CONSEIL D'ÉTAT
Étude annuelle

2022

CONSEIL D'ÉTAT

Étude annuelle 2022

Les réseaux sociaux : enjeux et opportunités pour la puissance publique

Les réseaux sociaux : enjeux et opportunités pour la puissance publique

73

CONSEIL D'ÉTAT

La Documentation française

df

CONSEIL D'ETAT

Étude annuelle 2022

Les réseaux sociaux : enjeux et opportunités pour la puissance publique

L'étude a été approuvée
par l'assemblée générale
du Conseil d'État
le 13 juillet 2022

Les rapports du Conseil d'État

Fondateur

René Cassin

Comité de direction

Didier-Roland Tabuteau, vice-président du Conseil d'État.

Martine de Boisdeffre, Sylvie Hubac, Rémi Bouchez, Christophe Chantepy, Edmond Honorat, Catherine Bergeal, Christophe Devys, présidents de section,

Thierry-Xavier Girardot, secrétaire général du Conseil d'État,

Fabien Raynaud, président adjoint et rapporteur général de la section du rapport et des études.

Directeur de la publication : Martine de Boisdeffre, présidente de la section du rapport et des études.

Secrétaire de rédaction : Corinne Mathey, secrétaire de la section du rapport et des études.

Comité de rédaction

Directeur de la publication : Martine de Boisdeffre, présidente de la section du rapport et des études (SRE),

Rédacteurs : Fabien Raynaud, président adjoint et rapporteur général de la section du rapport et des études,

Marie Grosset, rapporteure générale adjointe de la SRE,

Secrétaire de rédaction : Corinne Mathey, secrétaire de la SRE.

Cette étude a été délibérée en assemblée générale le 13 juillet 2022.

Publications du Conseil d'État chez le même éditeur

Collection « Les rapports du Conseil d'État » (ancienne collection « Études et documents du Conseil d'État », EDCE)
- Le droit souple – étude annuelle 2013, n° 64.
- Le numérique et les droits fondamentaux – étude annuelle 2014, n° 65.
- L'action économique des personnes publiques – étude annuelle 2015, n° 66.
- Simplification et qualité du droit – étude annuelle 2016, n° 67.
- Puissance publique et plateformes numériques : accompagner l'«ubérisation» – étude annuelle 2017, n° 68.
- La citoyenneté - Être (un) citoyen aujourd'hui – étude annuelle 2018, n° 69.
- Le sport : quelle politique publique ? – étude annuelle 2019, n° 70.
- Conduire et partager l'évaluation des politiques publiques – étude annuelle 2020, n° 71.
- Les états d'urgence : la démocratie sous contraintes – étude annuelle 2021, n° 72.

Collection « Les études du Conseil d'État »
- Le rescrit : sécuriser les initiatives et les projets, 2014.
- L'application du nouveau principe « silence de l'administration vaut acceptation », 2014.
- Les commissaires du Gouvernement dans les entreprises, 2015.
- Directives européennes : anticiper pour mieux transposer, 2015.
- Le droit d'alerte : signaler, traiter, protéger, 2016.
- Les règles applicables aux professionnels de santé en matière d'information et de publicité, 2018.
- La prise en compte du risque dans la décision publique, 2018.
- Révision de la loi bioéthique : quelles options pour demain ?, 2018.
- Les expérimentations : comment innover dans la conduite des politiques publiques ?, 2019.
- 20 propositions pour simplifier le contentieux des étrangers dans l'intérêt de tous, 2020.
- Les pouvoirs d'enquête de l'administration, 2021.
- Les conditions de ressources dans les politiques sociales : plus de simplicité, plus de cohérence, 2021.

Collection « Droits et Débats »
- L'accord : mode de régulation du social, n° 20, 2016.
- Entretiens sur l'Europe - Tome 1, n° 21, 2017.
- Droit comparé et territorialité du droit - Tome 1, n° 22, 2017.
- Droit comparé et territorialité du droit - Tome 2, n° 23, 2017.
- Les entreprises publiques, n° 24, 2017.
- Le droit social et la norme internationale, n° 25, 2018.
- Entretiens sur l'Europe - Tome 2, n° 26, 2018.
- L'ordre public - Regards croisés du Conseil d'État et de la Cour de cassation, n° 27, 2018.
- Les grands investissements publics, n° 28, 2019.
- Santé et protection des données, n° 29, 2019.
- La fiscalité internationale à réinventer ?, n° 30.
- La régulation économique de la santé, n° 31, 2020.

Collection « Histoire et mémoire »
- Conférences «Vincent Wright» - Volume 2, n° 4, 2015.
- Le Conseil d'État et la Grande Guerre, n° 5, 2017.
- Conférences «Vincent Wright» - Volume 3, n° 6, 2019.

Collection « Jurisprudences »
- Jurisprudence du Conseil d'État 2012-2013, 2014.
- Jurisprudence du Conseil d'État 2014-2015, 2016.
- Jurisprudence du Conseil d'État 2016-2017, 2018.
- Jurisprudence du Conseil d'État 2018-2019, 2020.
- Jurisprudence du Conseil d'État 2021.
- Jurisprudence du Conseil d'État 2022.

Sommaire

L'étude annuelle a été enrichie par de nombreuses auditions et interventions lors des colloques sur le cycle des réseaux sociaux. Que les participants en soient vivement remerciés.

L'étude a bénéficié de l'appui du comité d'orientation et du groupe de contact (v. listes des membres en annexe) et a été nourrie par les contributions de la délégation au droit européen de la section du rapport et des études, et d'Henri Plagnol pour les dossiers du participant des conférences du cycle sur les réseaux sociaux.

Dans le cadre de leur stage à la SRE, Roxane Abou, Elisabeth Buisson, Richard Chen, Emma Coroler, Charleene Eymard, Marie Hue, Marine Lebrun, Charles Morin, Evaristos Pimplis et Mélodie Roure ont contribué aux recherches et analyses documentaires.

Liste des abréviations et des acronymes

ANSSI	Agence nationale de la sécurité des systèmes d'information
ARCOM	Autorité de régulation de la communication audiovisuelle et numérique, née de la fusion du Conseil supérieur de l'audiovisuel (CSA) et de la Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet (Hadopi)
CC	Conseil constitutionnel
CCass	Cour de cassation
CE	Conseil d'État
CEDH	Cour européenne des droits de l'homme
CEPD	Comité européen de la protection des données institué par le règlement général sur la protection des données (RGPD - articles 68 à 76)
CESDH	Convention européenne de sauvegarde des droits de l'homme et libertés fondamentales, plus connue sous le nom de Convention européenne des droits de l'homme
CGU	Conditions générales d'utilisation
CJUE	Cour de justice de l'Union européenne
CNIL	Commission nationale de l'informatique et des libertés
CNNum	Conseil national du numérique, commission consultative française créée le 29 avril 2011 par décret du président de la République
CPC	Réseau européen de coopération en matière de protection des consommateurs (CPC) qui réunit les autorités publiques de tous les États membres de l'UE (et d'autres pays de l'EEE) chargées de l'application de la législation concernant la protection des consommateurs de l'UE
DDHC	Déclaration des droits de l'homme et du citoyen
DGCCRF	Direction générale de la concurrence, de la consommation et de la répression des fraudes du ministère de l'économie, des finances et de la souveraineté industrielle et numérique
DINUM	Direction interministérielle du numérique créée par décret du 25 octobre 2019, service du Premier ministre placé sous l'autorité du ministre de la transformation et de la fonction publiques
Directive DAMUN	Directive 2019/790 du Parlement européen et du Conseil du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique

Directive SMA	Directive (UE) 2018/1808 du Parlement européen et du Conseil du 14 novembre 2018 visant à la coordination de certaines dispositions législatives, réglementaires et administratives des États membres relatives à la fourniture de services de médias audiovisuels (directive «services de médias audiovisuels»)
DMA	Règlement (UE) *Digital Markets Act* présenté par la Commission européenne et adopté par le Parlement européen le 5 juillet 2022 et par le Conseil le 18 juillet 2022
DSA	Règlement (UE) *Digital Services Act* présenté par la Commission européenne, adopté par le Parlement européen le 5 juillet 2022 et devant être formellement adopté par le Conseil en septembre 2022, avant d'entrer en application en 2024
GAFAM	Acronyme des géants du Web — Google (Alphabet), Apple, Facebook (Meta), Amazon et Microsoft, désormais MAMAA — Méta (Facebook), Apple, Microsoft, Amazon, Alphabet (Google)
LCEN	Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique
Loi AVIA	Loi n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet
LOPPSI II	Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure
OCLCTIC	Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication, devenu sous-direction de la lutte contre la cybercriminalité au sein de la direction centrale de la police judiciaire
PeRen	Pôle d'expertise de la régulation numérique, service à compétence nationale créé par le décret n° 2020-1102 du 31 août 2020, rattaché au directeur général des entreprises (DGE) pour sa gestion administrative et financière et placé sous l'autorité conjointe des ministres chargés de l'économie, de la culture et du numérique
Rec.	Recueil Lebon
TCO	Règlement (UE) 2021/784 du Parlement européen et du Conseil du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne
RGPD	Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)
T.	Tables du Recueil Lebon
VIGINUM	Service de vigilance et de protection contre les ingérences numériques étrangères placé auprès du Secrétariat général de la défense et de la sécurité nationale (SGDSN)

Avant-propos

de Didier-Roland Tabuteau,
vice-président du Conseil d'État

L'étude annuelle pour 2022 marque une nouvelle étape dans la réflexion engagée de longue date par le Conseil d'État sur les développements du numérique. Dès 1997, il leur avait en effet consacré une première étude – Internet et les réseaux numériques – *qui avait ouvert la voie à ses études annuelles de 2014 sur* Le numérique et les droits fondamentaux *et 2017 sur* les plateformes numériques et l'« ubérisation » de l'économie*. Il vient par ailleurs de remettre à la Première ministre une étude, réalisée à sa demande, sur* l'intelligence artificielle, ses potentialités et ses risques pour l'action publique*.*

A chaque fois, grâce à sa situation au cœur de nos institutions et en tirant partie de la complémentarité de ses fonctions – consultative, juridictionnelle, d'étude et de proposition – et de l'expertise qu'il s'est progressivement forgée en la matière, le Conseil d'État a cherché à clarifier les termes des questions posées, à identifier leurs enjeux pour la démocratie et les politiques publiques, ainsi qu'à tracer des pistes pour l'avenir en formulant des recommandations pragmatiques et opérationnelles à destination des pouvoirs publics.

C'est la même approche qu'il a naturellement retenue pour appréhender le sujet des réseaux sociaux qui, dans un mouvement fulgurant, en sont venus à occuper, en moins de deux décennies, une place considérable dans notre société. En bouleversant nos manières de communiquer, ces lieux de rencontre et de dialogue numériques multiformes, qui ne cessent de se transformer, ont profondément remis en cause les cadres traditionnels de la vie en collectivité, au sein desquels s'étaient épanouis aussi bien la vie politique que la vie professionnelle, le débat public que les activités économiques, les relations internationales que l'action publique… Aucun domaine ni aucune institution ne semble ainsi épargné par l'émergence de ces outils, essentiellement privés, indifférents aux frontières nationales et qui reposent tous sur un modèle de relations horizontales et multicentriques, dénué d'autorité unique.

Face à ce phénomène bouillonnant, quasi-total et mondial, un diagnostic approfondi est apparu nécessaire : qu'est-ce qu'un réseau social ? Sur quels modèles technologiques et économiques reposent les principaux réseaux sociaux ? Quels sont leurs potentialités, mais aussi les risques qu'ils recèlent pour la société ? Car les réseaux sociaux, comme avant eux la plupart des grandes innovations technologiques, sont porteurs du meilleur, qu'il faut promouvoir, comme du pire, contre lequel il faut se prémunir.

Les défis auxquels ils nous confrontent sont d'ordres démocratique, stratégique, économique et sociétal ainsi qu'écologique. Les réseaux sociaux interrogent par ailleurs de front les fins et les moyens de l'action publique : la puissance publique doit-elle les réguler ? En poursuivant quels objectifs, à quel niveau et avec quels outils ?

Si, pendant longtemps, les États ont semblé renoncer à intervenir, laissant à ces plateformes numériques le soin de se réguler elles-mêmes, une telle retenue n'apparaît plus possible aujourd'hui, compte tenu, d'une part, de l'importance qu'elles ont de fait acquise, d'autre part des insuffisances de l'autorégulation, que de multiples dysfonctionnements voire scandales ont récemment mis en lumière.

L'Union européenne, qui s'est toujours voulue pionnière sur ces questions, a ainsi élaboré ces derniers mois un cadre juridique ambitieux visant à mieux réguler les réseaux sociaux tout en conservant leurs immenses bénéfices. Ce chantier vient de déboucher sur l'adoption des règlements sur les marchés numériques (Digital Markets Act) et sur les services numériques (Digital Services Act), qui doivent beaucoup à l'engagement et à l'action de la Commission européenne, sous l'impulsion de la présidence française de l'Union.

Ces règlements mettent en place un cadre et des outils. Le DMA, qui vise à rendre l'environnement numérique plus équitable et plus compétitif, instaure un nouveau modèle de régulation, centralisé auprès de la Commission européenne et fondé sur un système asymétrique d'obligations et d'interdictions ciblant exclusivement les grandes plateformes. Quant au DSA, s'il conserve aux plateformes leur rôle de modération des contenus sans leur imposer une obligation générale de surveillance, il impose une série d'obligations de transparence et de cohérence à leur charge coiffée, s'agissant des plus grandes plateformes, par un dispositif de supervision mené par la Commission européenne afin d'assurer un pilotage européen unique à la hauteur de la puissance de ces acteurs.

Les années à venir seront déterminantes : car beaucoup dépendra de la manière dont le cadre juridique européen et les nouveaux outils qu'il crée seront effectivement interprétés et utilisés. Il est ainsi indispensable que les autorités françaises, qui ont joué un rôle moteur dans l'adoption de ces textes, jouent également un rôle moteur dans leur mise en œuvre. Étant entendu qu'une approche nationale reste par ailleurs possible pour les questions qui ne sont pas réglées par ces textes, y compris pour préparer la voie à de futures initiatives au niveau européen : le cadre juridique devra rester dynamique pour s'adapter au développement des techniques et des usages.

Par les 17 propositions qu'il formule dans son étude, le Conseil d'État entend contribuer à ce que notre pays soit à la hauteur de la période décisive qui s'ouvre en ce domaine. Elles sont également nourries par la conviction que les pouvoirs publics doivent d'ores et déjà préparer les prochaines étapes, à la fois pour apporter des réponses pertinentes aux questions que les règlements européens ne permettent pas aujourd'hui de résoudre pleinement, et pour être prêts face aux nouveaux développements qui s'annoncent, comme par exemple celui du ou des métavers, qui ne manqueront pas de poser bientôt des questions juridiques, économiques et sociales nouvelles et complexes. Puisse cette étude contribuer au succès de ces initiatives.

Les réseaux sociaux : enjeux et opportunités pour la puissance publique

En 2022, on estime que près de 60 % de la population mondiale est active sur les réseaux sociaux (4,2 milliards d'utilisateurs) et que le temps moyen qui y est passé est de 145 minutes par personne et par jour. Mode de communication désormais incontournable, les réseaux sociaux suscitent enthousiasme ou crainte, et le rôle de la puissance publique dans cette sphère, qui concerne essentiellement la communication entre personnes privées, ne relève pas de l'évidence.

La présente étude intervient au moment crucial où l'Union européenne vient d'adopter deux règlements fondamentaux, le *Digital markets Act* et le *Digital services Act*, qui fixent le cadre général de régulation des marchés et des services des plateformes numériques en Europe. Elle souligne justement le rôle important que doit jouer la puissance publique dans ce domaine, même si elle ne devrait intervenir qu'avec retenue dans cet écosystème essentiellement privé. L'étude s'attache à **clarifier** la notion de réseau social ainsi que le cadre juridique applicable (première partie), puis à identifier les **enjeux** soulevés par cet outil y compris les opportunités qu'il offre pour les administrations (deuxième partie), enfin à développer une série de recommandations visant à permettre à la puissance publique de favoriser un usage plus équilibré de ces réseaux (troisième partie).

*

Afin de poser le cadre d'analyse, la **première partie** de l'étude, après avoir rappelé les conditions dans lesquelles sont apparus ces espaces conversationnels numériques, souligne la grande diversité des réseaux sociaux comme leur caractère protéiforme (plus ou moins publics, à usage professionnel ou de loisir, faisant des discussions ou échanges de contenus une fonctionnalité principale ou accessoire, etc.) et relève que les différences avec d'autres notions, comme celle de *médias sociaux* ou de *messageries*, sont faibles voire inexistantes. Compte tenu de la diversité des réseaux sociaux et du phénomène d'hybridation des plateformes (d'un côté, les réseaux sociaux s'ouvrent à l'activité purement commerciale des *market place* et, d'un autre côté, les plateformes de vente de services en ligne permettent la discussion entre internautes sur leurs sites), l'étude a pris le parti, dans un souci de pragmatisme, de retenir de la notion de « réseaux sociaux » une **définition large.**

C'est aussi celle retenue par le règlement européen *Digital Markets Act* (DMA), qui donne, pour la première fois dans un texte normatif, une définition de ce qu'est un réseau social (« *une plateforme permettant aux utilisateurs finaux de se connecter, de partager, de découvrir et de communiquer entre eux sur plusieurs appareils notamment* via *des* chats*, des publications, des vidéos et des recommandations. »*).

Poursuivant l'objectif de clarifier, y compris pour un public non averti, leur écosystème, l'étude rappelle les conditions d'inscription sur les réseaux sociaux, les principales fonctionnalités de ces réseaux ainsi que leur mode de fonctionnement, essentiellement fondés sur l'utilisation des données personnelles des utilisateurs et sur l'usage des algorithmes. L'étude précise les caractéristiques des modèles économiques des réseaux sociaux et souligne qu'ils conduisent à renforcer les plus importants d'entre eux, comme l'exprime la formule désormais consacrée du « *winner take most* » (le gagnant prend l'essentiel). La distinction entre les réseaux sociaux dits « grand public », qui reposent sur une organisation centralisée et poursuivent un but lucratif – même s'ils donnent l'illusion de la gratuité en faisant commerce des données – et les réseaux sociaux décentralisés, qui fonctionnent sur un modèle collaboratif, apparaît à cet égard fondamentale pour appréhender les enjeux que posent les réseaux sociaux.

La première partie présente le **régime juridique applicable aux réseaux sociaux**, qu'elle nomme, compte tenu de ses caractéristiques et en écho aux théories de l'économiste Jean Tirole, « *le droit multi-face des réseaux sociaux* ». Le réseau social numérique n'est pas une catégorie juridique à laquelle est attaché un droit spécifique. Relevant au contraire de nombreuses catégories juridiques, le droit qui lui est applicable se révèle composite. Par leur ingénierie, les réseaux sociaux sont soumis au droit des télécommunications, des données personnelles, des algorithmes et de l'intelligence artificielle. En leur qualité d'acteur du marché économique, ils sont soumis au droit de la concurrence et au droit du commerce. Par leur appartenance à la catégorie des personnes privées entretenant un lien contractuel avec les utilisateurs, ils sont soumis au droit des contrats et de la consommation. Par les fonctionnalités de discussion et d'échanges de contenus qu'ils offrent, ils sont soumis à l'ensemble des droits qui protègent la liberté d'expression, la vie privée, l'ordre public, la sécurité intérieure, les œuvres de l'esprit, les publics vulnérables (notamment les mineurs), etc.

Le droit des réseaux, quoique fragmenté, repose sur un **socle de valeurs communes** : la liberté d'entreprendre, la liberté d'expression, la protection de la vie privée et la protection de l'ordre public. L'étude relève que ce régime juridique s'est construit en **trois mouvements** qui sont encore à l'œuvre et s'influencent réciproquement : le premier a vu naître un droit spécifique à l'invention technique du numérique qui constitue désormais le *droit du numérique* ; le deuxième, duquel a émergé un droit largement européanisé spécifique aux nouvelles formes d'intermédiation des rapports économiques appelé *droit des plateformes*, vient d'être considérablement enrichi par l'adoption des règlements européens *Digital Services Act* (DSA) et le *Digital Markets Act* (DMA) ; le troisième transforme en profondeur les *droits traditionnels* à l'aune des réseaux sociaux et permet d'assurer une « couverture juridique » globale et cohérente des individus et de la société. Le droit régissant

les abus de la liberté d'expression, le droit pénal, le droit de la consommation, le droit de la publicité, le droit des mineurs, le droit de la concurrence et le droit des données personnelles, pour ne citer que les plus importants, se sont transformés sous l'effet des réseaux sociaux. Ce régime juridique multi-face conduit à ce que de nombreux régulateurs soient compétents, aux niveaux national et européen. Il ne cesse en outre d'être complété par de nouveaux textes dont certains sont en cours d'adoption à l'échelle de l'Union européenne (*Artificial intelligence Act*, *Media freedom Act*, *Data Act*, *règlement e-privacy*, etc.).

La deuxième partie de l'étude identifie les défis et enjeux soulevés par les réseaux sociaux, les réponses que les pouvoirs publics y ont déjà apportées et les questions sur lesquelles une intervention des pouvoirs publics reste nécessaire.

Le premier défi concerne **l'autonomie stratégique** française et européenne. Les réseaux sociaux, par leur maîtrise technologique, leur poids économique, par les modèles qu'ils promeuvent, par les informations qu'ils détiennent sur des centaines de millions d'individus grâce à leurs données personnelles, par leur capacité à s'affranchir de toute limite spatiale et temporelle pour imposer leurs conditions contractuelles à travers le monde et « optimiser » l'application des réglementations (y compris fiscales), fragilisent les États eux-mêmes. Cette hégémonie des grands réseaux, essentiellement américains et chinois, pose question en termes d'autonomie stratégique des acteurs économiques et même des États européens. Face à ces puissances nouvelles, de taille mondiale, le meilleur niveau d'action apparaît être celui de l'Union européenne, y compris pour proposer des alternatives techniques (*cloud* européen).

Le deuxième défi est lié au rapport complexe que les réseaux sociaux entretiennent avec **la démocratie**. S'ils permettent de donner du poids à l'expression citoyenne et se révèlent un outil de communication essentiel en période électorale, ils comportent aussi des risques : manipulations, campagnes de désinformation, tentatives de déstabilisation, etc.

Ce qui est certain, c'est que les réseaux sociaux ont changé le mode de fonctionnement du débat public, d'où un **troisième défi pour la vie en société** : de façon positive, en démultipliant les possibilités d'échanges individuels et en permettant à tout un chacun de faire entendre sa voix, y compris les plus minoritaires ou isolées ; de façon négative aussi, par la fragmentation voire l'atomisation du débat public qu'ils facilitent voire encouragent. Les groupuscules les plus extrêmes ont pu ainsi trouver dans cet outil de communication un moyen nouveau de diffuser leurs idées, y compris pour déstabiliser la démocratie représentative. Par ailleurs, pour accroître le temps de présence des utilisateurs sur les grands réseaux et multiplier les gains publicitaires, les contenus les plus virulents et les moins nuancés, qui accentuent l'engagement des utilisateurs, sont mis en avant par les algorithmes. Dans ces conditions, permettre un débat serein et constructif tout en préservant la liberté d'expression n'est pas une tâche facile, même si l'on peut constater un certain regain d'intérêt pour le journalisme « traditionnel » fondé sur l'indépendance éditoriale et la vérification des faits, y compris sur le Net.

Le quatrième défi concerne l'identité et l'intimité de **l'individu**. Au-delà des mots exprimés sur la toile, c'est l'existence de l'homme comme « animal social » qui se trouve modifiée par les réseaux sociaux. Les contours de la vie privée des individus se trouvent redessinés : de l'expression publique à l'expression privée et même de l'identité à la mort, les réseaux sociaux transforment le rapport de l'individu au monde. Maîtriser son image est désormais le souci de beaucoup et pas seulement des célébrités, l'e-réputation pouvant se détruire en quelques clics. Avec les réseaux sociaux apparaissent en outre des questions inédites comme celle de la mort numérique, de la sécurisation des identités et de la vérification des âges à l'ère du numérique, des traces numériques que les individus sèment à tous les vents…

Le cinquième défi est celui de la prise en compte des **mutations** économiques, sociales et écologiques provoquées par les réseaux sociaux. Les réseaux sociaux grand public, en raison de leur poids économique et du type particulier d'écosystème sur lequel ils reposent, ont transformé le secteur de la publicité, enrichi le marché de la data, permis l'émergence de nouveaux métiers ou activités (*social listenning*, *community managers*, influenceurs, créateurs de contenus, « travailleurs du clic »). L'étude souligne également le **défi écologique** induit par la démultiplication de l'usage des réseaux sociaux. Ils sont déjà responsables de 4 % des émissions des gaz à effet de serre et ce niveau pourrait atteindre 7 % en 2040. **Le dernier défi** est celui des **nouveaux dangers** induits par les réseaux sociaux, notamment pour les mineurs (addiction aux écrans, mésestime de soi, anxiété, isolement, exposition à la pornographie, harcèlement en ligne) mais aussi de façon plus générale pour la tranquillité publique (atteintes à la réputation, vengeances privées, fraudes).

En contrepoint de tous ces défis, il faut, il est vrai, rappeler les nombreuses **opportunités** que présentent les réseaux sociaux, y compris pour l'action publique elle-même, tant dans la modernisation et la fluidification des relations avec les usagers que pour accélérer sa mise en œuvre ou pour moderniser le fonctionnement interne de l'administration. Cette utilisation, déjà largement à l'œuvre, mérite parfois d'être mieux pensée et plus ordonnée.

Face à ces enjeux, la deuxième partie de l'étude, après avoir relevé le caractère indispensable mais insuffisant des mécanismes d'autorégulation des plateformes, décrit les outils d'expertise, d'analyse et de régulation dont dispose à ce stade la puissance publique. L'étude rappelle le rôle du juge, dans un secteur dominé par la régulation administrative, en particulier lorsqu'est en cause la liberté d'expression. De manière générale, il apparaît que les efforts des pouvoirs publics ont surtout porté ces dernières années sur la lutte contre la criminalité sur les réseaux sociaux, ce qui est parfaitement compréhensible.

Une fois analysés les défis posés par les réseaux sociaux et les instruments dont dispose à ce stade la puissance publique, l'étude présente les arbitrages cruciaux rendus par l'Union européenne avec l'adoption du *Digital services Act* et du *Digital markets Act*. Ces règlements ont fait le choix d'un encadrement des réseaux sociaux fondé sur la logique de **proportionnalité** (les réglementations étant asymétriques)**,** la **responsabilisation** des acteurs et une **supervision** renforcée confiée à la **Commission européenne** s'agissant des plus grandes plateformes. Ils

introduisent des mécanismes de régulation *ex ante* faisant reposer sur les acteurs eux-mêmes, notamment les très grands réseaux sociaux, la mise en place des instruments techniques permettant d'assurer effectivement le respect du principe de base selon lequel « *ce qui est légal hors ligne doit être légal en ligne et ce qui est illégal hors ligne doit être illégal en ligne* ». Lutter contre les propos illicites, exiger des opérateurs loyauté et transparence, astreindre les très grandes plateformes à des obligations supplémentaires notamment en termes de modération afin de mieux garantir la liberté d'expression, permettre aux chercheurs d'accéder aux algorithmes dans le cadre de recherches et d'audits, imposer des prescriptions en amont pour limiter les concentrations et les abus de position dominante, garantir un marché équitable, tels sont les objectifs que fixent les règlements *DSA* et *DMA* de manière nouvelle et ambitieuse. Ils constituent désormais le cadre juridique des politiques publiques en la matière.

Compte tenu des différents éléments ainsi analysés, le Conseil d'État propose, dans la **troisième partie** de l'étude, d'aller plus loin, en cohérence avec ce cadre juridique, pour permettre un meilleur usage et une meilleure régulation des réseaux sociaux. Les propositions qu'il a choisi de retenir ne portent pas principalement sur l'édiction de nouvelles normes, puisque le cadre normatif est désormais largement défini par les règlements que l'Union européenne vient d'adopter : il s'agit davantage de mobiliser des leviers d'actions visant à favoriser un usage plus raisonné et plus équilibré des réseaux sociaux. Dans un contexte en permanente évolution, il convient d'essayer de tirer le meilleur parti des opportunités incontestables qu'offrent les réseaux sociaux, tout en limitant autant que possible les risques de dépendance, d'addiction voire d'asservissement qu'ils comportent. Ses recommandations s'articulent ainsi autour de **trois axes** : **rééquilibrer le rapport de force** en faveur des utilisateurs, **armer la puissance publique** pour réguler et optimiser l'usage des réseaux sociaux sans oublier la sauvegarde de la souveraineté et la dimension environnementale, **penser** dès maintenant **les réseaux sociaux de demain.**

Le Conseil d'État estime d'abord que **l'objectif premier**, qui devrait guider l'action des pouvoirs publics tant dans la mise en œuvre des normes européennes que dans les recours éventuels à des instruments de droit interne, est celui d'un **rééquilibrage des forces en faveur des utilisateurs**, y compris par la promotion d'instruments garantissant l'autonomie stratégique et la préservation effective des droits fondamentaux des citoyens européens. Les textes que vient d'adopter l'Union européenne rendent possible un tel rééquilibrage. Mais des actions complémentaires ou renforcées paraissent possibles et souhaitables.

Ce rééquilibrage doit s'opérer tout d'abord au **niveau contractuel**. Au fondement de la relation entre l'utilisateur et la plateforme se trouve en effet un contrat, dont l'équilibre est aujourd'hui très favorable à la plateforme. Des efforts doivent être menés, tant au stade de la formation de ce contrat ou de sa modification, notamment en redonnant une réelle place aux utilisateurs ou aux associations qui les représentent, qu'aux différents stades de la vie du contrat. Le Conseil d'État recommande à cette fin d'engager une politique forte de soutien aux associations d'utilisateurs leur permettant de peser dans la négociation des clauses les plus

problématiques voire, à moyen terme, d'obtenir des standards minimums. Il propose également de promouvoir les **dispositifs de vérification d'âge et d'authentification des identités** afin de sécuriser les échanges contractuels et lutter contre le sentiment d'impunité.

Pour faciliter ce rééquilibrage, il souligne l'importance **d'aider les utilisateurs à mieux maîtriser l'outil** que constituent les réseaux sociaux, notamment les fonctionnalités de l'interface (à travers les paramétrages) et à faciliter l'exercice de leurs droits, d'améliorer leur information sur les plateformes afin de les guider dans leurs usages et choix, de rationaliser et simplifier le circuit des signalements de contenus et d'accompagnement des victimes. Le rééquilibrage devrait aussi s'exercer au bénéfice d'une meilleure connaissance des réseaux sociaux et formation à leur utilisation. Des propositions sont formulées en vue de soutenir **l'accès des chercheurs aux données** détenues par les plateformes, ainsi que le permettent le *DSA* et le *DMA*, d'améliorer l'accessibilité et la lisibilité du droit, de favoriser les contenus et médias de qualité, de renforcer les actions éducatives et de formation. L'étude propose également d'assurer une véritable sensibilisation au coût environnemental de l'usage des réseaux sociaux.

Enfin le rééquilibrage doit s'opérer au niveau stratégique en utilisant davantage les **réseaux dits alternatifs** qui, notamment par leurs modalités de fonctionnement et leur politique de sécurité, sont plus protecteurs de la vie privée des utilisateurs comme de la souveraineté des États. Le Conseil d'État recommande en outre aux pouvoirs publics de soutenir les initiatives visant à promouvoir les **communs numériques** et l'industrie numérique européenne.

Le **deuxième axe** des préconisations concerne **l'amélioration de l'organisation de la puissance publique** qui doit assurer la réussite des textes européens et améliorer son expertise dans le domaine des plateformes numériques. A cette fin, diverses mesures sont proposées pour assurer la coordination entre la Commission européenne et les États membres et entre les différents secteurs concernés. Comme l'a souligné la première partie de l'étude, le caractère multi-face du droit des réseaux sociaux implique l'intervention de nombreux régulateurs dont la coordination apparaît indispensable.

Les recommandations concernent évidemment au premier chef le niveau national. Il est proposé de créer un **service interministériel** permettant d'analyser et expertiser les questions soulevées par le numérique, de suivre l'exécution des politiques publiques dans le secteur et d'offrir un appui au **réseau des régulateurs** qui interviennent dans le champ de la régulation des plateformes numériques dont l'institution est également préconisée par le Conseil d'État. Ces instruments devraient notablement améliorer l'efficacité de la régulation qui doit s'appliquer aux plateformes pour assurer le respect effectif des règles en vigueur. Le Conseil d'État recommande également de formaliser une **stratégie de prévention des risques et de lutte contre les comportements malveillants et les contenus illicites** qui permettrait, outre de faire le point sur les effectifs des services de police et justice mobilisés à cette fin et de les renforcer si nécessaire, de rationaliser les dispositifs existants, de promouvoir des outils innovants d'enquête et de mieux coordonner leurs actions.

Pour mieux armer la puissance publique et les grands décideurs, le Conseil d'État recommande également d'agir résolument en faveur de la formation et de l'accompagnement en préconisant la **création d'une structure similaire à l'IHEDN consacrée au numérique** et à ses différents enjeux et dimensions. Par ailleurs, la définition d'une doctrine relative à la réutilisation des données personnelles apparaît nécessaire. Enfin, conscient que les réseaux sociaux, dans toute leur diversité, peuvent constituer de formidables atouts pour la puissance publique, il recommande d'en **généraliser l'usage** chaque fois que cela peut aider à une mise en œuvre plus efficace des politiques publiques et à un meilleur fonctionnement des administrations elles-mêmes, tout en accompagnant ce changement des garanties nécessaires.

Le **troisième axe** de propositions concerne le plus long terme.

Le Conseil d'État estime que la puissance publique devrait conduire dès maintenant une **réflexion approfondie permettant d'anticiper les enjeux des évolutions qui se profilent.** Certaines, comme celles relatives à l'encadrement de la **publicité ciblée** et la régulation des **messageries privées**, sont déjà en cours et doivent dès maintenant faire l'objet d'une attention particulière au regard des enjeux majeurs qu'elles représentent pour l'avenir. D'autres, comme celles du ou des **métavers**, sont encore à un stade préliminaire, mais risquent de poser des questions juridiques, économiques et sociales majeures au cours des prochaines années. Pour mieux se préparer à affronter les défis de demain et à préserver l'individu des mésusages de la technique numérique, le Conseil d'État suggère que la France prenne l'initiative, avec quelques partenaires proches, de proposer l'ouverture d'une négociation, à tout le moins européenne, sur **les droits de l'homme à l'ère du numérique**.

*

Au final, il apparaît qu'il n'existe pas de solution miracle mais une multitude d'actions à différents niveaux qui supposent toutes la responsabilisation de l'ensemble des acteurs et notamment des utilisateurs. La balle est dans le camp des opérateurs qui sont parties prenantes au processus de régulation, de la puissance publique qui se met en ordre de marche mais aussi des utilisateurs qui doivent raisonner leur usage pour faire des réseaux sociaux un outil au service de tous et non un instrument d'asservissement.

Introduction

«Les miroirs feraient bien de réfléchir un peu plus avant de renvoyer les images »
Jean Cocteau, *Le sang d'un poète* (1930)

« *L'amour est comme l'oiseau de Twitter*
On est bleu de lui, seulement pour 48 heures
D'abord on s'affilie, ensuite on se follow
On en devient fêlé, et on finit solo
Prends garde à toi
Et à tous ceux qui vous like
Les sourires en plastique sont souvent des coups d'hashtag »
Stromae, *Carmen* (Racine Carrée, 2013)

Printemps arabes (2010), mouvement #metoo (2017), révolte des gilets jaunes (2018), assassinat de Samuel Paty (octobre 2020), intrusion de manifestants dans le Capitole à Washington (janvier 2021), toutes ces entreprises, des plus prometteuses aux plus abjectes, ont pour point commun d'avoir prospéré grâce à l'intermédiation des réseaux sociaux. En passe de devenir le mode privilégié de communication, les réseaux sociaux ne bouleversent pas uniquement les rapports entre individus. Leur usage modifie en profondeur l'organisation des rapports sociaux et remet en cause les organisations institutionnelles sur lesquelles reposent nos sociétés contemporaines. Qu'on leur dénie un effet bénéfique pour l'humanité ou qu'on les considère, à l'inverse, à l'instar du numérique en général, comme le progrès majeur du XXI^{e} siècle, ils se sont imposés comme outils incontournables de la communication d'aujourd'hui. Dès lors, prendre la mesure des mutations dont ils sont le vecteur, apparaît indispensable.

Une chose est claire : **leur succès n'est pas fortuit**. En ce qu'il offre à chaque individu la potentialité d'une expression publique, l'outil « réseau social » semble idéal pour parvenir à une société démocratique fondée sur l'égalité des individus et la liberté d'expression des citoyens, comme une promesse d'accomplissement du rêve des Lumières. En ce qu'il prétend pouvoir fonctionner sans régulation externe et sans respect d'une quelconque autorité, il revendique aussi la possibilité d'ouvrir la voie à une sorte d'anarchie heureuse, chère à Proudhon. En ce qu'il repose sur une confiance très forte dans le progrès technique permettant l'épanouissement d'une société fraternelle et solidaire, on pourrait également lui trouver une parenté avec le Saint Simonisme. Mais quelle que soit l'idéologie à laquelle on pourrait le rattacher, le support qui est offert par les réseaux sociaux au langage, oral et écrit, lequel demeure l'outil premier de communication de l'être

humain, révolutionne, par ses fonctionnalités et ses potentialités techniques, le champ des possibles. A l'instar de l'invention de l'imprimerie, ce nouveau mode de communication rebat les cartes du jeu social. Il génère, jour après jour et à une vitesse jamais égalée, de si nombreuses mutations qu'on a peine à en mesurer l'ampleur. Il modifie l'échelle de transmission du savoir et l'organisation du pouvoir. Il transcende les frontières et les limites physiques qui auparavant cantonnaient les échanges, bousculant les notions fondatrices de la souveraineté nationale et de la démocratie représentative, donnant un nouveau sens à celle de souveraineté populaire. Il rappelle, comme l'avait énoncé Aristote, combien le langage, plus qu'un instrument de communication, est fondateur de la société.

Après avoir examiné au cours de **ses précédentes études**, les mutations engendrées par internet (1998), celles générées par le numérique sur les droits et libertés fondamentaux (2014), les transformations sociales, économiques et juridiques liées à *l'ubérisation* (2017) et l'utilisation de l'intelligence artificielle par la puissance publique (2022), le Conseil d'État, animé par le souci de promouvoir une action publique toujours plus en phase avec les évolutions de la société et les attentes des citoyens, a estimé indispensable de porter son attention sur ce nouveau mode de communication, d'en mesurer les atouts et les dangers et de réfléchir à ses implications politiques et publiques. Matière juridique récente, les réseaux sociaux se révèlent au carrefour de nombreuses disciplines. L'émergence de ce droit pluridisciplinaire en cours de formation nécessite la mobilisation de tous les jurisconsultes.

Entrelacs de communications[1], le réseau social, dans son acception contemporaine, repose, à l'instar des réseaux racinaires, nerveux ou ferrés, sur des interdépendances et des interconnexions qui forment un **tissu relationnel multicentrique et horizontal dénué d'autorité unique**. En ce sens, il diffère des systèmes relationnels binaires et hiérarchisés. La création du *réseau social numérique* appréhendé largement comme **un espace (service de communication en ligne) où il est possible, en se dotant d'un profil numérique, de se connecter avec d'autres internautes et de discuter et d'échanger des contenus préexistants ou créés par l'utilisateur**, – qui se distingue ainsi d'un simple *blog*, d'un mail ou d'une plateforme d'échange de biens et services, remonte à 1997, date de la mise en ligne de Sixdegrees, aujourd'hui disparu[2]. Mais le premier réseau social pérenne né en 2004 d'un système de discussion entre étudiants sur le campus d'Harvard, est **Facebook**. L'usage des réseaux sociaux est rapidement devenu **viral** et s'est largement étendu. Démultipliant les capacités d'expression instantanée des individus, il doit son avènement planétaire à la diffusion de la téléphonie mobile et du haut débit qui ont permis à chaque individu d'accéder à tout moment et rapidement au Web 2.0[3]. En 2021, on dénombrait ainsi environ 2.6 milliards d'abonnés à Facebook et plus d'un milliard pour Instagram.

1 L'étymologie du mot réseau nous renvoie au latin *rétis*, c'est-à-dire au filet, « *ouvrage formé d'un entrelacement de fils* ». Au XVII[e] siècle, le mot « réseau » désigne un entrecroisement de fibres textiles ou végétales utilisé par les tisserands et les vanniers.

2 Ce service, ancêtre de Facebook et de LinkedIn, proposait aux internautes de créer leur profil, d'entrer en relation avec leurs proches, amis, familles, collègues et de développer leur propre réseau social numérique. L'absence de photographies (la photographie numérique n'existait pas encore) ainsi que les vitesses réduites de connexion pour les utilisateurs ont sensiblement ralenti son développement.

3 Le Web 2.0 désigne l'ensemble des techniques, des fonctionnalités et des usages qui ont suivi la forme originelle du Web, www ou World Wide Web1, caractérisé par plus de simplicité et d'interactivité. Il concerne en particulier les interfaces et les échanges permettant aux internautes ayant peu de connaissances techniques de s'approprier des fonctionnalités du Web.

Découvrant les très importantes capacités de ces réseaux à générer du profit, puisque l'offre de contenu émane des internautes eux-mêmes et que l'entreprise a de très faibles coûts fixes, la très grande majorité des réseaux s'est constituée en **entreprises à but lucratif**, se finançant principalement par la publicité ciblée[4] et la monétisation des données personnelles des internautes. Ce modèle, qui permet un accès universel, donne aux usagers l'illusion de **la gratuité** au point que l'on pourrait croire que les réseaux sociaux sont des sortes de services publics de communication. Si quelques plateformes fonctionnent selon un modèle participatif et non lucratif, comme la célèbre encyclopédie digitale en ligne Wikipédia, tous les réseaux sociaux appartiennent au **secteur privé**. La plupart sont des **entreprises américaines** mais des réseaux majeurs comme TikTok, – réseau chinois, au demeurant interdit, sous sa forme occidentale, à l'intérieur de la Chine – et Telegram – fondée par des ressortissants russes – rencontrent un net succès. La plupart des réseaux sociaux français (Viadéo, Copains d'avant, Skyblog) qui existaient il y a 10 ans ont été supplantés par leurs concurrents américains. Seules des plateformes positionnées sur des secteurs de niche (tel Senscritique) ou des *civic tech* (comme Purpoz) ont résisté.

Ce point commun notable ne doit cependant pas faire oublier que le réseau social, loin de désigner une réalité univoque, est **protéiforme**, de sorte que le terme « réseaux sociaux », déjà pluriel, désigne des systèmes très divers qui évoluent constamment et se prêtent à de nombreuses interprétations.

Plusieurs catégories peuvent ainsi être distinguées.

Certaines plateformes proposent de favoriser les échanges et discussions à **titre principal** (Facebook, Twitter), d'autres à titre accessoire (YouTube, jeux vidéo, sites Web, forums de discussion). Et de même que les plateformes d'échanges commerciaux proposent à titre accessoire des fonctionnalités de discussions (comme les commentaires), les services traditionnels de réseaux sociaux diversifient eux aussi leurs offres et proposent des *markets place*, de sorte que les frontières entre les différents types de plateformes sont de plus en plus poreuses.

Il faut aussi noter que s'il est possible de communiquer sans cadre prédéfini sur les réseaux dits **généralistes**, certains réseaux sont spécialisés et structurés autour d'un type ou d'un format de contenu (la photo pour Pinterest). Les discussions peuvent se faire de **façon fermée** au sein d'une communauté rendue accessible par le consentement réciproque des utilisateurs (Instagram) ou de **façon ouverte** : les internautes peuvent ainsi avoir accès à des discussions sans même avoir un compte au sein du réseau (Twitter). **L'anonymat** est aussi plus ou moins utilisé selon les plateformes. Chaque réseau a sa spécificité (qui fait aussi sa force commerciale) : ainsi un tweet voit son nombre de signes limité à 280 caractères, Snapchat se singularise par le caractère éphémère des échanges réalisés, TikTok permet aux utilisateurs de réaliser des courtes vidéos de *lip-sync*[5], YouTube héberge des vidéos de toutes durées et permet aux internautes de les partager en streaming, Télégram permet d'échanger des messages cryptés qui peuvent s'autodétruire, etc. Certains réseaux, spécialisés comme LinkedIn ou Viadéo, permettent de mettre

4 Le chiffre d'affaire de la publicité ciblée de Facebook atteignait 95 milliards de dollars en 2020, soit 40% de plus qu'en 2019.

5 Synchronisation labiale.

en relation des professionnels, d'autres sont réservés aux rencontres amoureuses ou charnelles (Tinder, Grindr, etc.) ou aux *civic tech* (Make.org, etc.). Par ailleurs, aux côtés des mastodontes précités, existent de nombreux réseaux de petite et moyenne taille comme Valence community, réseau fondé aux États-Unis pour favoriser les relations professionnelles entre personnes de la communauté afro-américaine, Elpha community réservée aux femmes, Nextdoor destiné à former des communautés de vie autour des lieux de vie, MyHeritage permettant de réaliser sa généalogie, etc. En outre, les plateformes de « *gaming* » qui permettent à des joueurs en ligne de jouer en réseau sont à l'origine de véritables communautés virtuelles. Aussi divers et nombreux qu'il y a de centres d'intérêts, de multiples groupes immatériels voient le jour, au-delà des mers et des frontières.

