lisibles uniquement aux personnes à qui le message est adressé. Défini par lui comme « *un procédé permettant de transformer un message écrit et accessible à tous en un message codé, auquel seul ceux qui disposent du code ont accès* »[108], le codage, aussi appelé cryptage, s'avère nécessaire dans un Etat de droit pour garantir la vie privée face à l'intrusion des fichiers extérieurs. La CNCDH considère, en effet, que cette dimension de la protection de la vie privée ne doit pas être occultée, même si celle-ci connaît des mutations, dès lors que le principe d'efficacité dans les procédures judiciaires, régulièrement invoqué, peut favoriser les intrusions dans l'intimité des personnes. La CNCDH partage la position de l'Observatoire des libertés et du numérique sur cette question, en faveur d'un droit au cryptage sans restriction pour tous et de façon égale, « *non seulement pour conserver la confiance que les utilisateurs accordent aux services et outils numériques, mais également pour assurer le respect de la vie privée et la protection des données personnelles* »[109]. Si ce droit est déjà garanti par la loi sur la confiance dans l'économie numérique de 2004, celle-ci soumet encore l'importation et l'exportation des techniques de cryptage à une autorisation de l'ANSSI[110]. La levée de ces restrictions est d'autant plus nécessaire que le cryptage est déjà suffisamment fragilisé par les nombreuses possibilités dont disposent les services de police pour s'attaquer au cryptage[111].

---

102 http://videos.assemblee-nationale.fr/video.5388275_5a573555cfd7f.voeux-a-la-presse-de-m-francois-de-rugy-president-de-l-assemblee-nationale-11-janvier-2018.

103 http://www2.assemblee-nationale.fr/static/reforme-an/democratie/Rapport-1-GT6-democratie.pdf

104 Voir le paragraphe consacré à l'émergence des objets connectés dans un contexte d'apparition croissante de failles dans les systèmes de sécurité (première partie).

105 Note de l'ANSSI n°1085/ANSSI/DG.

106 https://www.lececil.org/node/20509.

107 Observatoire des libertés et du Numérique, « Chiffrement, sécurité et libertés », 2017.

108 *Ibid.*

109 *Ibid.*

110 Agence nationale de la sécurité des systèmes d'information.

111 Il ressort en effet du rapport de l'Observatoire des libertés et du numérique qu'outre les techniques de déchiffrement, les services de police ont recours au recueil systématique des métadonnées (ou « fadettes »), non soumises au chiffrement, ainsi qu'à l'enregistrement des conversations sur des cibles déterminées au moyens de sonorisations ou dispositifs tels que le « IMSI catcher », depuis la loi du 3 juin 2016. La CNCDH considère

La circulation et la diffusion des données personnelles sont non seulement propices à des atteintes à la vie privée, mais également à des discours de haine s'appuyant sur des éléments de vie privée. De plus en plus de discours de haine renvoient à l'intimité des personnes : leur religion, leurs convictions, leur mode de vie, leur orientation sexuelle font partie de la vie privée qui doit être protégée. Face à la violence des discours de haine sur la toile, la CNCDH ne peut donc que réitérer sa recommandation visant à initier une réflexion générale sur la définition d'un ordre public numérique, l'Internet devant demeurer un espace de liberté, respectueux des droits et libertés fondamentaux[112]. La Cour européenne des droits de l'homme n'a-t-elle pas énoncé en ce sens que « *l'internet est certes un outil d'information et de communication qui se distingue particulièrement de la presse écrite, notamment quant à sa capacité à emmagasiner et diffuser l'information. Ce réseau électronique, desservant des milliards d'usagers partout dans le monde, n'est pas et ne sera peut-être jamais soumis aux mêmes règles et ni au même contrôle. Assurément, les communications en ligne et leur contenu risquent bien plus que la presse de porter atteinte à l'exercice et à la jouissance des droits et libertés fondamentaux* »[113] ? L'avènement de la société numérique n'est pas le retour à un nouvel état de nature sans contrat social ni souveraineté politique[114]. A ce propos, la CNCDH entend rappeler que, s'agissant d'activités humaines, s'exerceraient-elles sur la toile, l'État a toute liberté pour les encadrer afin de garantir pleinement le respect des droits et libertés fondamentaux[115]. Cela est d'autant plus vrai que ces activités, virtuelles seulement en apparence, peuvent produire des conséquences bien réelles. A cela s'ajoute qu'il existe au demeurant une asymétrie des pouvoirs entre d'un côté, les usagers ou les associations, et de l'autre, les prestataires de l'Internet[116], ces derniers étant, bien souvent, des acteurs économiques extrêmement puissants.

## B. Education au numérique et formation au droit de la vie privée à tout âge

L'éducation aux droits de l'homme doit s'introduire dans le numérique à tous les niveaux où celui-ci est enseigné. La personne, si jeune soit-elle, doit comprendre le plus tôt possible que l'information qu'elle communique sur l'Internet fait partie intégrante

primordiale la levée des derniers conditionnements de la loi de 2004, notamment en matière de circulation des techniques de cryptage, pour enrayer la fragilisation croissant de celles-ci par les enquêteurs.

112 Voir : CNCDH, Avis sur les discours de haine, Assemblée plénière du 12 février 2015, JORF n°0158 du 10 juillet 2015, texte n°125

113 CEDH 5 mai 2011, Comité de rédaction Pravoye Delo et Shtekel c/Ukraine, req n°33014/05, § 63.

114 Pour plus de détails, voir B. Beaude, *op. cit.*, p. 28 et s.

115 Voir Conseil d'État, Etude annuelle 2014, *op. cit.*, p. 133.

116 Cette notion est entendue dans le présent avis au sens de l'article 2 de la directive 2003/31/CE du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur : « A*ux fins de la présente directive, on entend par : (…) b) «prestataire»: toute personne physique ou morale qui fournit un service de la société de l'information* ».
Par ailleurs, l'article 1er paragraphe 2 de la directive 2003/31/CE portant modification de la directive 98/34/CE prévoyant une procédure d'information dans le domaine des normes et réglementations techniques définit le service de la société de l›information comme « *tout service presté normalement contre rémunération, à distance par voie électronique et à la demande individuelle d'un destinataire de services* ».

d'elle-même, et que communiquer de cette manière implique d'être responsable de cette action. Au niveau politique enfin, où il est clair que la fracture numérique aujourd'hui peut être par elle-même une atteinte aux droits de l'homme. Une société ne peut s'engager dans une mutation aussi considérable des rapports entre l'individu et tout ce qui l'entoure, en tolérant que cette évolution se fasse à deux vitesses. L'éducation au numérique est fondamentale pour faire comprendre à l'utilisateur qu'il est un acteur à part entière de la protection de ses données.

La CNCDH rappelle l'importance d'une éducation au respect de la vie privée pour tous, y compris dans l'espace numérique qui est au cœur et la condition du droit à l'autodétermination informationnelle. Le RGPD n'envisage qu'inconsciemment le rôle des utilisateurs comme responsables de traitement. Or, depuis l'arrêt Lindqvist de 2003[117], la CJUE considère qu'une personne physique entre dans le champ d'application de la directive de 1995 : dès lors qu'une personne physique opère un traitement de données personnelles en dehors d'un cadre strictement « personnel et domestique » - même si ce traitement est effectué à titre gratuit - la personne devient « responsable de traitement ». En cela elle était soumise aux obligations fixées par la directive. Le RGPD n'ayant pas modifié les définitions sur lesquelles s'appuyait alors la CJUE[118], la jurisprudence Lindqvist est toujours applicable. Faut-il s'en émouvoir et juger que l'interprétation de la CJUE déforme les objectifs politiques affichés du législateur européen qui, à priori, ciblait les entreprises? En réalité, la CJUE rappelait en 2003 que l'utilisateur est aussi un acteur. Selon le principe même du « world wide web », où chaque ordinateur est un terminal actif, les internautes sont tous des animateurs de la toile. Concrètement, télécharger des images représentant une tierce personne sur son blog public constitue un traitement automatisé dont la finalité appelle à demander le consentement de la personne. Ainsi, de manière peut-être inattendue, le RGPD, axé sur le respect du consentement, constitue un fondement pour les victimes d'atteintes à leur intimité commises par d'autres internautes. Aussi, éduquer tous les internautes à la notion de consentement, ne consiste-t-il pas seulement à inviter l'utilisateur à la parcimonie en matière de versement de ses données : la sensibilisation au recueil du consentement est aussi une manière de mettre en garde l'utilisateur contre les mauvais usages des données d'autrui et le risque de tomber sous le coup de la loi européenne. À ce titre, on peut espérer que le RGPD devienne un moteur en faveur de la protection de la vie privée des jeunes en ligne.