Cependant, si aux débuts d'internet, fleurissaient de nombreux *blog, microblog,* messageries instantanées puis des réseaux regroupant plus ou moins ces différentes fonctionnalités, on assiste ces dernières années à un fort mouvement de **concentration** autour de quelques très importantes plateformes. Par un phénomène inéluctable d'attractivité, les réseaux les plus populaires attirent toujours un plus grand nombre d'internautes. Il est d'autant plus intéressant d'intégrer un réseau que de nombreuses personnes en font partie. C'est ce qu'on appelle ***l'effet de réseau***. Ce phénomène rend très difficile le maintien en vie des petits réseaux ou l'émergence de nouveaux réseaux sociaux hormis lorsqu'ils proposent une fonctionnalité innovante (comme l'a fait par exemple TikTok) ou un modèle différent (de type Mastodon[6]). Par la suite, pour survivre, celui-ci n'aura d'autre choix que de grandir et de ne pas se rendre dépendant des concurrents (les plus gros réseaux s'efforçant, après avoir aidé des Start up à grandir, à les copier ou les absorber). Ce phénomène de regroupement a largement participé à la modification du paysage économique mondial et à l'émergence de deux des GAFA : Google, qui détient YouTube depuis 2006, et Facebook, qui a racheté Instagram et WhatsApp. Ces deux sociétés, par une politique stratégique très agressive, défendent avec la plus grande vigueur leur pouvoir de marché, qui repose en grande partie sur le succès des réseaux sociaux parties prenantes de leurs écosystèmes.

Au fil des années, ce mode de communication a bousculé de nombreux champs, remis en cause des catégories et des frontières sur lesquelles sont fondées nos organisations, tout en nourrissant d'importants espoirs.

Les réseaux sociaux, en offrant un immense lieu de **débat public**, remettent en cause le modèle de la démocratie représentative ainsi que l'organisation verticale du **pouvoir**. Par l'horizontalité qui les caractérise et les nouvelles communautés qu'ils permettent de créer, ils constituent une alternative puissante aux organisations préétablies fondées sur la représentativité (syndicats, élus). Par ailleurs, alors que, jusqu'alors, la parole publique était pour l'essentiel l'apanage des élites, chacun peut dorénavant exprimer son opinion et faire valoir un point de vue particulier. Les réseaux sociaux détiennent un fort **pouvoir égalisateur**.

6 Mastodon est un réseau social libre, décentralisé, sans publicité et sur lequel l'internaute garde le contrôle de ses données.

Leur puissance planétaire pourra-t-elle aller jusqu'à faciliter l'émergence d'une **conscience planétaire universelle** déjà conceptualisée par Ernest Renan ou Pierre Theilhard de Chardin ? Les plus optimistes l'espèrent. Il est certain que ces échanges, fondés sur le partage de connaissance, révolutionnent ainsi la transmission du **savoir** et peuvent améliorer l'intelligence collective[7].

A une moindre échelle, ils peuvent faciliter de **nouveaux modes d'échange** au sein de la famille, des amis, de l'entreprise, du voisinage, d'une communauté syndicale, éducative, hospitalière, etc. En offrant à chacun la possibilité de s'exprimer, de diffuser des informations ou d'émettre des opinions et des critiques, sans filtre ni aucune autre forme d'intermédiation, ces services en ligne favorisent en effet une forme de réalisation nouvelle des **libertés d'opinion et d'expression** voire du **droit à l'information**. Ils favorisent également l'apparition de nouvelles formes de créativité artistique et intellectuelle. Ils peuvent également constituer un **moyen d'intensifier et d'élargir les liens sociaux**, en retrouvant des connaissances perdues de vue, en en rencontrant d'autres avec qui nous partageons des centres d'intérêts ou des amis en commun, ou tout simplement en offrant un nouveau canal de communication avec nos familles, nos collègues ou nos amis. Les réseaux sociaux offrent aussi aux entreprises, aux administrations et aux responsables publics de nouvelles façons de communiquer sur leurs actions. De nouveaux métiers ont vu le jour, comme celui d'influenceur ou de *community manager*. Les campagnes électorales se jouent dorénavant autant sur les réseaux sociaux que sur les traditionnels marchés. Il est en outre certain que de nouveaux usages, que nous ne sommes pas en mesure d'envisager pour l'instant, émergeront dans les années futures.

Face à ces immenses atouts porteurs de progrès, d'importants obstacles se dressent encore et la voie de la sagesse, – comme le soulignait déjà Voltaire avec ironie – semble encore lointaine. Outre le **fossé générationnel** qui se creuse entre ceux qui maîtrisent ses fonctionnalités et les autres, la communication par voie des réseaux sociaux exacerbe des difficultés déjà présentes dans les rapports sociaux et introduit de nouvelles vulnérabilités. Ne pas être présent sur les réseaux sociaux peut conduire à une forme d'ostracisme alors pourtant que l'individu doit demeurer libre d'y recourir.

Structuré pour **rendre captif son usager**, le modèle d'affaire du réseau social, aussi dénommé **marché de l'attention**, se révèle intrinsèquement problématique. Organisé autour de la stimulation permanente de l'utilisateur et jouant sur ses sentiments, notamment sa peur de perdre une information importante ou d'être exclu de la communauté (FOMO : *fear of missing out*), l'objectif est de le maintenir connecté le plus longtemps possible pour l'exposer au maximum de publicités ciblées. Cette économie, fondée sur l'addiction, a été désignée par la formule désormais célèbre de Shoshana Zuboff comme une manifestation du « *capitalisme de la surveillance.* » Pour attiser cette attention, le sensationnel, l'outrance, la haine et le complot sont des moteurs bien plus puissants que la nuance et la vérité.

7 B. Patino, *La civilisation du poisson rouge, Petit traité sur le marché de l'attention*, Grasset 2019, *Tempête dans le bocal, la nouvelle civilisation du poisson rouge*, Grasset 2022.

La **culture du soupçon** donne à chacun le sentiment de vivre dans un feuilleton plein de suspens, tenant en haleine l'ensemble des protagonistes. Ajoutés aux différents biais propres au numérique : biais cognitifs de confirmation (les moteurs de recherche permettent toujours de trouver ce que l'on cherche, y compris pour confirmer une erreur dont on ne souhaite pas se défaire), biais de représentation (une vérité contingente est présentée comme universelle) et biais d'exposition (la répétition finit par postuler l'importance de l'information) occasionnés par les algorithmes[8], tout converge pour faire primer la croyance sur la vérité, l'émotionnel sur le rationnel. Le risque d'addiction et de danger pour la santé mentale, des plus jeunes notamment, est en outre de plus en plus pris au sérieux.

Peu à peu, la frontière entre **vie privée et vie publique/professionnelle** se déplace voire s'efface, les réseaux devenant un immense théâtre où chaque individu promeut sa vie personnelle (*self-branding*), donne à voir ce qu'il souhaite (*auto-reporting*), se forge une image organisée dans une spontanéité qui n'est qu'apparente et soumet ses choix à la validation de ses pairs[9]. L'espace intime est toujours plus réduit, la pensée toujours plus uniformisée. Les réseaux apparaissent comme des galeries de portraits dont chaque personnage aurait exercé sa propre censure. Au sein de ces communautés virtuelles, rien ne semble pouvoir arrêter les manipulations consenties ou imposées. Les individus tendent à se trouver asservis par leur propre narcissisme, dans un monde virtuel dans lequel le *like* et le *retweet* font la loi. Ces effets néfastes sont visibles jusque dans les cours de récréation des écoles et les entreprises s'inquiètent également du dénigrement dont elles font l'objet par leurs salariés. Des individus préfèrent dénoncer leurs « agresseurs » sur les réseaux qu'aux services de police, les discours de haine et d'exclusion, pour avoir malheureusement toujours existé, trouvent dans les réseaux sociaux une caisse de résonance particulièrement puissante, « *(…) l'agora (est) transformée en arena (…)* » comme le souligne Bruno Patino[10]. Les utilisateurs tendent à s'auto-enfermer dans des « bulles d'information » dénuées de contradictions dans lesquelles la tendance est à la surenchère et à la diabolisation de ceux qui pensent différemment, devenant peu à peu des adversaires voire des ennemis. Dans ce véritable magma d'opinions, il faut, avec discernement, séparer le bon grain de l'ivraie : la *fake news* de l'information vérifiée, les lanceurs d'alerte des délateurs, les objections constructives des inquisitions.

Les réseaux sociaux sont donc capables du meilleur comme du pire.

Mettre de l'ordre dans ce champ bouillonnant en conservant les nombreux atouts de ces nouveaux modes de communication est donc devenu un enjeu majeur. Chaque évolution technique déstabilise des pans entiers de règles qui structurent les sociétés contemporaines et engendre des mutations et la perspective de l'utilisation généralisée du Métavers, monde virtuel fictif, accroît le champ des interrogations. Comme il a fallu réglementer l'usage des voitures lorsque les accidents se sont multipliés, la publicité lorsqu'elle menaçait d'envahir les écrans de télévision, il faut rendre possible l'assainissement des échanges sur les réseaux sociaux.

8 G. Bronner, *La démocratie des crédules*, PUF, 2013.
9 P. Escande-Gauquié, B. Naivin, *Monstres 2.0, l'autre visage des réseaux sociaux ?*, Ed. F. Bourin, 2018.
10 B. Patino, *op.cit.*

A la fin des années 1990, les pionniers des réseaux sociaux revendiquaient une *neutralité* et une liberté absolue sur le Web. La *déclaration d'indépendance du cyberespace* rédigé le 8 février 1996 au forum de Davos par John Perry Barlow pour protester contre une loi de censure sur les télécoms aux États-Unis en témoigne. Des années durant, les réseaux ont revendiqué leur incapacité à réguler les échanges au motif que, simples hébergeurs, ils ne pouvaient pas se voir confier la responsabilité des éditeurs de contenus. Malgré quelques tentatives, les États les ont laissés prospérer sans quasiment aucune contrainte. En 2016, le scandale de l'affaire *Cambridge Analytica*, société ayant analysé des milliers de données d'usagers de Facebook à leur insu durant la campagne électorale américaine pour influer sur le vote, a constitué un tournant. Outre les questions déjà identifiées du détournement des données et du mésusage des réseaux sociaux par le cybercrime, la société a découvert que le *design* de ces réseaux (mécanisme du *like*, du *retweet*, etc.) et les algorithmes de tri et de recommandation accroissent la brutalité des échanges et accentuent les mécaniques d'enfermement. En outre, face à la quantité exponentielle de données échangées, il a fallu se rendre à l'évidence : les réseaux sociaux hiérarchisent les contenus et ne sont plus de simples hébergeurs. Depuis, et alors que de nouveaux événements et révélations nourrissent jour après jour cette prise de conscience, la nécessité de **réguler** les réseaux sociaux est apparue cruciale. Certes des mécanismes d'auto-régulation sont mis en œuvre par les plateformes elles-mêmes mais ils montrent chaque jour leurs limites tant par leur insuffisante efficacité et fiabilité[11] que par le risque de privatisation de la censure qu'ils induisent. Par ailleurs, les outils classiques de régulation comme le droit de la presse, le droit de la concurrence ou le droit fiscal sont apparus insuffisants et, à certains égards, inadaptés[12].

L'accumulation de textes internationaux et de lois adoptés ces dernières années pour encadrer le secteur du digital et des données13 commence cependant à **inverser le rapport de forces**. La légitimité des États à intervenir pour réguler ces sociétés privées ou réfléchir à de nouvelles formes de réseaux sociaux, bien que tardive, est dorénavant admise, même par les pays les plus libéraux. Et si certaines questions relèvent du champ international, d'autres peuvent être définies par les États souverains. Que ce soit par la régulation des marchés, le contrôle des contenus, l'exigence de transparence et d'accessibilité aux algorithmes, la vérification de la fiabilité des données transmises aux autorités régulatrices, la protection des données, la responsabilisation des usagers, l'adaptation de la fiscalité ou l'adoption de législations transversales contraignantes, plusieurs leviers existent dont aucun ne semble à lui seul suffisant. La régulation peut donc s'opérer de différentes façons et l'articulation de ces différents mécanismes et des autorités chargées de les mettre en œuvre est une question majeure. Mais, là encore, un équilibre doit être recherché pour éviter de basculer dans un système déjà à l'œuvre dans

11 J. Toledano, *Gafa, reprenons le pouvoir,* Odile Jacob, p. 18-19, septembre 2020.

12 P. Collin, N. Colin, rapport, *Mission d'expertise sur la fiscalité de l'économie numérique*, janvier 2013 ; Autorité de la concurrence , *Contribution au débat sur la politique de concurrence et les enjeux numériques*, février 2020.

13 Directive 2000/31/CE du 8 juin 2000 sur le commerce électronique, RGPD du 27 avril 2016 ; directive (UE) 2019/790 sur le droit d'auteur et les droits voisins dans le marché unique numérique ; règlement (UE) 2019/1150 du 20 juin 2019 ; loi informatique et libertés du 6 janvier 1978 ; loi pour l'économie numérique du 21 juin 2004 ; loi pour une République numérique du 7 octobre 2016 ; loi du 22 décembre 2018 dite de lutte contre les *fake news* ; loi du 24 juin 2020 dite *Avia*.

certains pays comme la Chine où les réseaux sociaux soumis à la censure de l'État révèlent des mécanismes de surveillance plus puissants encore que ceux imaginés par les meilleurs auteurs de science-fiction.

Face au double enjeu de mieux réguler les réseaux sociaux tout en conservant les bénéfices immenses de cet outil technologique dont toutes les fonctionnalités n'ont pas encore été découvertes, des **questions politiques et juridiques** délicates se posent. Les arbitrages doivent tenir compte de certaines données comme le fait que les consommateurs plébiscitent l'usage des réseaux sociaux et semblent, en l'état actuel des choses, faire davantage confiance aux plateformes internationales qu'à leur propre État. Ils doivent aussi trouver un point d'équilibre dans le maniement des principes fondamentaux qui garantissent l'égal accès au net, sa neutralité, le droit à la protection des données, la liberté d'expression et de communication, le respect de la vie privée, la liberté du commerce et de l'industrie et le principe de responsabilité.

Quel espace public de communication promouvoir ? Que souhaitent les citoyens ? Faut-il combattre l'économie de l'attention alors que tant d'internautes apprécient l'usage des réseaux sociaux ? A quel point la puissance publique peut-elle s'immiscer dans les échanges privés ? Quel bon niveau de régulation adopter selon les domaines (interne, national, international) ? L'État dispose-t-il des informations et moyens suffisants pour adapter ses actions ? Comment éviter que la technicité des outils numériques ne soit un frein à la régulation ? Dans quelle mesure faut-il accéder aux algorithmes ? Quelle transparence et traçabilité imposer ? Comment exercer un contrôle des contenus sans porter atteinte à la liberté d'expression particulièrement protégée par notre Constitution ? A quel point faut-il éviter les concentrations d'entreprises sachant que le contrôle d'un marché trop éclaté est très difficile ? Quels contre-pouvoirs renforcer ? Faut-il réguler la publicité ciblée ? Faut-il s'appuyer sur l'engagement des internautes ? Quels usages faut-il promouvoir pour l'administration? L'État doit-il utiliser les réseaux sociaux pour se moderniser ? Faut-il créer un réseau social public ? L'État souverain est-il réellement menacé par ces nouveaux médias ?

Les questions abondent, les réponses foisonnent, les rapports s'accumulent, le sujet captive. Plus qu'un ordonnancement, c'est une vision d'ensemble qui paraît indispensable pour aborder les évolutions futures.

La présente étude poursuit l'ambition, quelque peu démesurée, de présenter l'économie contemporaine des réseaux sociaux et son régime juridique actuel (première partie), d'énoncer les grands enjeux pour la puissance publique qu'ils induisent (deuxième partie) et de formuler des recommandations pour y répondre (troisième partie). Le défi est stimulant car, avec ce sujet, c'est la transformation globale de la société qu'il s'agit d'explorer. C'est là ce qui rend la matière juridique si vivante et passionnante. En perpétuelle évolution, le droit doit sans cesse interroger le politique pour connaître les directions à suivre et formuler à son tour des réponses équilibrées et fidèles aux aspirations citoyennes.

En avant !

1. Le phénomène des réseaux sociaux, quand la palabre devient de l'or

Dans certaines sociétés traditionnelles africaines, il est un moment particulièrement important pour la vie de la communauté qui est celui où l'on se retrouve sous l'arbre à palabres pour se tenir au courant des derniers événements et bavarder. Du parvis de l'église au café de la place du village, du marché à la cour de récréation, ces lieux de discussion ont toujours existé, et sont fondateurs de nos sociétés. Le numérique, grâce à la technique, a ouvert des espaces nouveaux à ces palabres et la notion de « réseau social », terme autrefois surtout utilisé dans les sciences sociales, est entrée dans le langage courant. La virtualité de ces nouveaux réseaux sociaux a permis une amplification et une accélération des échanges sans aucune limite spatiale et temporelle. Parce qu'ils reposent sur des infrastructures et des opérateurs, parce qu'ils permettent de garder trace de toutes les conversations et sont une mine inépuisable de données et, enfin, car ils s'apparentent à des médias, le marché a pu aisément y prospérer[14]. Paradoxalement, c'est la technique numérique/digitale, qualifiée de virtuelle, qui a conféré un caractère concret et monnayable à cet « espace conversationnel » auparavant éphémère et hors commerce. Avant de déterminer les enjeux et les leviers d'action pour la puissance publique, il faut comprendre les rouages des réseaux sociaux et déterminer le régime juridique actuel.

14 D. Cardon, *Culture numérique*, Les presses de Sc Po, 2019.

1.1. Du réseau social aux «réseaux sociaux»

1.1.1. Le réseau social redéfini à l'aune du numérique

Le terme *réseau social* dans son acception contemporaine doit tout à internet de même qu'internet doit tout au concept de *réseau.* Tissant la toile des relations humaines, le web a révolutionné les liens sociaux et s'est réapproprié un terme réservé auparavant aux sociologues les plus érudits.

Une notion ancienne

Si la réflexion sur les réseaux n'est pas étrangère à la philosophie[15], celle sur le « réseau social » trouve son ancrage dans la sociologie moderne[16]. Emile Durkheim dans *Pragmatisme et sociologie* déclare que le « *monde est fait d'un nombre incalculable de réseaux qui unissent les choses et les êtres les uns aux autres* », posant ainsi les prémices des études et méthodes scientifiques d'analyse des structures relationnelles. On attribue généralement à John Arundel Barnes, anthropologue australien, l'emploi de ce terme dans son sens contemporain. En 1954, il étudie la ville norvégienne de Bremnes dans le but d'y décrire « *le fonctionnement du système des classes sociales* » et y fait le constat suivant : « *Chaque individu a un certain nombre d'amis, et ces amis ont leurs propres amis ; certains de ses amis se connaissent les uns les autres, et d'autres non. Il me semble approprié de parler de réseau pour désigner cette sphère sociale. L'image que j'ai en tête est celle d'un ensemble de points qui sont reliés par des lignes. Les points de cette image sont des individus, ou parfois des groupes, et les lignes indiquent quelles sont les personnes qui interagissent les unes avec les autres*. » Parmi les nombreux travaux sur ce sujet, se détachent ceux de Stanley Milgram, théoricien du « problème du petit monde » qui estime que dans une société de masse, pratiquement tous les individus sont reliés les uns aux autres dans un vaste réseau et que la distance moyenne entre deux individus quelconques est d'environ cinq intermédiaires et ceux de Mark Granovetter dans *The Américain Journal of Sociology* qui théorise la force des liens faibles[17]. Il distingue les liens « forts », caractérisés par une fréquence élevée de contacts et une certaine intensité émotionnelle, des liens « faibles ». Si les liens « forts » participent à la formation de groupes denses dont les membres partagent les mêmes ressources, « les liens faibles », eux, permettent un accès à une information plus vaste et nouvelle.

15 T. Zetlaoui, « Critique des réseaux, Pierre Musso (PUF 2003) ou la mort annoncée de la figure du réseau »*, in Secret et pouvoir : les faux-semblants de la transparence*, Quaderni, n° 52, Automne 2003, pp. 123-128.

16 E. Lazerga, *Réseaux sociaux et structures relationnelles*, Que Sais-je ?, Ed. 1998.

17 M. Granovetter. « The strenght of weak ties », *American journal of sociology*, 78, mai 1973.

L'apparition des réseaux sociaux numériques

L'invention d'internet révolutionne les modes d'interaction. En mettant en place entre les années 1960 et 1980, un protocole de communication unique (TCP/IP : TCP) permettant de mettre en communication différents ordinateurs, les inventeurs d'internet (dont Vinton Cerf et Robert Khan) créent les fondements d'une nouvelle façon d'entrer en relation. Il est désormais possible de communiquer notamment par e-mail. Mais au-dessus de ce que les informaticiens appellent la *couche basse*[18], un nouveau protocole de communication est mis en place, sur la *couche haute*, pour relier des pages internet ensemble *via* le système d'adressage http :// www. L'invention du *World Wide Web* par Tim Berners-Lee en 1989[19], infrastructure d'échanges décentralisés, permet aux individus, *via* leurs ordinateurs, de publier, échanger et partager des informations par des liens hypertextes. Le Web rend ainsi possible dès 1997 les premières formes de réseaux sociaux (Sixdegrees), mais le succès des premières **plateformes permettant aux internautes, après création d'un profil, de discuter ou d'échanger des contenus,** remonte au début des années 2000[20]. Les fonctionnalités du Web sont encore améliorées en 2004, par le Web 2.0 qui facilite l'interactivité entre internautes, et donnent aux réseaux sociaux la place centrale qui est aujourd'hui la leur. « Éditorialiser[21]» un contenu est désormais à la portée du plus grand nombre. L'accroissement de la rapidité du débit offert et le développement progressif du *smartphone* contribuent également au développement spectaculaire des réseaux sociaux. C'est donc avant tout **le perfectionnement de la technique** qui crée les conditions du succès des réseaux sociaux.

Une petite histoire des réseaux sociaux numériques

➲ *Pour une carte d'identité des principaux réseaux sociaux mentionnés en gras et en italique dans le texte, v. les* Fiches d'identité des principaux réseaux sociaux et assimilés*, p. 263)*

Le premier réseau social à rencontrer un succès durable est ***Facebook***. Né à Harvard, ce réseau social a été créé pour permettre à la communauté étudiante de l'université d'être connectée. Son usage a très vite été, dès 2005, disponible au sein d'autres établissements d'enseignement avant de s'élargir encore au-delà et de devenir aujourd'hui le réseau social le plus utilisé dans le monde. Entretemps, il s'est transformé en devenant une entreprise à but lucratif. Un des premiers réseaux sociaux à acquérir une importante rentabilité économique est le réseau social professionnel ***LinkedIn,*** créé en 2003, proposant des abonnements payants.

18 D. Cardon, *Culture numérique,* p. 28 : « *Dans le jargon des informaticiens, on dit que le web est une couche haute qui utilise une couche basse : le protocole TCP/IP d'internet. Le web est contenu dans Internet mais Internet contient beaucoup d'autres choses que le web. De nombreux services empruntent la couche basse comme le protocole SMTP qui permet de communiquer par messageries, le protocole FTP qui permet d'envoyer de gros fichiers, tous ces systèmes ne fonctionnent que parce qu'ils utilisent le protocole racine : TCP/IP qui est internet.* »

19 Invention qui sera versée dans le domaine public, permettant à la technologie de l'htlm d'être libre de droits.

20 MySpace fut créé aux États-Unis en 2003 et rencontra un succès particulier à partir de 2004. En France, le réseau social utilisé durant cette période était Skyrock.

21 Ce néologisme désigne les opérations de structuration, de mise en visibilité de contenus sur le web et sous-tend l'idée que la personne endosse la responsabilité éditoriale.

En 2005 est lancé ***YouTube,*** en 2007, **Tumblr**[22], en 2006 ***Twitter*** qui permet à ses utilisateurs de partager avec son réseau des messages de 140 caractères maximum (280 aujourd'hui). Twitter lance l'usage de l'*hashtag* en 2007 afin de classer et d'organiser ses contenus. A partir de 2009, l'*hashtag* devient un langage en lui-même. Il permet notamment l'éclosion de mouvements sociaux comme #Occupy, #BlackLivesMatter et #MeToo en permettant de sensibiliser et de mobiliser les citoyens-internautes autour de causes sociales et politiques. **2009 est une année fondamentale en termes d'émergence de nouveaux réseaux sociaux** : elle ouvre une période où presque chaque année voit apparaître un nouveau réseau social. **Weibo**[23], le premier réseau social chinois, voit donc le jour dans une Chine qui interdit les réseaux sociaux américains. Cette année marque également l'avènement du jeu social **FarmVille**[24], permettant de diriger une exploitation agricole virtuelle, mais aussi de **Foursquare**[25], premier réseau social à proposer de partager sa géolocalisation. 2009 marque enfin l'avènement de **Grindr**[26], application qui révolutionne les rencontres : initialement destinée aux rencontres entre hommes homosexuels et, aujourd'hui, à celles de l'ensemble des personnes de la communauté LGBTQIA+, elle ouvre la voie à des applications de rencontres géolocalisées et gouvernées par les algorithmes comme **Tinder**[27] lancée en 2012. En 2010, c'est au tour d'***Instagram*** d'émerger. Cette application permet de partager des contenus photographiques. Il en va de même pour **Pinterest**[28] qui à partir de 2010 permet d'épingler des contenus photographiques. En 2011, apparaît **Twitch**[29], plateforme plébiscitée par les « *gamers* »[30]. Cette année-là, les réseaux sociaux montrent la puissance de leur impact social et politique en jouant un rôle décisif dans les révolutions arabes, en particulier en Egypte. Les manifestations se structurent grâce aux réseaux sociaux et notamment à des *hashtags* comme #Jan25 en Egypte. En 2011 émerge également l'application ***Snapchat*** qui permet de partager des contenus, messages, images, vidéos, de manière éphémère, ceux-ci disparaissant au bout de 24 heures. A

22 Tumblr est un réseau social de microblogage créé en 2007 et permettant à l'utilisateur de poster du texte, des images, des vidéos, des liens et des sons sur son tumblelog. En 2020 il comptait 320 millions d'utilisateurs. Les utilisateurs peuvent rejoindre des communautés et discuter de leurs idées. Ce réseau est notamment populaire auprès des adolescents et des groupes de fans de personnalités connues.

23 Site de microblog chinois. Il compte plus de 500 millions d'utilisateurs actifs en 2022 chaque mois et fonctionne sur un modèle similaire à celui de Twitter. Weibo est un espace d'information important et relativement plus libre que les médias classiques chinois.

24 Jeu social permettant d'entrer en contact de différentes manières (partage des résultats, etc.) avec les autres joueurs de la communauté. Arrêtée fin 2020 sur les navigateurs web, la licence continue d'exister grâce à de nouvelles versions et des applications mobiles (Farmville 2, etc.);

25 Média social qui permet aux utilisateurs de se géolocaliser et de recommander des lieux de sorties autour d'eux à leurs amis. En 2022, il atteint 45 millions d'utilisateurs.

26 Réseau social de rencontre pour les personnes gays, bisexuelles et queers, basé sur la géolocalisation. L'application est utilisée par environ 11 millions de personnes tous les mois et a annoncé le 9 mai 2022 son intention d'entrer en Bourse.

27 Lancé en septembre 2012, Tinder est une application de rencontre en ligne. Les utilisateurs créent un profil et peuvent « matcher » (faire une correspondance) avec d'autres profils et lancer une discussion. L'application est présente dans plus de 190 pays en 40 langues.

28 Site web américain mélangeant les concepts de réseautage social et de partage de photographies, lancé en 2010. Il permet à ses utilisateurs de partager leurs centres d'intérêt et passions à travers des albums de photographies glanées sur internet. En 2019, Pinterest comptait 335 millions d'utilisateurs mensuels.

29 Twitch est un service de *streaming* vidéo en direct lancé en juin 2011. Il est surtout utilisé par des *gamers*, adeptes de jeux vidéo à partager, à suivre et à commenter en direct. Il est également utilisé par des politiciens pour des meetings interactifs.

30 On appelle « *gamers* » les personnes qui jouent aux jeux vidéo en ligne.

partir de 2015 est lancée la « guerre du *streaming* » sur les réseaux sociaux avec notamment l'application **Periscope** acquise par Twitter qui permet de partager des vidéos en direct et qui sera supprimée en 2021. En 2016, Facebook lance de même Facebook Live et Instagram ses « stories »[31].

A partir de 2016, les réseaux sociaux connaissent une remise en cause notamment en lien avec la diffusion de fausses nouvelles ou encore avec le scandale Cambridge Analytica *(cf. infra)* impliquant Facebook dans l'analyse des données des utilisateurs à des fins politiques, donnant lieu au *hashtag* #DeleteFacebook. 2016 voit aussi l'émergence de réseaux à la frontière des plateformes de vente de prestations en ligne (notamment pornographique) comme **OnlyFans**[32]. Cette même année apparait ***TikTok***, réseau social chinois destiné à un public non chinois qui permet le partage de contenus uniquement vidéo : TikTok a été à l'origine de nombreux bouleversements aussi bien technologiques que politiques ou culturels et est actuellement en pleine ascension, en particulier auprès des plus jeunes.

Parallèlement aux réseaux sociaux et au même rythme, ont émergé des **messageries** numériques qui permettent l'échange instantané entre plusieurs personnes de façon interactive (contrairement aux courriers électroniques) comme ***WhatsApp*** en 2009, **Viber**[33] et **Signal**[34] en 2010, ***Télégram*** en 2013 et **Discord**[35] en 2015 dont certaines comme **Messenger** avec Facebook sont incorporées aux réseaux sociaux. Sur certains aspects, leurs différences avec les réseaux sociaux sont difficiles à établir (*cf. infra*).

L'engouement planétaire pour un outil répondant à des aspirations sociales contemporaines

En quelques années, l'augmentation du nombre d'utilisateurs de ces réseaux a été fulgurante, surtout parmi les jeunes générations qui semblent avoir trouvé leur propre mode de communication et permettent l'émergence de nouveaux réseaux. Les dix sites à plus forte audience en 2005, parmi lesquels ne figurait aucun réseau social, ont disparu de ce classement en 2008. Ils sont alors remplacés notamment

31 Publication sur les réseaux sociaux pour raconter une histoire qui disparaît généralement au bout de 24 heures.

32 Lancée en septembre 2016, cette plateforme permet de mettre en relation des créateurs de contenus vidéo et photo et des utilisateurs, qui peuvent s'abonner à eux moyennant un abonnement mensuel, afin de recevoir des contenus exclusifs. En 2021, OnlyFans revendique 130 millions d'utilisateurs dans le monde.

33 Viber est fondé en 2010 par l'entreprise japonaise Rakuten. En 2019, cette messagerie fonctionnant sur le même modèle que WhatsApp comptait 1 milliard d'abonnés, pas forcément actifs.

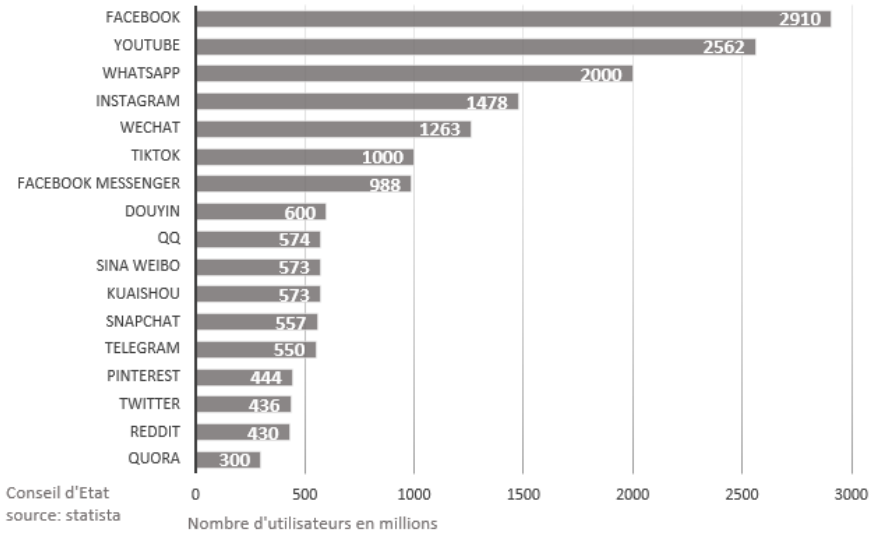
34 Signal est une application gérée par une entreprise américaine gratuite pour Android et iOS, permettant de communiquer (appels vocaux et vidéo, messages texte ou médias) de façon chiffrée et sécurisée et dont l'objectif est d'assurer un maximum de confidentialité à ses utilisateurs. Son fonctionnement est centralisé. Peu de données personnelles sont conservées et presque aucune modération ne s'exerce. A la suite de la modification des conditions générales d'utilisation de WhatsApp par son acheteur, Signal a été téléchargée plus de 47 millions de fois en deux semaines. Suite à l'appel de l'industriel Elon Musk de rejoindre cette messagerie, il y a un engorgement de la procédure d'inscription.

35 Discord est un logiciel gratuit de transport de voix et de messagerie instantanée. Il fonctionne sur les systèmes d'exploitation Windows, macOS, Linux, Android, iOS ainsi que sur les navigateurs web. La plateforme comptabilise le 21 juillet 2019 plus de 250 millions d'utilisateurs. En mars 2022, l'entreprise emploie environ 600 salariés et est valorisée à 15 milliards de dollars. Conçu initialement pour les communautés de joueurs de jeux vidéo, son utilisation s'est diversifiée avec le temps.

par Facebook, YouTube, Wikipédia et MySpace[36]. Cette progression n'a pas cessé. En 2010 on dénombrait 500 millions d'utilisateurs actifs sur Facebook dans le monde (dont 18 millions en France), puis 2,6 milliards en 2020[37] (dont près de 40 millions en France). **En 2020, 49% de la population mondiale était active sur les réseaux sociaux**.

Rétrospectivement, le succès des réseaux sociaux n'est pas si surprenant. Leurs fonctionnalités correspondent parfaitement à l'évolution des aspirations de l'homme du XXIe siècle, qui est souvent guidé par ses affects mais souhaite être pleinement maître de ses choix et les voir rapidement satisfaits et aspire à être reconnu. Les réseaux sociaux permettent à leurs utilisateurs de choisir eux-mêmes les contenus qu'ils souhaitent découvrir comme ceux qu'ils souhaitent partager. Ils peuvent rester en permanence en contact avec les personnes avec lesquelles ils ont noué un lien et choisi d'échanger. Il est ainsi possible à la fois de nourrir les *liens forts* et de maintenir les *liens faibles*, permettant potentiellement un enrichissement significatif du « **capital social** » de chaque individu[38]. Ce constat a été conforté durant la crise sanitaire : alors que les individus étaient contraints à ne plus avoir de contact physique avec les uns avec les autres, les contacts étaient toujours possibles sur les réseaux sociaux et nombreux sont ceux qui ont vu dans les réseaux sociaux la seule possibilité dont ils disposaient pour maintenir leur vie sociale. Pendant le confinement, leur utilisation aurait ainsi augmenté de 61%[39].

Classement des réseaux sociaux les plus populaires dans le monde en janvier 2022, selon le nombre d'utilisateurs actifs *(en millions)*



36 Myspace est un site web de réseautage social fondé aux États-Unis en août 2003, qui met gratuitement à disposition de ses membres enregistrés un espace web personnalisé, permettant de présenter diverses informations personnelles et d'y faire un blog. Il héberge notamment de nombreuses pages internet de groupes de musique et de DJ qui y entreposent et présentent leurs compositions musicales. Son succès s'est altéré depuis 2010.

37 *Techonoly trends*, Morgan Stanley, 20 juin 2008.

38 D. Cardon *op. cit.*

39 *Le Parisien*, site linternet, 29 décembre 2020, « Covid-19 : les réseaux sociaux boostés par le virus».

En outre, l'accès à la connaissance est démultiplié et désormais, « horizontalisé ». Chaque individu est un média potentiel. La visibilité est à la portée de tous. Par le miracle de la technique, les limites spatiales et temporelles sont dépassées. Les modes de vie s'en trouvent modifiés, l'accoutumance à la réalisation instantanée des attentes s'en trouve accentuée, l'individualisation des contenus visionnés toujours plus affinée. Comme le rappelle Dominique Cardon, l'information étant un *bien non rival*[40], cette nouvelle architecture de communication favorise les phénomènes d'intelligence collective : la valeur collective est redistribuée aux internautes, elle les enrichit en augmentant leur capacité d'agir et d'apprendre des autres, en les incitant à produire de nouveau. En partageant des contenus, la valeur est démultipliée. Cette *externalité positive* est utilisée de deux façons soit en étant mise au service de la communauté, constituant ainsi *un bien commun* (comme l'encyclopédie collaborative Wikipédia) soit en faisant l'objet d'une valorisation par les plateformes au service du marché.

Si les réseaux sociaux donnent l'impression aux individus d'être maîtres de leurs choix et d'être visibles, s'ils leur permettent de soigner leur « capital social » en étant déliés de toute contrainte spatiale et temporelle, ils sont aussi divers que nombreux de sorte qu'il faut appréhender avec une relative prudence la notion générique.

1.1.2. Une notion plurielle et plurivoque : la diversité des réseaux sociaux

La difficile définition des réseaux sociaux : un espace, un service, une plateforme, des opérateurs ?

Sous la terminologie unique de « réseaux sociaux », on désigne indistinctement l'*espace* de communication constitué par l'ensemble des échanges entre les utilisateurs des différentes plateformes (à l'instar des marchés financiers), le *service* de communication offert par des prestataires, la *plateforme* dont la fonction est de mettre en relation des utilisateurs du service de communication et les *opérateurs*, qu'ils agissent à but lucratif ou non, qui orchestrent ces communications. Cette polysémie ne facilite pas les débats mais démontre que le sujet peut être abordé sous de nombreux angles : organique, matériel, fonctionnel.

Critères d'identification et de classification

L'utilisation d'un terme unique pour désigner ces lieux de rencontres numériques qui permettent de converser ou de partager des contenus ne permet pas de percevoir la grande diversité qui les caractérise. Robert Putnam, politologue américain, théoricien du capital social, a distingué le renforcement des liens sociaux préexistants (le *bonding*, du mot anglais « *bond* » le lien) et l'interaction avec quelqu'un qu'on ne connaît pas forcément mais avec qui on partage un centre d'intérêt (*bridging*, du mot anglais « *bridge* » pont) et cette distinction s'est trouvée parfaitement adaptée aux fonctionnalités des réseaux sociaux. Mais d'autres critères peuvent aussi être choisis.

40 C'est-à-dire que sa consommation par un internaute n'empêche pas cette même consommation par un autre. D. Cardon *op. cit.*

Il est possible de classer ces réseaux selon :

- leur **objet**, en distinguant les réseaux généralistes, qui permettent avant tout de discourir (Facebook, Twitter, Snapchat), des réseaux spécialisés dans la mise en relation professionnelle (LinkedIn, Viadéo), dans le partage de photos (Instagram, Pinterest), le partage de vidéos (TiKtoK, YouTube), les rencontres (Tinder, Grindr), les réseaux d'entreprise (Whaler, Slack), ou les jeux en ligne (Twitch) ;
- le caractère **principal ou accessoire** du service de réseau social : ainsi les forums de discussion sur les sites web sont-ils une forme de réseau social qui ne sont souvent qu'accessoires aux services proposés (Google maps, Doctissimo) ; il en va de même des jeux en ligne qui permettent aux *gamers* de rester en contact et connaissent une croissance inégalée (Steam, Epic Games store) : on estime qu'en 2021 le nombre de *gamers* s'élèvera à 3,3 milliards soit 40% de la population mondiale ;
- leur **taille**, qui peut s'apprécier au nombre d'utilisateurs ou au montant du chiffre d'affaire : on compte en 2022 plus de 2 milliards d'abonnés chez Facebook et d'utilisateurs de YouTube mais il existe un nombre considérable de réseaux sociaux moins connus du grand public (on peut notamment citer MeWe, réseau social dit d'alt-tech ou technologie alternative, dépourvu de politique de modération des contenus, il est très populaire auprès des antivax ou des personnes partageant des idées non consensuelles ; eToro, réseau social de trading permettant aux utilisateurs de suivre des traders réputés) ;
- leur **modèle économique** (*cf. infra*) : certains reposent sur un modèle participatif (Mastodon), d'autres sur un modèle de marché ; les sources de revenus peuvent être exclusivement ou partiellement l'abonnement payant (Reddit) ou la publicité (Facebook, YouTube, Tiktok), beaucoup mettant en place des formules Premium avec abonnement pour ne pas reposer sur les seuls revenus publicitaires et pouvoir offrir à des abonnés des fonctionnalités plus poussées (Snapchat, Instagram, Twitter) ; certains ont un financement plus original, comme LinkedIn qui se rémunère majoritairement sur les services rendus ;
- leur **degré d'ouverture et leurs modalités de diffusion** : certains permettent à des non abonnés d'accéder à des contenus publics (Twitter), d'autres ne sont accessibles qu'aux utilisateurs du réseau ou aux abonnés qui ont un compte et ont créé un profil (ainsi Facebook, par exemple, peut être utilisé en compte privé ou public mais n'est pas visible par des personnes qui n'ont aucun lien avec le réseau) ;
- leur caractère **centralisé** (gouvernance centrale), très présent parmi les plus gros réseaux (Facebook, Tik Tok), ou décentralisé (multiples communautés qui gèrent une partie du réseau) comme par exemple chez Mastodon ;
- leur **public** : l'utilisation des réseaux sociaux varie selon des critères démographiques tels que l'âge et le sexe[41].

41 En 2021, la majorité des utilisateurs de Snapchat étaient des femmes, tandis que plus de 70% des utilisateurs de Twitter étaient des hommes. Par exemple Facebook était utilisé principalement par les

Les débats autour de ce qu'il convient d'intégrer dans le champ des réseaux sociaux sont donc récurrents.

Selon que l'on met plus ou moins en avant une fonctionnalité de discussion/contact ou de publication/partage de contenu, selon que l'on prend en compte des critères extérieurs comme le régime juridique applicable ou le modèle économique, les qualifications se différencient. Ainsi certains contestent à **Wikipédia** la qualité de réseau social en raison de son modèle collaboratif et totalement ouvert, bien que cette plateforme, dont l'objet principal est la construction d'une encyclopédie universelle en ligne, dispose d'une fonctionnalité accessoire de réseau social entre ses membres.

La frontière est aussi parfois difficile à définir avec les ***civic tech***[42] comme **Make. org**[43] par exemple qui est une plateforme dont la vocation est bien de favoriser la discussion citoyenne mais dont l'objectif n'est pas de discuter avec des personnes partageant les mêmes points de vue mais, au contraire, d'écouter des points de vue différents. Les débats sont organisés par la plateforme et les algorithmes sont utilisés pour mettre en lumière les divergences et les consensus et non pour recommander certains partis pris.

Le débat est aussi complexe au sujet des **messagerie**s telles WhatsApp, Telegram, Signal et Messenger. Lorsqu'on prend en compte le fait que certains échanges sont cryptés et obéissent au régime juridique des communications privées, on s'éloigne de la catégorie des réseaux sociaux. Cependant, lorsqu'on prend en compte la nécessité de créer un profil, la possibilité de constituer de très importantes listes de diffusion, de partager des contenus et l'existence de certaines formes de modération par la limitation de la taille des listes, par la possibilité de signaler des communications problématiques ou des harcèlements ou par la possibilité pour l'opérateur d'opérer un contrôle sur les comportements suspects sans même contrôler le contenu du message, il est difficile de percevoir avec évidence la différence avec les plateformes que l'on désigne usuellement sous le terme de « réseaux sociaux ». Surtout, la notion de *réseau social* est, depuis différents scandales (*cf. infra*), négativement connotée et, dans l'esprit du plus grand nombre, réservée aux plus grandes plateformes qui se rémunèrent par la monétisation des données personnelles. Or, comme il a été dit, il existe plusieurs modèles économiques et, selon les critères choisis, on peut intégrer ou exclure de cette notion de nombreuses plateformes. De même, plusieurs plateformes contestent leur qualité de « réseau social » au motif que leur activité

25-34 ans aux États-Unis en 2021, tandis que les adolescents préféraient utiliser Snapchat ou TikTok. (sources : Statista)

42 Selon le rapport de la Knight Foundation : Trends in Civic Tech de 2013, la « *civic tech* » – pour « civic technology » – désigne toute technologie visant à accroître le pouvoir du citoyen ou à rendre un gouvernement plus ouvert. Cette définition large des « technologies civiques », en français, englobe l'ensemble des outils numériques qui permettent d'améliorer le fonctionnement démocratique des sociétés et des communautés.

43 Make. org initie des consultations citoyennes massives sur des sujets d'intérêt général, comme la lutte contre les violences faites aux femmes, l'avenir des jeunes, l'accès à la culture, le soin apporté aux aînés, l'alimentation, le handicap, l'environnement. En répondant à une question ouverte, chacun peut faire des propositions et voter sur celles des autres participants. Les algorithmes développés permettent d'identifier les idées plébiscitées par le plus grand nombre. Le système a été conçu pour empêcher des individus ou des groupes d'intérêt de fausser les résultats ("*trolling*").

principale est de permettre l'échange de contenus et non de simples discussions et qui se définissent comme des **médias sociaux**. La pertinence de cette dernière distinction mérite donc d'être interrogée.

Réseaux sociaux et médias sociaux

Appelés indistinctement « *social media* » ou « *social network* » en langue anglaise, on distingue souvent, dans la langue française, les médias sociaux des réseaux sociaux, le premier concept étant présumé plus large que le second même si, à ce stade, aucun de ces termes n'est défini par le dictionnaire de l'Académie française. Si certains utilisent le terme de *média social* pour désigner les médias professionnels dont le moyen de communication est le réseau social (comme Brut), il semble que ce terme désigne en réalité les **médias créés par les utilisateurs eux-mêmes**, ce qui les rapproche beaucoup du terme réseau social. D'ailleurs, la directive 2018/1808 dite des services de médias audiovisuels (SMA) du 14 novembre 2018 comporte, dans ses considérants introductifs, un développement sur la notion de « *médias sociaux* » qu'elle définit comme les services de média dont le contenu est créé par l'utilisateur. L'encyclopédie collaborative Wikipédia estime que les médias sociaux sont des applications web qui permettent la création et la publication de contenus générés par l'utilisateur, qu'ils se déclinent sous différentes formes (*blog*, *microblog, mondes virtuels*, *messageries*, *jeux en ligne*) et comptent parmi eux *les réseaux sociaux de contact* pour lesquels les fonctionnalités de mise en relation sont principales (Méta-Facebook) et les *réseaux sociaux de contenu* pour lesquels les fonctionnalités de réseau sont secondaires et sont associés à une activité particulière (Instagram, TikTok, YouTube)[44]. Il est permis de se demander si cette distinction présente un intérêt et s'il ne faut pas appréhender ces deux concepts de façon unique en partant de l'idée que tout moyen de communication horizontal est un type de *média* ou de réseau et tout échange de contenu ou toute discussion **entre utilisateurs** révèle le caractère *social* de l'échange (*cf. infra*).