La CNCDH salue les dispositifs d'éducation au numérique tels que Le collectif EDUCNUM, initié en 2013 par la CNIL, qui met à disposition du public « *un ensemble d›outils pédagogiques visant à développer et promouvoir auprès des jeunes en particulier un usage responsable des technologies numériques* »[119]. Concrètement, en matière d'éducation au numérique, EDUCNUM propose une sensibilisation à la

117 Cour de justice de l'Union européenne, arrêt du 6 novembre 2003, Bodil Lindqvist, affaire C-101/01.
118 Article 2 du RGPD.
119 http://eduscol.education.fr/numerique/toutlenumerique/veilleeducationnumerique/archives/2015/octobre-2015/construire-education-au-numerique.

protection de la vie privée en ligne, en particulier auprès des plus jeunes[120].

De nombreuses associations proposent des services sans contrepartie en matière de données personnelles et des applications en open source et sont désireuses d'intervenir en milieu scolaire[121]. La CNCDH estime qu'on ne peut qu'encourager ces initiatives et invite le gouvernement à fixer dans la loi les modalités de la coopération entre ces organisations et les établissements scolaires.

120 Chaque année, le « Trophée Educunum » récompense un étudiant de 18-24 ans pour son projet pédagogique de sensibilisation aux enjeux du numérique à destination des collégiens, et met à sa disposition une somme de 10 000 euros pour l'aider à le réaliser.
121 Audition de l'association Framasoft, le 22 décembre 2018.

# Synthèse des recommandations

Recommandation n°1 : La CNCDH recommande, à la suite de l'ONU, de favoriser un accès à l'Internet pour tous, car elle le considère comme un bien de premier de première nécessité. Elle considère également qu'exclure quiconque des technologies numériques constitue une atteinte aux droits de l'homme, d'autant plus lorsqu'elles sont utilisées pour faire valoir ses droits économiques et sociaux.

Recommandation n°2 : La CNCDH recommande que l'autodétermination informationnelle soit partie intégrante des droits de la personnalité tel qu'il est consacré en droit français.

Recommandation n°3 : La CNCDH recommande de baisser significativement la durée légale pendant laquelle les opérateurs ont obligation de conserver toutes les métadonnées des utilisateurs.

Recommandation n°4 : La CNCDH invite les pouvoirs publics à renforcer les moyens de la CNIL, et à clarifier et préciser davantage son régime procédural et répressif.

Recommandation n°5 : La CNCDH préconise l'intégration de l'objectif de protection de la vie privée dès la conception de la technique (« *Privacy by design* ») ou du traitement de données.

Recommandation n°6 : La CNCDH recommande que le droit national comprenne un régime de protection particulier pour le statut de délégué à la protection des données prévu par le règlement européen, à l'instar des autres statuts de salarié protégé.

Recommandation n°7 : La CNCDH préconise que les enjeux liés à la place du numérique dans les lieux de travail fassent l'objet d'un cadre national réglementé plus protecteur au bénéfice de l'ensemble des salariés, dans le cadre de l'obligation faite à l'employeur de faire respecter le droit à la santé et à la sécurité des salariés et de faire en sorte que la qualité de vie au travail ne soit pas une variable économique d'ajustement.

Recommandation n°8 : La CNCDH recommande un droit au cryptage sans restriction pour tous et un accès égal à ces outils ainsi que la vulgarisation de ces techniques.

Recommandation n°10 : La CNCDH recommande que, dans le cadre éducatif, le régime des données personnelles soit aménagé pour l'utilisation de logiciels dit « open source ».