Limites de la notion : critères négatifs

Si les contours de la notion de réseau social sont flous et qu'une définition positive et universelle paraît difficile à retenir, certains critères peuvent être mobilisés pour déterminer une définition négative et dire ce que n'est pas un réseau social. S'il est certain que ne font pas partie des réseaux sociaux les sites qui proposent de façon unilatérale et verticale des informations, toute plateforme qui permet la discussion ou le partage de contenus n'est pas nécessairement un réseau social. La caractéristique d'un service de réseau social est que l'utilisateur, même lorsqu'il s'agit d'une entreprise qui produit du contenu ou des données, se comporte comme un simple utilisateur et non comme un prestataire en ce qu'il ne facture

44 Distinction établie par M. Boyd et N. Ellison, v. « Social Network Sites : Definition, History, and Scholarship », *Journal of Computer-Mediated Communication*, octobre 2007.

pas sa production. C'est ce que les textes européens qui régissent les plateformes nomment l'***utilisateur final***. En effet si l'utilisateur s'inscrit lui aussi dans un lien commercial, on bascule alors dans une plateforme d'échange de biens et de services. L'exemple le plus topique est à cet égard la plateforme Onlyfans, qui se présente comme un réseau social de personnes mais qui permet aux utilisateurs de verser jusqu'à 500 euros par jour à un autre utilisateur pour le « récompenser » de son contenu posté. Si ce réseau permet la mise en ligne de tutoriels de cuisine et de yoga, il est aussi prisé par ceux qui créent du contenu à caractère pornographique dans le but d'en tirer une rémunération. Le fait pour l'utilisateur de rechercher une rémunération directe semble donc pouvoir être regardé comme constituant un critère exclusif de toute « relation sociale ».

Les réseaux sociaux dits « alternatifs »

Certains réseaux sociaux qui fonctionnent sans publicité et sans réutilisation des données personnelles avec pour objectif de retrouver la fonction première d'un internet libre et partagé sont communément appelés « alternatifs », dans la mesure où ils prônent un modèle différent des réseaux sociaux très grand public. N'étant pas fondés sur l'économie de l'attention et agissant, pour certains d'entre eux, sans but lucratif, ils ne paraissent pas soulever de difficulté de principe en terme d'addiction, de temps d'engagement pour mieux placer les publicités ou de réutilisation des données personnelles.

Le plus connu est sans doute **Wikipédia** qui, s'il est d'abord une encyclopédie participative, héberge un important réseau de discussion d'individus qui appartiennent à une même communauté et respectent certaines règles assez strictes qui permettent de garantir la qualité des articles et de rapidement supprimer sur la plateforme les contenus illicites.

C'est le cas aussi de **Mastodon**, créé en 2016 qui comptait en 2022, 4,4 millions d'utilisateurs et comporte certaines similitudes avec Twitter. Sa principale caractéristique est d'être décentralisé de sorte qu'il est composé de plusieurs serveurs autonomes, sans point central ni poste de commandement. Par ce dispositif, il répond aux nombreux problèmes d'éthique et de sécurité liés à la centralisation des données sensibles sur les réseaux sociaux traditionnels, entre revente de ces données et risque de piratage. Le projet a été lancé par un informaticien allemand aujourd'hui âgé de 25 ans, Eugen Rochko. Le réseau fonctionne autour d'instances différentes. Sont utilisés des logiciels libres de droits. L'Union européenne a créé sa propre instance Mastodon et la CJUE a créé un compte. Mastodon est un « **Fédiverse** » c'est-à-dire qu'il appartient à une fédération de serveurs formant un réseau social utilisant le même protocole (Activity Pub) permettant leur interopérabilité, auto-hébergé (chacun peut créer son instance), libre (gratuit et utilisable par tous), et décentralisé.

Insaisissables réseaux sociaux : des plateformes- caméléon

Tant les réseaux sociaux que les autres plateformes et sites internet mutent en permanence. Non seulement ils diversifient leurs activités mais ils proposent, de plus en plus souvent, l'ensemble des services qui peuvent être souhaités par

les utilisateurs, au point que l'on assiste à un phénomène **d'hybridation**[45]. D'une part, les réseaux sociaux « historiques » intègrent des fonctionnalités numériques autres que celle de la discussion ou du partage de contenus, comme l'achat en tout genre (*market place*), la réalisation de sondages, ou la mise à disposition de logiciels de création artistique (comme lipstik sur TikTok) ou d'exploration virtuelle. D'autre part, les plateformes d'échange de biens et de services internalisent les fonctions du réseautage social et proposent des fonctionnalités de discussion et de partage de conseils entre utilisateurs : c'est par exemple le cas des jeux en ligne, des outils de cartographie[46] ou même des notations sur les sites de vente en ligne.

La notion juridique de « réseau social »

Jusqu'à peu, il n'existait ni en droit français ni en droit européen de notion juridique du réseau social numérique et aucune norme ne définissait *in extenso* ce terme.

En droit français, les réseaux sociaux ont été appréhendés par le droit par le biais d'autres notions plus larges comme celles de plateformes ou services de communication en ligne et seules certaines décisions de jurisprudence ou d'autorités administratives s'y sont aventurées[47]. Ainsi la Cour de cassation a-t-elle eu l'occasion de rappeler que : « *Le réseau social est simplement un moyen de communication spécifique entre des personnes qui partagent les mêmes centres d'intérêt* »[48], le Conseil constitutionnel, à l'occasion de contentieux électoraux, l'a défini comme un « *moyen de communication au public par voie électronique* »[49] puis « *comme un moyen de communication au public en ligne* »[50] pour les distinguer des moyens de communication à caractère privé, dont les contenus ne peuvent pas altérer la sincérité du scrutin. Quant à la CNIL, elle a pu les qualifier de « *nouveaux supports d'expression* »[51]. Si le juge a été ponctuellement amené à définir cette notion, notamment afin de délimiter le champ d'application de dispositions légales, il l'a fait avec une grande parcimonie tant la notion peut, comme il a été dit, être appréhendée de façon variable. Ainsi par exemple, le Conseil d'État, saisi d'un contentieux par lequel des associations contestaient la possibilité donnée à l'administration, par le code de la sécurité intérieure[52], d'enregistrer, dans le cadre d'enquêtes administratives liées à la sécurité publique, certaines données relatives aux activités sur les réseaux sociaux susceptibles de porter atteinte à la sécurité publique ou la sûreté de l'État, a jugé qu'« *au sens et pour l'application de ces dispositions* », « *les termes 'réseaux sociaux' désignent les plateformes en ligne permettant aux personnes qu'elles mettent en relation de communiquer entre elles, de mettre à la disposition des autres utilisateurs des contenus tels que des textes, des images et des vidéos et d'accéder à ceux-ci* »[53].

45 S. Abiteboul et J. Cattan, *Nous sommes les réseaux sociaux*, Odile Jacob, Sept.2022.

46 GoogleMaps serait très utilisé par les combattants pendant la guerre en Ukraine.

47 On trouve aussi quelques textes épars qui les évoquent au titre du moyen de communication qu'ils constituent mais ne les définissent pas, notamment à l'art. 441-1 du code du cinéma et de l'image animée, à l'art. L. 1453-1 du code de la santé publique et à l'art. R. 236-2 du code de la sécurité intérieure.

48 CCass., 2e civ., 5 janvier 2017,n° 16-12.394, Bull.

49 CC, 8 décembre 2017, *Essonne (1ère circ.), Mme Farida Amrani et autres*, *n° 2017-5074/5089 AN*.

50 CC, 18 décembre 2017, *Loiret (4e circ.), Mme Mélusine Harlé*, *n° 2017-5092 AN*.

51 Délibération 2011-343 du 10 novembre 2011.

52 d) du 5° de l'*art. R. 236-2* du code de la sécurité intérieure.

53 CE, 24 décembre 2021, *Ligue des droits de l'homme et autres*, *n° 447513* et suiv.

L'adoption du *règlement européen relatif aux marchés contestables et équitables dans le secteur numérique (**Digital Markets Act** dit **DMA**)* en 2022 marque l'apparition de la **première définition juridique des réseaux sociaux**, qui sont définis dans son article 2 comme une plateforme permettant aux utilisateurs finaux de se connecter, de partager, de découvrir et de communiquer entre eux sur plusieurs appareils notamment *via* des « *chats* », des publications (**posts**), des vidéos et des recommandations[54]. Elle est très proche de la définition proposée en 2009 par le groupe de concertation, réunissant en Europe les représentants nationaux de régulation du type de la CNIL dénommé G29[55] et de celle formulée en 2010 par le comité économique et social européen[56] mais elle introduit la **notion d'utilisateur final** qui permet de distinguer l'internaute (personne physique ou morale) qui fournit du contenu sur les réseaux sociaux en tant que simple utilisateur, du prestataire ou professionnel. En effet, l'article 2 du DMA définit l'utilisateur final comme toute personne physique ou morale utilisant des services de plateformes essentiels autrement qu'en tant qu'utilisateur professionnel (cette dernière notion étant pour sa part définie comme toute personne physique ou morale agissant à titre commercial ou professionnel qui utilise des services de plateformes essentiels aux fins ou dans le cadre de la fourniture de biens ou de services à des utilisateurs finaux). Comme la directive 2018/1808 dite des services de médias audiovisuels du 14 novembre 2018 qui définit les services de médias sociaux comme les services de médias dont le contenu est créé par l'utilisateur, le règlement DMA donne une importance particulière à **la qualité de l'utilisateur** qui participe à la création de contenus et au partage de discussions sans le faire dans un cadre professionnel. Le terme « social » sous-tend l'idée d'une utilisation de la plateforme comme instrument moderne de « bouche à oreille » et non comme lieu de vente.

S'agissant du critère matériel de la définition, il est assez large puisque toute plateforme qui permet à ses utilisateurs finaux, de se connecter, de partager, de découvrir ou de communiquer des discussions ou des contenus, entre dans le champ. Il n'est pas exigé que les fonctionnalités soient offertes à titre principal ou accessoire, de sorte que toute plateforme offrant un service, même accessoire, de réseau social entre *a priori* dans la définition.

Cependant, il faut relever que dans le règlement européen relatif à un marché intérieur des services numériques dit **Digital Services Act (DSA)** adopté en 2022, si la notion de réseaux sociaux n'est pas définie, en revanche l'article 2 (éclairé par le considérant 13), qui définit la notion de plateforme en ligne au sens et pour l'application de ce texte, exclut la mise à la charge des obligations définies par

54 (7) de l'art. 2 du DMA.

55 Dans son *avis n° 5/2009*, le G29 recommandait de définir les réseaux sociaux comme « *des plateformes de communication en ligne qui permettent à tout internaute de rejoindre ou de créer des réseaux d'utilisateurs ayant des opinions similaires et/ou des intérêts communs. Ils fonctionnent grâce à l'utilisation d'outils mettant à disposition une liste de contacts pour chaque utilisateur avec une possibilité d'interaction* ».

56 *Avis n° 2010/C 128/12* du Comité économique et social européen sur *L'impact des réseaux de socialisation et leur interaction dans le domaine du citoyen/consommateur*. Il définit les réseaux sociaux comme « *des services en ligne qui ont pour but de créer et de relier entre eux des groupes de personnes partageant des activités ou des intérêts communs ou souhaitant simplement connaître les préférences et les activités d'autres personnes, et qui mettent à leur disposition un ensemble de fonctionnalités permettant une interaction entre les utilisateurs* ».

le texte pour les opérateurs qui n'ont qu'une activité mineure et accessoire de stockage et de diffusion d'informations au public[57]. Il reviendra au juge d'apprécier au cas par cas ce qui relève de l'activité mineure et purement accessoire.

En tout état de cause, on peut retenir à ce stade qu'est préférée une **approche large** à l'instar de la définition proposée par le rapport de la mission « Régulation des réseaux sociaux - Expérimentation Facebook » remis au secrétaire d'État en charge du numérique en mai 2019 qui était la suivante : « *un service en ligne permettant à ses utilisateurs de publier les contenus de leur choix et de les rendre ainsi accessibles à tout ou partie des autres utilisateurs de ce service* »[58]. Implicitement cependant, elle semble exclure les services de messageries puisque le règlement DMA se réfère de façon spécifique aux «*services de communications interpersonnelles non fondés sur la numérotation* » en faisant une catégorie distincte[59]. Il faut ajouter que le DMA privilégie une approche par service ce qui ouvre la possibilité d'avoir des plateformes qui fournissent plusieurs services obéissant eux-mêmes à plusieurs réglementations.

La définition européenne présente donc le mérite d'être assez **minimaliste et englobante**, sans réduire ni restreindre ces services à des caractéristiques saillantes et originales des réseaux sociaux qui ont été mises en avant par exemple par Pierre Mercklé dans son ouvrage *Sociologie des réseaux sociaux*. Il définit en effet les réseaux sociaux en ligne de façon pertinente mais plus restrictive comme ayant pour caractéristiques communes d'offrir à leurs utilisateurs : 1. La possibilité de créer un espace personnel de présentation de soi avec les informations qui participent à la définition d'un profil ; 2. La possibilité d'accéder, selon les modalités du réseau, aux « profils » mis en ligne par les membres du réseau ; 3. La possibilité de nouer des relations avec des membres du réseau.

Il faut cependant relativiser la portée de la définition des réseaux sociaux figurant dans le DMA qui pourrait être cantonnée à l'application de ce texte dont l'objet est de réguler le marché et non l'ensemble des champs applicables aux réseaux sociaux.

La notion de réseau social dans le cadre de cette étude

Compte tenu du caractère pluriel de la notion et de l'hybridation de plus en plus importante des services offerts par les plateformes, retenir une définition trop stricte des réseaux sociaux semble peu opérationnel et anachronique par rapport à la définition qui vient d'être adoptée dans le DMA. L'objet de cette étude est bien de rendre compte de l'ensemble des problématiques des réseaux sociaux sans en écarter une de façon arbitraire.

57 Les obligations mises à la charge des fournisseurs de services d'hébergement dont font partie les réseaux sociaux concernent les plateformes qui stockent et diffusent des informations sauf « *lorsque la diffusion au public n'est qu'une caractéristique mineure et purement accessoire d'un autre servie et que cette caractéristiques ne peut, pour des raisons techniques objectives, être utilisées sans cet autre service principal, l'intégration de cette caractéristique n'étant pas un moyen de se soustraire à l'applicabilité des règles du présent règlement relatives aux plateformes en ligne.* ».

58 *Ibid.*

59 e du 2. de l'art. 2 du règlement, L. 32 du code des postes et des communications électroniques : « *On entend par service de communications interpersonnelles non fondé sur la numérotation, un service de communications interpersonnelles qui n'établit pas de connexion à un numéro ou des numéros figurant dans le plan national ou international de numérotation, ou qui ne permet pas la communication avec un numéro ou des numéros figurant dans un plan national ou international de numérotation.* » WhatsApp et Zoom entrent dans cette catégorie.

Aussi, dans le cadre de ce travail, est-il proposé de retenir une approche large des réseaux sociaux/médias sociaux et de se concentrer sur les **fonctionnalités des réseaux sociaux**, à savoir l'échange numérique, entre utilisateurs, de points de vue, de contenus, à titre principal ou accessoire, sur une plateforme. L'exercice de définition d'un sujet n'est jamais tout à fait neutre : il répond à un parti pris. Dans cette étude, le parti pris est celui de l'efficacité. Déceler les enjeux des réseaux sociaux pour les pouvoirs publics commande **d'adopter une vision large** afin de ne pas écarter trop rapidement des problématiques qui sembleraient à première vue un peu éloignées. En outre, il n'est pas inutile de dépasser ces querelles qui profitent trop souvent à des opérateurs qui jouent sur les définitions afin de louvoyer entre les réglementations. On connaît l'optimisation fiscale mais « l'optimisation sociale », à mesure que les règles vont s'agréger, pourrait aussi se développer.

1.1.3. L'écosystème des réseaux sociaux

Les réseaux sociaux reposent sur une infrastructure particulière et ont un fonctionnement propre[60]. Pour les apprivoiser et en discerner les enjeux, il faut faire un tour rapide dans la salle des machines, se familiariser avec le langage qu'ils manient et s'arrêter sur les modèles économiques qui les sous-tendent.

Des infrastructures de haute technicité

Derrière les connexions et les accès illimités à des données planétaires, se cachent des **réseaux de communication** utilisant notamment de très gros câbles, dorénavant en fibre optique, dont la capacité ne cesse d'augmenter, qui acheminent les données de serveurs en serveurs sur tout le globe. 99% des communications mondiales transitent par des câbles sous-marins. Ils étaient auparavant détenus majoritairement par les États. Aujourd'hui ce sont les GAFAM, désormais MAMAA[61], qui réalisent plus de 50% des investissements pour la pose des nouveaux câbles et ceux-ci, par la force des choses, représentent un enjeu stratégique et géopolitique majeur[62]. Le nombre de données en circulation est passé de 100 gigabits par jour en 1992 à 150 700 gigabits par seconde en 2022. Ces données sont réparties entre plusieurs lieux géographiques et répliquées pour des raisons de sécurité dans des centres de données qui les stockent massivement et sont dotés de puissances de calcul considérables. Chaque jour le système répond à des milliards de requêtes en quelques secondes grâce à la très haute technicité de son fonctionnement.

Des supports diversifiés pour accéder à la plateforme

L'accès aux réseaux sociaux a été démultiplié par le développement du smartphone qui a largement concurrencé l'ordinateur. Outre les objets connectés, un nouveau support promet de bouleverser l'accès aux réseaux sociaux : il s'agit des **univers virtuels** dont le célèbre Metaverse lancé par Marc Zuckerberg en 2021. Proches des jeux vidéo, ces mondes parallèles poursuivent l'objectif de permettre de nouveaux modes de relations sociales de façon virtuelle. Ils étaient déjà apparus dans les

60 S. Abiteboul et J. Cattan, *op. cit.*
61 Méta (Facebook), Apple, Microsoft, Amazon, Alphabet (Google).
62 T. Mendes-France, Q. Leeds, *Internet, une infographie*, CNRS Edition, 2021.

années 2000 lorsque Second Life proposait une « expérience virtuelle » entre le jeu vidéo et le réseau social. L'internaute pouvait déjà créer son avatar et évoluer dans un monde parallèle. Grâce au développement des casques virtuels et de la 5G, cette technologie connaît un nouveau succès dont l'ambition est de détrôner les vieux ordinateurs et smartphones.

L'accès au réseau social

Pour accéder à un réseau social, il faut utiliser un **navigateur web**[63] comme Google Chrome, Safari d'Apple ou Mozzila Firefox mais, depuis peu, une alternative à ces navigateurs est apparue. Sont ainsi de plus en plus utilisées les **applications** téléchargées à partir de magasins d'applications au moyen d'un ordinateur ou smartphone (*via* les systèmes d'exploitation Android ou IOS). Les deux principales plateformes de téléchargements de ces applications sont l'App Store et Google Play. Si on dénombrait 2 milliards de téléchargements d'applications en 2009, on en comptait 218 milliards en 2020[64]. Une fois cette étape franchie, on accède alors à l'**interface graphique** du réseau choisi. L'internaute dispose d'une page personnelle d'accueil et s'abonne à d'autres utilisateurs.

L'inscription sur le réseau

Sauf lorsqu'il visualise des contenus sans inscription préalable nécessaire[65], l'internaute, lors de la première utilisation et chaque fois qu'elles seront modifiées, doit approuver les **conditions générales d'utilisation (CGU)** qui regroupent les conditions du contrat de fourniture de services par l'opérateur et renvoient notamment à la **politique d'utilisation des données** (qui explique comment les données personnelles sont utilisées)[66]. L'importance des CGU est considérable car elles fixent le cadre contractuel des prestations offertes et les règles applicables aux relations entre l'opérateur et l'utilisateur. Elles définissent notamment qui peut utiliser le service, à quelles conditions, mais aussi la façon dont les contenus sont modérés et les modalités de blocage des comptes, l'existence d'un système de détection des « *trolls* »[67], le niveau de responsabilité de l'opérateur, le tribunal compétent en cas de litige, les paramètres ou fonctionnalités à disposition de l'utilisateur, les modalités de gestion des publicités, etc. Elles peuvent, en sus du document intitulé « politiques de confidentialité », rappeler quelles sont les données recueillies (adresses IP[68], adresse mail, âge, etc.) et comment vont être utilisées les données produites (*like, retweet,* etc.) Variables selon les plateformes, généralement très longues, elles sont, au moment de leur acceptation, peu lues par les utilisateurs, qui souhaitent avant tout accéder au service offert. Dès lors, la valeur et la portée du consentement donné peuvent être questionnées.

63 Les navigateurs sont des logiciels qui permettent d'accéder au web. C'est à travers eux que les sites ou réseaux sociaux apparaissent. Il ne faut pas les confondre avec les moteurs de recherche qui facilitent la navigation sur le net et permettent de sélectionner et classer les sites recherchés. Il est possible d'accéder directement à un site par son nom de domaine sans passer par un moteur de recherche.

64 T. Mendes-France et Q. Leeds, préc.

65 Ceci est notamment possible sur Twitter ou YouTube.

66 S'agissant du consentement des CGU par les mineurs, *cf. infra*

67 Personne qui poste des informations tendancieuses pour alimenter la polémique sur internet.

68 Internet Protocol : numéro d'identification attribué à chaque périphérique relié à un réseau informatique.

Lors de la première visite, et régulièrement, l'internaute est également interrogé sur son acceptation à être suivi par des « ***cookies*** » **ou traceurs**. Un *cookie* est un petit fichier (une suite d'informations), stocké par un serveur sur l'ordinateur, qui permet de collecter les données de navigation sur le web. Les *cookies* ont de multiples usages : ils peuvent servir à mémoriser l'identifiant client auprès d'un site, le contenu courant du « panier d'achat », à tracer la navigation pour des finalités statistiques ou publicitaires, etc. Dans ce cas, ils permettent de mémoriser les données (produits regardés, liens cliqués, temps passé…) pour créer un profil détaillé, mieux cibler la publicité et parfois revendre ces informations. Si les *cookies* ne proviennent pas du site consulté, on parle de ***cookies* tiers**. Les *cookies* doivent être expressément acceptés par les utilisateurs, sauf s'ils sont strictement nécessaires au fonctionnement du site ou de l'application[69]. Ainsi, les *cookies* liés aux opérations relatives à la publicité personnalisée et ceux des réseaux sociaux, notamment générés par leurs boutons de partage, doivent faire l'objet d'un consentement réel[70]. Plusieurs opérateurs ont été condamnés pour ne pas respecter ces obligations. Des techniques alternatives[71] sont de plus en plus utilisées mais ne dédouanent pas de l'obligation de recueillir le consentement de l'utilisateur (*cf. infra*).

C'est alors un univers qui s'ouvre, avec ses codes et son langage. Chaque invention s'accompagne d'évolutions linguistiques. Les réseaux sociaux n'échappent pas à cette règle et c'est dans la bouche des adolescents qu'ils sont les plus vivants.

Le langage des réseaux sociaux : **parler** « **Réseau social** »

Chaque jour, Emma, après voir *rep* (répondre) à ses *notifications* (information sur les nouveautés et les interactions sur un compte) va sur *le fil d'actu* (fil d'actualité) de chacun des réseaux où elle est inscrite, regarde le nombre de *followers* (c'est-à-dire le nombre de personnes abonnées à ses comptes) et le nombre d'*abo* (abonnements) aux comptes des personnes qu'elle suit. Elle a plusieurs *pseudo*s pour pouvoir s'exprimer librement et a utilisé plusieurs *filtres* pour embellir ou accessoiriser les photos de son profil. Sur Snapchat, elle s'est créé un *bitmoji* (icône personnalisée à l'effigie de l'utilisateur) et s'amuse à compter ses *flammes* (indice mesurant la régularité des relations sur ce réseau). Elle aime bien aussi ce réseau qui permet de lire un message sans que l'émetteur le sache, la fonction s'appelle « entrouvrir ». Sur Instagram, elle a deux comptes. L'un, qu'elle a paramétré pour n'être visible que par ses amis proches (*compte privé*) l'autre qu'elle n'a pas paramétré et qui est donc public par défaut (*compte public)*. Lorsqu'elle souhaite discuter en aparté, elle fait un *DM* (direct message entre deux personnes) ou un *MP* (message sur son groupe privé). Elle « lâche des vu » à ceux auxquels elle ne souhaite pas répondre. Lorsqu'elle souhaite partager en direct un moment avec toute sa communauté, elle active son *live.* Elle est prudente depuis qu'une de ses amies, après avoir envoyé des *nude* à son copain (photo dénudée envoyée sur les réseaux) a été

69 CNIL, site internet, *Cookies et traceurs : que dit la loi ?*.

70 Vidéos pour comprendre le fonctionnement des cookies sur YouTube : *Qu'est-ce qu'un COOKIE ?,* YouTube ; *Nouvelles règles de dépôt des cookies : qu'est-ce que ça change pour vous ?*, YouTube;

71 Notamment les empreintes numériques du navigateur (fingerprinting) ; l'authentification unique (Single Sign On) l'identifiant unique et le ciblage par cohorte. *Alternatives aux cookies*, site internet de la CNIL.

victime de *revenge porn*, ça l'a « mis en PLS » (très mal). Depuis, elle *stalk* (épie, surveille) certains comptes de soi-disant « amis » pour essayer de savoir qui a fait ça et *screene* (capture d'écran) les pages les plus douteuses. Elle *follow* (suit) plusieurs *influenceurs* (Norman, Natoo, Nabilla*)* notamment des *youtubeurs ou instagrameurs*. Avant, elle passait des heures à *scroller* (faire défiler) des *reels* (courtes vidéos divertissantes sur instagram ou musicales sur TikTok) des *mèmes* (image virale à vocation humoristique) ou des *shorts* (sur YouTube) mais désormais, elle préfère se mettre sur son *timeline* (flux d'actualités qui présente les *tweets* du plus récent au plus ancien) pour suivre l'actualité sur Twitter et sur YouTube. Engagée pour la protection de la biodiversité, elle assortit ses *post* (publication) d'*hashtag* (mot clé permettant de faciliter les recherches) pour qu'ils soient plus visibles et *retweet*, *regram,* ou *like* régulièrement les *tweets* et *messages* qu'elle trouve intéressants. Elle fait toutefois attention aux *haters* (personnes diffusant des critiques haineuses), derrière lesquels peuvent se cacher des *trolls*[72]. De temps en temps, elle « poste un tiktok » (une vidéo de moins 3 minutes réalisée sur TikTok dans les réels), réalise une *story* sur Insta (contenu éphémère posté sur les réseaux sociaux), modifie les *selfies* sur son *journal* qu'elle décore de nouveaux *emoji* (pictogramme utilisé dans les messages pour exprimer une émotion). Son meilleur ami est un *gamer* (adepte de jeux vidéo) assidu sur Twitch. Il s'est inscrit sur Tinder pour trouver des *match* (lorsque deux personnes se *likent* mutuellement) et peut-être avoir un *bail* ou un *crush* (coups de cœurs amoureux). Depuis peu, elle a rejoint la communauté *des wikipédiens et wikipédiennes* et est devenue *patrouilleure* (personne qui surveille les contenus illicites sur Wikipédia. Mais ce qu'elle préfère, c'est vivre *IRL* (in real life) ce qui lui permet aussi d'avoir des choses à raconter sur les réseaux ! ☺

Les fonctionnalités principales des réseaux sociaux

Si les **fonctionnalités offertes** sont, comme il a été dit plus haut, très diverses selon le type de réseau social (discuter, jouer, partager des vidéos, se rencontrer, etc.), certaines sont communes car inhérentes aux réseaux sociaux (stockage des données) et d'autres sont si fréquentes et spécifiques qu'elles méritent d'être signalées (hiérarchisation et tri des contenus). Tout réseau social, quel qu'il soit, **stocke** des données sur ses utilisateurs, constituant autant de bases de données que d'utilisateurs. Ce stockage sera d'autant plus massif que le réseau sera structuré de façon centralisée. En effet, les données récoltées sur les réseaux sociaux, qui fonctionnent selon un modèle participatif et décentralisé, sont, par définition, éparpillées sur de multiples serveurs et donc plus difficiles à réexploiter. A l'inverse, un réseau social centralisé comme Facebook ou Instagram conserve les informations personnelles sur l'internaute (son profil), les contenus publiés ou partagés, les réactions à ses contenus, etc. Tout réseau est responsable de la collecte et de la conservation des données dans le respect des règles applicables (*cf. infra*).

72 Le *troll* est une personne qui s'immisce ou crée un débat polémique au sein des plateformes de discussion en ligne dans l'objectif de déséquilibrer une communauté. Par la création d'un faux contenu, souvent associé à un personnage fictif qu'il a monté de toutes pièces, il diffuse des messages pour provoquer des réactions sur une plateforme.

En outre, la plupart des réseaux sociaux **interviennent sur l'agencement des contenus**, soit qu'ils les classent et en recommandent certains aux utilisateurs en les classant, soit qu'ils les « modèrent » en les supprimant ou les « invibilisant » lorsqu'ils sont illicites ou contraires aux conditions générales d'utilisation. L'ensemble des contenus publiés sur un réseau social ne peut être présenté à l'utilisateur sans ordonnancement. Le volume de contenus publiés implique nécessairement que la plateforme définisse un ordre d'apparition, opère une sélection, tout en laissant à l'usager la possibilité d'aller chercher, à son initiative, un contenu spécifique. Les contenus qu'il consultera effectivement dépendront en premier lieu de l'agencement de son interface et du recours à des **règles algorithmiques** pour hiérarchiser et individualiser la présentation des différents contenus. Certains réseaux peuvent aussi préférer un ordonnancement purement chronologique, sans intervention tierce. Contrairement à des médias traditionnels, l'ordonnancement des contenus sur les services de réseau social est généralement individualisé (sauf dans le cas des forums) et chacun voit le résultat de l'individualisation lorsqu'il accède au service. La question de l'emploi de ces algorithmes et de l'usage des données collectées est au cœur des principales polémiques. Cette dernière question est d'autant plus sensible que les réseaux sociaux collectent également, au moyen **des *cookies***, des données de tiers.

Le moteur et le carburant des réseaux sociaux : les algorithmes et les données

Pour prendre comme métaphore la voiture, il est possible de dire que les algorithmes constituent le moteur des réseaux sociaux et les données son carburant.

L'algorithme est classiquement défini comme «une suite d'instructions et d'opérations permettant de résoudre une catégorie de problèmes »[73]. Il faut distinguer entre les **algorithmes explicites et implicites**[74], selon que les règles logiques sont explicitement décrites par les scientifiques ou bien qu'elles sont apprises par la machine. Les algorithmes implicites regroupent les algorithmes dits d'apprentissage plus connus sous le nom de *machine learning* et que l'on classe souvent dans la catégorie de l'intelligence artificielle. Certains développent des critères implicites à partir d'un problème d'optimisation des données sur des données dites d'apprentissage. C'est le cas des algorithmes dits de **catégorisation** qui classifient les données d'apprentissage selon des ensembles distincts par similarité statistique.

Ces approches algorithmiques sont très souvent utilisées par les réseaux sociaux pour réaliser différentes tâches. La question de la **modération automatique** de contenu en est un premier exemple. À partir de publications antérieures jugées contraires aux règles d'utilisation d'une plateforme, il s'agit d'apprendre à étiqueter tout nouveau contenu comme autorisé ou, au contraire, prohibé. Cette phase d'apprentissage sert ensuite à identifier en temps réel (et sans nécessairement de supervision humaine) les contenus illicites avant qu'ils ne soient publiés sur les réseaux sociaux.

73 *Intelligence artificielle et action publique : construire la confiance, servir la performance*, étude du Conseil d'État à la demande du Premier ministre, mars 2022.

74 A. Jean, *Les algorithmes font-ils la loi ?*, L'édition de l'observatoire, 2021

L'autre service omniprésent dans l'activité des réseaux sociaux est la **recommandation automatisée** qui utilise également les algorithmes d'apprentissage pour personnaliser des contenus. À l'instar des moteurs de recherche, la tâche consiste à déterminer l'importance des contenus existants afin de sélectionner ceux qui seront proposés à l'utilisateur. Mais à la différence des moteurs de recherche qui sont, eux, aiguillés par les mots-clefs donnés par l'utilisateur, les réseaux sociaux doivent déterminer automatiquement, et de manière différente pour chaque utilisateur, quels contenus sont les plus à même de l'intéresser. Ils utilisent pour cela un ensemble d'algorithmes exploitant diverses informations comme l'origine du contenu, sa date, son niveau de partage (niveau d'engagement), sa nature (image, longueur, type), sa localisation, les centres d'intérêt de l'utilisateur et l'intérêt commercial pour la plateforme. Ces algorithmes réussissent ainsi à déterminer, sans l'aide explicite de l'utilisateur, quels sont les contenus les plus susceptibles de l'intéresser. Des études montrent cependant que, lorsqu'ils sont utilisés de façon rigide, ils conduisent à ce qu'on appelle « *des bulles de filtre* » en lien avec les phénomènes de confinement informationnel en ligne[75].

Quant aux **données** collectées par le réseau social, outre celles qui sont utilisées pour entraîner les algorithmes et dont le choix peut s'avérer crucial, on en distingue trois types : les *données fournies par l'utilisateur* lors de son inscription (identité, adresse mail, âge, etc.) pour créer son profil ; *les données* « *observées* » (informations susceptibles d'être retenues par l'algorithme, par exemple les pages « likées » par l'utilisateur) et les *données inférées* (qui sont les données déduites du croisement d'informations par exemple des préférences de l'utilisateur ou des modes d'utilisation tels que le temps d'observation, le type de contenus, etc.[76]).

L'utilisateur n'est pas nécessairement conscient que de telles informations sont données au réseau social et sont utilisées à des fins de profilage notamment pour lui proposer de la publicité ciblée. En effet, l'utilisation qui en est ensuite faite dépend du modèle économique du réseau, de ses conditions générales d'utilisation (CGU), des politiques de confidentialité et des règles juridiques applicables. En réalité, autant qu'un carburant, les données constituent **le produit** des réseaux sociaux. Elles servent aussi, une fois pseudonymisées[77] et croisées avec des millions d'autres données, à des fins statistiques et de recherche. On dit souvent qu'elles sont le nouvel « or noir ». Elles sont porteuses d'immenses progrès[78] dans de nombreux domaines notamment pour les sciences sociales[79] et ont ouvert de

75 Eli Pariser a théorisé ce concept, *The Filter Bubble : What the Internet Is Hiding From You*, Londres, Penguin Press, 2011.

76 Par ex., si l'usager a 30 ans, qu'il a liké des pages de robes de mariées, et que l'algorithme déduit de son comportement sur le réseau que son couple est stable, on lui proposera des plans de financement d'acquisition de logement ou des couches pour les bébés.

77 La pseudonymisation est un traitement de données personnelles réalisé de manière à ce qu'on ne puisse plus attribuer les données à une personne physique identifiée sans information supplémentaire. En pratique, la pseudonymisation consiste à remplacer les données directement identifiantes (nom, prénoms, etc.) d'un jeu de données par des données indirectement identifiantes (alias, numéro séquentiel, etc.). La pseudonymisation permet ainsi de traiter les données d'individus sans pouvoir identifier ceux-ci de façon directe. Contrairement à l'anonymisation, la pseudonymisation est une opération réversible : il est possible de retrouver l'identité d'une personne si l'on dispose d'informations supplémentaires.(source : site CNIL).

78 *Rapport* de la mission Bothorel, *Pour une politique publique de la donnée*, décembre 2020.

79 *Le Monde*, site internet, 26 avril 2022, « L'humeur de la planète sondée grâce aux réseaux sociaux ».

nouveaux horizons économiques ; mais, s'agissant des données personnelles, elles augmentent aussi, très notablement, du fait de leur sensibilité, la vulnérabilité de chacun. Les enjeux relatifs à la possession et à l'utilisation de ces données sont majeurs pour nos sociétés contemporaines. Un équilibre acceptable est encore à trouver entre protection des personnes et promotion du progrès (*cf. infra*).

L'économie des réseaux sociaux

• *Les différents modèles économiques*

Les réseaux sociaux, entendus de façon large (principaux ou accessoires), peuvent reposer sur des modèles économiques différents. Hormis ceux qui fonctionnent sur un modèle totalement libre et collaboratif (comme Mastodon), ils tirent leurs ressources de systèmes différents. Certains bénéficient de dons (*cf.* Wikipédia, qui reçoit des dons, y compris des GAFAM, moyennant un montant maximal censé garantir l'indépendance de la plateforme), d'autres soumettent leurs utilisateurs à des abonnements (tel Rédit) mais la très grande majorité s'appuie, à l'instar des grandes plateformes numériques, sur les aspects bi-face du marché au sein duquel ils prospèrent et se financent par la publicité en contrepartie de la gratuité affichée. Ce modèle économique particulier mérite un examen approfondi.

• *Le capitalisme des plateformes et les réseaux sociaux*

Dans son étude de 2017, *Puissance publique et plateformes numériques : accompagner l'ubérisation*, le Conseil d'État, poursuivant son analyse de 2014[80], avait identifié quatre caractéristiques faisant des plateformes des écosystèmes particulièrement performants pour le développement de l'économie. Les réseaux sociaux entrent parfaitement dans cette catégorie. En effet, ils mettent en **système la** « **multitude** » dans la mesure où ils mettent en relation des initiatives individuelles convergentes assemblées de façon cohérente soit au bénéfice d'un échange soit dans la perspective de la création d'un bien commun. Ils sont fondés sur l**'individualisation** la plus grande possible au profit de l'utilisateur, grâce notamment à la sophistication des algorithmes et de l'intelligence artificielle. Ils reposent sur **une relation de confiance** qui favorise la multiplication des échanges et sur **un coût marginal** des transactions très faible puisque la matière première est essentiellement l'information numérique.

Si pour l'économie traditionnelle, l'ubérisation a conduit à la « désintermédiation », (c'est-à-dire à la substitution aux intermédiaires de l'économie traditionnelle) elle a aussi permis l'émergence d'une nouvelle économie théorisée notamment par l'économiste Jean Tirole à travers la notion de **marchés bi-faces**[81], configuration dans laquelle la plateforme attire simultanément plusieurs utilisateurs de deux marchés différents au sein d'un même écosystème, faisant bénéficier chaque face du marché d'une externalité positive de l'autre. Pour les réseaux sociaux, d'un côté les utilisateurs vont sur la plateforme pour être mis en relation avec les autres

80 Dans son étude annuelle de 2014, *Le numérique et les droits fondamentaux*, le Conseil d'État avait défini la plateforme comme une catégorie de « *prestataires intermédiaires* » pour le partage de « *services de référencement ou de classement de contenus, biens ou services édités ou fournis par des tiers* ».

81 J.-C. Rochet , J. Tirole, « Plateform competition in two-sided markets », *Journal of the european economic association*, I (4) 2003, p. 999-1029, J. Tirole, *Economie du bien commun,* Paris, PUF, 2016.

utilisateurs et, d'un autre côté, les annonceurs accèdent à la plateforme pour vendre leur publicité. Le marché publicitaire sera d'autant plus florissant que le réseau permettra au plus grand nombre d'utilisateurs de discuter et d'échanger des contenus. Les plateformes peuvent dès lors s'appuyer sur un système de tarification qui profite de l'externalité positive d'un côté du marché et fait reposer le coût financier sur l'autre côté. Ainsi, en est-il pour les réseaux sociaux à but lucratif qui attirent des internautes par la gratuité du service mais se rémunèrent par la monétisation des données par les annonceurs. La gratuité n'est donc qu'apparente et ne répond qu'à une stratégie commerciale visant à attirer le maximum d'utilisateurs. L'adage « *si c'est gratuit, c'est que vous êtes le produit* » résume bien le dispositif.

• *L'économie de l'attention et la publicité ciblée*

On estime que c'est après le développement de l'imprimerie, puis de la presse, et avec l'émergence de la « réclame » ou de la publicité, que l'attention est devenue un véritable objet du marché. Comme le dit Bruno Patino, « *Facebook n'a évidemment pas créé l'économie de l'attention, puisque celle-ci date du développement des médias financés par la publicité et notamment de la radio dans les années 1920 et de la télévision quelques décennies plus tard* »[82]. La captation de l'attention est cependant devenue un enjeu clé du système économique avec le développement de la société de consommation, la multiplication de la publicité et du marketing. Le développement des technologies audiovisuelles puis numériques a exacerbé ces tendances car le numérique et les vidéos en particulier sont beaucoup plus efficaces à cet égard[83]. Il n'est ainsi pas anodin que YouTube soit le deuxième site internet le plus visité au monde (2 milliards d'utilisateurs par mois)[84]. Les mécanismes pour capter à grande échelle et sur un temps le plus long possible l'attention des utilisateurs et cibler au mieux les publicités, sont apparues à l'ère du numérique.

-- *L'alerte comme système d'organisation*

Pour capter le plus longtemps possible les utilisateurs, les réseaux sociaux favorisent des contenus ou des modes de propagation qui suscitent un fort « engagement ». Bruno Patino explique combien les plus grands réseaux sociaux ont bâti leur système pour stimuler notre attention toutes les 9 secondes[85]. A l'instar du poisson rouge qui tourne dans son bocal, le réseau social crée « *un instantané infini* » et entretient l'internaute dans « *une servitude volontaire numérique* ». Comme les machines à sous, qui génèrent la dépendance par l'aléa et le plaisir immédiat, les réseaux sociaux fournissent de façon aléatoire des contenus qui génèrent l'engagement et deviennent rapidement viraux. Le « *fear of missing out* » (FOMO) ou la crainte d'être exclu par l'ignorance, nourrit cette dépendance.

-- *Le succès de la publicité ciblée fondée sur l'économie de la donnée*

L'instauration de ce modèle économique remonte aux années 2010, après l'éclatement de la première bulle financière internet. En effet, pendant des années, le réseau Facebook notamment, a prospéré sans financement. Puis, s'inspirant du

82 B. Patino, *Tempête dans le bocal*, 2021 p. 36.
83 CNNUM, *Votre attention s'il vous plaît ! Quels leviers face à l'économie de l'attention*.
84 T. Mendes-France et Q. Leeds, *op. cit.*
85 B. Patino, *La civilisation du poisson rouge, Petit traité sur le marché de l'attention*, Grasset, 2019.

développement par Google du modèle de la publicité ciblée lancée en 2000 avec les « *adwords* » (vente de mots clés), l'idée de valoriser les réseaux sociaux grâce aux données récoltées permettant de mieux profiler les publicités s'est affirmée[86]. En effet, grâce à la collecte massive des données des utilisateurs et aux capacités de calcul démultipliés, il est aisé de cibler et profiler au mieux les clients. Ce dispositif a rencontré un immense succès. La publicité est ainsi devenue le revenu principal des réseaux sociaux[87]. Le marché mondial de la publicité en 2020 représentait 131 Mds de dollars (dont 50 Mds de dollars aux États-Unis et 49 Mds de dollars en Asie, la Chine représentant 35 Mds de dollars à elle seule). Le groupe Meta (Facebook, Instagram, WhatsApp et Messenger) était le groupe leader dans ce secteur avec 84 Mds de dollars de chiffre d'affaires. Selon le baromètre unifié du marché publicitaire 2020[88], la part des recettes publicitaires nettes totales issues du secteur de l'internet est passé de 2% en 2005 à 24% en 2015, pour atteindre 46% des recettes publicitaires totales en 2020. Alors que la part des recettes issues du secteur de la presse est passé de 46% en 2005 à 25% en 2015, et 14% en 2020.

Concrètement, les annonceurs proposent des publicités en précisant l'objectif recherché et le budget dont ils disposent. Les publicités sont choisies par les réseaux sociaux selon un procédé de vente aux enchères qui se déroule en une fraction de seconde à l'aide d'algorithmes[89]. Le réseau social a intérêt à cibler au mieux la publicité pour augmenter ses impacts et à ce que les internautes restent le plus longtemps possible sur les réseaux. Le profit dépend alors du temps passé sur les écrans et du nombre de publicités visualisées. Cette pratique soulève de nombreuses questions qui seront évoquées dans la deuxième partie (*cf. infra*). La manne publicitaire est d'autant plus importante que les effets de réseau jouent à plein. Google et Facebook captent ainsi 75% du marché français de la publicité digitale et disposent de *walled gardens* (jardins clos) tels que Facebook, Instagram, Google Search et YouTube, sur lesquels les annonceurs ne peuvent acheter des espaces qu'en passant par les régies intégrées des plateformes ou par des solutions achat-vente d'espaces publicitaires intégrés[90].

- *Réseaux sociaux et lois de l'économie numérique*

Les réseaux sociaux sont une source de profit économique car ils obéissent aux lois de l'économie numérique que sont ***la loi des rendements croissants*** (contrairement à l'économie traditionnelle, plus les clients sont nombreux, meilleur est le service

86 Sur le marché de la publicité digitale, on distingue le *search* (publicité liée aux recherches et à certains mots-clefs. Le moteur de recherche vend de l'espace publicitaire) et le *display* (publicité d'affichage de messages en ligne sur les réseaux sociaux dite *display* social, ou sur les autres sites internet dite *display* non social).

87 « *En 2021, l'ensemble des leviers de la publicité digitale a fortement rebondi après la crise avec une croissance de 24% (7,7Mds €) par rapport à 2020 : Le Search enregistre une forte croissance de +28% et pèse 42% (3254 M€) du marché. Le Social croît de +22% sur l'année tandis que son poids se stabilise à 26% (2034 M€), Le Display, qui avait plus souffert de la crise que les deux premiers leviers, affiche une croissance exceptionnelle de +31% (1501M€). (…) Dès 2021, Le marché retrouve sa dynamique pré-Covid avec une croissance de 29% par rapport à 2019.* » « L*e marché de la publicité digitale est ultra dynamique – en 5 ans, il a plus que doublé, pour atteindre 7,7 milliards d'Euros, soit 17% de croissance annuelle. Le trio Google-Meta-Amazon représente désormais près de 67% du marché total* » *Source : SRI*

88 Réalisé par IREP, France Pub et Kantar Media.

89 S. Abiteboul et J. Cattan.

90 A. Perrot, M. Emmerich, Q. Jagorel, *Publicité en ligne : pour un marché à armes égales*, nov. 2020, p. 7-10.

sans accroissement des coûts ni du prix), la loi ***des effets de réseau*** qui permet à un produit d'augmenter sa valeur à mesure que le nombre d'utilisateurs augmente, et enfin **le faible coût de transaction** – les technologies numériques rendant le marché plus vaste, fluide et réduisant le nombre d'intermédiaires. Les réseaux sociaux facilitent, par l'utilisation de techniques numériques, les échanges entre internautes de discussions ou de contenus dont la plupart sont produits par les internautes eux-mêmes. La valeur de ce qui est partagé augmente à mesure du nombre de personnes participant à la plateforme, les coûts de partage étant très faibles et à peu près invariables quel que soit le nombre de participants. Face à un contenu aussi peu coûteux que l'information, **l'économie d'échelle** joue à plein. Il en est de même pour les effets de réseau : pour discuter avec ses amis, il faut aller sur la plateforme où le plus grand nombre d'entre eux évolue.

A l'instar des plateformes d'échanges de biens et services, ces différentes propriétés du marché économique numérique engendrent un fort phénomène de **concentration** au profit des réseaux sociaux les plus importants, appelés à toujours grandir plus et rendre difficile l'émergence de nouveaux acteurs. Ce phénomène, souvent dénommé « ***winners take most*** », déstabilise les règles classiques de la concurrence. Il se trouve renforcé par l'absence d'interopérabilité des réseaux même si, grâce au RGPD, les plateformes doivent assurer la portabilité des données. En outre, les plus gros acteurs, dont certains se nourrissent également d'autres fonctionnalités que celles des réseaux sociaux, se trouvent avantagés par l'antériorité et la richesse des données qu'ils détiennent. C'est ainsi que Google, grâce aux données collectées par son moteur de recherche, peut sans cesse améliorer le fonctionnement de ses algorithmes et des services fournis. La possession de données sur les utilisateurs devient, pour les opérateurs, un atout capital au sein du marché. Ainsi, dans la galaxie des réseaux sociaux, il existe quelques énormes et très grosses « planètes » (Google, Facebook, TikTok et Twitter, certes beaucoup moins important en nombre d'utilisateurs mais très influent) et une multitude de petits réseaux périphériques qui parviennent difficilement à grossir. Cette structuration rend difficile l'application de règles identiques à tous.

Réseaux sociaux et « contrôleurs d'accès »

L'effet de réseau a permis à des géants du numérique d'émerger. Leur puissance financière est telle qu'elle leur permet de financer l'innovation, de racheter les *start up* les plus prometteuses ou des plateformes bénéficiant déjà d'un grand nombre d'utilisateurs afin d'augmenter l'effet de réseau (*cf.* le rachat de WhatsApp par Facebook[91]) et rend la concurrence difficile. On rassemble souvent sous cette appellation les GAFAM, maintenant MAMAA, dont deux sont de puissants réseaux sociaux : Meta (qui possède Facebook et Instagram) et Youtube qui appartient à Google (Alphabet) mais il ne faut pas oublier les géants asiatiques (BATX : Baidu, Alibaba, Tencent, Xiaomi) et le réseau social Tiktok qui ne cesse de gagner des parts de marché[92].

91 Facebook a racheté la messagerie WhatsApp en 2014 qui ne produisait aucun revenu mais avait 450 millions d'utilisateurs pour 19 milliards de dollars.

92 Il convient cependant de relativiser un peu ce phénomène car, comme le soulèvent souvent les opérateurs, la position dominante des plus gros réseaux repose essentiellement sur la confiance (ou sur des effets de mode) et non sur des infrastructures solides, de sorte qu'elle reste relativement fragile.

On désigne souvent ces plateformes sous le nom anglais de ***gatekeepers*** qui signifie **contrôleurs d'accès** car, du fait de leur puissance, elles contrôlent l'accès aux utilisateurs et fixent les règles de transmission de l'information. Par exemple, Facebook et Google contrôlent l'accès à l'essentiel de l'audience mondiale pour les annonceurs. Ils sont donc des « gatekeepers » pour le marché publicitaire. Jusqu'à récemment, il n'existait pas de définition de ces plateformes dites *structurantes* et plusieurs rapports avaient tenté d'en proposer[93]. Depuis plusieurs années a émergé l'idée qu'il était nécessaire de les soumettre à des obligations particulières afin de restaurer une concurrence équitable sur le marché, les instruments classiques du droit de la concurrence s'avérant imparfaits (*cf. infra*). L'article 3 du *Digital Markets Act* (DMA) consacre la notion de *gatekeepers* qui repose désormais sur des critères d'audience, de poids économique et de pérennité. Seront pris en compte le chiffre d'affaires ou la valeur marchande de la plateforme qui fournit son service dans au moins trois États membres, le nombre d'utilisateurs finaux actifs établis dans l'Union européenne, sachant que ces critères devront être remplis durant trois années pour présumer l'appartenance à cette catégorie[94].

De l'écosystème au système juridique ?

L'écosystème particulier des plateformes et des réseaux sociaux a bouleversé de nombreux domaines comme celui – ainsi qu'il vient d'être dit – de la concurrence. Il a même engendré des bouleversements terminologiques, notamment sur la distinction entre la sphère publique et privée (*cf. infra*). Le terme « d'ami » n'a ainsi plus le même sens selon qu'il est utilisé dans le langage courant ou dans la communauté de Facebook. Ce point a d'ailleurs fait l'objet d'un contentieux juridique. La Cour de cassation a ainsi été amenée à juger que le lien avec un « ami » sur un réseau social ne renvoie « *pas à des relations d'amitié au sens traditionnel du terme et que l'existence de contacts entre ces différentes personnes par l'intermédiaire de ces réseaux ne suffit pas à caractériser une partialité particulière* »[95].

Cet arrêt, qui tranche un point aussi badin que la notion d'*ami* – concept *a priori* assez indépendant de la sphère juridique – illustre l'ampleur des retentissements que l'écosystème des réseaux sociaux produit sur l'ensemble de l'édifice juridique. Tout d'abord, le phénomène des réseaux sociaux a remis en cause certaines catégories juridiques bien enracinées. Par exemple, la distinction entre un *consommateur* et un *professionnel,* déstabilisée par le fonctionnement des plateformes, a donné lieu à des interprétations innovantes des juges dans le cadre de l'application du droit de la consommation[96] et engendré la création de la notion *d'utilisateur* dans le

On constate d'ailleurs l'émergence ces dernières années de nouveaux réseaux sociaux chez les jeunes générations pour qui Facebook fait figure de réseau préhistorique.

93 Rapport d'information de la commission des affaires économiques sur les plateformes numériques, Assemblée Nationale, n° 3127 enregistré le 4 juin 2020 ; rapport d'information de la commission des affaires européennes de l'Assemblée nationale n° 4409 et du Sénat n° 34 sur le DMA.

94 Art. 3, du DMA,

95 CCass., 2e civ., 5 janvier 2017, n° 16-12-394, Bull.

96 L'arrêt C-105/17 du 4 octobre 2018 a donné à la CJUE l'occasion de préciser la notion de « professionnel » au sens de la directive sur les pratiques commerciales déloyales ainsi que les critères à prendre en compte par les juridictions nationales lors de l'appréciation de cette notion dans le cadre particulier de la vente en ligne. La Cour conclut qu'une « personne physique, qui publie sur un site

cadre des réglementations du secteur numérique. De même, la distinction entre le *contrat à titre gratuit* et celui à *titre onéreux* a dû être interprétée à l'aune de ces changements, démontrant, s'il en était besoin, le caractère indispensable de l'office du juge pour adapter le droit au réel.

Surtout, par sa nature de *place de village* extrêmement vivante et propice à tous les excès, où circule tout type de personnes et d'informations, l'apparition des réseaux sociaux a *de facto* bouleversé toutes les branches du droit. On s'invective sur les réseaux sociaux, on diffame, on colporte des fausses nouvelles, on plagie, on contrefait, on usurpe des identités, on commet des escroqueries, on corrompt des mineurs, on recrute pour le djihad, on incite à la haine, on détourne des données personnelles, on viole des correspondances privées, on recommande des produits dangereux, on conclut des contrats, on rencontre son partenaire, etc. Finalement, toutes les branches du droit sont concernées et leurs systèmes au départ construits autour du monde réel doivent s'adapter aux univers virtuels. Ainsi, dans le champ nouvellement institué du droit du numérique, celui des réseaux sociaux se construit peu à peu mais, loin de constituer une branche autonome, il emprunte à de nombreuses autres branches du droit et révèle un régime juridique fragmenté.

1.2. Le droit multi-face des réseaux sociaux

Au-delà de leur diversité, les réseaux sociaux se caractérisent généralement par leur dimension transnationale. Dans l'idéal, celle-ci appellerait un régime juridique et une gouvernance au niveau international. Si des travaux sont en cours concernant l'internet[97] et hormis l'Appel de Christchurch (qui a conduit des chefs d'État dont le président français à prendre des engagements sur la lutte contre les contenus terroristes en ligne[98]), il n'en va pas de même des réseaux sociaux. Ce sont les différents États qui font face à cette question et s'agissant des États membres de l'Union européenne, ils le font principalement à travers celle-ci.

A l'instar du type de marché qu'il régit, le droit des réseaux sociaux se révèle en France **multi-face**. Le réseau social numérique n'est pas, ou est encore peu, une catégorie juridique à laquelle est attaché un droit spécifique. Entrant dans de nombreuses catégories, **son droit se révèle composite**. Par leur ingénierie, les

internet, simultanément, un certain nombre d'annonces offrant à la vente des biens neufs et d'occasion, telle que la défenderesse au principal, ne saurait être qualifiée de « professionnel » et une telle activité ne saurait constituer une « *pratique commerciale » que si cette personne agit à des fins qui entrent dans le cadre de son activité commerciale, industrielle, artisanale ou libérale, ce qu'il appartient à la juridiction de renvoi de vérifier, au vu de toutes les circonstances pertinentes du cas d'espèce.* »

97 Internet governance Forum, *IGF Annual Meetings Proceedings.*

98 L'attentat du 15 mars 2019, à Christchurch en Nouvelle-Zélande, a été prémédité par son auteur pour être diffusé en direct sur les réseaux sociaux. La vidéo a ainsi pu être diffusée de longues minutes et relayée à une très large audience même après avoir été interrompue. V. site internet du ministère des affaires étrangères, rubrique diplomatie-numerique.

réseaux sociaux sont soumis au droit des télécommunications, des données personnelles, des algorithmes et de l'intelligence artificielle. Par leur qualité d'acteur du marché économique, ils sont soumis au droit de la concurrence et au droit du commerce. Par leur appartenance à la catégorie des personnes privées entretenant un lien contractuel avec les utilisateurs, ils sont soumis au droit des contrats et de la consommation. Par les fonctionnalités de discussion et d'échanges de contenus qu'ils offrent, ils sont soumis à l'ensemble des droits qui protègent la liberté d'expression, la protection de la vie privée, l'ordre public, la sécurité intérieure, les œuvres de l'esprit et les publics vulnérables (mineurs), etc. L'éclairage apporté par le droit comparé démontre que cette fragmentation n'est pas propre à la France.

Le droit des réseaux sociaux est aussi un **droit européanisé**. Face à un outil sans frontières, à un marché globalisé et à des acteurs dominants étrangers, l'effectivité du droit des réseaux sociaux et des plateformes commande qu'il soit instauré au niveau le plus large possible. Mais, devant une régulation internationale inexistante voire inatteignable et face à la nécessité pour la France et l'Union européenne (UE) de défendre des valeurs et un marché communs, le droit européen s'est finalement imposé comme le niveau pertinent d'encadrement. Cette tendance s'est confortée au fil des années, au point que les directives sont désormais remplacées par des règlements, poursuivant l'objectif d'un droit exhaustif et efficace. Conformément à la logique de la subsidiarité, les États membres conservent la maîtrise des champs qui nécessitent une approche spécifique (comme l'appréciation de ce qu'est un contenu haineux) mais le droit des réseaux sociaux est dorénavant construit, dans sa majeure partie, par l'UE.

Le droit des réseaux s'est construit **en trois mouvements** qui sont encore à l'œuvre et s'influencent réciproquement : le premier, qui a vu naître un droit spécifique à l'invention technique du numérique (le droit du numérique) ; le deuxième, duquel a émergé un droit spécifique aux nouvelles formes d'intermédiation des rapports économiques (le droit des plateformes) ; le troisième, qui transforme en profondeur les droits traditionnels à l'aune des réseaux sociaux et permet d'assurer une « couverture juridique » globale et cohérente des individus et de la société. Ces processus pluriels révèlent un droit multi-face qui est mis en œuvre par plusieurs régulateurs. Il est à souligner qu'après une période exempte de toute réglementation particulière laissant libre cours à l'innovation et au développement du secteur, les premiers textes qui interviennent pour réglementer les différentes composantes du secteur numérique (données personnelles, infrastructures, commerce électronique) le font moins pour en limiter les abus que pour en faciliter l'épanouissement. Ce n'est que récemment, notamment suite à certains scandales et crises, que les pouvoirs publics se sont convaincus de la nécessité d'une régulation protectrice des intérêts communs et particuliers des individus et plus adaptée aux défis particuliers posés par les réseaux sociaux.

1.2.1. Du « *no man's land* » à la régulation fragmentée des réseaux sociaux

Internet a longtemps bénéficié d'une forme de *no man's land* juridique : lorsque les réseaux sociaux sont apparus, au début des années 2000, le paysage juridique était relativement vierge.

Quand l'utopie d'un internet sans encadrement profite à la concentration du marché

Les réseaux sociaux n'ont pas prospéré dans un environnement vide de droit. Ils sont au contraire apparus dans des sociétés où le numérique avait déjà commencé à transformer les différentes branches du droit (*cf. infra*). Mais leur propre régulation et celle, antérieure, de l'internet s'est faite tardivement. Longtemps, les pionniers du net ont soutenu avec ferveur **sa liberté absolue**. John Perry Barlow, ancien *hacker*, figure de proue de ce mouvement libertaire, a marqué les esprits par sa déclaration d'indépendance du cyberespace, rédigée le 8 février 1996 prônant une civilisation de l'esprit et un monde sans territoire ni propriété dont le principe unique serait la liberté d'accès et d'expression sans entraves[99]. Le changement de société passe par le réseau des individus connectés sans prise de pouvoir par un organe centralisé.

Cette philosophie semblait d'autant plus attrayante que les **libertés d'expression et de communication** qui fondent les démocraties occidentales sont consacrées par les chartes constitutionnelles et garanties par les cours. En outre, en France à partir de la fin de l'ORTF (office de radiodiffusion-télévision française) est venue l'heure de la libéralisation massive de la radio et de l'audiovisuel[100] et il pouvait paraître à contretemps d'encadrer ces nouveaux modes de communication.

Si la « doctrine Barlow » a trouvé un prolongement dans l'émergence des plateformes collaboratives et la défense des biens communs, elle s'est aussi, pour certains de ses amateurs, parfaitement associée aux valeurs de l'économie libérale, contribuant à l'esprit inclassable de la Silicon Valley mêlant « créativité, technologie et entreprenariat »[101]. Comme le rappelle Dominique Cardon, qui souligne l'ambiguïté des mondes numériques, « *avec une infrastructure de réseaux entre individus, on peut faire de la coopération ou du marché* ». C'est donc surtout pour des raisons économiques que la régulation du marché numérique est intervenue, et encore de manière tardive. Les pouvoirs publics ont en effet longtemps considéré, tant outre Atlantique qu'en Europe, que la régulation, au-delà du seul souci d'assurer le « *level playing field* »[102], nuirait au développement du **marché numérique et à l'innovation technologique**. De fait, ce dernier a connu un développement spectaculaire, au point que les chiffres d'affaires des géants de l'internet rivalisent avec les PIB de certains États. Cependant, au fil des années, l'instauration de règles de droit adaptées au numérique s'est révélée nécessaire car la régulation, en sécurisant un marché, lui offre une assise plus solide pour grandir.

99 Ce texte a été écrit en réaction à la promulgation d'une loi américaine sur les télécommunications qui imposaient les premières contraintes aux opérateurs.

100 En 1981 apparaissent les « radios libres » et en 1984 la première télévision privée avec Canal +.

101 D. Cardon. *op. cit.*

102 Expression anglaise qui fait référence à un terrain de jeu parfaitement plat qui ne favorise ni ne défavorise l'une des équipes en présence.

L'évolution du contexte normatif global : la naissance du droit européen et français de la société de l'information fondé sur des valeurs communes

Internet puis le *web*, en permettant la diffusion illimitée de la connaissance par la communication électronique, a fait basculer les sociétés industrielles en ***sociétés de l'information***. L'information (ou donnée) et la nouvelle économie qu'elle engendre, ont contraint le législateur à inventer de nouveaux droits ou à adapter les principes du droit commun à ce nouveau système. Avant les scandales comme celui de *Cambridge Analytica*, révélé en 2018, qui ont modifié le regard de la communauté internationale sur les entreprises du numérique et notamment des réseaux sociaux (*cf. infra*), il est apparu nécessaire à l'Union européenne d'harmoniser les règles juridiques applicables aux services offerts par les industries du numérique pour faciliter leur libre circulation et adapter les législations sur les télécommunications à l'apparition d'internet.

Compte tenu des **enjeux planétaires soulevés** par le numérique et faute qu'une régulation internationale soit sérieusement envisageable, les États membres de l'Union européenne l'ont rapidement regardée comme le niveau le plus pertinent de régulation. Il faut relever que, s'agissant de la protection des données personnelles et de l'encadrement des plateformes, le droit français et les autorités françaises ont joué un rôle moteur. Ce sont **les droits des données personnelles, du commerce électronique et du réseau internet** institués par le législateur national et européen, qui **ont constitué les premières briques du droit du numérique**, briques qui intéressent directement les réseaux sociaux[103].

Les droits fondamentaux, socle du droit du numérique

L'édifice qui va peu à peu émerger a pour **fondation commune** plusieurs principes fondamentaux[104] qu'il convient de concilier, sachant que le numérique est avant tout une avancée technologique venant se greffer sur un édifice de droits et libertés institués bien auparavant.

Il s'agit notamment de :

- La **liberté d'entreprendre** et la **liberté du commerce et de l'industrie**[105] qui trouve un champ de réalisation en droit européen à travers la **libre circulation** des personnes et des marchandises ainsi que la liberté d'établissement[106] : comme on le sait, le haut niveau de protection dont bénéficie cette liberté implique qu'elle ne puisse être limitée que par le législateur lui-même et de manière proportionnée aux objectifs qu'il poursuit[107] ;

103 F. Pellegrini, S. Canevet, *Le droit du numérique : une histoire à préserver,* HAL Open sciences. 00741198.

104 X. Bioy, « Droits fondamentaux et libertés publiques », *Lextenso*, octobre 2020. .

105 Fondée sur l'art. 4 de la DDHC, et issue du décret d'Allarde des 2 et 17 mars 1791 et de la loi le Chapelier de 14 et 17 juin 1791, CC n° 81-132 DC du 16 janvier 1982.

106 V. notamment l'art. 16 de la Charte de l'UE ; CJUE, 22 avril 1999, *Kernkraftwerke Lippe-Ems c/ Commission,* n° C-161/97 ; CJUE, 14 mai 1974, *J. Nold, Kohlen- und Baustoffgroßhandlung c/ Commission des Communautés européennes*, n° 4-73.

107 CC, n° 2013-686 DC du 23 janvier 2014, *Loi relative aux modalités de mise en œuvre des conventions conclues entre les organismes d'assurance maladie complémentaire et les professionnels, établissements et services de santé*, cons. 11 ; V. aussi la décision CC n° 2000-439 DC du 16 janvier 2001

- La **liberté d'expression**, qui a pour corollaire la liberté de penser, est garantie par de très nombreux textes : les articles 10 et 11 de la Déclaration des droits de l'homme et du citoyen de 1789, l'article 10 de la convention européenne de sauvegarde des droits de l'homme et les articles 10 et 11 de la Charte des droits fondamentaux de l'Union européenne. De nombreuses jurisprudences en font application. L'ensemble des juridictions suprêmes ont reconnu, dans des décisions de principe, le rôle éminent d'internet dans la liberté d'expression[108].
- La **liberté de communication**, qui comporte deux volets : **la libre communication des opinions** et **le libre accès aux services de communication en ligne**, garantis par le Conseil constitutionnel depuis la décision du 10 juin 2009. Ce principe a été peu après renforcé par celui d'un internet « ouvert », consacré par la loi pour une République numérique du 7 octobre 2016, principe confié à la surveillance de l'Arcep. L'Europe reconnaît aussi directement un tel droit d'accès à internet, ou de « neutralité du net », notamment à travers le Règlement UE 2015/2120 du 25 novembre 2015[109] dont le but était d'assurer l'égal accès de tous les citoyens de l'Union européenne à internet.
- La **protection de la vie privée**, garantie par l'article 8 de la CESDH[110] et reconnue comme ayant valeur constitutionnelle par le Conseil constitutionnel qui la rattache à l'article 2 de la DDHC depuis la décision n° 99-416 DC du 23 juillet 1999[111]. Les articles 7, relatif à la protection de la vie privée, et 8, relatif à la protection des données personnelles, de la Charte des droits fondamentaux de l'Union européenne, sont également applicables aux contenus en ligne, notamment comme tempéraments de la liberté d'expression et d'information sur internet (par exemple avec la récente décision CJUE, 24 septembre 2019, C-136/17 élargissant le droit au déréférencement sur internet[112]).

Loi relative à l'archéologie préventive pour un exemple du contrôle exercé par le Conseil constitutionnel.

108 Not., CJUE, 8 septembre 2016, *GS Media BV c/ Sanoma Media Netherlands BV e.a,* C-160/15 ; CC, décision DC n° 2009-580 DC du 10 juin 2009 CEDH, gr. ch., 16 juin 2015, *Delfi AS c/ Estonie*, n° 64569/09;

109 Règlement (UE) 2015/2120 du Parlement européen et du Conseil du 25 novembre 2015 établissant des mesures relatives à l'accès à un internet ouvert et modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques et le règlement (UE) no 531/2012 concernant l'itinérance sur les réseaux publics de communications mobiles à l'intérieur de l'Union. Ce texte a donné lieu à une interprétation récente de la part de la CJUE saisie de plusieurs questions préjudicielles, v. CJUE, 15 septembre 2020, *Telenor*, n° C-807/18 et C-39/19 (voir CJUE communiqué de presse n° 106/20 du 15 septembre 2020).

110 La CEDH a eu l'occasion de renforcer cette protection par sa jurisprudence, notamment à raison des risques plus forts encourus pour le droit à la vie privée sur internet (CEDH, 5e Sect., 5 mai 2011, *Comité de rédaction de Pravoye delo et Shtekel c. Ukraine*, n° 33014/05). V. pour des exemples d'application à internet et de conciliation du droit à la vie privée et de la liberté d'expression, CEDH, gr. ch., 7 février 2012, *Axel Springer AG c. Allemagne*, n° 39954/08, CEDH, *Arnarson c. Islande*, du 13 juin 2017, n° 58781/13, CEDH, 16 décembre 2010, *Aleksey Ovchinnikov c/ Russie,* n° 24061/04. Cette protection européenne est renforcée par le Conseil de l'Europe notamment par la Convention 108 pour la protection des individus au regard du traitement automatisé des données à caractère personnel de 1981.

111 V. aussi la décision n° 2012-652 DC du 22 mars 2012 qui affirme que, la liberté proclamée par l'article 2 de la DDHC impliquant le droit au respect de la vie privée, la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel doivent être justifiés par un motif d'intérêt général et mis en œuvre de manière adéquate et proportionnée à cet objectif.

112 La CJUE a ainsi pu contrôler la conformité de la directive 2006/24 CE du 15 mars 2006, relative à la conservation de données par les fournisseurs de communications électroniques, à l'art. 8 de la Charte, car cette directive comportait une ingérence grave et « *susceptible de générer dans l'esprit des personnes concernées (…) le sentiment que leur vie privée fait l'objet d'une surveillance constante* » (v. CJUE 8 avril

- La **sauvegarde de l'ordre public** qui est un objectif à valeur constitutionnelle dont la protection peut justifier des restrictions sur internet[113]. Parallèlement, la « défense de l'ordre » fait partie des motifs légitimes de restriction de la liberté d'expression sur internet prévus par le §2 de la CESDH[114].

La question peut se poser de savoir si le **principe de pluralisme des opinions**, objectif à valeur constitutionnel[115] consacré lors de la révision constitutionnelle du 23 juillet 2008 à l'article 4 de la Constitution[116], habituellement mobilisé à l'égard des médias et de la vie politique, pourrait être applicable aux réseaux sociaux. Par ailleurs, des principes comme la sauvegarde de la dignité humaine, le droit à la protection de la santé et l'intérêt supérieur de l'enfant pourraient être mis en balance avec la liberté d'expression pour apprécier la constitutionnalité de certaines suppressions de contenus.

Souvent, le législateur se retrouve sur une ligne de crête. Il doit en effet concilier la nécessité de permettre aux individus d'accéder à tous les moyens de communication à disposition, celle de communiquer librement avec autrui dans le respect des limites fixées par la loi, notamment pénale, celle de voir leur liberté de penser garantie et leur vie privée protégée, sans interdire aux entreprises qui fournissent les infrastructures et les services de communication de prospérer au sein d'une économie de marché. Plusieurs décisions ont ainsi été rendues par le Conseil constitutionnel qui censuraient des dispositions législatives[117]. La CEDH est, elle aussi, très attentive aux ingérences susceptibles d'être apportées par les États à la liberté d'expression, notamment en y appliquant un triple test de légalité, de légitimité et de nécessité dans une société démocratique de l'ingérence étatique[118]. La CJUE opère de la même façon[119].

2014, *Digital Rights Ireland et Seitlinger et a.*, n° C-293/12 et C-594-12, pt. 37). En matière de droit à l'oubli sur internet, v. la décision de référence CJUE, gr. ch., 13 mai 2014, *Google Spain SL, Google Inc. c. Agencia Española de protección de datos (AEPD), M. Costeja Gonzalez*, n° C-131/12, dans laquelle la CJUE lie le droit à la vie privée de l'art. 7 à celui à la protection des données personnelles.

113 En matière de consultations de contenus pédopornographiques, le Conseil constitutionnel a estimé, à l'occasion de sa décision n° 2011-625 DC du 10 mars 2011, *Loi d'orientation et de programmation pour la performance de la sécurité intérieure* que, compte tenu des garanties encadrant le dispositif déféré, les dispositions conférant à l'autorité administrative le pouvoir de restreindre, pour la protection des utilisateurs d'internet, l'accès à des services diffusant des images de pornographie infantile, était conforme à la Constitution.

114 V. CEDH, 14 novembre 2006, n° 2842/02, *Medya Fm Reha Radyo Ve İletişim Hizmetleri A. Ş. C. Turquie*. CEDH, 21 janv. 1999, n° 25716/94, *Janowski c. Pologne*. L'art. 11 de la charte européenne des droits fondamentaux devant être interprétée suivant l'article 10 de la CEDH, s'y applique aussi le contrôle du motif légitime de défense de l'ordre.

115 CC, décision n° 93-333 DC, 21 janvier 1994.

116 Art. 4 de la Constitution : « *La loi garantit les expressions pluralistes des opinions et la participation équitable des partis et groupements politiques à la vie démocratique de la Nation* ».

117 CC, 10 février 2017, *M. David P. [Délit de consultation habituelle de site internet terroristes]*, n° 2016-611 QPC, pt. 15, suivant avis du Conseil d'État du 5 avril 2012, ou plus récemment, CC, n° 2020-801 DC du 18 juin 2020 *loi visant à lutter contre les contenus haineux sur internet*.

118 Les motifs légitimes d'ingérence sont limitativement listés au §2 de l'art. 10 de la CEDH, et doivent être considérés selon le principe de proportionnalité de l'ingérence au but légitime poursuivi.

119 Par ex., n'admettant pas la possibilité d'une obligation de filtrage généralisée des contenus (CJUE, 24 novembre 2011, *Scarlet Extended*, aff. C-70/10), ou arbitrant les conflits entre libre circulation des biens et liberté d'expression (CJCE, 12 juin 2003, *Eugen Schmidberger*, aff. C-112/00).

Sur ces fondations, le droit du numérique s'est construit brique par brique.

Première brique : La protection des données personnelles et de la vie privée dans le secteur des communications électroniques

La première brique du droit du numérique est celle **des données personnelles**[120] d'abord posée par la France dans la visionnaire loi informatique et libertés (LIL) de 1978 puis par l'Union européenne en 2016, au sein du règlement général sur la protection des données dit RGPD (règlement 2016/679 du 27 avril 2016 entré en vigueur le 25 mai 2018). La **société de l'information**, comme son nom l'indique, est fondée sur *l'information* et sur la notion clé de *donnée*. Celle-ci devient une sorte de nouvel étalon-or. Le législateur français a pris très tôt conscience de la nécessité de **protéger la vie privée** face aux conséquences du développement des techniques de diffusions et croisements larges de données personnelles, tout en assurant la libre circulation des données sans oublier la sécurisation du marché pour permettre son plein épanouissement.

L'entrée dans le droit du numérique se fait donc par la porte des données personnelles avec l'adoption de la *loi relative à l'informatique, aux fichiers et aux libertés* de 1978 qui encadre les traitements automatisés des « informations nominatives », par la suite dénommées « données personnelles »[121] et met en place une autorité administrative indépendante, **la Commission nationale informatique et libertés**[122] **(CNIL)** chargée de sa mise en œuvre. Si au départ, la LIL est surtout pensée pour protéger les citoyens des fichiers informatiques (suite au scandale SAFARI), elle s'avère rapidement particulièrement adaptée à l'émergence d'internet et ses adaptations vont progressivement en faire un des piliers de ce nouveau droit. Son article 1er dispose que « *L'informatique doit être au service de chaque citoyen (...) Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques* ». Ce droit a ceci de particulier qu'il ne consacre pas pour les individus un droit réel sur un bien (une propriété) mais qu'il s'apparente plus à un droit subjectif attaché à un élément de la personnalité, une information qui compose en partie la « *sphère d'intimité de la personne* »[123]. La donnée personnelle n'a pas de valeur intrinsèque et n'a pas de propriétaire en tant que tel. Ainsi, elle ne peut être vendue à un tiers qui en userait comme bon lui semble. En revanche, son titulaire bénéficie **d'un droit d'usage** qui lui permet de décider et de contrôler les utilisations qui en sont faites. C'est pour cela que le **consentement** de l'individu est au cœur de ce droit. Cette particularité le rend complexe et atypique. De fait, il génèrera de délicates questions, notamment dans le domaine des réseaux sociaux (*cf. infra*).

120 Les données personnelles recouvrent toute information se rapportant à une personne identifiée ou identifiable.

121 Directives 95/46 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 et directive 2002/58 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques)

122 Elle crée la Commission nationale informatique et libertés (CNIL), impose une obligation de déclarer auprès de cette instance des fichiers contenant des données personnelles, interdit la collecte des données à caractère sensible, impose aussi le principe de collecte loyale des données, oblige d'assurer la sécurité des données collectées, d'informer les individus concernés de la collecte de leurs données et enfin le droit à l'accès, la modification et la suppression de ces données.

123 Carbonnier, *Droit des personnes*, PUF.

Le droit des données personnelles a largement influencé celui de la **protection de la vie privée dans le secteur des communications électroniques**, qui est adossé au droit des télécommunications. Ainsi la *directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques* dite ***e-privacy***, souvent abordée aux côtés du RGPD, fait partie du « Paquet Télécom »[124] (*cf. infra*). Modifiée par *la directive 2009/136/CE*, elle contraint les États à garantir la **confidentialité des communications** effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles au public, ainsi que la confidentialité des données relatives au trafic y afférentes. Elle règlemente notamment l'utilisation des **traceurs** (*cookies*) et pose le principe d'un consentement préalable de l'utilisateur, sauf si ces actions sont strictement nécessaires à la fourniture d'un service de communication en ligne expressément demandé par l'utilisateur ou ont pour finalité exclusive de permettre ou faciliter une communication par voie électronique.

Les réseaux sociaux qui fournissent des modules de partage sont concernés par ses dispositions. C'est au responsable de traitement qui dépose ses traceurs soumis à consentement de veiller à recueillir le consentement de l'utilisateur. Celui-ci doit être libre, spécifique, univoque et éclairé (*cf. infra*).

Dans le droit fil de ces législations, l'UE a adoptée la *directive 2016/680 du 27 avril 2016* « *Police-Justice* » qui établit les règles de protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités **compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution des sanctions pénales** : pour qu'un traitement de données rentre dans le champ de la directive, il doit correspondre à l'une des finalités de l'article 1er et être mis en œuvre par une autorité compétente.

Deuxième brique : le droit des services de la société de l'information (ou droit du commerce électronique)

La deuxième brique est celle du **droit des échanges commerciaux et contractuels en ligne**, qui s'intéresse tant à l'activité commerciale sur le net qu'à la responsabilité des opérateurs quant aux contenus diffusés ou hébergés. Ce droit des services de la société de l'information, c'est-à-dire des « *services réalisés à distance par voie électronique, contre rémunération et à la demande du destinataire* »[125], initié par l'Union européenne, a ensuite connu, sous l'effet de « l'ubérisation » de l'économie, une importante évolution jusqu'à sa mue en **droit des plateformes** (*cf. infra*).

Le premier texte emblématique est la directive 2000/31 CE du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment

124 La directive *e-privacy* a abrogé la directive 95/46/CE puis la directive 97/66/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications, pour tenir compte de l'apparition des nouveaux services de communication électroniques.

125 Définition issue de la directive 98/34 CE du 22 juin 10998 prévoyant une procédure d'information dans le domaine des normes et réglementations techniques relatives aux services de la société de l'information. (art. 1er) modifiée par la directive 98/48.

du commerce électronique, dans le marché intérieur dite *directive e-commerce*, dont la vocation est de faciliter l'épanouissement du commerce électronique au sein du marché intérieur, dont l'idée première est de favoriser l'innovation et l'épanouissement de la révolution numérique (*cf.* son troisième considérant : « *Le droit communautaire et les caractéristiques de l'ordre juridique communautaire constituent un atout essentiel pour que les citoyens et les opérateurs européens puissent bénéficier pleinement, sans considération de frontières, des possibilités offertes par le commerce électronique.* »). La directive concerne quasiment **toutes les activités économiques en ligne** y compris celles qui consistent à transmettre des informations par le biais d'un réseau de communication, à fournir un accès à un réseau de communication ou à héberger des informations fournies par un destinataire de service. Si les services de radiodiffusion et de télévision n'en font pas partie car ils ne sont pas fournis sur demande individuelle, les services transmis de point à point comme la vidéo à la demande sont inclus[126]. Elle invente la catégorie juridique des « ***prestataires intermédiaires*** », parmi lesquels figurent les hébergeurs, et pose le principe de leur **absence de responsabilité** du fait des contenus stockés à la demande d'un destinataire du service sauf à avoir connaissance de l'activité ou du contenu illicite et à ne pas agir rapidement pour y mettre fin. Elle interdit même aux États membres d'imposer aux prestataires une obligation générale de surveillance ou de rechercher activement des activités illicites.

En France, *la loi pour la confiance dans l'économie numérique* (LCEN) du 21 juin 2004[127] qui transpose la directive e-commerce cherche à renforcer la confiance dans le commerce électronique et la lutte contre les publicités indésirables en sécurisant davantage les échanges et en amplifiant les moyens de lutte contre la cybercriminalité (les hébergeurs se voyant ainsi imposer une obligation de conservation des données). Elle pose **le principe de la liberté de communication en ligne** et dispose à son article 1er : « (…) *la communication au public par voie électronique est libre. L'exercice de cette liberté ne peut être limité que dans la mesure requise, d'une part, par le respect de la dignité de la personne humaine, de la liberté et de la propriété d'autrui, du caractère pluraliste de l'expression des courants de pensée et d'opinion et, d'autre part, par la sauvegarde de l'ordre public, par les besoins de la défense nationale, par les exigences de service public, par les contraintes techniques inhérentes aux moyens de communication, ainsi que par la nécessité, pour les services audiovisuels, de développer la production audiovisuelle.* ». Cette loi définit et distingue trois catégories juridiques qui sont la **communication au public par voie électronique, la communication au public en ligne et le courrier électronique**[128].

126 Considérant 18 de la directive *e-commerce*.

127 Loi n° 2004-575 pour la confiance dans l'économie numérique.

128 Art. 1er de la LCEN : « *On entend par communication au public par voie électronique toute mise à disposition du public ou de catégories de public, par un procédé de communication électronique, de signes, de signaux, d'écrits, d'images, de sons ou de messages de toute nature qui n'ont pas le caractère d'une correspondance privée. /On entend par communication au public en ligne toute transmission, sur demande individuelle, de données numériques n'ayant pas un caractère de correspondance privée, par un procédé de communication électronique permettant un échange réciproque d'informations entre l'émetteur et le récepteur. / On entend par courrier électronique tout message, sous forme de texte, de voix, de son ou d'image, envoyé par un réseau public de communication, stocké sur un serveur du réseau ou dans l'équipement terminal du destinataire, jusqu'à ce que ce dernier le récupère.* »

Suite à des décisions de justice jugeant des plateformes responsables à raison de la publication d'images interdites alors que ces dernières avaient été postées par un utilisateur, le législateur français, approfondissant la ligne établie par la directive de 2000, établit la distinction cardinale entre **l'hébergeur et l'éditeur** du service de communication au public en ligne. L'éditeur est la personne qui détermine les contenus mis à la disposition du public sur le service qu'il a créé ou dont il a la charge. Il a une obligation de contrôle *a priori* des contenus et est donc responsable de tous les contenus publiés sur la plateforme. Il dispose également d'une obligation de vigilance dans la modération en amont (avant la publication) et en aval (après la publication). L'hébergeur, lui, ne voit sa responsabilité engagée qu'*a posteriori* et de manière conditionnelle après signalement du client. Il a une obligation de mettre en place des dispositifs permettant aux internautes de signaler des contenus illicites et d'informer les autorités publiques de toutes activités illicites signalées qu'exerceraient les destinataires de leurs services. Il se distingue du fournisseur d'accès en ce qu'il fournit une prestation durable d'hébergement et se distingue de l'éditeur en ce qu'il rend seulement accessible les contenus mis en ligne sans avoir à leur égard de rôle actif.

Le Conseil Constitutionnel, saisi de la constitutionnalité de la LCEN, a, par sa décision n° 2004-496 DC du 10 juin 2004, apporté une réserve d'interprétation qui restreint encore la responsabilité d'un hébergeur en précisant qu'il ne pourra pas voir sa responsabilité engagée s'il « *n'a pas retiré une information dénoncée comme **illicite** par un tiers si celle-ci ne présente pas **manifestement** un tel caractère ou si son retrait n'a pas été ordonné par un juge* ». Cette distinction, précisée par la suite par la jurisprudence[129] devient, pendant des années, « ***la colonne vertébrale du droit du numérique*** »[130]. Elle se montre cependant peu opérationnelle, le nombre de signalements étant très faible par rapport à la masse des informations échangées et conduisant à une quasi-immunité des hébergeurs. En outre, compte tenu de l'évolution de l'activité numérique et de « l'*ubérisation* de la société », la distinction s'avère de moins en moins opérante, notamment pour les réseaux sociaux. En effet, ces derniers, s'ils n'éditent pas les contenus qui sont apportés par des tiers, jouent, notamment à travers l'usage d'algorithmes, un **rôle actif dans le référencement et la présentation des contenus** aux utilisateurs de leurs plateformes et disposent d'une ligne éditoriale. Le Conseil d'État, dans le cadre de son rapport sur le numérique et les droits fondamentaux, avait d'ailleurs, dès 2016, proposé de supprimer ce régime juridique binaire opposant les éditeurs et les hébergeurs, pour que soit instauré un statut intermédiaire de «plateforme». L'idée sous-jacente est alors de

129 Cette lecture sera complétée par l'arrêt de la CJUE du 23 mars 2010, aff. C-236/08 à C-238/08, *Société Google contre Société Louis Vuitton Malletier* qui rappelle que l'activité d'hébergement a un « *caractère purement technique, automatique et passif* », « *le prestataire n'a pas la connaissance ni le contrôle des informations transmises ou stockées* ». V. aussi CCass, Civ. 1, 17 février 2011, *n° 09-67896* et CJUE, gr. ch., 22 juin 2021, *Peterson c/ YouTube* et *Elsevier c/ Cyando*, *aff. C-682/18 et C-683/18*) qui juge qu'un exploitant de plateforme ne peut être reconnu comme simple hébergeur lorsqu'il met à disposition de façon illicite des œuvres protégées alors qu'il en a expressément connaissance. Sur le fondement de la directive 2019/790 relative au droit d'auteur, la décision va encore plus loin en jugeant qu'un hébergeur peut voir sa responsabilité engagée pour la diffusion de contenus protégés par le droit d'auteur lorsqu'il « *abstient de mettre en œuvre les mesures techniques appropriées qu'il est permis d'attendre d'un opérateur normalement diligent dans sa situation pour contrer de manière crédible et efficace des violations du droit d'auteur sur cette plateforme* » (cst 102).

130 D. Cardon, *Culture numérique*, *op. cit.*

renforcer la responsabilité civile et pénale des services en ligne qui ne sont pas de simples hébergeurs se limitant à mettre à disposition un serveur et de la bande passante, ni des éditeurs choisissant voire produisant les contenus qu'ils diffusent sur internet. Il explique que « *les plateformes doivent être tenues à une obligation de loyauté, tant à l'égard des utilisateurs finaux que des tiers* » et propose que ce principe guide l'action du juge qui « *pourra (en) découvrir toutes les implications au fil des litiges* ». Cependant, reconnaissant que la France ne peut pas agir seule sur ce terrain, compte tenu des prescriptions de la directive de 2000 sur le commerce électronique, il suggère de porter le sujet au niveau de l'Union européenne.

Troisième brique : le droit des réseaux et services de communication électronique

La régulation des réseaux et des infrastructures du net est une condition du bon fonctionnement de ce dernier. Plusieurs textes ont dû notamment encadrer l'ouverture du marché des télécommunications à la concurrence ainsi que l'apparition des réseaux internet et mettre en œuvre les politiques visant à assurer une ouverture à tous (service universel à haut débit).

En 2002, par l'adoption de cinq directives, le « paquet Télécom »[131], transposé en France par la loi du 9 juillet 2004, fixe un cadre réglementaire commun aux **réseaux et services de communication électronique** (audiovisuel et télécommunications) même s'ils demeurent soumis à des régimes distincts[132]. Les autorisations concernant les opérateurs sont remplacées par des déclarations, un cadre relatif au choix des opérateurs chargés du service universel est défini et un mécanisme nouveau de régulation des opérateurs historiques est mis en place. Ce cadre, révisé par les directives 2009/140/CE et 2009/136/CE, consacre notamment le principe de **la neutralité du net**, qui consiste à garantir l'égalité de traitement et d'acheminement de tous les flux d'information sur internet quel que soit leur émetteur ou leur destinataire, pose un **droit à la portabilité du numéro fixe et mobile**.

L'ordonnance du 24 août 2011 transposant ces dernières directives a aussi notamment renforcé les obligations des fournisseurs de services de communications électroniques et l'information ainsi que l'exigence de consentement précis et éclairé des abonnés ou utilisateurs d'un service de communication électronique en cas d'utilisation de cookies[133]. Pour mieux lutter contre les atteintes à la vie privée, préserver le **secret des correspondances** et la sécurité des systèmes d'information dans le domaine des communications électroniques, est instaurée pour les fournisseurs une **obligation de notification** sans délai à la CNIL, pénalement sanctionnée, en cas de perte de données personnelles, notamment en cas de faille

131 Directive 2002/21/CE « cadre » ; directive 2002/19/CE « accès » ; directive 2002/20/CE « autorisation » ; directive 2002/22/CE « service universel » ; directive 2002/58/CE « vie privée ».

132 Mise en place d'un mécanisme entièrement nouveau pour la régulation des opérateurs historiques, conforme au droit de la concurrence ; suppression des autorisations délivrées aux opérateurs pour les remplacer par de simples déclarations ; encadrement des conditions dans lesquelles les États membres désignent les opérateurs chargés du service universel et renforcement considérablement des dispositions protectrices déjà prévues par les textes européens.

133 Ne sont pas concernés les cookies qui ont « *pour finalité exclusive de permettre ou faciliter la communication par voie électronique* » ou « *qui sont strictement nécessaires à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur* ».

de sécurité ayant entraîné de manière accidentelle, l'atteinte, la perte ou l'accès non autorisé aux données personnelles des abonnés ou utilisateurs[134].

La loi du 7 octobre 2016 *pour une République numérique* renforce le rôle de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (Arcep) en lui confiant la protection de la **neutralité du net** assortie d'un pouvoir d'enquête et de sanction afin de la rendre effective[135]. Cette loi intervient à la suite de l'adoption du *règlement européen sur l'Internet ouvert et des lignes directrices fournies par l'ORECE* (Organe des régulateurs européens des communications électroniques).

En 2018, les textes européens sont refondus dans **un code des communications électroniques européen** (directive (UE) 2018/1972) dont l'objectif, au-delà d'instaurer un cadre harmonisé au sein de l'Union européenne, est d'accompagner les investissements dans **les réseaux de nouvelle génération** (fibre, 5G) et de réguler les nouveaux acteurs tels que les fournisseurs de services OTT (*Over the top* ou « services par contournement de réseaux »). Ces derniers sont désormais inclus dans la définition des opérateurs de communications électroniques, ce qui conduit à un alignement de leurs droits et obligations. En conséquence, les fournisseurs de services de messagerie instantanée, courriels, appels téléphoniques sur internet et messages personnels émis par le biais de réseaux sociaux ont désormais de nouvelles obligations, notamment en matière d'information et de protection des utilisateurs finaux, de sécurité publique et de défense nationale, d'interopérabilité ou encore de financement du service universel. Ces nouveaux acteurs doivent donc, à l'instar des fournisseurs de télécommunications traditionnels, se conformer aux obligations de confidentialité des données électroniques établies par la directive et proposer à leurs utilisateurs un certain degré de protection et de transparence. En outre, ils sont soumis aux obligations qui découlent de l'extension par le code de l'application de la *directive e-privacy*, laquelle devrait prochainement être remplacée par le *règlement* « *vie privée et communications électroniques* ». Ces dispositions ont été transposées, pour l'essentiel, par l'ordonnance n° 2021-650 du 26 mai 2021.