Recommandation n°11 : La CNCDH recommande qu'à tous les niveaux d'accès aux techniques numériques soit associée une formation concernant ces utilisations. Cette formation peut être dispensée dès l'école par les moyens appropriés, afin que

la protection des données personnelles et le respect de la vie privée soient toujours garantis en tant que droits fondamentaux.

Recommandation n°12 : Elle encourage l'éducation nationale à développer chez les élèves des pratiques d'usage du numérique favorisant le regard critique sur leur activité en informatique, le sens de la responsabilité et l'aptitude à la coopération.

# Liste des personnes auditionnées

**Come Berbain**, Conseiller transformation numérique de l'Etat et sécurité numérique au Secrétariat d'Etat charge du numérique, 22 décembre 2017

**Anthony Duplan**, Chef du bureau droit constitutionnel et droit public général à la Direction des Affaires civiles et du Sceau du Ministère de la Justice, 22 décembre 2017

**Sophie Kwasny**, Directrice de l'unité de protection de données du Conseil de l'Europe, 22 décembre 2017

**Christophe Masutti et Pierre-Yves Gosset**, respectivement co-président et directeur de Framasoft, 22 décembre 2017

**Benjamin Bayart**, co-fondateur de la « quadrature du net », 23 janvier 2018

**Bernard Benhamou**, secrétaire général de l'institut de la souveraineté numérique, défenseur de la neutralité des réseaux et délégué dans le cadre du sommet des Nations Unies sur la question des données personnelles, 23 janvier 2018

**Jean Lessi**, secrétaire général de la CNIL, 29 janvier 2018

**Pierre-Olivier Gibert**, président de l'Association française des correspondants aux données personnelles (AFCDP), 29 janvier 2018

**Clyde Long de Lugo**, Directeur des relations institutionnelles de Snap Inc, 11 janvier 2018

**Anton Battesti et Ophélie Gerullis**, de la direction des relations institutionnelles de Facebook France, 11 janvier 2018

**Jean-Marc Merriaux**, Inspecteur général de l'administration de l'Education nationale et de la recherche (IGAENR), 11 janvier 2018

**Philippe Coen**, Respect Zone, 5 février 2018

**Olivier Esper** et **Benjamin Du Chaffaut**, Google France, 5 février 2018

**Marylou le Roy** et **Yann Bonnet**, équipe permanente du Conseil national du Numérique, 5 février 2018

CNCDH
COMMISSION NATIONALE CONSULTATIVE DES DROITS DE L'HOMME
RÉPUBLIQUE FRANÇAISE

Créée en 1947 sous l'impulsion de René Cassin, **la Commission nationale consultative des droits de l'homme (CNCDH) est l'Institution nationale de promotion et de protection des droits de l'homme française, accréditée de statut A par les Nations unies.**

L'action de la CNCDH s'inscrit dans une quadruple mission :
- conseiller les pouvoirs publics en matière de droits de l'homme ;
- contrôler l'effectivité des engagements de la France en matière de droits de l'homme et de droit international humanitaire ;
- assurer un suivi de la mise en oeuvre par la France des recommandations formulées par les comités de suivi internationaux et régionaux ;
- sensibiliser et éduquer aux droits de l'homme.

L'indépendance de la CNCDH est consacrée par la loi. Son fonctionnement s'appuie sur le principe du pluralisme des idées. Ainsi, seule institution assurant un dialogue continue entre la société civile et les experts français en matière de droits de l'homme, elle est composée de 64 personnalités qualifiées et représentants d'organisations non gouvernementales issues de la société civile.

La CNCDH est le rapporteur national indépendant sur la lutte contre toutes les formes de racisme depuis 1990, sur la lutte contre la traite et l'exploitation des êtres humains depuis 2014 et sur la lutte contre la haine anti-LGBT depuis avril 2018. Elle est l'évaluateur de nombreux plans nationaux d'action, dont depuis avril 2017 le plan national « Entreprises et droits de l'homme ».

20 Avenue Ségur - TSA 70334 - 75334 PARIS Cedex 07
Tel : 01.42.75.77 .09
Mail : cncdh@cncdh.fr
www.cncdh.fr

@CNCDH
@cncdh.france