Malgré ces premières briques, le sentiment général partagé a longtemps été celui d'une insuffisante régulation d'internet, dans la mesure où aucune règle réellement contraignante ne concernait les **contenus** échangés sur la toile et notamment les réseaux sociaux. Plusieurs événements vont bousculer cette situation et engendrer des réactions des plateformes elles-mêmes et des gouvernants.

134 Cette nouvelle obligation implique pour les fournisseurs une obligation de tenir un registre récapitulant les violations de données personnelles et les solutions mises en place pour y remédier. Ce registre doit être mis à la disposition de la CNIL (art. 34 bis III de la Loi Informatique et Libertés). L'art. 34 *bis* prévoit également une obligation de notification aux personnes physiques concernées lorsque cette violation « *peut porter atteinte aux données à caractère personnel ou à la vie privée d'un abonné ou d'une autre personne physique* ». Néanmoins, les fournisseurs peuvent s'exonérer de cette notification à l'intéressé lorsque la CNIL constate que « *des mesures de protection appropriées ont été mises en œuvre* ». Cette obligation de notification peut être lourde de conséquences pour les fournisseurs, notamment en termes de réputation. Les fournisseurs devront ainsi prendre les mesures adéquates en interne (notamment audits internes) pour renforcer la sécurité des données et adopter des mesures de protection « *appropriées* » pour rendre les données « *incompréhensibles à toute personne non autorisée à y avoir accès* ».

135 J.-Y. Ollier, « De la neutralité des réseaux à celle des prestataires de service de partage de données », *Enjeux numériques,* juin 2022.

La prise de conscience et les débuts de l'auto-régulation

En janvier 2000, Lawrence Lessig, professeur de droit à Harvard, publie un texte reconnu aujourd'hui comme fondateur (« *Code is Law - On liberty in cyberspace* »[136]) dans lequel il affirmait l'urgente nécessité de réguler une technologie numérique – le code d'internet – qui tendait déjà à devenir une forme de norme. Il dénonçait son caractère incontrôlable et soulignait que cette technique pouvait être mise au service des meilleures intentions comme des pires, précisant que, dans une démocratie, les citoyens devaient décider collectivement de la façon dont le « code » devait garantir le respect des valeurs fondamentales. Malgré son retentissement, cet article n'a pas été suivi d'effet concret dans les années qui ont suivi.

Dans cet espace laissé presque vide – en France, la loi du 29 juillet 1881 qui interdit les diffamations, injures et discours de haine est demeurée applicable – les réseaux sociaux ont été accusés de laisser se propager des contenus haineux et illicites voire d'avoir laissé leurs algorithmes en accélérer la diffusion (« viralité ») compte tenu de leur paramétrage pour capter toujours plus longtemps l'attention des utilisateurs. D'un autre côté, ils ont été aussi accusés de pratiquer une censure excessive de nombreux contenus (*cf.* la censure du tableau de Courbet, *L'origine du monde*) et de porter ainsi atteinte à la liberté d'expression. Certains n'ont pas manqué de faire valoir en réponse que les réseaux sociaux constituaient le bouc-émissaire idéal pour éviter de mettre chacun face à ses responsabilités.

Pour répondre à ces critiques virulentes et exercer correctement la police interne de ces espaces devenus démesurés, les réseaux sociaux ont, pour la plupart, décidé de durcir leurs règles de **police interne**. Ils ont ainsi mis en place des **modérateurs humains** et/ou des techniques de modération par algorithmes chargés de supprimer ou rendre peu visibles les contenus illicites ou contraires aux CGU. Ces clauses se sont d'ailleurs enrichies d'informations sur les règles de modération. Selon la nature du réseau social, cette modération s'exerce en sous-traitance, par les salariés eux-mêmes ou par les utilisateurs. C'est ainsi que Wikipédia possède des *patrouilleurs* chargés de surfer sur l'océan de ses pages pour identifier les ajouts sans source ou polémiques ou ne répondant pas aux conditions de l'encyclopédie. Mais ces règles de régulation internes sont aussi vivement critiquées.

L'effet des crises

Comme toute crise ou scandale [137], l'affaire *Cambridge Analytica* a permis une prise de conscience très large des risques liés aux réseaux sociaux. Outre les questions de sécurité de conservation des données, elle a montré aux utilisateurs la valeur inestimable des données personnelles et combien celles-ci peuvent être utilisées à des fins différentes de celles qu'ils auraient souhaitées. Plus encore, elle a souligné combien la manipulation de ces données peut même peser directement dans le jeu politique et pervertir la démocratie. D'autres scandales comme la captation en direct de l'attentat de Christchurch (*cf. infra*), l'assassinat de Samuel Paty[138]

136 L.Lessig, Harvard Magazine, janvier 2000.

137 *Les états d'urgence, la démocratie sous contraintes*, étude du Conseil d'État 2021, p. 83 et s.

138 Après l'assassinat de Samuel Paty, Facebook et Twitter ont été accusés d'avoir laissé prospérer des messages haineux en ligne contre l'enseignant. L'attentat a été revendiqué sur Twitter.

ainsi que les révélations en 2021 d'une ancienne employée de Facebook, Frances Haugen, ont mis en lumière les effets nocifs de l'économie de l'attention.

L'affaire *Cambridge Analytica* (2016-2018)

En mars 2018, une enquête menée par *The Guardian* suite au signalement d'un lanceur d'alerte canadien accuse la société britannique Cambridge Analytica[139], implantée aux États-Unis et spécialisée dans le conseil en communication et l'analyse de données, d'avoir profité du laxisme sécuritaire de Facebook pour récupérer les données personnelles de 87 millions de comptes, cette collecte ayant permis de soutenir massivement la campagne électorale de Donald Trump en 2016 en ciblant la campagne auprès des électeurs indécis. Selon cet article, Facebook se serait bien rendu compte qu'une opération massive de collecte des données avait lieu mais n'aurait pas prévenu ses utilisateurs ni banni la société Cambridge Analytica de son réseau. Les travaux d'une commission parlementaire britannique démontrent que les données ont été collectées par le biais d'un questionnaire de personnalité en ligne prétendument à des fins de recherche académique. Accessible depuis Facebook, ce test a permis de dresser, grâce aux données récoltées, le "profil électeur" des répondants mais aussi de l'ensemble de leurs connexions Facebook ce qui était autorisé à l'époque par les CGU de la plateforme. Le scandale est donc lié à la manipulation à grande échelle de données personnelles à des fins électorales. Mark Zuckerberg a été sommé de s'expliquer devant le Congrès Américain en avril 2018. Il a accusé Cambridge Analytica de mensonges à l'égard de Facebook tout en reconnaissant une faille de sécurité du côté de son entreprise. Il a, par la même occasion, présenté ses excuses aux utilisateurs lésés. Les mêmes justifications ont été menées devant le Parlement européen en mai 2018 tout en y admettant qu'une meilleure régulation était nécessaire. En 2019, une amende de 5 milliards de dollars a été infligée à Facebook par la *Federal Trade Commision* obligeant la plateforme à mieux protéger la vie privée de ses utilisateurs. Par la suite, en 2020, une action collective contre Facebook pour utilisation abusive des informations de près d'un million d'utilisateurs a été formée en Angleterre et au Pays de Galles.

Enfin la crise du coronavirus, qui s'est accompagnée durant toute la période de l'épidémie d'une très haute fréquentation des réseaux sociaux et d'un foisonnement de fausses informations et de « théories complotistes », a fini de convaincre de la nécessité de mettre en place une réglementation adéquate.

139 La société Cambridge Analytica (CA), entreprise britannique spécialisée dans le conseil en communication et l'analyse de données, a été fondée à Londres en 2013. Son slogan était : "*Data drive all we do*" (les données déterminent tout ce que nous faisons). Spécialisée dans l'analyse de données à grande échelle et le conseil en communication, elle se donne pour mission « *de changer le comportement grâce aux données* » et fonctionne en mélangeant le traitement quantitatif de données, la psychométrie et la psychologie comportementale. V. Le Monde, site internet, 22 mars 2018, « Ce qu'il faut savoir sur Cambridge Analytica, la société au cœur du scandale Facebook ».

1.2.2. L'émergence d'un droit des réseaux sociaux

D'une part, la directive *e-commerce*, dont découle la distinction cardinale entre les **hébergeurs et les éditeurs** et son régime dual de responsabilité, est apparue inadaptée, malgré les tentatives de la Cour de justice de l'Union européenne de préciser ce régime en distinguant le rôle actif ou passif de l'hébergeur[140]. Il a notamment semblé inopportun de maintenir une totale irresponsabilité des hébergeurs qui fournissent des contenus provenant de tiers dont la « viralité » et la masse rendent insuffisant le système de contrôle par le seul prisme du signalement. En outre, la mise en place par les réseaux sociaux de leur propre système de modération a fait craindre l'instauration de véritables censures privées contraires à la liberté d'expression.

D'autre part, à mesure que la puissance des plateformes s'est affirmée, certains instruments traditionnels ont paru insuffisants voire obsolètes et l'idée d'une **régulation spécifique des plateformes** s'est imposée. Force a notamment été de constater que l'asymétrie d'informations entre les acteurs du numérique et leur environnement ainsi que les modifications constantes des fonctionnements internes de ces entreprises (modification des algorithmes, des fonctionnalités, des CGU, etc.) ont mis à l'épreuve les outils classiques de contrôle. Or, les réseaux sociaux, qui recourent à un dispositif technique pour mettre en relation des individus discutant ou échangeant des contenus, constituent bien une catégorie de plateforme. C'est donc naturellement que le changement de paradigme visant à aborder le droit du numérique à travers celui des plateformes s'est traduit dans celui des réseaux sociaux. Au fil des années, sont ainsi apparues des normes régissant les réseaux sociaux *via* le droit des plateformes numériques tandis que, parallèlement, les branches traditionnelles du droit s'adaptaient peu à peu à ce phénomène en s'enrichissant et se renouvelant.

Deux blocs peuvent ainsi être distingués même s'il existe une forte porosité entre eux : le *premier* comportant un ensemble de règles applicables aux plateformes, dont les réseaux sociaux font partie et qui vient d'être considérablement enrichi par l'adoption du *Digital Markets Act* et du *Digital Services Act* ; le *second* composé des nombreuses branches du droit traditionnel bousculées par l'émergence des réseaux sociaux. Si, au départ, le droit des plateformes, essentiellement européen, s'est construit de façon sectorielle, **les derniers textes adoptés ont vocation à constituer un droit commun des plateformes et des marchés numériques**. Le socle des valeurs communes qui en constituent les principes directeurs est resté inchangé.

1.2.2.1. Le droit des réseaux sociaux à travers les droits des plateformes numériques[141]

Si la France a été précurseur dans l'adoption d'un texte instaurant un droit des plateformes visant à protéger le consommateur, **ce champ est désormais largement traité par l'Union européenne** qui, en multipliant le recours à des

140 CJUE, 12 juillet 2011, *aff. C-324/09*.

141 « L'émergence d'un droit des plateformes », dir. X. Delpech, collection Actes, *Dalloz*, 2021.

règlements européens, entend unifier et sécuriser le plus largement possible un marché avant tout international. C'est certainement, en termes de subsidiarité, le niveau le plus adapté.

A. L'émergence d'un droit commun des plateformes

a. Le droit des plateformes régissant les relations entre professionnels et non professionnels (code de la consommation)

La France, par l'adoption de la *loi pour une République numérique du 7 octobre 2016*, qui crée la nouvelle catégorie juridique d'**opérateurs de plateformes en ligne**, s'est montrée innovante en privilégiant une nouvelle approche de la régulation du marché numérique par le prisme de la *plateforme.* L'opérateur de plateforme en ligne, catégorie dans laquelle entre les réseaux sociaux, est désormais défini par l'article L. 111-7 du code de la consommation comme « *toute personne physique ou morale proposant, à titre professionnel, de manière rémunérée ou non, un service de communication au public en ligne reposant sur : 1° Le classement ou le référencement, au moyen d'algorithmes informatiques, de contenus, de biens ou de services proposés ou mis en ligne par des tiers ; 2° Ou la mise en relation de plusieurs parties en vue de la vente d'un bien, de la fourniture d'un service ou de l'échange ou du partage d'un contenu, d'un bien ou d'un service* ». **Les obligations** vis-à-vis du consommateur, quoique non assorties de sanctions dissuasives, sont clarifiées et répertoriées. Cet article ajoute ainsi que tout opérateur de plateforme en ligne « *est tenu de délivrer au consommateur une* ***information loyale, claire et transparente*** *sur : 1° Les conditions générales d'utilisation du service d'intermédiation qu'il propose et sur les modalités de référencement, de classement et de déréférencement des contenus, des biens ou des services auxquels ce service permet d'accéder ; 2° L'existence d'une relation contractuelle, d'un lien capitalistique ou d'une rémunération à son profit, dès lors qu'ils influencent le classement ou le référencement des contenus, des biens ou des services proposés ou mis en ligne ; 3° La qualité de l'annonceur et les droits et obligations des parties en matière civile et fiscale, lorsque des consommateurs sont mis en relation avec des professionnels ou des non-professionnels* ». La loi de 2016 impose aux plateformes d'une certaine taille d'élaborer et diffuser aux consommateurs des bonnes pratiques visant à renforcer leur obligation de clarté, de transparence et de loyauté et permet à l'autorité compétente d'enquêter sur ces pratiques.

*b. Le droit des plateformes régissant les relations entre professionnels (*Plaform to business*)*

En 2019 a été adopté le *règlement (UE) 2019/1150 du Parlement européen et du Conseil du 20 juin 2019 promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne* dit P2B (*platform to business*). Ce règlement, qui est entré en vigueur en juillet 2020, s'applique **à tous les services d'intermédiation en ligne et tous les moteurs de recherche en ligne**, quelles que soient leur taille ou leur position sur le marché, dans leurs relations contractuelles avec les entreprises dès lors que les entreprises utilisatrices de leurs services sont établies dans l'Union européenne et qu'elles proposent leurs biens ou services à des consommateurs situés dans l'Union au moins pour une partie de la transaction,

c'est-à-dire qu'elles orientent leurs activités vers des consommateurs situés dans un ou plusieurs États Membres. Il vise ainsi à la fois les places de marché en ligne (*market places*), les places collaboratives où les entreprises sont présentes, les magasins d'applications (applications gratuites ou payantes téléchargeables sur téléphone mobile) ou encore **les services de réseaux sociaux en ligne**. Si les plateformes présentent de nombreux avantages pour les entreprises utilisatrices (comme la facilitation de l'entrepreunariat ou l'accès à de nouveaux marchés), des difficultés peuvent aussi en résulter : dépendance des entreprises utilisatrices, déséquilibre dans les négociations, nécessité de comprendre l'algorithme de classement, modalités de présentation sur le site, etc. Pour y répondre, le règlement instaure **une obligation de transparence** à la charge des plateformes. Ainsi, les CGU doivent être claires et précises, facilement accessibles, définir les motifs de décision de suspension, de résiliation ou d'imposition de toute restriction et indiquer les principaux paramètres déterminant le classement des offres. Tout changement dans les CGU doit être notifié aux entreprises utilisatrices. Les décisions de suspension, résiliation ou imposition doivent être motivées. Les plateformes ont également des obligations de transparence concernant l'accès des entreprises utilisatrices aux données transmises ou produites par elles et doivent respecter un certain délai de préavis en cas de résiliation de la fourniture de service. L'objectif poursuivi par le règlement *Platform-to-Business* est donc de créer un « *environnement équitable, prévisible, durable et inspirant confiance* » protecteur des entreprises utilisant des plateformes et sites internet et permettre « *une concurrence saine qui aboutisse à un choix plus large pour le consommateur* ». Le règlement vise également, dans une moindre mesure, les services fournis par les **moteurs de recherche en ligne**, qui sont d'importantes sources de trafic internet pour les entreprises proposant leurs biens ou services en ligne et, à ce titre, susceptibles d'influer considérablement sur la réussite commerciale de ces entreprises, notamment par le classement des sites internet.

c. Le droit des marchés numériques : le Digital Markets Act ou DMA

Le règlement du Parlement européen et du Conseil relatif aux marchés contestables et équitables dans le secteur numérique (législation sur les marchés numériques) dit DMA, qui a fait l'objet d'un accord politique le 24 mars 2022, est, à l'heure où cette étude est rédigée, en cours de finalisation. Il vise à rendre l'environnement numérique plus équitable et plus compétitif et constitue un tournant dans le droit de la régulation économique des plateformes tant en raison des obligations qu'il met à la charge des plus grandes plateformes que parce qu'il désigne la Commission européenne comme autorité de contrôle, laissant une place seconde aux autorités nationales.

Tirant les conclusions d'une efficacité insuffisante de l'application du droit de la concurrence existant[142] pour faire face efficacement à certaines pratiques des principales entreprises qui contrôlent l'accès à l'ensemble des services en ligne (les contrôleurs d'accès ou *gatekeepers*), il met en place un nouveau dispositif

142 Not. les très longs délais de constatation d'une infraction et d'instruction du dossier et sanctions modestes au vu de la taille des entreprises visées.

visant les grandes plateformes fondé sur un système asymétrique d'obligations et d'interdictions, au travers d'une liste de « services de plateformes essentiels » qu'elles fournissent. Cette liste comprend les systèmes d'exploitation (OS), moteurs de recherche, magasins d'applications, places de marchés, plateformes de partage de vidéos, messageries, services publicitaires, services de *cloud*, les navigateurs et les assistants virtuels et les **réseaux sociaux**, cités pour la première fois expressément dans un texte de droit positif[143].

Ces acteurs sont qualifiés de « *contrôleurs d'accès* » lorsque les **trois critères cumulatifs suivants sont remplis** : ils ont un impact significatif en Europe[144], leurs services jouent un rôle de point d'accès majeur pour les entreprises utilisatrices vis-à-vis de leurs clients finaux[145] et ils ont acquis une position solide et durable[146].

Le DMA met ainsi en place un **dispositif d'encadrement *ex ante*** (préventif) des comportements de ces acteurs, les contraignant à se conformer à certaines règles inspirées de la pratique des autorités de concurrence dans le numérique, et permettant ainsi d'agir sur les marchés en amont, ce qui permet une plus grande efficacité. Cet encadrement se traduit par un régime d'obligations et d'interdictions qui poursuivent plusieurs objectifs : **la** « **contestabilité** »**,** c'est-à-dire la possibilité d'une concurrence effective, **l'équité dans le partage de la valeur entre contrôleurs d'accès et utilisateurs professionnels** ainsi que **la liberté de choix des consommateurs**. Il vise en particulier à lutter contre les environnements fermés et à favoriser le libre choix des utilisateurs finaux, notamment en assurant **l'interopérabilité progressive des services de messageries et la portabilité effective des données**, en imposant au contrôleur d'accès de recueillir **le consentement des utilisateurs** pour utiliser ou combiner à des fins de ciblage publicitaire des données personnelles recueillies par les entreprises utilisatrices, en interdisant des pratiques abusives comme le recours à des « *interfaces trompeuses* » (*dark patterns*) visant à obtenir le consentement de l'utilisateur final, en interdisant également au contrôleur d'accès, en cas de refus de l'utilisateur de donner son consentement, de solliciter à nouveau son consentement avant un an et en l'obligeant à fournir une solution alternative moins personnalisée permettant un accès non dégradé.

Les contrôleurs d'accès devront en outre notifier à la Commission européenne leurs acquisitions afin de prévenir d'éventuels comportements de prédation et réaliser un audit indépendant de toutes les techniques de profilage des consommateurs qu'ils appliquent au moins une fois par an.

143 *Cf.* 1.1.2 sur la notion juridique de réseau social

144 Ce critère est rempli si la plateforme réalise un chiffre d'affaires annuel dans l'UE supérieur ou égal à 7,5 milliards d'euros au cours des trois derniers exercices ou si sa capitalisation boursière s'élève à 75 milliards d'euros sur le dernier exercice de l'entreprise à laquelle il appartient, et si elle fournit un service de plateforme essentiel (ou plus) dans au moins 3 États membres.

145 Ce critère est rempli si la plateforme fournit un service à plus de 45 millions d'utilisateurs finaux actifs par mois dans l'UE et à plus de 10 000 entreprises utilisatrices de l'UE par an.

146 Ce critère est rempli si la plateforme remplit le critère précédent sur les trois derniers exercices.

Le DMA proscrit également les **comportements déloyaux** vis-à-vis des entreprises utilisatrices[147]. Il poursuit également l'objectif d'améliorer la **transparence et l'accès aux données** pour les professionnels, notamment **en matière publicitaire** en imposant aux contrôleurs d'accès plusieurs obligations : fournir aux services tiers un accès gratuit et continu aux données générées dans le cadre de l'utilisation de ces services par les consommateurs finaux sur la plateforme, lutter contre l'opacité des pratiques publicitaires du contrôleur d'accès en donnant accès aux annonceurs et aux éditeurs aux informations relatives aux prix payés par les annonceurs ainsi qu'aux montants versés aux éditeurs pour la publication des annonces publicitaires et au mode de calcul de ces montants, fournir un accès gratuit aux données de performance *marketing* pour les annonceurs et aux éditeurs/vendeurs d'espaces publicitaires.

L'identification des acteurs concernés, parfois après enquête[148], comme la supervision de ces obligations est confiée à la **Commission européenne**, dotée de pouvoirs d'accès aux données et aux algorithmes[149]. Elle pourra engager un dialogue sur les mesures réglementaires pour s'assurer que les contrôleurs d'accès ont une compréhension claire des règles à respecter mais aussi en préciser l'application si nécessaire. Un comité consultatif et un groupe à haut niveau seront mis en place pour assister la Commission et faciliter son travail. Les États membres pourront habiliter les **autorités nationales de concurrence** à ouvrir des enquêtes sur d'éventuelles infractions et à transmettre leurs conclusions à la Commission. En France, une loi devrait y habiliter **l'Autorité de la concurrence**.

Enfin, en cas de non-respect de ses obligations ou des injonctions imposées par la Commission, le DMA prévoit qu'un *gatekeeper* pourra être sanctionné par la Commission d'une **amende pouvant aller jusqu'à 10% de son chiffre d'affaires mondial** et même jusqu'à 20% en cas de récidive.

d. Le droit des services numériques : le Digital Services Act dit DSA

Sans mettre à bas l'équilibre de la directive e-commerce sur laquelle il s'appuie, le règlement du Parlement européen et du Conseil relatif à un marché intérieur des services numériques et modifiant la directive 2000/31/CE dit *Digital Services Act* constitue une **véritable révolution dans la conception de la régulation des**

147 Tels que proscrire les comportements d'auto-préférence des services du *gatekeeper*, notamment par un classement plus favorable de ses propres produits ou services.

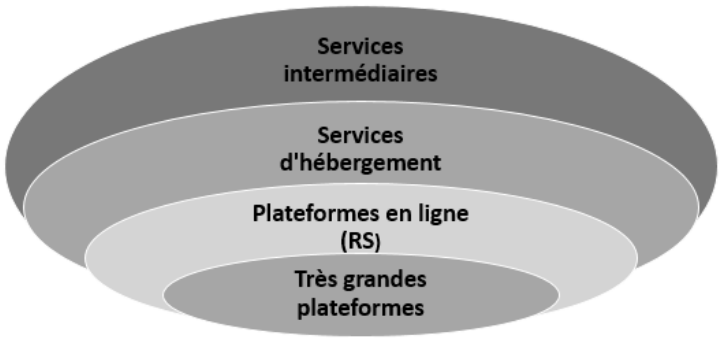
148 Un mécanisme de contestation permet toutefois de faire valoir une demande d'exemption auprès de la Commission, après justification de l'absence d'influence significative des services en cause sur leur marché. La liste des contrôleurs d'accès, rendue publique, peut être actualisée par la Commission sur demande ou de sa propre initiative.

149 En vertu de l'art 16 *DMA*, la Commission peut, par simple demande ou par voie de décision, demander aux entreprises et associations d'entreprises de fournir tous les renseignements nécessaires, y compris aux fins de contrôler, de mettre en œuvre et de faire respecter les règles prévues par le présent règlement. La Commission peut également demander l'accès aux bases de données et algorithmes des entreprises, ainsi que des explications les concernant, par simple demande ou par voie de décision. En vertu de l'art. 21 *DMA* : « 3. Au cours des inspections sur place, la Commission et les auditeurs ou experts nommés par cette dernière peuvent exiger de l'entreprise ou de l'association d'entreprises qu'elle donne accès à son organisation, son fonctionnement, son système informatique, ses algorithmes, son traitement des données et ses pratiques commerciales et qu'elle fournisse des explications sur ces différents éléments. La Commission et les auditeurs ou experts nommés par celle-ci peuvent poser des questions aux membres clés du personnel. »

plateformes et dans le degré d'investissement de l'Union européenne sur ces questions. S'agissant d'un règlement, il sera directement applicable dans les États membres.

Alors que, jusqu'à présent, l'attention ne portait que sur la question du contrôle des contenus illicites et sur l'extension des obligations de retrait de contenus par les plateformes après signalement[150], l'idée s'est imposée d'une régulation plus large fondée **sur l'analyse de risques**, dans la ligne de celle promue par le rapport de la mission dite *Facebook* remis au Gouvernement français en mai 2019[151]. S'affranchissant de la seule logique d'une responsabilité contenu par contenu, le DSA promeut un cadre de **supervision systémique** et oblige les très grandes plateformes à identifier les risques, justifier des mécanismes de modération qu'elles utilisent et évaluer l'efficacité *via* des régulateurs. Dès lors, l'objectif du texte n'est pas uniquement de mieux lutter contre les contenus illicites mais de prévenir les risques d'atteinte à la liberté d'expression provenant des modérations opérées par les plateformes elles-mêmes et des clauses figurant dans les CGU.

Face à l'inadaptation de la distinction cardinale entre hébergeur et éditeur instaurée par la directive e-commerce (alors notamment que nombreux sont les contenus postés par des tiers sur les plateformes), le DSA met en avant « **les services intermédiaires en ligne** » qui entrent dans la catégorie des hébergeurs mais sont soumis à une responsabilité accrue. Elle procède par cercles concentriques d'acteurs : d'abord le cercle plus large des ***fournisseurs de services intermédiaires*** qui comportent ceux qui ne gèrent que des activités de *simple transport* et de *mise en cache* – dont la responsabilité est très limitée – et la catégorie générale des *hébergeurs* ; ensuite le cercle plus resserré ***des plateformes en ligne***, hébergeurs qui stockent et diffusent au public des informations (sauf à titre purement accessoire) ; enfin le cercle restreint des ***plus grandes plateformes*** qui sont des hébergeurs qui fournissent leurs services à un nombre mensuel moyen de bénéficiaires actifs du service au sein de l'UE égale ou supérieure à 45 millions (art. 25 du DSA). Ce sont celles qui, par leur taille et donc leur influence potentielle (notamment en raison de la viralité des contenus), présentent les risques systémiques les plus lourds et sont astreintes par le règlement aux obligations les plus contraignantes.



150 *Cf.* épisode de la loi Avia à rebours des préconisations de la mission Facebook *cf. infra*.

151 *Rapport* de la mission « Régulation des réseaux sociaux – Expérimentation Facebook », remis au secrétaire d'État en charge du numérique en mai 2019.

Les réseaux sociaux entrent, selon leur taille, dans ces deux dernières catégories.

Ce règlement ne remet pas en cause les instruments sectoriels comme le système particulier de responsabilité mis en place par la directive 2019/790/UE du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique (notamment son article 17, consacrant un régime spécial de responsabilité des plateformes qui diffusent des contenus protégés télé versés par leurs utilisateurs) ni le RGPD, qui constitue une réglementation spéciale, ni les principes majeurs de la directive e-commerce que sont l'absence d'obligation générale de surveillance et l'obligation d'agir une fois le signalement effectué.

Le DSA vise à mettre en œuvre des **outils de contrôle et des obligations proportionnées à la taille et aux risques que présentent les structures.** Les différents prestataires visés supportent des **obligations graduelles** de transparence et de loyauté au bénéfice des utilisateurs, portant sur la modération des contenus, la publicité, les *markets place* et les processus algorithmiques de modération et de recommandation. Les très grandes plateformes font l'objet d'obligations supplémentaires, plus lourdes, en lien avec l'évaluation des risques qu'elles engendrent et parmi lesquels devrait figurer la viralité des contenus les plus choquants. Elles doivent encore prendre des mesures visant à atténuer ces risques. Le DSA fixe donc des objectifs et les régulateurs contrôlent les diagnostics établis ainsi que les mesures prises par les opérateurs selon les principes classiques du **droit de la compliance** (V. en annexe le Tableau sur les différentes obligations selon la catégorie de plateforme).

Si le principe du pays d'origine du lieu où la plateforme est établie est maintenu pour déterminer la compétence territoriale des autorités de régulation, **la supervision directe des très grandes plateformes en ligne est confiée à la Commission européenne** : elle disposera à cet égard d'une compétence exclusive pour les obligations qui sont propres à ces très grandes plateformes et d'une compétence partagée avec le régulateur du pays d'établissement pour les autres obligations du règlement. C'est un changement très important, qui constitue potentiellement une arme très efficace pour assurer l'effectivité de la régulation des plus grandes plateformes.

Sont chargés, dans chaque État membre, du contrôle de ces obligations, les « **coordinateurs des services numériques** », qui disposent de pouvoirs d'enquête, d'injonction et de sanction. S'agissant des très grandes plateformes, la régulation sera donc assurée par la Commission qui pourra, en tant que de besoin, rendre des décisions de non-conformité, enjoindre des mesures contraignantes et prononcer des sanctions, ces amendes pouvant aller jusqu'à 6% du chiffre d'affaires annuel mondial de la plateforme concernée. Tous les intermédiaires en ligne offrant leurs services au sein du marché unique, qu'ils soient établis dans l'UE ou en dehors de celle-ci, devront se conformer aux nouvelles règles. Les micro et petites entreprises auront des obligations proportionnées à leur capacité et à leur taille, tout en veillant à ce qu'elles restent responsables.

B. Le développement de droits spéciaux applicables aux plateformes

a. Le droit des plateformes de partage de vidéos et de contenu audiovisuel crée par l'utilisateur – les médias sociaux (directive SMA 2010/13/UE modifiée par la directive 2018/1808)

La directive européenne sur les services de médias audiovisuels (dite SMA), transposée par l'ordonnance du 21 décembre 2020, régit la coordination, à l'échelle de l'UE, des législations nationales couvrant tous les médias audiovisuels, qu'il s'agisse des émissions traditionnelles de télévision ou des services de médias audiovisuels à la demande. Elle n'est pas spécifique aux plateformes de partage de vidéos et concerne la régulation du marché audiovisuel dans son ensemble. Cependant, ainsi que le mentionnent les considérants 4 et 5, « *afin de protéger les mineurs des contenus préjudiciables et de mettre l'ensemble des citoyens à l'abri des contenus incitant à la haine, à la violence et au terrorisme* », cette directive s'applique également aux **médias sociaux**[152] « *qui se disputent les mêmes publics et les mêmes recettes que les services de plateforme de partage de vidéos* », et « *qui ont un impact considérable en ce qu'ils permettent plus facilement aux utilisateurs de façonner et d'influencer l'opinion d'autres utilisateurs* ». La directive précise qu'elle n'a pas pour objet de réguler les services de médias sociaux en tant que tels mais qu'elle devrait « *s'appliquer à ces services si la fourniture de programmes et de vidéos créées par l'utilisateur en constitue* ***une fonctionnalité essentielle*** » et elle incite la Commission à publier des orientations sur l'application du critère de fonctionnalité essentielle. Ainsi la directive étend son application aux « *services de plateformes de partage de vidéos* » qui comporte « *la fourniture au grand public de programmes, de vidéos crées par l'utilisateur (…) qui ne relèvent pas de la responsabilité éditoriale du fournisseur de la plateforme* » c'est-à-dire ce que l'on nomme souvent les médias sociaux[153].

Cette directive s'applique aux plateformes de partage de vidéos établies sur le territoire d'un État membre ou dont une filiale est établie dans un État membre. La responsabilité des services reste mesurée puisque, conformément à la directive e-commerce, ils ne sont pas tenus à une obligation générale de surveillance. Cependant, parce qu'ils « *déterminent l'organisation des contenus dont les programmes, vidéos créées par l'utilisateur et les communications commerciales audiovisuelles, notamment par des moyens automatiques ou des algorithmes* »,

152 Extrait du considérant 4 : « *Les services de plateformes de partage de vidéos fournissent un contenu audiovisuel qui est de plus en plus consulté par le grand public, en particulier les jeunes. Cela vaut également pour les services de médias sociaux qui sont devenus un vecteur important de partage de l'information, de divertissement et d'éducation, notamment en fournissant un accès à des programmes et à des vidéos créées par l'utilisateur.* »

153 Le b du 1 de l'art. 1er de la directive SMA dispose que « *un ''service de plateformes de partage de vidéos'' [est] un service tel que défini aux articles 56 et 57 du traité sur le fonctionnement de l'Union européenne, pour lequel l'objet principal du service proprement dit ou d'une partie dissociable de ce service ou une fonctionnalité essentielle du service est la fourniture au grand public de programmes, de vidéos créées par l'utilisateur, ou des deux, qui ne relèvent pas de la responsabilité éditoriale du fournisseur de la plateforme de partage de vidéos, dans le but d'informer, de divertir ou d'éduquer, par le biais de réseaux de communications électroniques au sens de l'article 2, point a), de la directive 2002/21/CE, et dont l'organisation est déterminée par le fournisseur de la plateforme de partage de vidéos, à l'aide notamment de moyens automatiques ou d'algorithmes, en particulier l'affichage, le balisage et le séquencement* ».

la directive les oblige à prendre les **mesures appropriées** pour protéger les **mineurs** des contenus ou publicités[154] susceptibles de nuire à leur épanouissement physique, mental ou moral et pour protéger le **grand public** de vidéos et publicités comportant une incitation à la haine ou la violence contre un groupe ainsi que de celles comprenant des contenus illicites (infractions terroristes, pédopornographie, racisme ou xénophobie). Ces mesures comprennent notamment des mécanismes permettant aux utilisateurs de signaler un contenu non conforme et des procédures pour le traitement des réclamations des utilisateurs, des outils d'éducation aux médias, la mise en place d'une sensibilisation des utilisateurs à ces mesures et outils. En outre, elle protège les données à caractère personnel de mineurs en interdisant leur traitement à des fins commerciales. Par ailleurs, la directive renforce la promotion des contenus européens et renforce l'indépendance des autorités de régulation nationales.

b. Le régime spécifique de responsabilité des plateformes de partage de contenus en ligne donnant accès à des œuvres protégées par le droit d'auteur (Directive 2019/790)

Le régime juridique instaurant l'irresponsabilité des hébergeurs tel qu'issu de la directive e-commerce s'est révélé délétère pour la protection des droits d'auteurs puisqu'il a eu pour effet de placer une large partie de l'exploitation en ligne de biens culturels hors du périmètre du droit d'auteur. Il a semblé vital de rééquilibrer ce rapport asymétrique entre les titulaires de droits et ces plateformes en ligne qui tirent profit de l'exploitation des œuvres protégées par le droit d'auteur auxquelles elles donnent accès sans pour autant rémunérer de manière appropriée les créateurs. *La directive 2019/790 du Parlement européen et du Conseil du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique* (dite DAMUN) a réglé la difficulté en excluant explicitement du régime issu de la directive *e-commerce* **les plateformes donnant au public accès à des œuvres protégées par le droit d'auteur**. A été instauré un régime de **responsabilité hybride** qui conduit les plateformes de partage de contenus en ligne à répondre à deux types d'obligations : fournir leurs meilleurs efforts pour obtenir les autorisations idoines auprès des titulaires de droits, fournir également leurs meilleurs efforts mais dans l'optique de garantir l'indisponibilité des contenus non autorisés par les titulaires de droits. L'idée est d'inciter les plateformes à conclure des **licences** avec les titulaires de droits qui le souhaitent et, à défaut, de rendre les contenus non-autorisés, sous certaines réserves et modalités, indisponibles.

1.2.2.2. Les droits traditionnels saisis par les réseaux sociaux

Outre les législations fondatrices de la régulation du secteur numérique et des plateformes, de nombreuses autres branches du droit, qui toutes obéissent à des logiques qui leurs sont propres, ont dû s'adapter aux questions soulevées par les réseaux sociaux. Dans certains cas, le législateur a dû intervenir pour permettre cette adaptation ; dans d'autres cas, cet exercice est revenu au juge ou aux instances administratives chargées de la régulation. Au fil du temps, s'est constitué un droit applicable aux réseaux sociaux fragmenté et qui se perd parfois dans les

154 La directive parle de « communications commerciales audiovisuelles ».

méandres de chaque domaine. Seules les branches du droit les plus directement concernées sont ici évoquées[155].

• *Le droit des abus de la liberté d'expression*

Le premier responsable des abus d'expression sur le net est l'**auteur des contenus en cause**. Cette responsabilité variera selon le cadre dans lequel il s'est exprimé (public/privé/professionnel). S'agissant des **opérateurs**, leur responsabilité pour avoir laissé des propos illicites prospérer et les avoir diffusés, parfois même accélérés, varie selon leur nature (propos haineux, fausses informations, contenus pédopornographiques, terroristes, etc.). De nombreux textes ont récemment modifié et enrichi les dispositions applicables.

-- Le cadre général posé par la loi du 29 juillet 1881

Le cadre juridique général de la liberté d'expression est issu de la **loi du 29 juillet 1881 sur la liberté de la presse**[156]. Afin de protéger au mieux la liberté d'expression, la liberté de la presse et celle de l'imprimerie, la poursuite et la sanction des abus contre cette liberté sont très limitées et encadrées par la loi. Ainsi, pour limiter les abus inhérents à la liberté d'expression, y compris commis hors voie de presse, une série limitative d'infractions réprime les abus commis : la **diffamation** (article 29), **l'injure** (article 33), la **provocation aux crimes et délits** (article 23), qui sont des délits lorsqu'elles sont commises en public et des contraventions lorsqu'elles sont commises en privé. Au fil du temps, plusieurs lois sont venues ajouter de nouvelles infractions comme la **provocation à la discrimination, la haine ou la violence** dans une série de cas limitatifs (origine, ethnie, nation, race, religion) par la loi n° 72-546 du 1er juillet 1972 relative à la lutte contre le racisme et l'interdiction de toute contestation de l'existence des crimes contre l'humanité qui furent définis dans le statut du Tribunal militaire international de Nuremberg de 1945 par la loi n° 90-615 du 13 juillet 1990. La loi du 30 décembre 2004 a également rajouté le « *sexe, l'orientation sexuelle et le handicap* » comme objet des délits de provocation à la discrimination. Il faut noter que les discours haineux sont aussi sanctionnés par le **droit pénal général** à travers l'infraction d'apologie du terrorisme et de menaces de mort.

Ces infractions souples et équilibrées, spécifiques au droit de la presse (bien que non limitées à ce cadre d'expression) se sont révélées adaptables à l'univers du numérique et aux évolutions des jurisprudences européennes et constitutionnelles[157]. En effet, alors que les réseaux sociaux ont rendu difficile l'appréhension de la distinction classique entre l'espace public et l'espace privé indispensable à la qualification de ces infractions, la Cour de cassation[158], reprenant le critère juridique éprouvé et solide de la « ***communauté d'intérêts*** » entre les destinataires des propos, a pu sans trop de difficulté apprécier ***la publicité*** des

155 Le droit régissant notamment la sécurité des produits et des biens échangés applicable aux *markets place* des réseaux sociaux ne sera ainsi pas évoqué.

156 Concernant les délits commis par voie de presse, le directeur de publication est responsable et à défaut, par un mécanisme « de responsabilité en cascade » celle de l'auteur, l'imprimeur, le vendeur et le distributeur. Le principal mécanisme protecteur de la liberté de l'information réside dans un délai de prescription très court de trois mois (art. 65 de la loi du 29 juillet 1881).

157 N. Bonnal, *Apologie de la loi de 1881*, Institut Villey.

158 CCass., 1e civ., 10 avril 2013, n° 11-19.530, Bull.

propos litigieux, élément de qualification commun à ces infractions. En l'espèce, elle a approuvé la solution par laquelle la cour d'appel de Paris avait regardé un message posté sur une page Facebook fermée au public réunissant quelques « personnes agréées » comme n'étant pas public au motif que ce groupe constituait une communauté d'intérêts. Dans une autre affaire, la cour d'appel de Paris, dans un arrêt du 7 novembre 2019, a pu, à l'inverse, estimer qu'un groupe réunissant plusieurs milliers de personnes, nonobstant le fait qu'elles partageaient la même profession, ne constituait pas une « communauté d'intérêts »[159].

L'expression d'un individu sur les réseaux sociaux, sans qu'elle soit forcément illicite, peut avoir des conséquences sur la vie de cette personne en raison du cadre dans lequel elle s'est exprimée. La jurisprudence a dû prendre en compte l'apparition de ce nouveau mode de communication dans différents contentieux. La cohérence des décisions doit être mise au bénéfice du juge.

La liberté d'expression du salarié et du fonctionnaire sur les réseaux sociaux

La question de l'expression du salarié ou du fonctionnaire sur les réseaux sociaux est le plus souvent appréhendée, respectivement, par le prisme du **droit du licenciement** ou du **droit de la fonction publique** s'agissant des manquements au devoir de réserve. Elle n'est pas sans affinités avec le droit de la presse car elle repose en partie sur la nature privée ou publique du propos tenu.

S'agissant des travailleurs du secteur privé, la Cour de cassation a ainsi pu juger que les propos injurieux tenus par un salarié sur un groupe Facebook fermé accessible à un petit groupe de personnes agréées ne constituaient pas une **faute grave**, dès lors qu'ils relevaient « *d'une conversation de nature privée* »[160]. Toutefois, les éléments de preuve tirés du compte privé d'un réseau social sont recevables si la preuve a été obtenue loyalement, si elle est indispensable pour l'exercice du droit de la preuve et si l'atteinte à la vie privée est proportionnée au but poursuivi[161]. Elle a par ailleurs récemment accepté que les informations contenues sur le profil LinkedIn d'un salarié soient utilisées comme élément de preuve lors d'un contentieux[162].

S'agissant des agents publics, le juge administratif s'est prononcé dans le sens d'une **appréciation exigeante du devoir de réserve des agents publics sur les réseaux sociaux**. Le Conseil d'État a ainsi jugé que constitue une faute la publication de contenus critiquant en termes outranciers les autorités de l'État de la part d'un officier de la gendarmerie nationale, alors même qu'il avait

159 Ces problématiques tenant à la frontière « quantitative » entre la communauté de pairs et l'agora ouverte s'étaient déjà posées à propos d'un stade antérieur des méthodes d'échange numériques, s'agissant de la diffusion sur des boucles de mails. La Cour de cassation a ainsi pu valider le raisonnement tenu par une cour d'appel dont l'arrêt relevait qu'un courriel envoyé sur deux listes de diffusion syndicale et partisane, bien qu'elles regroupaient chacune des personnes de la même orientation politique et syndicale, pouvait être regardé comme public (CCass., crim., 28 avril 2009, n° 08-85.249, Inéd).

160 CCass., soc., 12 septembre 2018, n° 16-11. 690, Bull., 2018). L'avis de l'avocat-général sur cette affaire laisse à penser que les critères d'appréciation de ce caractère privé devraient, en pratique, être convergents avec ceux de la jurisprudence pénale sur la communauté d'intérêts.

161 CCass., soc.,.30 septembre 2020, n° 19-12.058, Bull.

162 CCass., soc., 30 mars 2022, n° 20-21.665, Inéd.

eu recours à l'usage d'un pseudonyme[163]. Dans une décision de mars 2020 relative à la légalité de la charte de déontologie de la juridiction administrative, le Conseil d'État a jugé qu'elle avait pu légalement recommander l'abstention de tout commentaire social et politique sur les réseaux sociaux, compte tenu des « *caractéristiques techniques des réseaux de communication au public en ligne en général et des réseaux sociaux en particulier et de la difficulté pour l'utilisateur qui y publie des propos de s'assurer de leur caractère privé ou de leur diffusion restreinte, d'en garantir l'intégrité ou d'en maîtriser la portée, eu égard notamment aux réactions auxquelles ils sont susceptibles de donner lieu, parfois presque instantanément* »[164].

Devant la Cour européenne des droits de l'Homme, la question s'est aussi posée de savoir si l'apposition d'un *like* sur des contenus diffamatoires pouvait justifier la légalité d'un licenciement. La Cour a été saisie à la suite du licenciement sans droit à indemnisation d'une employée en qualité d'agente de nettoyage contractuelle d'une administration publique, à laquelle il était reproché d'avoir apposé des mentions « J'aime » sur plusieurs contenus publiés par des tiers sur Facebook qui accusaient des professeurs de viol. La Cour, suivant l'approche casuistique qui lui est familière, a estimé que, en l'espèce, l'affaire n'avait pas fait l'objet d'un examen suffisamment approfondi quant à la teneur des contenus litigieux et de leur contexte et quant à l'étendue et les portée de ces faits auprès du public et a jugé que la sanction était disproportionnée et qu'il y avait eu ainsi méconnaissance de la convention[165].

-- L'expression politique sur les réseaux sociaux en période électorale

La communication politique sur les réseaux sociaux est soumise aux règles du **code électoral**. Elle ne bénéficie pas d'un régime spécifique. Elle a donné lieu à des décisions de jurisprudence intéressantes, souvent, là encore, à propos du caractère public ou privé de la communication. En effet, là où l'audience d'un tract peut être connue ou mesurée assez facilement, y compris par d'autres personnes que celles qui l'ont distribué – par exemple, par des attestations d'habitants l'ayant reçu –, la preuve de l'audience est nettement plus délicate s'agissant d'un message envoyé sur les réseaux sociaux. Si les animateurs de pages peuvent disposer d'indicateurs de diffusion sur Facebook par exemple, leurs adversaires politiques, seuls susceptibles de soulever le grief, ne connaissent pas nécessairement ces chiffres. Les données relatives aux interactions – mentions « J'aime », partages –, quant à elles, constituent un net minorant du nombre de personnes réellement exposées à un contenu. Au surplus, dans le cas d'élections locales, le public des électeurs n'est pas forcément équivalent à celui des pages ou profils du réseau social, là où la distribution de tracts ne touche que des habitants de la commune dont la grande majorité sont en principe électeurs. Le Conseil d'État a ainsi jugé que la seule population d'abonnés de comptes diffusant un message ne pouvait suffire à apprécier son effet sur le suffrage (CE, 27 juin 2016, *Élections régionales de Normandie*, n^{os} 395413, 395547, T. sur ce point).

163 CE, 27 juin 2018, M. B., *n° 412541*.
164 CE, 25 mars 2020, Syndicat de la juridiction administrative, *n° 421149*, Rec.
165 CEDH, 2° sect., 15 juin 2021, *Melike c. Turquie*, *n° 35786/19*.

-- La lutte contre les contenus illicites

Pour tenir compte de la particularité des activités des plateformes et notamment des réseaux sociaux qui accroissent les risques et la gravité des atteintes à des intérêts privés ou publics mais sans qu'ils en soient les auteurs premiers, un cadre de responsabilité *ad hoc* a été instauré par la **directive e-commerce** transposée dans la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique dite LCEN. Refusant de mettre à la charge des fournisseurs d'accès et d'hébergement une obligation générale de surveillance des informations – que la CJUE a interprétée comme une absence d'obligation de mise en place de filtrage[166] – leur responsabilité ne peut être engagée que dans deux hypothèses : lorsqu'ils ne retirent pas promptement un contenu ***manifestement illicite*** qui a été notifié par un tiers ou lorsqu'ils ne retirent pas un contenu dont le retrait a été ordonné par un juge[167]. La liste des domaines concernés par cette obligation figure au 7 de l'article 6 de la loi du 21 juin 2004 et s'est allongée[168]. Au départ, les dispositions de cet article **imposaient aux hébergeurs de concourir** à la répression de l'apologie des crimes contre l'humanité, de l'incitation à la haine raciale ainsi que de la pornographie enfantine[169]. Y figurent en outre désormais les atteintes à la dignité humaine et l'incitation à la violence, la haine à l'égard de personnes à raison de leur sexe, de leur orientation ou identité sexuelle ou de leur handicap, et enfin la provocation à la commission d'actes de terrorisme et leur apologie[170].

Le législateur a tenté à plusieurs reprises d'instaurer de nouvelles infractions ou mécanismes pour lutter contre les **contenus illicites** mais le Conseil constitutionnel les a, plusieurs fois, jugées contraires à la Constitution, ce qui illustre, s'il en était besoin, les fragiles équilibres à préserver dès lors qu'une norme touche à la liberté d'expression et d'opinion.

S'agissant des **contenus terroristes**, plusieurs infractions telles que la diffusion de procédés de fabrication de bombe (art. 322-6-1 du code pénal) et l'interdiction de la provocation et de l'apologie du terrorisme, qui s'applique que les propos aient tenus dans une enceinte privée ou publique (art. 421-2-5 du code pénal), permettent de poursuivre la promotion du terrorisme et de caractériser des comportements manifestement illicites sur les réseaux sociaux. Le Conseil constitutionnel a toutefois jugé contraire à la Constitution la création d'une infraction punissant la **consultation habituelle de sites terroristes**[171]. *A contrario*,

166 CJUE, 24 novembre 2011, *Scarlet Extended* : pas d'obligation de mise en place d'un système de filtrage.

167 La CEDH a retenu un critère similaire en évoquant les propos « clairement illicites » : CEDH, gr. ch., 16 juin 2015, *Delfi AS c. Estonie,* n° 64569/09 ; CEDH, 2 février 2016, *Index. Hu c. Hongrie*, *n° 22947/13*.

168 F. Donnat, « Contenus illicites sur internet et hébergeurs », *Les nouveaux cahiers du Conseil constitutionnel*, juin 2016.

169 L'art. 25 de la *directive 2011/92* du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants fait obligation aux États membres de prendre « *les mesures nécessaires pour faire rapidement supprimer les pages Internet contenant ou diffusant de la pédopornographie* ».

170 Art. 6-7 LCEN

171 Ce délit punissait de 2 ans d'emprisonnement et 30 000 € d'amende celui qui consulte habituellement un service de communication en ligne mettant à la disposition du public des messages, images ou représentations soit provoquant directement à la commission d'un acte de terrorisme, soit faisant l'apologie de cet acte lorsque, à cette fin, ce service comporte des images ou représentations montrant la commission de tels actes consistant en des atteintes volontaires à la vie. Le Conseil

en matière de **consultations de contenus pédopornographiques**, le Conseil constitutionnel a estimé, à l'occasion de sa décision sur la *loi LOPPSI II*[172] que, compte tenu des garanties encadrant le dispositif (recours au juge), les dispositions conférant à l'autorité administrative le pouvoir de restreindre, pour la protection des utilisateurs d'internet, l'accès aux services de communication au public en ligne diffusant des images pédopornographiques était conforme à la Constitution.

Outre le dispositif de police administrative de retrait, blocage et déréférencement des contenus illicites (*cf. infra*) et les dispositifs de signalement (*cf.infra*), existe un mécanisme judiciaire. La loi n° 2021-1109 du 24 août 2021 confortant les principes de la République, a amélioré **ce cadre d'intervention du juge**. Auparavant celui-ci ne pouvait être saisi en urgence que selon la procédure de référé pour faire retirer un contenu ou bloquer un site. Dorénavant, il peut être saisi selon la **procédure accélérée au fond** pour prescrire des mesures propres à prévenir un dommage ou faire cesser un dommage occasionné par le contenu d'un service de communication en ligne (art. 839 et 481-1 du code de procédure civile). Cette procédure se révèle **efficace** à l'usage pour bloquer des sites et peut être initiée par le Procureur de la République.

S'agissant des **contenus haineux,** le Conseil constitutionnel a été saisi de la loi n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet dite loi Avia créant une **obligation positive de retrait** par les plateformes de certains contenus manifestement illicites. Cette loi permettait, d'une part, à l'autorité administrative de demander aux hébergeurs ou aux éditeurs d'un service de communication en ligne de retirer sous une heure certains contenus à caractère terroriste ou pédopornographique et sanctionnait la méconnaissance de ce manquement d'une peine d'un an d'emprisonnement et de 250 000 euros d'amende et, d'autre part, imposait à certains opérateurs de plateforme en ligne déterminés selon plusieurs critères, de retirer ou de rendre inaccessibles dans un délai de vingt-quatre heures des « *contenus manifestement illicites* » en raison de leur caractère haineux ou sexuel sous peine, là aussi, de sanction pénale. Le législateur cherchait à instaurer un principe de coopération des opérateurs à la lutte contre les contenus « les plus odieux ». Souhaitant tenir compte du rôle de certains opérateurs, notamment des réseaux sociaux, qui en permettant le partage de contenus et en accélérant l'accès par leurs processus algorithmiques de hiérarchisation et d'optimisation, ne se bornent pas à un rôle purement technique, il estimait le régime instauré par la LCEN dépassé et soutenait s'inspirer de la loi allemande « NetzDG » du 1er septembre 2017 (*cf. infra*). Bien que comprenant les motivations de cette proposition, le Conseil d'État (ainsi que la Commission nationale des droits de l'hommes) a émis des réserves sur ce dispositif et proposé

constitutionnel, rappelant que le législateur ne pouvait porter atteinte à la liberté d'expression que par des dispositions qui présentent un triple caractère nécessaire, adapté et proportionné, a jugé que le délit n'était pas nécessaire, compte tenu de l'arsenal répressif existant et que « *pénaliser l'auteur d'un propos provocateur ou apologétique en matière de terrorisme se justifie par les effets potentiels des paroles et la diffusion du discours haineux qui l'alimente ; punir celui qui le reçoit, sans autre exigence, revient à poser une présomption de projet terroriste, incompatible avec la liberté d'accéder à l'information ainsi qu'avec la présomption d'innocence* »

172 CC, 10 mars 2011, *Loi d'orientation et de programmation pour la performance de la sécurité intérieure*, n° 2011-625DC.

des amodiations[173]. Par la décision n° 2020-801 DC, le Conseil constitutionnel a confirmé qu'il était loisible au législateur d'instituer des dispositions destinées à faire cesser des abus de l'exercice de la liberté d'expression et de communication qui portent atteinte à l'ordre public et aux droits des tiers, mais a jugé que ces dispositifs portaient une **atteinte disproportionnée à la liberté d'expression**. Il a notamment estimé que l'obligation de retrait par les plateformes n'était pas subordonnée à l'intervention préalable d'un juge et que la notion de « *contenu manifestement illicite* » est difficile à apprécier. Par cette décision importante, le Conseil constitutionnel prend en compte le risque de « surmodération » par les plateformes. La loi, même ainsi partiellement invalidée par le Conseil constitutionnel, crée cependant **l'observatoire de la haine en ligne**, dont le rôle est d'analyser les propos haineux et de partager les informations entre les acteurs concernés, et instaure le **pôle national de lutte contre la haine en ligne ou** « **parquet national numérique** ». Celui-ci complète l'action des magistrats spécialisés de la chambre correctionnelle compétente dans les affaires de presse et traite, dans un champ de compétence national, de délits relevant du code pénal comme de la loi de 1881.

La loi n° 2021-1109 du 24 août 2021 confortant le respect des principes de la République marque un **tournant** dans la lutte contre les contenus haineux. Elle retient l'approche proposée par la « mission Facebook »[174], et adoptée depuis par le ***Digital Services Act***, fondée sur l'analyse des risques systémiques en prévoyant un nouveau **régime de modération des contenus illicites** : il s'agit finalement de mettre en œuvre par anticipation le futur règlement européen par une loi dont la vocation transitoire est prévue par une clause d'extinction au 31 décembre 2023. En effet, toutes les obligations imposées aux plateformes – obligation de transparence sur les CGU, de coopération avec les autorités publiques, de désignation d'un point de contact, d'évaluation des risques, de facilitation des signalements – figurent dans le DSA. L'ARCOM se voit chargée par la loi de superviser les processus de modération mis en place notamment par les réseaux sociaux et les plateformes de partage de vidéos, et est dotée de la faculté de prononcer des sanctions financières (jusqu'à 20 millions d'euros ou 6% du chiffre d'affaires mondial).

Cette loi instaure également **d'autres mesures pérennes.** Afin de lutter contre les **sites miroirs** qui reprennent des contenus illicites déréférencés ou bloqués par la justice, de nouvelles dispositions sont insérées dans la LCEN[175]. Dans son avis rendu public, le Conseil d'État a relevé que, dans les deux cas prévus par la loi, la demande de blocage ou de déréférencement ne peut être formulée pour une durée excédant celle restant à courir pour les mesures judiciairement ordonnées et que, lorsqu'elle demeure infructueuse, les demandeurs doivent à nouveau solliciter l'autorité judiciaire pour qu'elle ordonne toute mesure destinée à faire cesser l'accès aux contenus des services concernés. Le Conseil d'État a estimé que

173 CE, avis n° 397368 sur la proposition de la loi visant à lutter contre la haine sur internet, Assemblée Nationale ; CNCDH, avis relatif à la proposition de loi visant à lutter contre la haine sur internet, NOR : CDHX1920513V, JORF n° 0161 du 13 juillet 2019, Texte n° 107.

174 Rapport de la mission « Régulation des réseaux sociaux – expérimentation Facebook, mai 2019, Créer un cadre français de responsabilisation des réseaux sociaux : agir en France avec une ambition européenne.

175 Art. 6-3 de la LCEN modifiée.

le dispositif proposé ne contrevenait pas aux exigences résultant de la Constitution et du droit de l'Union, qui ne permettent pas de procéder à l'interdiction des sites et contenus « miroirs », quels que soient le degré et la gravité de leur illicéité, sans l'intervention d'un juge[176]. Ce dispositif spécifique ne semble pas remis en cause par le DSA, qui n'a pas prévu de mécanisme comparable.

Cette loi crée également un **nouveau délit de mise en danger de la vie d'autrui par diffusion d'informations relatives à la vie privée, familiale ou professionnelle** puni de 5 ans de prison et 75 000 euros d'amende si la victime est un agent public, un élu ou un journaliste ou si elle est mineure[177] et permet l'utilisation de la procédure de comparution immédiate pour les délits de la loi du 29 juillet 1881 sur la liberté de la presse (provocations publiques à la haine ou à la violence, négationnisme...)[178]. Il s'agit de sanctionner efficacement les abus les plus graves et manifestes à la liberté d'expression, favorisés notamment par l'usage des réseaux sociaux.

Dans une logique beaucoup plus stricte, a été adopté le 29 avril 2021 *le règlement 2021/784 du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne* dit TCO qui vise principalement à **faire retirer dans le délai d'une heure les contenus à caractère terroriste** par l'hébergeur directement, et ce au moyen d'une injonction de retrait prise par les autorités compétentes de n'importe quel État membre. Lorsque l'autorité compétente à l'origine de l'injonction ne se trouve pas dans le même État membre que celui de l'établissement principal de l'hébergeur, ou de son représentant légal, les autorités compétentes de l'État membre de l'hébergeur auront 72 heures, à compter de la communication obligatoire de la copie de l'injonction de retrait par l'autorité d'émission ou à compter de la contestation de l'injonction de retrait par l'hébergeur ou l'auteur du contenu (qui lui-même dispose d'un délai de 48 heures pour ce faire), pour analyser et éventuellement contester la décision d'injonction de retrait, par exemple si cette injonction constitue une violation des libertés et droits fondamentaux garantis par la Charte. A l'issue, le contenu signalé pourra soit redevenir disponible, soit être définitivement supprimé. Le règlement établit aussi une liste des « contenus terroristes » en excluant le matériel diffusé à des fins de recherche ou éducatives[179] et impose aux services d'hébergement plusieurs obligations notamment de vigilance, d'identification, de retrait et de coopération entre les services compétents *(cf. infra),* Europol et les opérateurs concernés. Le règlement s'applique aux fournisseurs de services d'hébergement qui proposent des services dans l'Union, quel que soit le lieu de leur établissement principal, dans la mesure où ils diffusent des informations au public. Il est entré en vigueur le 7 juin 2022.

176 Avis n° 397368 du 16 mai 2019 sur la proposition de loi visant à lutter contre la haine sur internet, points 36 et 37 et n° 398829 des 27 et 28 novembre 2019 sur le projet de loi relatif à la communication audiovisuelle et à la souveraineté culturelle à l'ère numérique, points 52 et suivants.

177 Nouvel art. 223-1 du code pénal.

178 Cette procédure rapide de jugement ne concernera pas les contenus contrôlés par des directeurs de publication de presse (régime de la responsabilité en cascade).

179 Il procède par renvoi à la *directive 2017/541* relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la *décision 2005/671/JAI* du Conseil qui fixe à son art. 3 la liste des infractions terroristes.

La lutte contre la haine en ligne s'exerce aussi à travers des instruments de droit souple, comme la diffusion de codes de conduite, de recommandations ou de communications[180].

L'**Allemagne** dispose d'un dispositif innovant pour lutter contre les **contenus illicites**, les discours haineux et la désinformation en ligne. La loi visant à améliorer l'application du droit sur les réseaux sociaux (**NetzDG**), entrée en vigueur le 1er octobre 2017 s'applique aux opérateurs de réseaux sociaux[181] comptant plus de 2 millions d'utilisateurs enregistrés en Allemagne (Facebook, Twitter et YouTube). Ces derniers sont obligés de supprimer ou de bloquer les « contenus manifestement illicites » dans les 24 heures et les « contenus illicites » dans un délai de 7 jours suivant la réception d'un signalement. Des amendes peuvent être infligées jusqu'à 5 millions d'euros par l'Office fédéral de la justice. Deux dispositions, dont l'une concernant le champ d'application territoriale de la loi, ont été récemment jugées contraires au droit de l'Union européenne (Tribunal administratif de Cologne, 1er mars 2022)[182]. Deux lois ont modifié la NetzDG, la première ayant instauré une obligation de signalement des opérateurs auprès de l'office fédéral de police criminelle des infractions les plus graves, la seconde renforçant les droits des utilisateurs (notamment celui de voir la décision prise par la plateforme de supprimer son contenu être réexaminée).

De façon générale, une attention particulière est accordée à ce que la liberté d'expression ne porte pas atteinte de façon disproportionnée « *au droit général de la personnalité* »[183] découlant de la Loi fondamentale. S'agissant de la

180 *Code de conduite* de la Commission européenne de mai 2016 relatif aux discours haineux illégaux en ligne. *Communication* sur la lutte contre le contenu illicite en ligne de la Commission du 28 septembre 2017 qui fournit des orientations aux plateformes concernant les procédures de notification et les actions contre les contenus illicites en ligne. *Recommandation* (UE) 2018/334 de la Commission du 1er mars 2018 sur les mesures destinées à lutter, de manière efficace, contre les contenus illicites en ligne, définissant notamment les modalités de notification des contenus illicites et les mesures que peuvent prendre les hébergeurs.

181 Sont définis comme des réseaux sociaux au sens de la loi : « les plateformes en ligne, à but lucratif, destinées à permettre aux utilisateurs de partager tout contenu avec d'autres utilisateurs, ou de rendre ce contenu accessible au public ». Les plateformes qui gèrent des contenus éditoriaux ou journalistiques, les services de messagerie et les plateformes de vente sont expressément exclus du champ d'application de la loi.

182 Le tribunal administratif de Cologne a jugé que le § 3a de la NetzDG, prévoyant une obligation pour les opérateurs de réseaux sociaux de signaler et de transmettre certains contenus à l'Office fédéral de la police criminelle, porte atteinte au « principe du pays d'origine » (Herkunftslandprinzip) prévu par la directive 2000/31/CE sur le commerce électronique. Par ailleurs, le tribunal juge que le § 4a de la NetzDG est contraire à la directive 2018/1808 sur les services de médias audiovisuels. Selon cette directive, les États membres sont tenus de désigner des autorités de régulation juridiquement distinctes et fonctionnellement indépendantes des pouvoirs publics. Les juges considèrent que l'Office fédéral de la justice (Bundesamt für Justiz), qui est subordonné au ministère fédéral de la justice et reçoit des instructions de ce dernier, ne remplit pas les conditions d'indépendance prévues par la directive.

183 En droit constitutionnel allemand, le droit de la personnalité est un droit fondamental développé par la Cour constitutionnelle fédérale qui comprend plusieurs aspects tels que la garantie de la vie privée, la protection de l'honneur et le droit à l'image. Dans une affaire très médiatisée en Allemagne dans laquelle une politicienne allemande a été victime de plus d'une vingtaine d'insultes et de propos dégradants sur Facebook, la Cour constitutionnelle fédérale a jugé que la liberté d'expression sur les réseaux sociaux devait toujours être mise en balance avec d'autres droits fondamentaux, en particulier avec « le droit général de la personnalité » (Allgemeines Persönlichkeitsrecht, *Cour constitutionnelle*

protection des mineurs sur les réseaux sociaux, les réglementations y afférant sont prévues principalement dans « l'accord sur la protection des mineurs dans les médias », qui permet notamment de définir les contenus « absolument illicites » et dont la diffusion est interdite.

S'agissant de la lutte contre les fausses nouvelles, le législateur français a souhaité se doter d'outils particuliers, outre ceux déjà prévus par le code pénal et le droit de presse. La loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information dite de lutte contre les « *fake news* », a mis en place un dispositif de **signalement des fausses informations**, ainsi que **des obligations de transparence et de loyauté à la charge des plateformes**. Le CSA, devenu l'ARCOM le 1er janvier 2022, a reçu la mission de veiller au suivi de ces mesures. Pour cela, l'autorité de régulation a adopté une recommandation le 17 mai 2019, destinée aux plateformes, pour les inciter à prendre des mesures concrètes pour lutter contre les fausses informations[184]. En complément de ces mesures, l'ARCOM peut inviter les plateformes à sensibiliser les utilisateurs à l'univers des réseaux sociaux, mais également à instaurer un dialogue lui permettant d'accéder aux informations relatives à la diffusion de *fake news*. A ce titre, il est demandé aux plateformes de nommer un **interlocuteur référent**, avec lequel l'autorité peut instaurer un contact.

Par ailleurs, pour répondre au problème spécifique de la **diffusion de fausses informations en période électorale** pouvant alors peser sur la sincérité du scrutin, cette loi impose, en période électorale, des obligations de transparence aux opérateurs de plateforme en ligne (article L. 163-1 du code électoral) et instaure une procédure de **référé** « **anti *fake news*** » visant à faire cesser toute diffusion de fausses informations durant les trois mois précédant un scrutin national dans le cadre des élections (article L. 163-2 du code électoral). Les demandeurs en référé peuvent être le Ministère public, tout candidat, tout parti ou groupement politique ou toute personne intéressée. Les défendeurs peuvent être les hébergeurs ou les fournisseurs d'accès à internet. La décision sera rendue sous 48 heures à compter de la saisine. Par deux décisions du 20 décembre 2018 (n° 2018-773 DC et n° 2018-774 DC), le Conseil constitutionnel a jugé conforme la nouvelle voie de référé visant à faire cesser la diffusion de fausses informations durant les trois mois précédant un scrutin national dans le cadre des élections. Il a toutefois émis une réserve d'interprétation sur la notion de fausse information en jugeant, sachant que le référé peut avoir pour effet de faire cesser la diffusion de certains contenus, que « *les allégations ou imputations mises en cause ne sauraient, sans que soit méconnue la liberté d'expression et de communication, justifier une telle mesure que si leur caractère inexact ou trompeur est **manifeste.** Il en est de même pour le risque d'altération de la sincérité du scrutin, qui doit aussi être **manifeste***. » Aucune application de ce texte n'est pour l'heure connue.

fédérale, 19 décembre 2021, 1 BvR 1073/20.

184 Recommandation n° 2019-03 du 15 mai 2019 : Dans le cadre du devoir de coopération pour la lutte contre la diffusion de fausses informations (instauré par la loi du 22 décembre 2018) : le CSA précise comment pourrait être mis en place un dispositif de signalement accessible et visible, comment assurer une transparence des algorithmes, promouvoir des contenus issus d'entreprises et d'agences de presse et de services de communication audiovisuelle, lutter contre les comptes propageant massivement de fausses informations et permettre une meilleure information des utilisateurs sur l'origine de ces contenus.

S'agissant de l'accès aux **contenus protégés par la propriété littéraire et artistique**, la directive européenne 2001/29/CE transposée en droit français par la loi droit d'auteur et droits voisins dans la société de l'information dite DADVSI (2006), a cherché spécifiquement à **protéger les droits d'auteur sur internet**. Une autorité publique indépendante, la Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet (HADOPI), avait été créée pour rechercher et sanctionner le manquement à l'obligation de surveillance instituée par la loi, la recherche et le constat des infractions de contrefaçon ressortant, pour leur part, toujours de la compétence de l'autorité judiciaire. Les dispositions autorisant l'HADOPI selon un mécanisme de « riposte graduée », à prononcer des sanctions vis-à-vis des abonnés, y compris la suspension de l'accès à internet, **sans intervention du juge**, ont été censurées par le Conseil constitutionnel (décision n° 2009-580 DC du 10 juin 2009). La loi dite *Hadopi 2* du 20 octobre 2009 a ainsi limité les pouvoirs de l'HADOPI à des mesures d'avertissement. Elle est aussi dotée de la mission d'encouragement de l'offre légale d'oeuvres en ligne et de protection des œuvres. Elle a publié en octobre 2019 une étude sur *L'accès illicite à des contenus culturels* via *les réseaux sociaux*[185] qui a démontré que 28% des internautes sont des consommateurs illicites sur les réseaux sociaux. Au 1er janvier 2022, le CSA et l'HADOPI ont fusionné en une seule autorité : l'Agence de régulation de la communication audiovisuelle, l'ARCOM.

• *Le droit pénal : la criminalité facilitée par l'usage des réseaux sociaux*

Le droit pénal a été profondément enrichi par l'arrivée du numérique. En effet, ce nouvel espace constitue un terrain favorable pour les activités délinquantes les plus diverses[186]. Si certaines infractions de droit commun se sont aisément adaptées au numérique (infractions du droit de la presse, atteinte au secret des correspondances[187], atteinte à la vie privée[188], provocation et apologie du terrorisme), d'autres comportements ont suscité plus d'interrogations. Il en est ainsi par exemple de la pratique du ***revenge porn*** (qui consiste à publier sur internet un contenu sexuellement explicite sans le consentement de la personne concernée, dans un but de vengeance). Pour répondre à la nécessité d'incriminer ce comportement[189], la loi pour une République numérique du 7 octobre 2016 a créé un nouvel article 226-2-1 du code pénal qui incrimine le fait, en l'absence d'accord de la personne pour la diffusion, de porter à la connaissance du public ou d'un tiers tout enregistrement ou tout document portant des paroles ou images présentant un caractère sexuel, obtenu avec le consentement exprès ou présumé de la personne ou par elle-même. La qualification du délit est caractérisée et ce, quelle que soit l'intention de l'auteur (vengeance, volonté d'humilier, moquerie, chantage, etc.). Il suffit de diffuser un contenu sexuel en l'absence d'accord de la personne, étant précisé que le consentement à la captation n'emporte pas

185 Étude sur le site internet de l'Hadopi.

186 M. Quéméner, *Le droit face à la disruption numérique. Adaptation des droits classiques. Émergence de nouveaux droits*, Gualino, 2018.

187 Art. 226-15 du code pénal.

188 Art. 226-1 du code pénal.

189 *Cf.* CCass., crim., 16 mars 2016 (n° 15-82 676, Bull) qui juge que l'infraction de l'atteinte à l'intimité ne peut être appliquée à cette situation.

accord de diffusion dans les cas visés à l'article 226-2-1. Les peines sont en outre aggravées (deux ans de prison, 60 000 € d'amende). Une autre incrimination a également été créée par la loi n° 2007-297 du 5 mars 2007 relative à la prévention de la délinquance pour sanctionner la pratique de « ***Happy slapping*** » (ou vidéo lynchage) consistant à photographier ou filmer avec un téléphone portable l'agression par un ou plusieurs complices de tiers dans le but de diffuser la vidéo-agression sur internet et les réseaux sociaux[190].

En outre, de nouvelles infractions ont été instaurées pour lutter contre des comportements illicites facilités par l'usage du numérique et notamment les réseaux sociaux. La LOPPSI II, promulguée le 14 mars 2011, a introduit dans le code pénal un **délit spécifique d'usurpation d'identité s'étendant aux réseaux numériques** (article 226-4-1 du code pénal). Son application positive à un délit commis sur un site internet laisse penser que cette qualification peut saisir des situations variées dépassant nettement le cas du « faux profil »[191]. Par ailleurs, le législateur, craignant que le « cyber harcèlement» ne soit pas, en tant que tel, susceptible d'être sanctionné, a instauré, par la loi n° 2014- 873 du 4 août 2014 pour l'égalité réelle entre les femmes et les hommes, un délit réprimant **le harcèlement commis notamment sur internet**[192]. Le harcèlement en ligne est ainsi punissable, que les échanges soient publics (sur un forum par exemple) ou privés (entre amis sur un réseau social). Les **raids numériques**, ou harcèlements en meute, sont passibles des mêmes sanctions[193]. La loi n° 2022-299 du 2 mars 2022 crée un **délit de harcèlement scolaire** qui pourra être puni jusqu'à dix ans de prison en cas de suicide ou tentative de suicide de la victime. De même, s'agissant de la **protection des mineurs**, ont été instaurées des infractions sanctionnant la consultation de sites pédopornographiques (art. 227-13 du code pénal) et le fait de faire des propositions sexuelles à un mineur de quinze ans par le biais d'internet (art. 227-22-1 du code pénal). Certaines infractions préexistantes ont aussi été utilisées, notamment celles réprimant **les fausses informations** lorsqu'elles ont causé un trouble[194]. De nombreuses infractions comme l'infraction d'abus frauduleux de l'état d'ignorance ou de la situation de faiblesse (art. 223-15-2 du code pénal) qui permet de sanctionner les comportements de prédation sur le net (dérive sectaire, prédation financière ou sexuelle) peuvent être mobilisées pour lutter contre les comportements délictueux sur les réseaux sociaux[195].

190 Une telle pratique ne pouvait être sanctionnée que lorsque l'image avait été fixée dans un lieu privé pour atteinte à l'intimité de la vie privée ou non-assistance à personne en danger (par exemple s'agissant de la vidéo de l'agression d'un professeur dans la classe d'un lycée : TGI Versailles, 27 juin 2007).

191 CCass., crim., 16 novembre 2016, n° 16-80.207, *inéd*. V. pour des ex. : E. Stella, *L'application du droit pénal aux réseaux sociaux en ligne*, thèse, 2019, §. 226.

192 Art. 222- 33-2-2 du code pénal.

193 Ce phénomène vise les cas où plusieurs personnes harcèlent une même victime en même temps ou de manière successives. V. affaire « Mila » dans laquelle le tribunal correctionnel de Paris, par une décision du 7 juillet 2021, a condamné les 11 prévenus à des peines de quatre à six mois de prison avec sursis.

194 L'art. 322-14 du code pénal réprime le fait de communiquer ou de divulguer une fausse information dans le but de faire croire qu'une destruction, une dégradation ou une détérioration dangereuse pour les personnes va être ou a été commise. L'art. 224-8 du code pénal incrimine quant à lui le fait par quiconque, en communiquant une fausse information, de compromettre sciemment la sécurité d'un aéronef en vol ou d'un navire. L'art. 443-2 du code du commerce réprime le fait de diffuser par quelque moyen que ce soit des informations mensongères ou calomnieuses visant à altérer les prix. L'art. 97 du code électoral réprime le délit de diffusion de fausses nouvelles en punissant d'un an les individus ayant partagé de fausses informations ayant pesé sur le vote.

195 Lorsqu'il s'agit d'abus sur mineurs, ces faits seraient susceptibles de recevoir une qualification

Enfin, de nouvelles infractions spécifiques ont été créées pour sanctionner la méconnaissance des manquements portant atteinte aux **données personnelles** (art. 226-16 et s. du code pénal) et les atteintes aux systèmes de **traitement automatisé des données** (art. 323-62 et s. du code pénal).

Plus généralement, l'ensemble des droits régissant les relations économiques et le marché a été bousculé par l'arrivée d'internet et des réseaux sociaux.

• *Le droit de la consommation : un droit au service du rééquilibrage contractuel*

Le droit des réseaux sociaux est aussi celui des relations contractuelles entre les utilisateurs et les plateformes.

L'objet du droit de la consommation

Si le droit civil, droit commun des contrats, impose aux cocontractants une obligation de bonne foi, la diversification des rapports commerciaux a conduit à la création d'un droit spécifique pour régir les relations entre les consommateurs et les professionnels : *le droit de la consommation*. Celui-ci a pour objet de **rééquilibrer les relations contractuelles entre ces deux acteurs**. A cette fin, il comporte un arsenal de dispositions pour lutter contre les pratiques commerciales trompeuses ou déloyales notamment dans les **contrats d'adhésion** où le consommateur n'a pu librement discuter des conditions du contrat et dans lesquels les relations sont régies par **les conditions générales d'utilisation**, appelées couramment les CGU. Le droit de la consommation impose aux professionnels des **obligations d'information et de loyauté**, interdit et sanctionne pénalement certains comportements et prohibe certaines **clauses dites** « **abusives** « *c'est-à-dire celles qui ont pour objet ou pour effet de créer au détriment du non professionnel ou du consommateur un déséquilibre significatif entre les droits et obligations des parties au contrat*. » Droit privé par nature, il relève du juge judiciaire.

Les plateformes ont tenté de s'extirper de ce droit en estimant qu'il ne leur était pas applicable, soit que l'utilisateur ne serait pas un « consommateur » au sens du code de la consommation soit que le contrat ne serait pas conclu à titre onéreux, les services étant gratuits, et ces discussions ont donné l'occasion au juge de déterminer les critères d'applicabilité du code de la consommation aux réseaux sociaux. Par plusieurs décisions, les juridictions judiciaires ont rappelé que **les réseaux sociaux sont soumis au droit de la consommation** dans leurs relations contractuelles avec les utilisateurs, que le contrat soit aussi adressé à des professionnels ou qu'il soit conclu à titre gratuit ou onéreux[196].

Les litiges portés devant les juridictions judiciaires portent le plus souvent sur deux questions : **la licéité et l'opposabilité des CGU**.

pénale au sens de l'art. 313-1 pour escroquerie ou provocation de mineur à commettre un crime ou un délit telle que précisée à l'art. 227-21. Ces modes opératoires pourraient également relever d'une pratique trompeuse, comme l'établissent les art. L. 121-1 et L. 121-2 du code de la consommation, ou bien encore d'un système pyramidal, comme en dispose l'art. L. 121-15 du code de la consommation.

196 En ce sens TGI Paris, 7 août 2018 ; CA Paris, 12 février 2016, n° 12/12401.

Sur le premier point, il s'agit tout d'abord, une fois l'ensemble des règles de droit applicables identifiées – plus largement que le seul droit de la consommation – de vérifier que les clauses respectent les cadres normatifs applicables (droit d'auteur, droit des données personnelles, protection de la vie privée, protection des mineurs etc.). En ce sens, les CGU, véritables « règlements internes » des réseaux sociaux en sont la pierre angulaire. Dans cette tâche, le juge est guidé par les textes qui dressent une liste noire des clauses illicites et aidé par la **Commission nationale des clauses abusives** qui a notamment pour rôle de rechercher dans les modèles de contrats habituellement proposés par les professionnels aux non professionnels ou consommateurs, les clauses qui peuvent présenter un caractère abusif notamment car elles sont ambiguës, déloyales ou mensongères[197]. Celle-ci a d'ailleurs adopté une **recommandation spécifiquement consacrée aux réseaux sociaux** le 7 novembre 2014 (n° 14-02) qui a servi de base à des jugements civils[198]. La direction générale de la consommation, de la concurrence et de la répression des fraudes (DGCCRF) a, dans un communiqué publié le 9 février 2016, indiqué avoir trouvé plusieurs clauses abusives dans les CGU de Facebook (notamment celles l'autorisant à retirer des contenus ou informations publiés par l'internaute sur le réseau de façon discrétionnaire, ainsi que celles qui réservent à Facebook le droit de modifier unilatéralement la politique de confidentialité sans en informer l'internaute) et a enjoint Facebook de supprimer ces clauses. Grâce la loi n° 2014-344 du 17 mars 2014 dite Hamon qui a permis les actions de groupe des associations de consommateurs, la lutte contre les clauses abusives a été améliorée. Lorsqu'un juge, saisi par une association de consommateurs, prononce la suppression de la clause abusive, cette suppression s'appliquera non seulement dans le contrat pour lequel il a été saisi mais aussi dans tous les contrats identiques comportant la même clause abusive. Mais, pour l'instant, dans le champ des réseaux sociaux, ce dispositif n'a pas eu le succès escompté.

S'agissant de l'**opposabilité des CGU**, le juge vérifie que l'utilisateur a été mis en mesure d'en prendre connaissance et de les accepter afin de leur reconnaître une valeur contractuelle. Comme pour le droit des données personnelles, la question de la portée du *consentement* donné par l'utilisateur demeure la plus épineuse. Un examen attentif de la nature des informations délivrées, de leur clarté et de leur exhaustivité doit être fait au cas par cas.

Le droit de la consommation a été adapté au numérique par plusieurs textes et notamment la *loi pour la confiance sur l'économie numérique du 21 juin 2004* (n° 2004-575) transposant la directive européenne 2000/31/CE du 8 juin 2000 sur le commerce électronique et certaines dispositions de la directive du 12 juillet 2002

197 Parmi elles, ont pu être identifiées par les différentes instances compétentes, la clause qui présume le consentement du représentant légal lors de l'inscription d'un mineur sur le réseau, celle qui affirme que le service fourni est gratuit, la clause qui exclut le régime de protection des données personnelles pour les traces laissés par l'utilisateur –cookies, données de géolocalisation-, la clause permettant un accord implicite au recueil des données personnelles, clause permettant le partage des données à des tiers et pour des finalités non précisées, la clause prévoyant une durée illimitée de conservation des données personnelles, ou encore la clause prévoyant que le retrait d'un contenu signalé comme illicite est facultatif, la non-responsabilité du fournisseur de service au titre du contenu, la clause prévoyant la modification unilatérale des CGU.

198 Décisions contre Google + (TGI de Paris du 12 février 2019, n° 14/07224) et Twitter (TGI Paris, 7 août 2018).

sur la protection de la vie privée dans le secteur des communications électroniques et la *loi du 7 octobre 2016 pour une République numérique* qui a notamment soumis les plateformes à des obligations de loyauté et d'informations du consommateur (art. L.111-7- 1 du code de la consommation). Récemment, la *loi n° 2020-1508 du 3 décembre 2020 portant diverses dispositions d'adaptation au droit de l'Union européenne en matière économique et financière* a renforcé les pouvoirs de la DGCCRF et transposé plusieurs directives, notamment la directive 2019/2161 dite Omnibus qui modernise le droit européen de la consommation. Elle précise les obligations des plateformes qui doivent correctement rédiger les CGU et mieux informer les utilisateurs sur les modalités de classement et les différenciations de traitement ; elle renforce également la lutte contre les « faux avis » sur les plateformes.

Face à l'hybridation des réseaux sociaux, à l'apparition des *market place* et des *influenceurs*, le droit de la consommation s'applique aussi aux réseaux sociaux pour d'autres aspects. Une influenceuse réputée a ainsi été condamnée pour **pratiques commerciales trompeuses** car elle ne signalait pas être rémunérée par l'entreprise pour laquelle elle plaçait les produits. Enfin, le droit de la consommation réglemente une partie de celui de **la publicité** dont la place sur certains réseaux sociaux est très importante.

- *Le droit de la publicité à l'épreuve de la publicité en ligne*

Dans le domaine de la publicité, il faut distinguer la réglementation du contenu et celle du marché.

S'agissant du contenu, plusieurs dispositions s'appliquent. Le code de la consommation[199] interdit les **publicités mensongères ou trompeuses** (allégations fausses pouvant induire le public en erreur). Dans ce domaine, un organisme paritaire, le BVP (Bureau de vérification de la publicité), a la charge d'émettre des avis négatifs sur toutes formes de messages au contenu trompeur[200]. La loi n° 92-60 du 18 janvier 1992 renforçant la protection des consommateurs délimite très précisément les modalités de la **publicité comparative** qui doit « *être limitée à une comparaison objective qui ne peut porter que sur des caractéristiques essentielles, pertinentes et vérifiables* ». Par ailleurs, la loi interdit complètement **la publicité pour le tabac** (loi n° 91-32 du 10 janvier 1991 relative à la lutte contre le tabagisme et l'alcoolisme), alors que celle **pour l'alcool** est proscrite uniquement à la télévision comme dans les publications destinées à la jeunesse. La plupart des textes relatifs aux plateformes renvoient aux dispositions relatives aux « communications commerciales diffusées sur des services de plateformes » contenues dans la directive 2005/29/CE du Parlement européen et du Conseil[201], qui interdit les pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs, notamment les pratiques trompeuses ou agressives utilisées dans les services liés

199 Dispositions issues de la loi n° 73-1193 du 27 décembre 1973 d'orientation du commerce et de l'artisanat, dite Royer.

200 Il existe aussi l'autorité de régulation professionnelle de la publicité (ARPP) qui est un organisme de régulation professionnelle de la publicité.

201 Directive 2005/29/CE du Parlement européen et du Conseil du 11 mai 2005 relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs dans le marché intérieur et modifiant la directive 84/450/CEE du Conseil et les directives 97/7/CE, 98/27/CE et 2002/65/CE du Parlement européen et du Conseil et le règlement (CE) n° 2006/2004 du Parlement européen et du Conseil (directive sur les pratiques commerciales déloyales).

à la société de l'information. S'agissant du contrôle des contenus, la responsabilité des fournisseurs de services est limitée puisqu'ils ne sont responsables ni de la promotion, ni de la vente, ni de l'organisation.

Le marché de la publicité est quant à lui réglementé par la loi du 29 janvier 1993 dite Sapin qui réserve aux seules agences de médias l'autorisation d'acheter des espaces publicitaires et aux seules régies publicitaires, celle de commercialiser cet espace[202]. Un rapport de novembre 2020 sur la **publicité en ligne** réalisé à la demande du ministre de la culture et du secrétaire d'État chargé du numérique souligne toutefois la complexité du sujet, notamment la difficulté d'appliquer cette législation à la publicité en ligne du fait notamment du caractère instantané des transactions. Il préconise d'aligner les contraintes des acteurs de la publicité en ligne sur celles de la publicité traditionnelle et d'agir tant sur les comportements des plateformes structurantes que sur les sources de leur pouvoir de marché[203]. Le droit de la concurrence peut également constituer un levier efficace pour lutter contre les pratiques déloyales d'opérateurs dont certains disposent, au sein de leur groupe, d'une régie publicitaire (*cf. infra*).

• *Le droit des mineurs et la protection spécifique des influenceurs*

Le droit des mineurs n'est pas une branche autonome du droit mais il est constitué de multiples dispositions qui visent à apporter une protection particulière à cette catégorie plus vulnérable de la population, en fonction de l'âge. Des dispositions ont été prises tant dans le domaine du droit des données personnelles que dans celui de la cybercriminalité pour les protéger des atteintes que les réseaux sociaux peuvent faciliter, mais le législateur a dû également intervenir pour réguler la nouvelle **activité d'influenceurs**[204] pratiquée par certains mineurs et s'adressant souvent à eux. La *loi n° 2020-1266 du 19 octobre 2020 visant à encadrer l'exploitation commerciale de l'image d'enfants de moins de seize ans sur les plateformes en ligne* a permis d'étendre les règles du code du travail applicable aux enfants mannequins, du spectacle et de la publicité aux employeurs dont l'activité consiste « *à réaliser des enregistrements audiovisuels (…) en vue d'une diffusion à titre lucratif sur un service de plateforme de partage de vidéos* »[205]. Ne sont concernées par ces règles que les vidéos dont le sujet principal est un mineur de moins de seize ans. Les représentants légaux doivent désormais demander une autorisation individuelle ou un agrément auprès de l'administration et une partie des revenus perçus par leur enfant doit être placée à la Caisse des dépôts et consignations jusqu'à leur majorité ou leur émancipation, sur le modèle applicable aux enfants travaillant dans le spectacle. Des sanctions sont prévues si ces règles ne sont pas respectées. Lorsque la diffusion de vidéos ne se fait pas dans le cadre d'une activité soumis au code du travail mais atteint certains seuils de durée ou occasionne au profit de la personne responsable de la réalisation, de la production ou de la diffusion de ceux-ci, des revenus directs ou indirects supérieurs à un seuil fixé par décret en Conseil d'État, l'activité doit être déclarée. Par ailleurs,

202 Selon cette loi, l'acheteur de la publicité ne peut être revendeur, le contrat entre les deux parties doit indiquer clairement le prix et l'achat doit faire l'objet d'une facture.

203 A. Perrot, M. Emmercih, Q. Jagorel, *Publicité en ligne : pour un marché à armes égales*, novembre 2020.

204 L'influenceur est une personne qui, sur les réseaux sociaux, produit fréquemment des contenus et est suivi par un très grand nombre d'internautes. Certains profitent de cette notoriété pour faire du placement de produits et travaillent pour des marques.

205 Le décret d'application n° 2002-727 est paru le 28 avril 2022.

les plateformes de partage de vidéos sont incitées à adopter des **chartes** notamment pour favoriser l'information des mineurs sur les conséquences de la diffusion de leur image sur leur vie privée ainsi que sur les risques psychologiques et juridiques, en lien avec les associations de protection de l'enfance. L'ARCOM est chargé de promouvoir la signature de ces chartes. Enfin, le texte renforce **leur droit à l'effacement ou à l'oubli**, prévu par la loi Informatique et libertés du 6 janvier 1978. Sur demande directe des intéressés, les plateformes de vidéos doivent retirer leurs vidéos sans que le consentement des parents ne soit exigé.

• *Le droit de la concurrence confronté aux réseaux sociaux*

En France, le droit de la concurrence permet de prévenir et sanctionner des pratiques abusives et anticoncurrentielles d'un opérateur vis-à-vis de ses concurrents. Mis en œuvre sous la houlette de l'Autorité de la concurrence, autorité administrative indépendante qui agit aux côtés de ses homologues européens dans le cadre d'un réseau des autorités de régulation (REC : réseau européen de la concurrence), il compte deux principaux moyens d'actions particulièrement plastiques car s'appliquant de façon transversale, sans limites sectorielles ou techniques : **l'abus de position dominante**[206] (art. L. 420-2 du code de commerce) et la **concentration** mentionnée (art. L. 430-1 à L. 430-10 du code du commerce), qui ont permis de freiner certains excès[207].

Les plus importants réseaux sociaux et entreprises du numérique ont acquis, grâce notamment aux données qu'ils détiennent, aux effets de réseau, à leur expertise technologique, aux économies d'échelle dont ils bénéficient et à certaines pratiques anti-concurrentielle (notamment rachat massif d'entreprises), de très importants **pouvoirs de marché**. Des auteurs invoquent ainsi « *leur stratégie de verrouillage du marché* »[208]. Certaines décisions de l'Autorité de la concurrence française, prononcées notamment dans le domaine de la publicité en ligne[209] – bien que non intervenues dans le domaine spécifique des réseaux sociaux –, ont démontré qu'il était possible de mettre en place des mesures conservatoires[210] et de réprimer significativement des pratiques commerciales abusives rendues possibles par la domination du marché comme la rupture brutale des relations commerciales dans

206 La notion d'abus de position dominante qui permet de saisir une large palette de comportements, qu'il s'agisse d'abus d'exploitation, mais également d'abus d'éviction, s'est avérée particulièrement adaptée pour appréhender les comportements des grandes plateformes et a connu une application renouvelée ces dernières années.

207 Contribution de l'Autorité de la concurrence au débat sur la politique de concurrence et les enjeux numériques, 19 février 2020.

208 J. Toledano, *Gafa, reprenons le pouvoir*, 2020, Odile Jacob.

209 Décision 19-D-26 du 19 décembre 2019 relative à des pratiques mises en œuvre dans le secteur de la publicité en ligne liée aux recherches dite *Google Ads*. L'autorité de la concurrence estime que Google a abusé de la position dominante qu'elle détient sur le marché de la publicité liée aux recherches, en adoptant des règles de fonctionnement de sa plateforme publicitaire *Google Ads* opaques et difficilement compréhensibles et en les appliquant de manière inéquitable et aléatoire. Elle inflige une sanction de 150 M d'euros, et enjoint Google de clarifier la rédaction des règles de fonctionnement de *Google Ads*, ainsi que la procédure de suspension des comptes.

210 Dans l'attente de sa décision au fond, elle a prononcé des mesures d'urgence afin d'obtenir notamment de Google : qu'elle clarifie les règles de *Google Ads* qu'elle entend appliquer aux services payants de renseignements par voie électronique ; et qu'elle réexamine la situation d'Amadeus (décision 19-MC-01 du 31 janvier 2019) au regard de ces nouvelles règles en vue de lui redonner accès, le cas échéant, au service *Google Ads* si ces annonces y sont conformes.

des conditions peu transparentes et objectives ou l'application discriminatoire de règles de fonctionnement[211]. La Commission européenne, pour sa part, dans ses fonctions de gardienne de la concurrence au niveau de l'Union, a pris des décisions historiques en infligeant par exemple à Google une amende de 2,42 milliards d'euros pour abus de position dominante de son moteur de recherche, estimant qu'il donnait un avantage illégal à son propre service de comparateur commercial[212].

Pour autant les grilles d'analyse du droit de la concurrence se sont révélées, en raison notamment du caractère multi-face, évolutif et congloméral des plateformes et de la « gratuité » de certaines prestations, souvent peu adaptées ou difficiles à mobiliser rapidement et efficacement, dans un secteur en évolution rapide et où l'efficacité suppose la célérité[213]. Les opérations de fusion-acquisition d'acteurs innovants ou n'ayant pas encore monétisé leur innovation par les géants du numérique ont ainsi, par exemple, pu échapper au contrôle des autorités de concurrence. En effet, la valeur n'est, dans ce cas, pas reflétée par le chiffre d'affaire naissant et les seuils de notification ne sont souvent pas franchis. La notion de ***marché pertinent*** est aussi apparue difficile à manier dans ce contexte. Ainsi, alors même que WhatsApp ne générait que des revenus faibles à l'époque, elle a été rachetée par Facebook pour 19 milliards de dollars et le rachat n'a pas été considéré comme un abus de position dominante.

L'exemple de l'examen du rachat de WhatsApp par Facebook

Lorsque la Commission européenne a examiné le rachat de WhatsApp par Facebook, elle a réalisé son appréciation par rapport à trois marchés pertinents identifiés : les services de communications grand public, les services de réseaux sociaux et les services de publicité en ligne. Elle a ainsi constaté qu'ils n'étaient pas des concurrents proches sur le marché de la communication grand public, les applications étant souvent utilisées de façon cumulative par les utilisateurs. Elle a estimé que WhatsApp n'était pas un réseau social au même titre que Facebook, les fonctionnalités offertes étant bien moins importantes. Enfin, sur le marché de la publicité en ligne, elle a constaté que malgré cette fusion, le nombre de fournisseurs de publicité ciblée demeurera important. Par cette approche essentiellement statique et non dynamique du marché, qui ne prend pas en compte l'accroissement de l'accès au marché par l'effet de réseau et le transfert sur les marchés latéraux de ces entreprises, la puissance concurrentielle ne pouvait pas être correctement appréciée. Sans tomber dans l'écueil d'une approche trop large, les critères d'appréciation classiques semblent souvent difficiles à manier. Le DMA vise à apporter une réponse à ces difficultés.

211 *Google Amadeus*, décision 19-MC-01 du 31 janvier 2019 ; ·*Google News Corp*, décision 21-D-11 du 7 juin 2021.

212 Not. *Moteur de recherche Google Shopping*, Aff. AT. 39740. Le 27 juin 2017, la Commission inflige à Google une amende de 2,42 milliards d'euros pour abus de position dominante de son moteur de recherche qui donne un avantage illégal à son propre service de comparateur commercial (Google Shopping). Google accorde dans son moteur de recherche un traitement préférentiel à son propre site de comparaison, *Google Shopping*.

213 Rapport d'information sur les plateformes numérique, Assemblée nationale, Commission des affaires économiques n° 3127 ; rapport d'information sur le DMA, Assemblée nationale n° 4409, juillet 2021 ; rapport d'information sur le DMA, Sénat, n° 34, octobre 2021.

Si l'inadaptation des critères de contrôles, la longueur des procédures[214] et le caractère insuffisamment dissuasif des sanctions ont fini de convaincre les plus réticents de la nécessité de mettre en place d'un système complémentaire de régulation *ex ante* (DMA), il n'exclut pas la **modernisation du droit de la concurrence** pour mieux appréhender le secteur numérique[215].

Ce changement est à l'œuvre en France, même s'il demeure encore plus timide qu'en Allemagne qui a montré la voie du DMA en adoptant une législation novatrice en janvier 2021.

• *Le droit des données personnelles et de la protection de la vie privée stimulé par les réseaux sociaux*

Le RGPD, texte de référence pour la protection des données personnelles, a fixé un cadre de protection concernant la collecte et l'utilisation des données personnelles et une organisation institutionnelle au niveau européen. Il consacre un **droit à la protection des données à caractère personnel** c'est-à-dire de la protection des informations qui sont propres à l'individu et permettent de l'identifier. Il exige que les données soient traitées de **façon loyale, licite et transparence**, et contient cinq grands principes qui sont **le principe de finalité** (le responsable d'un traitement ne peut enregistrer et utiliser des informations sur des personnes physiques que dans un but précis, légal et légitime), **le principe de proportionnalité et de pertinence** (à savoir que les informations enregistrées doivent être pertinentes et strictement nécessaires au regard de la finalité du fichier), **le principe de limitation notamment de la durée de conservation** (une durée précise doit être fixée et dépend du type d'information enregistrée et de la finalité du traitement), **le principe de sécurité et de confidentialité** (le responsable du traitement doit garantir cela et veiller à ce que l'accès soit réservé aux seules personnes autorisées) et plus généralement le **principe de responsabilité** qui permet notamment la protection et la mise en œuvre des droits des personnes concernées**.**

Lorsque le consentement est le fondement légal du traitement, chaque individu doit consentir à ce que ses données personnelles soient utilisées et conservées pour **une finalité déterminée, explicite et légitime** et peut s'y opposer à tout moment[216]. Outre ce droit d'opposition, il bénéficie du droit à la transparence des informations et des modalités d'exercice de ses droits, le droit d'accès à ses données, le droit à rectification, le droit à l'effacement[217] et le droit à la portabilité des données ; mais tous ces droits ne bénéficient pas de la même effectivité en pratique[218].

214 Affaire AT. 39740, *Moteur de recherche Google Shopping*.

215 Contribution de l'Autorité de la concurrence au débat sur la politique de concurrence et les enjeux numériques, 19 février 2020.

216 Le droit d'opposition a pour corollaire la protection de la vie privée prévue et sanctionnée par l'art. 9 du code civil et par les art. 226-1 du code pénal.

217 Ce droit est souvent confondu avec le droit à l'oubli qui concerne en réalité le droit au déréférencement opposable à un moteur de recherche et qui a été consacré par la CJUE dans le célèbre arrêt Google Spain du 14 mai 2014 et placé sous l'égide du RGPD dans les arrêts du 24 sept.2019 (C 136/17 et C 507/17)

218 N. Martial-Braz, « Le renforcement des droits de la personne concernée », *Dalloz* IP/IT, 2017, p. 253.

-- Les réseaux sociaux, responsables de traitement

Le RGPD s'applique à toute organisation, publique et privée, qui traite des données personnelles[219] pour son compte ou non, dès lors qu'elle est établie sur le territoire de l'Union européenne, ou que son activité cible directement des résidents européens. Le RGPD concerne aussi les sous-traitants qui traitent des données personnelles pour le compte d'autres organismes. Parce qu'ils réalisent des opérations appliquées à ces données, les **réseaux sociaux** sont des **responsables de traitement de données**. Parfois cette responsabilité est partagée. Ainsi la CJUE a-t-elle jugé l'administrateur d'une page *fan* sur Facebook, responsable conjoint du traitement de données avec le réseau[220]. De même le gestionnaire d'un site internet équipé du bouton « j'aime » de Facebook est-il conjointement responsable avec Facebook de la collecte et de la transmission à Facebook des données à caractère personnel des visiteurs de son site (en excluant sa responsabilité pour le traitement ultérieur de ces données par Facebook seule)[221].

-- Les données recueillies par les réseaux sociaux

Les données personnelles sont, comme il a été dit plus haut, le **carburant des réseaux sociaux**. Ces derniers fonctionnent grâce et à partir des données personnelles de leurs utilisateurs. Ces derniers, dès l'ouverture de leur compte puis à travers les discussions et contenus qu'ils partagent avec les autres internautes, alimentent les réseaux en informations sur leurs goûts, leurs opinions et leurs comportements qui constituent des réserves inépuisables de données personnelles. Outre les **données qui sont directement fournies par l'utilisateur ou par les tiers** (*cookies*) et **celles qui sont observées** (par exemple une page *likée*), existent des données qui sont déduites des différentes informations dont dispose le réseau. On parle de **données « inférées »**. Ces dernières sont particulièrement sensibles car elles permettent notamment de réaliser du profilage. Ainsi la majorité des données analysées par Facebook ne sont pas celles que l'on publie spontanément, mais celles qui ressortent de nos activités (*cf.* la politique d'utilisation des données de Facebook[222]). Une question préjudicielle importante a été renvoyée récemment par *l'Oberlandesgericht Düsseldorf* à la Cour de justice de l'UE. La question est de savoir si les données recueillies par les *modules sociaux* (*like*, *retweet*, etc.) lors

219 art. 9 du RGPD.

220 CJUE, 5 juin 2018, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c/ Wirtschaftsakademie Schleswig-Holstein GmbH*, C 210/16. L'administrateur d'une page *fan* sur Facebook offre à cette société la possibilité de placer des cookies sur l'ordinateur ou tout autre appareil de la personne ayant visité sa page fan, que cette personne dispose ou non d'un compte Facebook. En cela, l'administrateur de la page fan participe à la détermination des moyens et des finalités statistiques du traitement et doit être considéré comme responsable conjoint du traitement (csdt 35).

221 CJUE, 29 juillet 2019, *Fashion ID GmbH & Co. KG/Verbraucherzentrale NRW eV*, aff. C-40/17.

222 Les données analysées par Facebook sont : les contenus publics (texte, image, vidéo) que l'on diffuse sur la plateforme ; les messages privés envoyés sur Messenger (qui dit quoi, à qui, quand, à quelle fréquence) ; la liste des personnes, pages et groupes que l'on suit ou « aime », ainsi que la manière dont on interagit avec ; la façon dont on utilise le service et accède aux contenus (les articles, photos et vidéos qu'on lit, commente ou « aime », à quel moment, à quelle fréquence et pendant combien de temps) et les informations sur l'appareil depuis lequel on accède au service (adresse IP, identifiant publicitaire de l'appareil, nom des applications, fichiers et *plugins* présents sur l'appareil, mouvements de la souris, points d'accès Wi-Fi et tours de télécommunication à proximité, accès à la localisation GPS et à l'appareil photo).

de la navigation de l'internaute sur des sites tiers particulièrement susceptibles de générer de telles données (sites médicaux, de rencontre, etc.) doivent être qualifiées de « *données sensibles* » au sens du RGPD[223]. Une telle qualification emporterait un régime très protecteur et strict. Cette affaire révèle l'enjeu de ces fonctionnalités sociales étendues qui peuvent conduire les utilisateurs à confier à un réseau social des données personnelles qu'ils n'auraient jamais spontanément diffusé sur le service lui-même.

-- *La base légale du traitement*

Pour répondre à leurs obligations, il incombe aux responsables de traitement de s'assurer de la **conformité** de leur politique de gestion des données personnelles avec les règles du RGPD. Dans ce cadre, la **première obligation** est de s'assurer de la **licéité du traitement**. Le RGPD prévoit six fondements possibles pour qu'un traitement de données soit licite[224] mais, s'agissant des réseaux sociaux, seuls trois sont adaptés : le *consentement au traitement*, la *nécessité contractuelle* ou *l'intérêt légitime*. S'agissant du fondement de **la nécessité contractuelle** (le traitement des données est nécessaire pour fournir le service), il ne peut pas être mobilisé pour justifier d'un traitement sur les données inférées et observées car ce n'est pas dans l'objet du contrat : il n'est donc pas mobilisable. S'agissant de **l'intérêt légitime,** il pourrait être mobilisé si les plateformes reconnaissaient que le traitement est réalisé dans un but économique pour réaliser de la publicité ciblée et rendre l'accès au réseau « gratuit » pour l'internaute, mais cela supposerait que cet intérêt soit jugé supérieur à celui de protéger la vie privée de l'utilisateur, ce qui est douteux[225]. Ainsi, le *consentement* apparait comme la base légale de traitement des données la plus solide. Elle est, de fait, la plus utilisée. Pour que le traitement soit licite, celui-ci doit alors être **libre, spécifique, éclairé et univoque**[226]. En outre, il doit être valable. En France, les enfants de moins 15 ans ne peuvent consentir seuls au traitement de leurs données.

Dans la plupart des litiges, la question cruciale est souvent celle de la **portée du consentement** donné par l'utilisateur. La jurisprudence exige que l'utilisateur soit préalablement correctement informé sur les différentes finalités et sur l'ampleur du traitement. Le consentement donné doit être univoque et ne peut ni être recueilli au moyen d'une case cochée par défaut ni dans le cadre de l'acceptation globale des conditions générales d'utilisation[227]. Dans les faits, il est souvent difficile de démontrer que l'internaute a consenti de façon éclairée – et dans les conditions précitées – à l'utilisation de ses données personnelles à des fins publicitaires. Cette preuve, très difficile à rapporter, est une arme potentielle pour les utilisateurs.

Le 16 mai 2017, **la CNIL a condamné Facebook** à 150 000 euros d'amende (montant maximal à l'époque) pour avoir réalisé ses traitements sans base légale estimant que « *l'objet principal du service est la fourniture d'un réseau social […], que la combinaison des données des utilisateurs à des fins de ciblage publicitaire ne correspond ni à l'objet principal du contrat ni aux attentes raisonnables des*

223 CJUE-252/21 Meta Platforms et autres.
224 Art. 6 du RGPD.
225 Conclusions A. Lallet. CE, 19 juin 2020, n° 430810 et CE, 10 décembre 2020, n° 429571.
226 CJUE arrêt 673/17 du 1er octobre 2019.
227 CE, 19 juin 2020, n° 430810.

utilisateurs [et qu'il incombe donc à Facebook] de veiller à ce que les droits des personnes concernées soient respectés et notamment à ce que l'exécution d'un contrat ne les conduise pas à y renoncer ». Ainsi, la CNIL « *estime que les sociétés ne peuvent se prévaloir du recueil du consentement des utilisateurs [ni] de la nécessité liée à l'exécution d'un contrat* ».

Le 28 mai 2018, soit 3 jours à peine après l'entrée en vigueur du RGPD, la Quadrature du net a déposé 5 plaintes contre les GAFAM (Google, Apple, Facebook, Amazon et Microsoft) devant la CNIL, reprochant notamment à Facebook d'analyser sans base légale les contenus et les comportements à partir des données personnelles des utilisateurs (à des fins de publicité ciblée). Pour cette association, ni la nécessité contractuelle (le bon emploi du réseau social n'étant pas conditionné à une telle activité), ni le consentement, qui n'a pas été recueilli conformément aux exigences légales, ne peuvent donner une base légale au traitement. Hormis celle contre Google[228], ces plaintes sont toujours en cours devant l'autorité de protection des données irlandaise.

-- L'information de l'utilisateur

La plupart des informations relatives au traitement des données personnelles des réseaux sociaux figurent dans un document intitulé « **politique de confidentialité** » qui sont parfois reproduites dans les **conditions générales d'utilisation**. Y sont précisées la nature des données collectées, les conditions d'utilisation, et la finalité de la collecte[229]. Le plus souvent, ces documents précisent que les données sont collectées pour améliorer le service offert, les prestations au service de l'utilisateur et vérifier la bonne utilisation du réseau. Ils précisent aussi que certaines informations analysées sont déduites (données inférées) à des fins publicitaires ou commerciales. Tiktok explique ainsi : « *Nous déduisons vos attributs (tranche d'âge, genre) et vos intérêts sur la base des informations dont nous disposons à votre sujet. Nous utilisons les inférences pour, par exemple, assurer la sécurité de la Plateforme, la modération du contenu et lorsque cela est autorisé, pour vous proposer des publicités personnalisées en fonction de vos intérêt*s. »

-- L'acceptation des cookies

La question de la portée du consentement donné par l'utilisateur à l'usage de ses données personnelles intéresse également la législation sur les ***cookies*** bien que le cadre juridique et la portée du consentement soient différents[230]. Les *cookies*

228 *Le Monde*, site internet, 21 janvier 2019, « Données personnelles : la CNIL condamne Google à une amende record de 50 millions d'euros » : Google est condamné pour ne pas informer suffisamment ses utilisateurs et les contraindre à consentir en bloc pour toutes les finalités poursuivies par Google.

229 Ainsi par ex., le réseau social Snapchat, distingue, dans ses CGU trois types de données qui sont collectées : les informations directement fournies par l'utilisateur, notamment lors de la création du compte (nom, mot de passe, adresse mail, numéro de téléphone, date de naissance, etc.) ; les informations obtenues lorsque les services sont utilisés (données relatives à la façon dont sont utilisés les services, informations relatives au contenu posté, données relatives à l'appareil utilisé - modèle du téléphone, applications installées, type de navigateur, niveau de la batterie, adresse IP, infirmations sur les connexions réseau mobile etc. -, répertoire téléphonique de l'appareil - avec autorisation -, photos du téléphone, localisation, informations recueillies par les *cookies*, etc.) et les informations obtenues par des tiers (informations recueillies auprès des autres utilisateurs, des filiales ou de tiers).

230 Le cadre juridique des traceurs est fixé par la directive *e-privacy* transposée l'art. 82 de la loi informatique et libertés.

doivent être expressément acceptés par les utilisateurs, sauf s'ils sont strictement nécessaire au fonctionnement du site ou de l'application. L'éditeur du site doit s'assurer de ce consentement y compris s'il s'agit de *cookies* tiers dans les conditions définies par la loi[231]. La question se pose régulièrement de savoir si le consentement a été pleinement et librement donné. Le Conseil d'État a été plusieurs fois conduit à préciser les conditions d'un consentement éclairé s'agissant notamment des informations à donner sur l'identité du responsable de traitement, la liste des destinataires ou la catégorie des destinataires de ses données[232]. La CNIL a reçu plusieurs plaintes concernant les modalités de refus des *cookies* sur les sites web google.fr et youtube.com. A la suite de contrôles, elle a constaté que, s'ils proposent un bouton permettant d'accepter immédiatement les *cookies*, ces sites ne mettent que rarement en place de solution équivalente (bouton ou autre) pour permettre à l'internaute de refuser aussi facilement le dépôt des *cookies*, plusieurs clics étant nécessaires pour refuser tous les *cookies*, contre un seul pour les accepter. L'autorité de régulation a estimé que ce procédé portait atteinte à la liberté de consentement des internautes et a condamné Google à une amende de 150 millions d'euros[233]. Afin de rappeler et d'expliciter le droit applicable au dépôt et à la lecture de traceurs dans le terminal de l'utilisateur, la CNIL a adopté le 17 septembre 2020 des lignes directrices, complétées par une recommandation visant notamment à proposer des exemples de modalités pratiques de recueil du consentement[234]. Le nouveau règlement *e-privacy* devrait apporter des réponses à ces sujets.

-- L'utilisation des données par des tiers

La question s'est posée de savoir dans quelle mesure les données personnelles des internautes figurant notamment sur les réseaux sociaux peuvent être **exploitées par des tiers** et notamment par **l'État**.

Le Conseil constitutionnel a eu l'occasion de se prononcer sur cette question du *scraping* des données (*cf.infra*)

L'exploitation illicite de données par des tiers peut donner lieu à des sanctions pénales[235] ou administratives. Dans l'affaire dite des *Pages jaunes*, était contestée une sanction infligée par la CNIL au gestionnaire du service d'annuaire « Pages Blanches » : le Conseil d'État a confirmé la sanction prononcée par la CNIL à l'encontre de la société qui proposait une fonctionnalité permettant d'ajouter aux résultats de recherche obtenus sur une personne déterminée, des données à caractère personnel la concernant collectées sur les réseaux sociaux[236].

La conservation des données personnelles par les réseaux sociaux

Les données personnelles ne peuvent pas être **conservées** indéfiniment par les réseaux sociaux mais l'appréciation de la durée et de la nature des données concernées est d'autant plus délicate que la poursuite des auteurs d'infractions nécessite une conservation longue.

231 CE, 6 juin 2018, *n° 412589*.
232 CE, 19 juin 2020, *n° 434684*.
233 Sanction confirmée par le Conseil d'État (CE, 19 juin 2020 n° 430810).
234 Elles ont été censurées partiellement par le Conseil d'État (CE, 19 juin 2020).
235 Sur la collecte déloyale de données nominatives : CCass., crim., 14 mars 2006, n° 05-83.423, Bull;
236 CE, 12 mars 2014, n° 353193, T.

Le RGPD prévoit que les données à caractère personnel peuvent être conservées sous une forme permettant l'identification des personnes physiques pour une durée fixée en fonction des **finalités** du traitement, qui doit être **nécessaire** et **proportionnée**. Cette durée de conservation relève de **l'analyse de conformité** que le responsable doit mener pour son traitement. La plupart du temps, la durée n'est pas fixée par un texte. Les responsables de traitement fixent eux-mêmes le temps de conservation mais doivent garantir les droits des personnes physiques dont les données font l'objet du traitement, notamment le **droit à l'effacement des données**. Il appartient alors au responsable du fichier de la déterminer en fonction de la finalité du traitement[237]. Par ailleurs, la *directive Police-Justice* du 27 avril 2016 a instauré, avant même le RGPD, l'obligation **pour les responsables de traitement de données de déterminer les finalités qui justifieraient la conservation des données et l'obligation de proportionner cette durée.** Toujours applicable, elle fournit une liste des motifs de droit pénal pouvant justifier cette conservation longue et généralisée à tout type de données. Enfin le code des postes et des communications électroniques **oblige** les opérateurs de communication, les hébergeurs et les FAI (fournisseurs d'accès à internet) **à conserver l'ensemble des données de trafic et de localisation de leurs utilisateurs**

La question de la conservation généralisée et indifférenciée des données de connexion imposée aux opérateurs en France a donné lieu à des contentieux. SI la **CJUE** prohibe une conservation généralisée et indifférenciée des données de connexion imposée aux opérateurs (autres que les données d'identité) sauf exception limitée pour des motifs liés à la « *sauvegarde de la sécurité nationale* », et si l'État « *fait face à une menace grave, (…) réelle et actuelle ou prévisible* » (CJUE 6 oct. 2020), le **Conseil d'État**, par une décision de l'Assemblée du contentieux du 21 avril 2021 (n° 393099) juge la conservation généralisée des données justifiée par l'existence d'une menace terroriste remplissant les conditions posées par l'arrêt de la CJUE, tout précisant que le Gouvernement devra procéder à un réexamen périodique de cette menace pour la sécurité nationale. Le **Conseil constitutionnel**, pour sa part, a récemment jugé contraire à la Constitution, comme portant atteinte à la vie privée, un texte imposant aux opérateurs de communications électroniques la conservation générale et indifférenciée des données de connexion, sans la réserver à la recherche des infractions les plus graves ni la subordonner à l'autorisation ou au contrôle d'une juridiction ou d'une autorité indépendante[238]. Le 5 avril 2022, par un arrêt de grande chambre (*Commissionner of the Garde Siochana e.a*, C140/20), la **CJUE** a confirmé que le droit de l'Union s'oppose à une conservation généralisée et indifférenciée des données relatives au trafic et à la localisation afférentes aux communications électroniques même aux fins de lutte contre les infractions graves.

237 Art. R. 10-13 du code des postes et des communications électroniques et le décret du 25 février 2011, pris respectivement pour l'application de l'art. L. 34-1 du même code et de l'art. 6 de la loi du 21 juin 2004.

238 Décision n° 2021-976/977 QPC du 25 février 2022.

-- Le transfert des données

Les réseaux sociaux sont également tenus de respecter les règles du RGPD s'agissant du **transfert de données**. Ce règlement prévoit que le transfert de données en dehors de l'UE ne peut avoir lieu que dans un pays bénéficiant **d'un niveau de protection adéquat de ses données**, celui-ci étant constaté par la Commission. A défaut, un tel transfert ne peut être réalisé que si l'exportateur et l'importateur démontrent que l'importateur établi hors UE prévoit des garanties appropriées. Dans un arrêt désormais célèbre dit *Shrems II*[239] la CJUE a invalidé la décision 2016/1250 de de la Commission relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États Unis au motif que la réglementation interne des États Unis portant sur l'accès et l'utilisation par les autorités publiques américaines de données à caractère personnel transférées depuis l'UE n'est pas encadrée d'une manière à répondre à des exigences substantiellement équivalentes à celles requises, en droit de l'Union, à l'article 52, paragraphe 1, seconde phrase, de la Charte. La Commission européenne a adopté ne le 4 juin 2021 de nouvelles **clauses contractuelles types mais le CEPD préconise l'adoption de mesures complémentaires** (comme des mesures de chiffrement renforcé et/ou de mesures de pseudonymisation des données, la documentation et l'enregistrement des demandes d'accès des autorités publiques, etc.). Il est préconisé d'apprécier au cas par cas, en pratique et pour le transfert envisagé, si ces clauses contractuelles types permettent d'assurer aux données transférées un niveau de protection essentiellement équivalent à celui assuré en Union européenne. Une partie importante de la doctrine estime cependant que ces clauses n'épuisent pas les difficultés[240]. La Commission et les États Unis ont réalisé une déclaration conjointe le 25 mars 2022 affirmant être sur la voie d'un « *Privacy Shield 3* ». À la suite l'arrêt *Shrems II*, la commission irlandaise de protection des données à décider d'ouvrir une enquête afin de vérifier si les transferts de données opérés par Facebook respectent le RGPD, notamment à la lumière de la décision *Schrems II* et a émis une ordonnance provisoire (*Preliminary Draft Decision*, 28 août 2020). Facebook a contesté cette décision devant la *High Court of Justice* irlandaise. La Cour a rejeté le recours de Facebook dans un arrêt du 14 mai 2021. L'enquête relative à la plainte de M. Schrems de décembre 2015 saisissant l'autorité irlandaise d'une plainte contre Facebook au motif que ce réseau transfère illicitement des données personnelles aux États Unis se poursuit donc.

Le rachat de WhatsApp par Facebook (suites)

Le droit des données personnelles a été utilisé par les autorités italiennes et la Commission européenne pour condamner **le transfert de données** de WhatsApp vers Facebook à la suite du rachat par ce dernier. En effet, dans le cadre de son contrôle des concentrations, Facebook avait informé la Commission européenne qu'elle ne serait pas en mesure de synchroniser les numéros de téléphone des utilisateurs de WhatsApp avec les profils Facebook de ces derniers et que, par conséquent, il n'y aurait pas de recoupement de données sans le consentement

239 CJUE, 16 juillet 2020, *Data Protection Commissioner c/ Facebook Ireland Ltd et Maximillian Schrems,* C 311/18 (Schrems II).

240 J.-L. Sauron, « Le tohu-bohu de l'arrêt Shrems II : l'Union européenne pourra-t-elle sortir de l'impasse dans laquelle elle s'est elle-même placée ? », *DPONews*, Ed. Anthémis

de leurs titulaires. Or, en août 2016, WhatsApp a annoncé, lors d'une mise à jour de ses Conditions Générales d'Utilisation, qu'elle allait désormais associer les numéros de téléphone des utilisateurs de WhatsApp aux profils d'utilisateur de Facebook.

La Commission a donc constaté que, contrairement à ce qu'avait déclaré Facebook en 2014 dans le cadre de la procédure de contrôle des concentrations, la possibilité technique de mettre en correspondance les identités des utilisateurs de Facebook et de WhatsApp existait déjà cette année-là et que les employés de Facebook étaient au courant de cette possibilité. Elle a prononcé une amende pour informations trompeuses portant sur les transferts de données, emboîtant le pas à l'autorité de la concurrence italienne qui avait précédemment condamné Facebook à la même sanction pour des faits similaires.

Par la suite, l'autorité de protection des données personnelles irlandaises (chef de file), après un avis du comité européen du 28 juillet 2021, a prononcé à l'encontre de Facebook une amende de 225 millions d'euros le 2 septembre 2021, pour violation du RGPD et, en particulier, à cause du manque de transparence concernant le partage des données des utilisateurs avec les autres entités de Facebook (méconnaissance de l'article 13 du RGPD)[241].

Il incombe enfin aux responsables de traitement de **signaler tout problème** aux autorités de contrôle. Twitter a ainsi été reconnu responsable par le CEPD le 9 novembre 2020 pour ne pas avoir notifié à l'autorité de contrôle une violation des données personnelles ayant eu lieu à la suite d'un changement de code de la plateforme[242].

1.2.2.3. La fabrication continue du droit : les textes européens en cours d'adoption

Pour parfaire la construction d'un droit européen du numérique qui favorise l'innovation et la croissance d'entreprises européennes, plusieurs textes sont en cours d'adoption dont certains qui auront des impacts forts sur le domaine des réseaux sociaux.

Si le début de l'année 2022 a été fructueux avec **l'adoption du DSA et du DMA**, d'autres textes significatifs, qui s'inscrivent dans la politique dynamique de l'Union européenne sur le numérique, sont en cours de négociation au niveau européen[243].

Leur utilité n'est pas contestée mais leur nombre peut faire craindre un mille-feuille normatif peu digeste.

241 Cette intersection entre droit de la concurrence et droit des données personnelles est assez fréquente. *Cf.* une décision de la Federal Trade Commission (FTC), dans sa décision C-4365 du 27 juillet 2012, modifiée et complétée par sa décision du 27 avril 2020, qui constitue une forme de « mini-RGPD » américain imposé par le régulateur à Facebook et qui prend également en compte en son point III la possibilité d'un accès aux données initialement rendues publiques par un utilisateur par des tiers.

242 CEPD, 9 novembre 2020, Décision 01/2020 concernant le litige relatif au projet de décision de l'autorité de contrôle irlandaise concernant Twitter International Company en application de l'art. 65, paragraphe 1, point a), du RGPD :

243 Commission européenne, Façonner l'avenir numérique de l'Europe et La Commission présente une déclaration sur les droits et principes numériques au bénéfice de tous dans l'Union.

L'*Artificial intelligence Act* vise à instaurer le premier cadre juridique sur l'intelligence artificielle pour assurer la sûreté des systèmes d'IA mis sur le marché de l'Union européenne et le respect des droits fondamentaux, garantir la sécurité juridique pour faciliter l'innovation ; faciliter le développement d'un marché unique pour des applications d'IA légales, sûres et dignes de confiance. Ce texte intéresse directement les réseaux sociaux puisque ces derniers utilisent l'IA pour les classements de contenus et leurs modérations. A cet égard, la proposition prévoit d'interdire quatre pratiques particulièrement sensibles, qu'elles soient ou non intentionnelles : la manipulation mentale, l'abus de faiblesse, le crédit social et l'identification biométrique en temps réel dans les lieux publics. Il prévoit par ailleurs de subordonner la mise sur le marché des systèmes d'IA à plusieurs obligations imposées au fournisseur du système tout en proportionnant les exigences à la taille de l'organisation de ce fournisseur (mise en place d'un système de gestion des risques, respect de standard de qualité pour l'utilisation des données d'apprentissage, contrôle humain, respect d'exigence d'exactitude, de robustesse et de cybersécurité, etc.). Le principe de base est que le règlement IA s'appliquerait sans préjudice du RGPD et de la directive police-justice, c'est-à-dire que les deux corps de règles s'appliqueraient cumulativement aux fournisseurs et utilisateurs dès lors que les SIA peuvent être qualifiés de traitements de données à caractère personnel[244]. Le manquement à ces obligations pourra donner lieu à des sanctions administratives significatives. La proposition prévoit la création d'un **comité européen de l'intelligence artificielle** réunissant les autorités de contrôle nationales et le Contrôleur européen de la protection des données[245].

Le **règlement *e-privacy*** remplacera la directive 2002/58/CE du 12 juillet 2002 dite directive *e-privacy*. Il permettra de prendre en compte les nouveaux services sur internet qualifiés de services de communication par contournement (services « OOT ») comme la voix sur IP[246], le courrier électronique web et la messagerie instantanée, qui ne sont pas régulés dans le cadre européen des communications électroniques, d'éviter les divergences d'interprétation (le règlement étant directement applicable) et de mettre en place les conditions d'une concurrence stable.

---

244 Mais, d'une part, il est prévu que les opérations de "débiaisement" des SIA peuvent justifier le traitement de données sensibles, sous réserve d'apporter des garanties appropriées (limitations techniques à la réutilisation, pseudonymisation et cryptage…) et, d'autre part, la Commission propose de créer un cadre sécurisé pour le développement, la mise à l'essai et la validation de SIA innovants avant mise en service, dénommé "bacs à sable réglementaires", qui permettraient de traiter à cette fin des données à caractère personnel collectées à d'autres fins.

245 Elle comporte en outre des règles concernant la désignation des autorités nationales compétentes pour assurer la mise en œuvre du règlement. La notion d'"autorité nationale compétente" renvoie à trois autorités : l'autorité de contrôle nationale chargée de la mise en oeuvre et de l'application du règlement, de la coordination des activités de l'État membre, du rôle de point de contact unique pour la Commission (elle doit notamment assurer la synthèse et la transmission à la Commission des résultats des activités de surveillance du marché) et de la représentation de l'État membre au sein du comité européen de l'IA ; l'autorité notifiante qui accrédite et évalue les organismes notifiés, chargés de procéder à l'évaluation de la conformité des SIA à haut risque avec le règlement, l'autorité de surveillance du marché chargée du bon fonctionnement du marché.

246 « *Toute représentation numérique d'actes, de faits ou d'informations et toute compilation de ces actes, faits ou informations, notamment sous la forme d'enregistrements sonores, visuels ou audiovisuels* »

Le ***Média Freedom Act*** vise à soutenir la relance et la transformation des secteurs des médias et de l'audiovisuel de l'Union européenne (dans un domaine habituellement régi par les droits des pays membres). Dans sa prise de position, l'ARCOM demande que le futur texte puisse inclure les plateformes en ligne, y compris lorsqu'elles n'ont pas, ou pas entièrement, la responsabilité éditoriale du contenu auquel elles donnent accès afin qu'elles contribuent aux « *mêmes objectifs généraux que les médias* » et qu'une concurrence équitable soit assurée.

Le ***Data Gouvernance Act*** qui vise à mettre en place un marché unique des données, celles-ci étant entendues comme « *toute représentation numérique d'actes, de faits ou d'informations et toute compilation de ces actes, faits ou informations, notamment sous la forme d'enregistrements sonores, visuels ou audiovisuels* ». Le nouveau cadre européen aura pour objet de faciliter le partage et la réutilisation des données dont les acteurs européens ont besoin pour être en mesure de concurrencer efficacement leurs concurrents, notamment américains ou chinois, et développer des applications innovantes dans des secteurs stratégiques (santé, transport, énergie, etc.). Ce texte doit non seulement garantir la confiance en fournissant un cadre juridique européen de partage des données mais aussi proposer une base technique pour encourager la circulation des données entre entreprises ainsi qu'entre entreprises et administrations publiques.

Enfin, une proposition de règlement visant à prévenir et à combattre les abus sexuels sur les mineurs[247] a été publiée le 11 mai 2022 par la Commission européenne.

Pour mettre en œuvre l'ensemble de ces règles de droit, de multiples autorités de régulation interviennent. Ainsi la fragmentation matérielle du droit des réseaux sociaux se double mécaniquement d'une fragmentation organique.

1.2.3. La fragmentation organique

Par son aspect multi-face, la régulation des réseaux sociaux implique, outre différents juges (juge civil, juge pénal, juge administratif, juge européen), de nombreuses autorités administratives. Et, en raison de sa forte dimension européenne, de nombreux régulateurs européens sont aussi concernés. En France, quatre autorités de régulation et un service de l'État interviennent principalement dans la régulation des réseaux sociaux. Ils sont tous en lien avec les services européens et les autorités de régulation des États membres.

- **l'ARCOM (autorité de régulation de la communication audiovisuelle et numérique)** née de la fusion du Conseil supérieur de l'audiovisuel[248] (CSA) et de la Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet (Hadopi[249]) a été mise en place le 1er janvier 2022 pour réguler la

247 Commission européenne, proposition de réglement du Parlement européen et du Conseil établissant des règles en vue de prévenir et de combattre les abus sexuels sur enfants, 11 mai 2022.

248 Le CSA avait à l'origine quatre fonctions : affecter les fréquences aux opérateurs hertziens et conventionner les services non-hertziens ; négocier avec chaque acteur privé un cahier des charges ; désigner les présidents des entreprises audiovisuelles publiques ; surveiller le respect des obligations et engagements.

249 *Cf.* 1.2.3 sur la Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet

communication audiovisuelle et numérique. Elle est notamment chargée de la régulation systémique des plateformes ayant une activité d'intermédiation en ligne, telles que les plateformes de partage de vidéo, les **réseaux sociaux**, les moteurs de recherche, les agrégateurs et les magasins d'application. En matière de lutte contre la manipulation de l'information, la loi du 22 décembre 2018 lui a confié un rôle de supervision et de recommandation aux plateformes qui doivent rendre accessible et visible leur dispositif de signalement et déployer des mesures complémentaires, notamment en faveur de la transparence de leurs algorithmes. Depuis août 2021, les plateformes ont également des obligations de moyens et de transparence en matière de lutte contre la haine en ligne, et s'exposent à des sanctions prononcées par l'ARCOM si elles ne les respectent pas. La mise en œuvre du DSA modifiera ses cadres d'intervention notamment en soustrayant les très grandes plateformes de son contrôle direct mais certaines attributions, complémentaires au DSA, subsisteront. L'ARCOM héberge en son sein l'**observatoire de la haine en ligne**, instauré par la loi dite Avia » de 2020 qui réunit des chercheurs, des associations, des opérateurs et des administrations. Elle publie chaque année un rapport examiné ensuite au Parlement, dans une approche « *name and shame* »[250]. A été également constitué en son sein un Comité d'experts sur lutte contre la désinformation en ligne. Elle peut émettre des recommandations[251]. L'ARCOM participe au **groupe des régulateurs européens de médias audiovisuels (ERGA**[252]) placé auprès de la Commission européenne, qui a pour mission d'apporter à celle-ci une contribution coordonnée et opérationnelle des régulateurs sur toute question relative aux services de médias audiovisuels et le cadre réglementaire.

- **la CNIL (Commission nationale informatique et libertés)** est une autorité administrative indépendante chargée de veiller à la bonne application des règles régissant les données personnelles. Elle aide les acteurs à se mettre en conformité avec le RGPD et contrôle sa mise en œuvre. Le RGPD[253] a mis en place un système d'autorité ***chef de file*** selon le système dit « *de guichet unique* » qui permet aux entreprises établies dans l'Union européenne, lorsqu'elles mettent en œuvre un traitement de données transfrontalier, de dépendre de la seule autorité de protection des données du pays où se trouve l'établissement principal de l'entreprise. Celle-ci est alors seule compétente et

(l'HADOPI). La fusion devrait permettre de donner plus de poids à la lutte contre le piratage grâce à la mutualisation des moyens et à l'accroissement de l'autorité de l'instance de régulation.

250 Le premier, en 2020, était intitulé « La propagation des fausses informations sur les réseaux sociaux : étude de la plateforme Twitter ».

251 Par ex., v. la recommandation n° 2019-03 du 15 mai 2019 prononcé dans le cadre de son devoir de coopération (instauré par la loi anti « *fake news* » du 22 décembre 2018) pour la lutte contre la diffusion de fausses informations, précisant comment pourrait être mis en place un dispositif de signalement accessible et visible des contenus manifestement faux publiés en ligne, comment assurer une transparence des algorithmes, ou encore comment lutter contre les comptes propageant massivement de fausses informations et permettre une meilleure information des utilisateurs sur l'origine de ces contenus.

252 European régulators'group for audiovisual media services. L'ERGA est un organe consultatif de la Commission européenne créé par une décision du 3 février 2014. Il rassemble les dirigeants des autorités de régulation de l'audiovisuel des vingt-sept États-membres de l'Union européenne. Il a pour mission d'apporter à la Commission européenne une contribution coordonnée et opérationnelle des régulateurs sur toute question relative aux services de médias audiovisuels et le cadre réglementaire européen. Il doit également faciliter la coopération et l'échange d'expériences et de bonnes pratiques entre régulateurs.

253 Art. 4. 23 du RGPD.

devra coordonner la prise de décision avec les autres autorités concernées. Ce dispositif n'est pas applicable lorsqu'est mise en œuvre la législation sur les *cookies,* qui ne figure pas dans le RGPD mais dans la directive *e-privacy*[254]. Les autorités européennes disposent d'un cadre de dialogue et d'harmonisation de leurs actions au sein du **Comité européen de la protection des données** (ancien G 29), qui veille à l'application cohérente du RGPD dans tous les pays de l'Union européenne. Il peut ainsi adopter des documents d'orientations générales afin de clarifier les dispositions des actes législatifs européens en matière de protection des données et, de cette manière, fournir aux acteurs concernés une interprétation cohérente de leurs droits et obligations, adopter des avis pour garantir l'application cohérente du RGPD, et des décisions contraignantes pour trancher les différends entre autorités de contrôle qui lui seraient soumis[255]. Comme il a été dit plus haut, la CNIL et ses homologues européens sont très fréquemment conduites à connaître de l'application des données personnelles par les réseaux sociaux.

- **l'ARCEP (autorité de régulation des communications électroniques, des postes et de la distribution de la presse)** a été créée par la loi du 26 juillet 1996 pour préparer l'ouverture à la concurrence du secteur des télécoms. L'ARCEP est une autorité administrative indépendante chargée, comme son nom l'indique, de réguler le secteur des télécommunications[256]. Son rôle a été renforcé ces dernières années dans le domaine numérique. La loi du 7 octobre 2016 pour une République numérique lui a notamment confié la protection de la neutralité du net en conformité avec le principe de non-discrimination assortie d'un pouvoir d'enquête et de sanction afin de la rendre effective. Elle veille aussi à la régulation environnementale du numérique[257]. L'ARCEP siège aux côtés des autres régulateurs européen et d'observateurs au sein de l'organe des régulateurs européens des communications électroniques (ORECE plus connu sous son acronyme anglais BEREC : *Body of European Regulators for Electronic Communications*). Il s'agit d'un organe indépendant européen qui a été créée en 2009 et dont la mission est de renforcer la coopération entre les régulateurs européens et les institutions européennes. Ses objectifs premiers sont de garantir l'accès équitable pour tous à l'internet et à ses services, la neutralité du réseau et la mise en cohérence à échelle européenne des systèmes nationaux de régulation.

254 CE, 28 janvier 2022, n° 449209 : le Conseil d'État a confirmé la compétence de la CNIL à prendre des sanctions sur les cookies en dehors du mécanisme de guichet unique prévu par le RGPD et ainsi validé la sanction de la CNIL prononcée à l'encontre des sociétés GOOGLE LLC et GOOGLE IRELAND LIMITED.

255 Le contrôleur européen de la protection des données est quant à lui une autorité de contrôle indépendante des institutions européennes qui veille à ce que les organes de l'UE respectent le droit des citoyens à la protection de leur vie privée.

256 Sa mission historique tient à l'attribution par décision individuelle des ressources en fréquence et en numérotation, à veiller au financement et à la fourniture du service universel, à définir *ex ante* la réglementation applicable à tout ou partie des opérateurs et à analyser le marché, dialoguer avec les acteurs et édicter des lignes directrices ou recommandation.

257 Loi n° 2021-1755 du 23 décembre 2021 visant à renforcer la régulation environnementale du numérique par l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse.

- **L'Autorité de la concurrence** est une autorité administrative indépendante qui veille à l'équilibre de la concurrence sur le marché. Elle contrôle, préalablement à leur réalisation, les opérations de concentration, lutte contre les ententes et les abus de position dominante par des procédures d'injonction voire de sanction. Elle agit en étroite coopération avec la **Commission européenne** et les 27 autres autorités nationales de concurrence européennes pour assurer une régulation cohérente et unifiée au sein de l'espace européen par l'intermédiaire du **Réseau européen de concurrence** (REC) qui coordonne les mécanismes de lutte contre les pratiques anti-concurrentielles transfrontalières. Par l'intermédiaire du REC, les autorités de concurrence s'informent mutuellement des décisions proposées et prennent en compte les commentaires des autres autorités de concurrence. Le REC permet ainsi aux autorités de la concurrence de mettre en commun leur expérience et d'identifier les bonnes pratiques.
- La **Direction générale de la concurrence, de la consommation et des fraudes (DGCCRF)** est une direction du ministère de l'Économie. Outre les compétences en matière de régulation du marché qu'elle partage avec l'Autorité de la concurrence, elle a pour mission de protéger la sécurité des consommateurs. Ses missions sont notamment "la contribution à la définition du cadre juridique de la concurrence et de la consommation ; l'information et l'accompagnement des professionnels comme des consommateurs ; l'incitation à l'autorégulation des secteurs économiques ; le contrôle du respect des règles de concurrence et de protection des consommateurs ; la définition des suites à donner aux pratiques contraires au droit notamment la mise en œuvre de mesures de protection en cas de risques pour la santé ou la sécurité des consommateurs". Présente sur le territoire à travers des services déconcentrés, elle est dotée de services d'enquête dont un spécialisé sur l'outil numérique qui permet notamment de détecter les faux avis en ligne, les pratiques commerciales trompeuses par les influenceurs et de sécuriser les achats sur internet. Elle a notamment enjoint à Facebook de modifier ses CGU pour informer le consommateur de l'utilisation commerciale des données personnelles recueillies.

Au niveau européen, le **Réseau de coopération en matière de protection des consommateurs** (CPC) créé en 2007 réunit les autorités publiques de tous les États membres de l'UE chargées de l'application de la législation en matière de protection des consommateurs de l'UE.

Pour encadrer de façon efficace les réseaux sociaux, l'articulation de ces régulations est un défi majeur pour les prochaines années. En outre, tant la question du droit applicable que de l'autorité compétente dépendent de critères d'application territoriale. Dans un domaine mondialisé où les opérateurs sont presque tous extra-européens, cette question est cruciale (*cf. infra*).

Après cette esquisse de l'écosystème et du droit des réseaux sociaux, il est temps d'identifier les défis et les enjeux que ces derniers engendrent pour les politiques publiques.

Le droit des réseaux sociaux en synthèse

2. Les réseaux sociaux : quand la *technique* engage le *pouvoir* à se réinventer

Le *pouvoir* et la *technique* ont traditionnellement des relations ambivalentes. Le développement foudroyant des réseaux sociaux, outils d'abord techniques de communication, leur donne une puissance considérable qui modifie les équilibres et oblige l'État, garant de l'intérêt général, à s'adapter pour faire face aux défis que ce nouvel outil lui pose.

2.1. Les défis pour l'autonomie et la préservation de la démocratie

Les plus grands réseaux sociaux, qui rassemblent des centaines de millions voire des milliards d'utilisateurs de toutes nationalités y compris des dizaines de millions de Français, se sont imposés comme les nouveaux forums du XXIe siècle. Faisant commerce de l'expression publique, élément clé de l'exercice de la souveraineté nationale dans une démocratie[258], la question de leur influence sur les démocraties, y compris la démocratie française, est un enjeu décisif pour l'avenir de notre pays. Par ailleurs, la présence désormais incontournable des réseaux sociaux en France et en Europe soulève des enjeux stratégiques, géopolitiques, économiques et juridiques cruciaux, compte tenu de ce que ces réseaux sont des sociétés privées essentiellement américaines et chinoises, dont la puissance est à la mesure de la taille.

2.1.1. La puissance des grands réseaux sociaux face à l'autonomie stratégique française et européenne

On le sait, les réseaux sociaux présents sur le marché européen sont essentiellement américains et chinois. Au vu du poids économique de ces sociétés et de la place centrale qu'elles occupent désormais comme l'un des lieux privilégiés d'expression du débat public, la question de la **dépendance** de la France et de l'Europe à

258 La liberté d'expression et la démocratie sont indéfectiblement liées. Dans sa décision du 10-11 octobre 1984 n° 84-181 DC *Loi visant à limiter la concentration et à assurer la transparence financière et le pluralisme des entreprises de presse,* le Conseil constitutionnel rappelait que la liberté d'expression est « *une liberté fondamentale, d'autant plus précieuse que son exercice est l'une des garanties essentielles du respect des autres droits et libertés et de la souveraineté nationale* ».

ces entreprises est réelle même si elle n'est pas toujours perçue. Le philosophe Éric Sadin décrit ainsi de manière provocatrice une «*colonisation d'un nouveau genre (…) qui ne se vit pas comme une violence subie, mais comme une aspiration ardemment souhaitée par ceux qui entendent s'y soumettre*»[259]. Ce phénomène concerne, plus largement que les réseaux sociaux, le numérique dans son ensemble. Souvent désigné sous le terme générique de « souveraineté numérique », il a suscité au cours des dernières années de très nombreux travaux parlementaires[260] et universitaires[261]. Presque tous les **GAFAM, désormais MAMAA**, abritent en leur sein un voire plusieurs réseaux sociaux. Youtube appartient à Google/Alphabet, Facebook – qui appartient désormais à Méta, aux côtés d'Instagram et WhatsApp – est un réseau social à part entière et Microsoft a racheté LinkedIn en 2017. Quant au controversé Twitter, les offres d'achat récentes dont il fait l'objet témoignent de son importance stratégique. La puissance de ces réseaux sociaux, d'origine extra-européenne, peut constituer une menace pour l'autonomie stratégique française. « *La réflexion sur la souveraineté numérique naît d'une préoccupation : le refus de voir les peuples, les communautés d'utilisateurs, les États, les individus perdre le contrôle de leur destin au profit d'entités mal identifiées, non légitimes, et dont l'objectif n'est pas la promotion de l'intérêt général* »[262].

Les risques que la puissance des réseaux sociaux présente pour l'autonomie stratégique de la France et l'Europe sont d'ordre technologique, économique, juridique et culturel.

La maîtrise technologique et les risques d'atteinte à la sécurité de l'État

La maîtrise des infrastructures du net est stratégique. Les États-Unis dominent notamment le marché des câbles sous-marins en fibre optique par lesquels transitent 99% des échanges de données mondiaux[263] et sont les destinataires de 80% des flux internet grâce à leurs *data centers*[264]. Quant à la Chine, elle développe un projet de « route de la soie numérique ». Outre la dépendance à ces infrastructures, cette situation rend la France et l'Europe vulnérables aux risques de non-respect du principe de neutralité et à ceux de **surveillance et d'espionnage**. L'affaire Snowden est venue renforcer la crainte de ces menaces[265]. Différentes

259 E. Sadin, *La siliconisation du monde : l'irrésistible expansion du libéralisme numérique*, Paris, éd. L'échappée, 2016, p. 24 ; v. aussi C. Morin Desailly (*L'Union européenne, colonie du monde numérique ?*, rapport d'information, commission des affaires européennes du Sénat, n° 443, 2013.

260 *Nouvelle stratégie pour l'Union européenne dans la gouvernance mondiale de l'internet*, rapport d'information du Sénat, n° 696, 2014 ; *Le devoir de souveraineté numérique*, G. Longuet, rapport de la commission d'enquête du Sénat, n° 7, 2019 ; Mission d'information sur le thème "Bâtir et promouvoir une souveraineté numérique nationale et européenne" lancée en septembre 2020 rapportée par M. Philippe Latombe, député Modem.

261 A. Blandin-Obernesser, *Droits et souveraineté numérique en Europe*, Bruxelles, Bruylant, 2016 ; P. Türk et Ch. Vallar (dir.), *La souveraineté numérique, le concept, les enjeux*, Mare & Martin, janvier 2018, B. Benhamou et L. Sorbier, « Souveraineté et réseaux numériques », *Politique étrangère*, 2006/3 ; P. Bellanger, *La souveraineté numérique en 2014*, Stock.

262 P. Turk, « La souveraineté numérique », *Les cahiers français*, La documentation française.

263 Les parts de marché des GAFAM ont aujourd'hui dépassé 50% et devraient atteindre 95% dans trois ans.

264 M. Jausions, *Câbles sous-marins : un risque pour la souveraineté française ?*, Centre de ressources et d'information sur l'intelligence économique et stratégique, 20 janvier 2022, consultable sur : https ://portail-ie.fr.

265 Edward Snowden, ancien agent de la CIA et de la NSA a rendu publiques des informations secrètes

actions sont menées en France et en Europe pour diminuer cette dépendance, promouvoir la sécurité du cyberespace et organiser la cyberdéfense[266]. La France s'est notamment dotée d'un service de veille d'internet dénommé **Viginum** afin de détecter à tout instant les menaces informationnelles numériques provenant de l'étranger pouvant conduire à des manipulations de l'information.

La **collecte massive de données et l'avance importante en termes d'expertise**, acquise au fil des années par ces géants de l'internet, qui leur permettent de garder leur pouvoir de marché, renforcent encore leur prédominance. Certains chercheurs ou observateurs considèrent qu'il faudrait s'alarmer de la présence de nombreux Européens sur les réseaux sociaux chinois comme TikTok ou Weibo au motif que les autorités chinoises utiliseraient ces réseaux comme de potentiels outils de contrôle des populations et de propagande et qu'ils récolteraient une quantité phénoménale de données sur les citoyens français[267]. Ils évoquent aussi les progrès fulgurants de l'IA qui vont permettre dans un futur proche de créer des « *bots* » de plus en plus efficaces, susceptibles à terme de fausser le débat public sans que personne ne puisse être en mesure de les détecter[268].

Dans sa communication intitulée « Façonner l'avenir numérique de l'Europe » du 19 février 2020, la Commission européenne souligne que la **souveraineté technique** de l'Europe commence par « *la capacité de garantir l'intégrité et la résilience de nos infrastructures de données, de nos réseaux et de nos communications* ». Elle ajoute que cela exige de « *créer les conditions qui permettront à l'Europe de développer et de déployer ses propres capacité critiques, réduisant ainsi notre dépendance vis-à-vis d'autres régions du globe pour les technologies les plus cruciales* »[269]. Elle préconise notamment le développement de la 5G, l'interopérabilité des infrastructures numériques essentielles et un effort massif dans les « *deep tech* »[270]. Dans le cadre de la stratégie européenne en matière de **cybersécurité**, une directive sur la sécurité des réseaux et des systèmes d'information (SRI) dite NSI (*Network and information system security*) qui régit notamment la régulation des opérateurs critiques, a été adoptée[271].

La France et l'Allemagne ont lancé un projet Gaia-X, prolongé dans l'idée d'un ***cloud* européen**, qui vise à concevoir une plateforme regroupant des offres de stockage conformes aux règles européennes afin d'assurer une véritable sécurité et une confidentialité de ces données pour les utilisateurs européens. Dans cette

concernant la captation de métadonnées, d'appels téléphoniques et d'internet.

266 Le siècle digital. L'Espagne investit massivement dans la production de semi-conducteurs, un plan qui contribue à la souveraineté économique de l'Europe dans le secteur. 27 mai 2022.

267 D. Chavalarias, *Toxic Data,* Flammarion, 2022.

268 *Op. cit.*

269 Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, Façonner l'avenir numérique de l'Europe, 19 février 2020.

270 Le *deep tech* est le calcul à haute performance, technologies quantiques, chaînes de blocs et capacités en nuage sécurisées. La Commission préconise aussi une augmentation massive des investissements portant sur les infrastructures et les réseaux numériques, le renforcement des soutiens dans la recherche et le développement et des actions de nature à permettre la mise à disposition de produits sûrs et « cyber-résilients » pour protéger les citoyens contre les menaces numériques.

271 Directive 2016/1148 NIS du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union sachant que la directive NIS II devrait être prochainement adoptée.

ligne, l'Agence nationale de sécurité des systèmes d'information[272] s'est dotée d'un instrument de qualification des prestataires de services d'hébergement d'informatique en nuage, en établissant un référentiel intitulé le *SecNumCloud* attestant du respect de règles de sécurité et du RGPD. Trois fournisseurs de *cloud* sont actuellement certifiés SecNumCloud : OVHcloud, 3DS outscale et Oodrive. Le code de la défense a aussi été enrichi de dispositions protégeant les lanceurs d'alerte qui s'adressent à l'ANSSI[273].

Les défis économiques, monétaires et fiscaux

En 2016, selon les données de la Banque mondiale[274], l'économie numérique représentait 11 500 milliards de dollars, soit 15,5% du PIB mondial. Chaque jour dans l'Union européenne, 150 millions de contributions sont postées sur les réseaux sociaux[275]. Conformément à la logique du « *winners take most* » déjà évoquée dans la première partie, les plus importants réseaux sociaux ont acquis un pouvoir de marché considérable fondé sur leur expertise technologique, l'importance des effets de réseau, la collecte massive de données, les économies d'échelles dont ils bénéficient, voire sur certaines pratiques anticoncurrentielles. Face à la suprématie de quelques multinationales et à ce phénomène de **forte concentration**, certains économistes ont dénoncé l'inversion du rapport de force avec les États et le risque de « vassalisation » de ces derniers[276]. Outre la mise en place du *Digital Markets Act* les autorités de la concurrence s'efforcent de lutter contre certains abus de position dominante et proposent d'accentuer le contrôle de concentrations des plateformes structurantes[277], par exemple en les dotant du pouvoir d'enjoindre la notification d'opérations de concentration sous les seuils, si ces opérations sont, au regard de certaines conditions prédéfinies, susceptibles de soulever des préoccupations de concurrence. La taille démesurée des GAFAM

272 Service du Premier ministre, rattaché au Secrétariat général de la défense et de la sécurité nationale (SGDSN), l'Agence nationale de la sécurité des systèmes d'information est l'autorité nationale chargée d'accompagner et de sécuriser le développement du numérique. Son action est défensive, elle ne contrôle pas les contenus des systèmes, ne réalise aucune surveillance ni activité de renseignement.

273 Art. L. 2321-4 du code de la défense : « *pour les besoins de la sécurité des systèmes d'information, l'obligation prévue à l'article 40 du code de procédure pénale n'est pas applicable à l'égard d'une personne de bonne foi qui transmet à la seule autorité nationale de sécurité des systèmes d'information une information sur l'existence d'une vulnérabilité concernant la sécurité d'un système de traitement automatisé de données. (…)* ».

274 Banque mondiale, *Développement numérique*, avril 2019, consultable sur www.banquemondiale.org.

275 Chambre d'industrie et de commerce, *Fiscalité du numérique*, Étude, juin 2021.

276 J. Tolédano, art. précité.

277 Dans sa contribution au débat sur la politique de concurrence et les enjeux numériques du 19 février 2020, l'Autorité de la concurrence française pointe différents comportements mis en œuvre par les plateformes dites « structurantes » tels que « *la discrimination de produits ou services concurrents, l'entrave à l'accès aux marchés sur lesquels elles ne sont pas structurantes, l'utilisation de données sur un marché dominé pour en rendre l'accès plus difficile, l'entrave à l'interopérabilité des produits ou services ou la portabilité des données, l'entrave à la multi-domiciliation (multi-homing), sans qu'il soit toujours possible de caractériser, au vu du standard actuel, un abus de position dominante* ». Elle rappelle l'utilité des mécanismes composant le droit de la concurrence pour encadrer les comportements anti-concurrentiels des entreprises. A titre d'exemple, plusieurs sanctions ont été prises par la Commission européenne sur les fondements de l'abus de position dominante, l'abus d'exploitation et l'abus d'éviction à l'époque (par exemple en 2019, dans le cadre de l'affaire *Google AdSense,* condamnée pour abus de position dominante à travers la régie publicitaire AdSense, à une amende de 1,49 milliard d'euros).

les conduit à collecter, détenir et exploiter de très vastes masses **de données numériques**, renforçant également leur pouvoir sur des marchés voisins[278].

• *Le défi monétaire*

Les réseaux constituent également des lieux d'échange et de promotion des **monnaies numériques**. On assiste en effet depuis quelques années à l'apparition de crypto-monnaies, actifs qui s'échangent de pair-à-pair sans tiers de confiance car ils utilisent la **technologie** « ***blockchain*** »[279]. Face à leur montée en puissance, la France a décidé de les définir à l'article L. 54-10-1 du code monétaire et financier[280] et d'imposer aux prestataires de services d'actifs numériques établis sur le sol français de respecter certaines conditions et d'être enregistrés par l'Autorité des marchés financiers, sous peine d'interdiction de leur activité[281]. L'encadrement des crypto monnaies au niveau européen est en cours d'élaboration et deux accords majeurs ont été conclus à cette fin durant la présidence française de l'Union européenne[282]. Leur régime fiscal, qui a donné lieu à du contentieux[283], a fait l'objet de dispositions spécifiques[284]. L'Union européenne envisage, par l'adoption de plusieurs textes, d'améliorer la traçabilité des transferts de crypto-actifs et de bloquer les transactions suspectes, souvent liées au blanchiment d'argent et au financement du terrorisme[285]. **Certains réseaux sociaux ont même souhaité créer leur propre monnaie virtuelle**, se heurtant pour l'instant à de fortes réserves des régulateurs et des États. Facebook a finalement abandonné son projet de crypto-monnaie nommé *Libra* puis *Diem* mais le groupe Meta envisage de créer une nouvelle monnaie virtuelle qui aurait cours dans le Métaverse sous forme de jetons[286] (*token*). Il a aussi ajouté pour ses utilisateurs une nouvelle fonctionnalité leur permettant de mettre en valeur des NFT[287]. Télégram a été condamné au paiement d'une amende de 18,5 millions de dollars par la SEC (*Security and Exchange Commission* : organisme fédéral américain chargé de la réglementation et du contrôle des marchés financiers) pour ne pas avoir respecté les règles en vigueur.

278 « *Pour déterminer le lien entre données et pouvoir de marché il faut s'intéresser aux éléments suivants : la rareté et la capacité à reproduire ou à accéder aux données d'une part, le volume et la variété des données d'autre part.* » Droit de la concurrence et données, 10 mai 2016.

279 Chaîne de blocs, base de données sans autorité centrale et infalsifiable, qui permet de réaliser des transactions et d'en tenir registre sans avoir à passer par un tiers de confiance. Ces chaînes peuvent être privées, publiques, ou semi-publiques M. Verdier, « La *blockchain* et l'intermédiation financière », *Revue d'économie financière*, vol. 129, n°. 1, 2018, pp. 67-87.

280 « *Toute représentation numérique d'une valeur qui n'est pas émise ou garantie par une banque centrale ou par une autorité publique, qui n'est pas nécessairement attachée à une monnaie ayant cours légal et qui ne possède pas le statut juridique d'une monnaie, mais qui est acceptée par des personnes physiques ou morales comme un moyen d'échange et qui peut être transférée, stockée ou échangée électroniquement* ».

281 Art. L.54-10-1 et suivants du code monétaire et financier.

282 Projet de règlement TFR (pour «Transfer of Funds Regulation») obligeant les acteurs cryptos à fournir des informations d'identification sur les transactions en crypto monnaies et projet de règlement MiCa (pour «Market in crypto assets»).

283 CE, 26 avril 2018 n° 417809 418030 418031 418032 418033.

284 Art. 150 VH bis du CGI.

285 Projet de loi contre le blanchiment d'argent et le financement du terrorisme, consultable sur www.europarl.europa.eu.

286 Objet numérique qui peut être émis et échangé par la *blockchain.*

287 *Non fungible token*, type spécial de jetons cryptographiques qui représentent quelque chose d'unique qui ne peut pas être remplacé par d'autres choses de même nature. Ils sont particulièrement utilisés dans l'art numérique.

• *Le défi fiscal*

Les réseaux sociaux échappent en outre, au moins dans une certaine mesure, à l'impôt car **les systèmes fiscaux** aux niveaux français, européen et mondial se révèlent aujourd'hui mal adaptés pour **appréhender la valeur créée dans l'économie numérique**. Alors que la clef de voûte des systèmes traditionnels repose sur la notion d'établissement stable, ce critère est largement inopérant pour déterminer le lieu de réalisation des bénéficies numériques immatériels. En effet l'économie numérique présente quatre spécificités : la non-localisation des activités et leur mobilité[288], l'exploitation des données[289], la prédominance des effets de réseau[290], le rôle central des plateformes sur un marché biface. Les sources de recettes sont très diverses : publicité, abonnements, services d'achat ou de location de contenu numérique, licences, vente de données, etc. De fait, la valeur est souvent créée, dans l'économie du numérique, « *à partir de la combinaison d'algorithmes, de données utilisateur, de fonctions commerciales et de connaissances* »[291]. La soumission à l'impôt est rendue complexe par la difficulté à mesurer la valeur ajoutée créée par les réseaux sociaux et le fait qu'une grande partie de celle-ci « *s'échappe du territoire national vers les comptes des sociétés établis dans des paradis fiscaux* », sans que les gains de productivité n'engendrent donc de recette fiscale supplémentaire pour les États[292]. La refonte de la fiscalité au regard de la numérisation de l'économie a fait l'objet de nombreux travaux et, suite à l'impossibilité de parvenir à un accord au niveau européen, a donné lieu à l'instauration de la taxe GAFA en France[293].

Des progrès importants ont toutefois été réalisés. Un rapport de l'OCDE a défini deux piliers de travail afin de répondre aux défis fiscaux posés par le numérique. Le premier a pour ambition de réexaminer les règles concernant la répartition des bénéfices[294]. Le second vise à fixer un niveau d'impôt minimum sur les bénéfices

288 La mobilité est double, à la fois des utilisateurs – localisation et identification des profils très complexes – et des fonctions de l'entreprise – étendues sur des marchés mondiaux, sans nécessairement une augmentation considérable d'effectifs du fait des avancées technologiques, avec une logistique moins coûteuse, rendant les modèles économiques du numérique flexibles.

289 Une entreprise du numérique peut exploiter les données en masse grâce à ses grandes capacités de traitement de l'information, générant une nouvelle chaîne de valeur. Déjà en 2011, le McKinsey Global Institute estimait la valeur qui pourrait être créée en analysant les données à 250 milliards d'euros dans le secteur des administrations publiques en Europe (v. « The next frontier for innovation, competition, and productivity »,2011, consultable sur *www.mckinsey.com.*

290 Ces effets renforcent les modèles économiques du numérique, car les firmes du numérique réunissent un nombre d'utilisateurs considérable ce qui augmente leur productivité en leur permettant d'améliorer leur service pour un même prix, provoquant un phénomène de rendement croissant avec un effet « boule de neige » augmentant la popularité du réseau. Ces effets de réseau sont complétés par l'effet de réseau croisé : l'aspect biface des entreprises du numérique crée des « pôles de centralisation des interactions sociales » sur lesquels les annonceurs ciblent leurs publicités.

291 Commission européenne, *Une fiscalité équitable de l'économie numérique*, consultable sur : *https ://ec.europa.eu*

292 P. Collin, N. Colin, rapport, *Mission d'expertise sur la fiscalité de l'économie numérique*, janvier 2013.

293 La taxe GAFA, adoptée le 24 juillet 2019 par le Parlement, est ciblée sur « *3 types d'activités numériques : la publicité ciblée en ligne, la vente de données utilisateurs à des fins publicitaires, les activités des plateformes d'intermédiation* ». Il s'agit d'une imposition à hauteur de 3% sur le chiffre d'affaires numérique réalisé en France, avec deux seuils à dépasser pour être assujetti à cette taxe : 750 Md'€ de chiffre d'affaires dans le monde et 25 Md'€ de chiffre d'affaires en France. Elle a rapporté 277 Md'€ en 2019 et devrait rapporter, selon la loi de finances pour 2022, 518 Md'€ en 2022.

294 Il vise à instituer un nouveau droit d'imposition, à fixer un rendement pour certaines activités de distribution et de commercialisation exercées physiquement et à améliorer la sécurité juridique en matière fiscale grâce aux mécanismes de prévention et de règlement de différends.

des grandes entreprises numériques, indépendamment de la localisation de leurs activités.

En octobre 2021, un **accord majeur** a été conclu afin de garantir un taux d'imposition minimum de 15% aux entreprises multinationales à compter de 2023, ce qui concerne de nombreux réseaux sociaux. Il rendra dès lors caduques les taxes nationales sur les services numériques, dont la taxe GAFA française. Cet accord, approuvé par 136 pays (et leurs juridictions) représentant plus de 90% du PIB mondial, permet d'espérer une réallocation au niveau mondial de plus de 125 milliards de dollars américains de bénéfices d'environ 100 entreprises multinationales. Le rétablissement de l'équité fiscale dépend dorénavant de la mise en œuvre de cet accord. Il doit notamment encore être mis en œuvre au niveau européen par l'Union européenne.

Souveraineté juridique et extraterritorialité du droit

> • *Quand les conditions générales d'utilisation concurrencent le droit territorialement applicable*

Il faut rappeler que les réseaux sociaux sont des **entités de droit privé** qui entretiennent des **relations de droit privé** avec leurs utilisateurs. Compte tenu de la nature de la prestation, il s'agit d'un contrat d'adhésion, dont les conditions sont fixées unilatéralement par le professionnel, qui se forme entre les deux co-contractants de sorte que l'utilisateur est face à un choix binaire : tout accepter ou tout refuser. Cet outil implacable conduit à ce que tous les utilisateurs d'un réseau, quels que soient leur nombre et leur nationalité, peuvent se voir imposer par ce réseau le même cadre contractuel, formalisé dans les conditions générales d'utilisation (CGU). S'affranchissant des limites et des frontières entre États, les plateformes, surtout les plus grandes, refusent, pour la plupart, de se soumettre entièrement aux lois du pays où l'utilisateur se trouve[295]. **Le droit des États, manifestation de leur puissance souveraine, se trouve ainsi concurrencé par des contrats de droit privé**.

Dans un monde régi par une économie globalisée, cette situation n'est pas inhabituelle. Mais, s'agissant d'entreprises devenues aussi centrales, notamment parce que leurs prestations constituent un support désormais essentiel de la liberté d'expression, cette situation apparaît problématique. Régissant de façon centralisée et quasi uniforme des espaces publics de millions voire milliards d'individus, les CGU ont ainsi, par leur portée et leur poids une force quasi constitutionnelle (*cf.* la suspension puis la fermeture des comptes de Donald Trump en janvier 2021, dans un pays pourtant attaché à une conception particulièrement extensive de la liberté d'expression[296]). Bruno Patino dans son dernier ouvrage *Tempête dans le bocal*[297]

295 Surtout que les règles de droit international privé permettent aux parties de librement décider de la loi applicable au contrat à condition de ne pas priver le consommateur de règles plus protectrices (Règlement n° 592/20028 sur le droit applicable aux contrats internationaux).

296 Mais le Premier amendement à la constitution américaine a été élaboré pour limiter l'oppression de la puissance publique sur les citoyens, non celle des entreprises privées par rapport à leurs clients. (Cour de district des États-Unis pour le district Est de la Virginie, 26 février 2019, *Davison v. Facebook,* 370 F. Supp. 3d 621 (E.D. Va. 2019), p. 11/ Cour de district des États-Unis pour le district Nord de la Californie, 10 janvier 2022, *O'Handley v Padill,*, n°. 21-cv-07063-CRB, p. 21).

297 B. Patino. Grasset, 2022.

soulève à cet égard le paradoxe qu'il y a à s'inquiéter de l'apparition des crypto-monnaies pour la souveraineté des États et ne pas s'inquiéter de la puissance des CGU qui ne font « *rien moins que l'interprétation du 1er amendement des* États *Unis ou de l'article 11 de la Déclaration des droits de l'homme et du citoyen.* ». Henri Verdier et Jean-Louis Missika dénoncent aussi des géants du numérique devenus de véritables « *institutions politiques privées* » qui « *négocient avec les États, censurent, autorisent ou interdisent les expressions publiques, stockent et commercialisent des données personnelles*. »[298].

La Cour suprême fédérale allemande en matière civile a été saisie de la question de l'articulation des CGU de Facebook avec ses normes suprêmes. Par un arrêt du 21 juillet 2021[299], elle juge que l'opérateur d'un réseau social est autorisé à imposer aux utilisateurs de son réseau le respect de ses propres règles même si ces règles vont au-delà de ce qui est prévu par la législation allemande en vigueur. Il a donc, en principe, le droit de supprimer des contenus bien que ceux-ci ne soient pas considérés comme des « contenus illicites » au sens de la loi allemande visant à améliorer l'application du droit sur les réseaux sociaux (NetzDG). La Cour précise toutefois que les conditions d'utilisation peuvent être soumises à un contrôle judiciaire visant à vérifier qu'elles ne sont pas abusives (AGB-Kontrolle). A cet égard doivent être pris en compte et mis en balance les droits fondamentaux des utilisateurs (notamment la liberté d'expression garantie par l'article 5 de la Loi fondamentale) et les droits fondamentaux des opérateurs de réseaux sociaux (notamment la liberté professionnelle garantie par l'article 12 de la Loi fondamentale). La Cour estime que **les grands réseaux sociaux tels que Facebook occupent une position si importante et si puissante dans la création d'espaces publics de communication et de vie sociale qu'ils sont soumis à une obligation de respecter les droits fondamentaux de leurs utilisateurs** (*mittelbare Drittwirkung der Grundrechte*)[300], qui peut être comparable à l'obligation de l'État de respecter les droits fondamentaux de ses citoyens. La Cour considère ensuite que l'opérateur du réseau social doit s'engager, dans les conditions générales d'utilisation de son réseau, à informer l'utilisateur, au moins *a posteriori*, de la suppression de sa publication et à l'informer préalablement de toute intention de bloquer son compte. Il est également tenu d'informer l'utilisateur des raisons pour lesquelles sa publication a été supprimée ou son compte bloqué et de lui donner la possibilité de contester cette décision. La Cour en conclut que, **en l'absence d'une telle disposition, les conditions générales de Facebook ne sont pas valables et créent un déséquilibre significatif** *(unangemessene Benachteiligung*) pour les utilisateurs[301].

298 H. Verdier, J.-L. Missika, *Le business de la haine : Internet, la démocratie et les réseaux sociaux*., Calman Levy, 2022.

299 Cour suprême fédérale, 29 juillet 2021, III ZR 179/20, III ZR 192/20.

300 Pour plus de détails sur cette question v. M. Friehe, « Soziale Netzwerke in der Grundrechtsklemme ? », *Verfassungsblog*, 9 mai 2021.

301 A ce stade, la Cour constitutionnelle fédérale allemande ne s'est pas encore prononcée de manière définitive sur la question de savoir si et dans quelle mesure les opérateurs de réseaux sociaux sont tenus de respecter les droits fondamentaux de leurs utilisateurs. Dans deux affaires portant sur le déblocage d'un compte d'un parti d'extrême droite appelé « Der III. Weg » (La IIIe voie) sur Facebook, la Cour a estimé qu'une telle obligation pourrait potentiellement s'imposer aux opérateurs de réseaux sociaux. Toutefois, comme il s'agissait de procédures d'urgence dans les deux affaires, la Cour n'a pas statué de manière définitive sur cette question.

Sachant que les CGU sont souvent modifiées sans que l'utilisateur en soit nécessairement informé, qu'elles contiennent parfois des clauses abusives qui ne sont pas toujours détectées, qu'elles peuvent être floues et que plusieurs heures sont nécessaires à leur lecture, on peut s'interroger sur la portée du consentement donné par l'utilisateur. Certains auteurs estiment nécessaire qu'un suivi des CGU soit opéré notamment à l'aide des bases de données créées à cette fin et qu'une réflexion sur les liens entre la loi et le contrat soit approfondie[302].

• *La question de la reterritorialisation du droit*

Les législations des États ne sont en principe pas applicables au-delà de leur territoire. Les plateformes, pour majorité américaines, se retranchent souvent derrière le refus de l'extra-territorialité pour ne pas donner suite aux demandes des autorités nationales. Le parquet spécialisé de Paris rencontre ainsi d'importantes difficultés à obtenir, pourtant sur réquisitions, communication des propos visés dans des plaintes dont il est saisi.

Le législateur européen n'a toutefois pas hésité, dans certains cas, à adopter des normes ayant une portée extraterritoriale, comme le règlement *Terrorist content on line* qui prévoit que les autorités du pays où le **contenu est vu** peuvent en exiger le retrait et que, en cas de manquement, les opérateurs peuvent être sanctionnés par le pays dans lequel l'établissement a son siège.

La Cour de Justice de l'Union Européenne s'est également montrée audacieuse pour faire respecter les règles de droit de l'Union européenne par les grands réseaux sociaux. Ainsi par un arrêt *Eva Glawischnig-Piesczek/Facebook Ireland Limited* du 3 octobre 2019 intégrant dans sa motivation le caractère viral des partages sur les réseaux sociaux, la Cour a jugé, d'une part, que le droit de l'Union (directive e-commerce) ne s'oppose pas à ce qu'un hébergeur tel que Facebook soit enjoint de supprimer des commentaires équivalents à un commentaire précédemment déclaré illicite et, d'autre part, que le droit de l'Union ne s'oppose pas non plus à ce qu'une telle injonction puisse produire des effets à l'échelle mondiale[303]. Par son arrêt du 24 septembre 2019 *Google LLC contre CNIL* (C-507/17), la Cour a aussi rappelé que le droit de l'Union n'interdit pas qu'une demande de déréférencement porte sur l'ensemble des versions du moteur de recherche en cause (tout en rappelant que l'appréciation suppose une mise en balance entre, d'une part, le droit de la personne concernée au respect de sa vie privée et à la protection des données à caractère personnel la concernant et, d'autre part, le droit à la liberté d'information). Le Conseil d'État a jugé que cet arrêt n'a pas reconnu qu'un tel déréférencement pourrait nécessairement excéder le champ couvert par le droit de l'Union européenne pour s'appliquer hors du territoire des États membres de l'Union européenne[304].

302 H. Verdier, J.-L. Missika, *Le business de la haine : Internet, la démocratie et les réseaux sociaux*. *Open Terms Archive* : base de données ouverte de toutes les entreprises mondiales, pour pouvoir suivre en temps réel les changements de CGU, grâce à une alliance avec les contributeurs *via* l'*open source*. *Scripta Manent* : plateforme sur laquelle l'utilisateur peut choisir deux dates afin d'afficher le différentiel entre ce qui a été ajouté et retiré des CGU (V. sur le site internet de l'Ambassadeur pour le numérique).

303 CJUE, 3 octobre 2019, *Eva Glawischnig-Piesczek/Facebook Ireland Limited,* aff. C-18/18.

304 CE 27 mars 2020 n° 399922, Rec.

Le tableau figurant en annexe[305] souligne que des critères pragmatiques et assez larges tendent à être retenus pour permettre à l'utilisateur européen d'être protégé quelle que soit la loi du pays du réseau en cause. Afin de permettre une meilleure répression des infractions commises sur internet, la loi du 3 juin 2016 a introduit dans le code pénal un article 113-2-1 selon lequel « *tout crime ou tout délit réalisé au moyen d'un réseau de communication électronique, lorsqu'il est tenté ou commis au préjudice d'une personne physique résidant sur le territoire de la République, est réputé commis sur le territoire de la République* ». L'étude annuelle du Conseil d'État de 2014, qui avait identifié le caractère stratégique de cette question, préconisait d'ailleurs de définir un socle de règles impératives applicables à tous les acteurs quel que soit leur lieu d'établissement et promouvait le principe du pays de destination pour un socle de règles choisies qui seraient particulièrement importantes et applicables aux sites dirigeant leurs activités vers la France ou l'Union européenne[306]. La difficulté réside ensuite dans la mise en œuvre de ce droit et les conflits qui peuvent naître entre législations.

• *La souveraineté juridique européenne : l'exigence d'efficacité*

Face à la puissance mondiale des plus grands réseaux sociaux, les autorités françaises ont fait le choix de privilégier une action au **niveau européen**. Ce choix, qui implique de renoncer dans une certaine mesure à une réglementation propre, apparaît réaliste et pertinent, dès lors que les compétences transférées sont effectivement exercées. **L'enjeu est donc désormais, pour l'Union européenne, ses institutions et ses États membres, de mettre en œuvre efficacement les nouveaux outils mis en place au niveau européen.**

A cet égard, la mise en œuvre du mécanisme du guichet unique (mis en place par le RGPD pour harmoniser au niveau européen les décisions des autorités de protection des données concernant les traitements transfrontaliers) qui permet d'attribuer la compétence à une **autorité chef de file** ayant dans son ressort l'établissement principal du réseau social au sein de l'Union européenne, pose de **réelles difficultés**. Construit pour offrir un interlocuteur unique aux responsables de traitement, éviter des saisines multiples engendrant des incohérences et des frais inutiles, ce dispositif a conduit à ce que la grande majorité des réseaux sociaux choisissent de s'établir dans l'État membre présumé, à tort ou à raison, comme le moins exigeant – en l'occurrence l'Irlande – ce qui pose en outre un problème d'afflux de contentieux à traiter par les autorités compétentes de cet État. Outre les délais pour rendre les décisions, plusieurs États membres critiquent ce dysfonctionnement qui les dépossède de toute possibilité d'action sur des sujets d'une grande sensibilité sans permettre une action effective au plan européen.

Si le CEPD, en cas de désaccord entre les autorités concernées[307], peut trancher le litige, il ne peut le faire que s'il est effectivement saisi du dossier. Il parait difficilement acceptable de laisser de tels dysfonctionnements prospérer. Des lignes directrices qui clarifient les conditions découlant de l'article 60 du RGPD viennent d'être

305 CF annexe du rapport.

306 Étude du Conseil d'État, synthèse, 2.3, p. 23.

307 En effet l'autorité chef de file prépare le projet de décision mais doit en référer aux autorités de protection des données concernées afin de prendre une décision consensuelle. En cas de désaccord ou de refus d'amender le projet, le CEPD peut être saisi pour trancher le litige.

adoptées par le CEPD pour essayer répondre à cette difficulté[308]. Il est heureux que ce système n'ait pas été repris dans les règlements DSA et DMA, qui ont privilégié à juste titre, par souci notamment d'efficacité et d'effectivité, un contrôle exercé directement par la Commission européenne pour les plus grandes plateformes.

Il faut également citer les décisions rendues en matière de protection des données, notamment pour mettre fin à des transferts vers les États-Unis à la suite des recours exercées par l'association Noyb (*None of your Business*), fondée par l'activiste Maximilen Shrems (décisions des autorités autrichienne et italienne de protection des données, puis de la CNIL[309], déclarant illégal l'usage de Google Analytics au regard du RGPD[310]). Ces décisions illustrent que le droit peut constituer un bouclier utile pour assurer une forme de protection de la souveraineté des États.

La fragilisation de l'identité culturelle française ?

Dans la mesure où les réseaux sociaux ne sont pas soumis aux mêmes obligations et quotas que les médias traditionnels ou les nouveaux services de médias audiovisuels (Netflix, Amazon Prime, Disney plus) – inclus dans la directive SMA et sa transposition – il leur est souvent reproché de ne pas mettre suffisamment en avant les contenus culturels français et européens. Ils soulignent en réponse que la logique algorithmique fait avant tout apparaître des contenus correspondant aux goûts des utilisateurs, ce qui conduira l'algorithme à proposer à un amateur de chanson française ou de cinéma français des contenus essentiellement français.

De manière concrète, il apparaît que la fragilisation de l'identité culturelle française et européenne sur les réseaux sociaux réside davantage dans le non-respect de certains droits d'auteurs par les plateformes. En effet, l'agrégation par ces plateformes de contenus culturels, et parmi ceux-ci de contenus issus de la presse en ligne, s'est longtemps faite au détriment du droit d'auteur.

Une prise de conscience du danger de la destruction induite de valeur et de l'amoindrissement de l'identité culturelle a conduit l'Union européenne à adopter le 15 avril 2019 la directive sur le droit d'auteur afin de rétribuer plus justement les éditeurs de presse mais aussi les artistes et, plus généralement, les créateurs de contenu. Elle crée un droit voisin au profit des agences de presse et des éditeurs de presse, socle commun des contrats portant sur l'exploitation des droits d'auteur et des droits voisins et un nouveau mécanisme dit de « licence collective étendue » grâce auquel l'organisme de gestion collective des droits, comme la SACEM par exemple, négocie les accords au profit de ses membres mais aussi des non adhérents ce qui permet une protection accrue de l'ensemble des artistes face aux plateformes. Plus largement, l'article 17 de la directive, qui vise spécifiquement à accroître la responsabilité des plateformes – notamment des réseaux sociaux – a été transposé en droit français aux articles L. 137-1 et suivants du code de la propriété intellectuelle. Il est reconnu que ces plateformes ne peuvent plus bénéficier du régime de responsabilité allégé bénéficiant aux fournisseurs de services en ligne. Les plateformes de réseaux sociaux doivent désormais obtenir une autorisation préalable

308 Consultables sur https ://edpb.europa.eu.
309 Décision GPDP, 9 juin 2022 ; décision DSB, janvier 2022.
310 Décision de la CNIL, février 2022.

des titulaires de droit pour l'exposition de leurs contenus. Si cette autorisation n'est pas obtenue, les plateformes pourront tout de même démontrer qu'elles ont fourni les meilleurs efforts pour l'obtenir et qu'elles ont mis des dispositifs en place, en concertation avec les ayants droit, pour empêcher l'apparition et la réapparition en ligne de contenus non autorisés, notamment à base de filtres (par exemple, Youtube peut censurer la bande-son de certaines vidéos dont la musique est exploitée sans autorisation préalable). Par ailleurs les moyens de lutter contre le piratage sur les plateformes de partage de contenus en ligne sont renforcés.

2.1.2. Les réseaux sociaux et la démocratie : risque ou atout ?

Avant l'ère des réseaux sociaux, le débat politique était en pratique structuré autour des médias traditionnels, sur lesquels pesait une réglementation (différente suivant qu'était en cause la presse écrite ou la radio et la télévision) établie pour l'essentiel par le législateur lui-même et dont le respect était assuré soit par une autorité de régulation (pour la radio et la télévision) sous le contrôle du juge administratif soit directement par le juge (la presse). Le pluralisme, élément indispensable au bon fonctionnement d'une démocratie, était assuré par la diversité des organes de presse, d'une part, par les obligations d'équilibre du temps de parole et d'objectivité pour les stations de radio et les chaînes de télévision, d'autre part. Ces règles étaient définies plus strictement et leur respect surveillé de manière plus exigeante en période électorale voire pré-électorale. Les réseaux sociaux ont bousculé cet ordonnancement traditionnel, en permettant une efflorescence du débat au-delà de ce cadre traditionnel, mais aussi en favorisant « l'écrasement » des points de vue et la multiplication des contenus les plus polémiques ainsi que des *fake news* grâce à la viralité particulière que promeuvent les réseaux sociaux par leur fonctionnement algorithmique.

Les réseaux sociaux lors des rendez-vous électoraux

- *L'utilisation des réseaux sociaux confronté au droit électoral*

Le « mégaphone virtuel », d'une puissance inédite, que constituent les réseaux sociaux, notamment en période électorale, a vite démontré les limites du régime traditionnel des médias. Soumis uniquement au droit commun, les réseaux sociaux ne se préoccupent pas du pluralisme, qui ne repose dès lors, concrètement, que sur la capacité de chaque utilisateur à assurer un minimum de diversité aux contenus qu'il recherche en ligne[311], ce qui est d'autant plus difficile que la logique de l'algorithme conduit au contraire à lui proposer du contenu correspondant à celui qu'il a l'habitude de consommer… L'effet est particulièrement délétère pour les personnes qui assurent l'essentiel de leur information sur les réseaux sociaux, ce qui tend à se développer, en particulier chez les jeunes.

Sans imposer un respect du principe du pluralisme qui, pour l'instant, ne s'applique qu'aux médias traditionnels, **diverses règles ont été adaptées à l'apparition des**

311 M.-L. Denis, « La régulation audiovisuelle et l'élection présidentielle », *NCCC*, n° 34, janvier 2012

réseaux sociaux. La modification de l'article L. 49 du code électoral par la loi pour la confiance dans l'économie numérique en 2004 a **interdit à partir de la veille du scrutin à zéro heure la diffusion par tout moyen de communication au public par voie électronique** de tout message de propagande électorale. Cette disposition a servi de fondement à la régulation des campagnes en ligne[312]. Les doutes relatifs à la sincérité du scrutin[313] lorsque le résultat du scrutin témoigne d'un faible écart de voix, peuvent également conduire le juge à annuler une élection, comme cela a été le cas en raison de tracts de campagne irréguliers postés sur Facebook[314], ou simplement de l'utilisation d'une page Facebook de nature à créer une confusion dans l'esprit des électeurs[315].

Par ailleurs, **l'interdiction faite aux candidats d'utiliser des moyens publics à l'occasion des campagnes** a trouvé à s'appliquer aux communications sur les réseaux sociaux. Ainsi, la Commission nationale de contrôle de la campagne **électorale** en vue de l'élection présidentielle a-t-elle rappelé que l'exercice de fonctions publiques, qu'elles soient de nature présidentielle, gouvernementale, administrative ou relevant d'une collectivité territoriale, est soumis au principe de neutralité du service public, excluant toute utilisation de moyens publics et fixant les principes applicables aux visites de candidats dans les services publics. Elle a rappelé aussi dans un communiqué du 11 mars 2022 que l'utilisation de tous moyens publics dans le cadre de la campagne électorale en vue de l'élection présidentielle est strictement prohibée par la loi n° 62-1292 du 6 novembre 1962 relative à l'élection du Président de la République au suffrage universel et a demandé au candidat Emmanuel Macron de ne pas utiliser le compte Twitter du Président de la République conformément à l'article L. 52-1 du code électoral[316]. Dans un même registre, l'utilisation de Facebook par un maire sortant comme outil de propagande électorale a été sanctionnée par le juge, car cette page mélangeait les informations institutionnelles et la propagande liée à sa campagne[317].

---

312 CE, 27 juin 2016, n° 395413, JurisData n° 2016-013195, JCP A 2016, act. 584.

313 Le juge de l'élection sanctionne uniquement les irrégularités susceptibles d'influencer le résultat de l'élection, c'est-à-dire de manipuler le libre arbitre des électeurs, v. par exemple CC, 2 février 2018, n° 2017-5052 *AN, Français établis hors de France, 5e circ.*

314 Un faible écart (de 17 voix) a suffi à conduire le juge à annuler une élection municipale où des tracts avaient été ajoutés sur la page Facebook du maire sortant, rédigés sur un ton particulièrement polémique et alors que la campagne de communication était close, et avaient récolté 16 mentions "J'aime" (TA Strasbourg, 10 juin 2014, 1re ch., n° 1402111, *M. Frédéric H. c/ M. V., Mme S,* diffusion illicite de documents de propagande électorale sur la page Facebook d'un candidat à la veille du scrutin, Legipresse, 2014. 319, p. 460. – M. Soulez et C. Legris, « Communication sur Facebook pendant la période électorale », *Lexing Contentieux Propriété intellectuelle*, 14 juillet 2014) ; Y. Gaudemet, *Encyclopédie des collectivités locales*, Chap. 2 (folio n° 11320), « Élections locales : propagande électorale », Coll. Loc.,

315 CE, 6 mai 2015, *Él. mun. de Hermès [Oise]*, n° 382518, T., AJDA 2015. 957 ; AJDA 2015. 1846, chron. G. Odinet et L. Dutheillet de Lamothe ; AJCT 2015. 450, Pratique M. Yazi-Roman pour un contre-exemple, ou en dépit du faible écart de voix, les messages postés même irrégulièrement n'ont pas eu d'effet de nature à altérer la sincérité du scrutin, v. CE, 27 juin 2016, *Él. des membres du conseil régional de Normandie*, n° 395413, Rec., note N. Escaut, « L'interdiction de diffuser des messages de propagande électorale la veille et le jour du scrutin à l'épreuve des réseaux sociaux », *JCP Adm,* 13 février 2017, p. 22.

316 Les sites institutionnels du Gouvernement ou de la présidence de la République, comme ceux des collectivités territoriales, ne doivent pas être utilisés pour assurer la promotion de l'action du Gouvernement, du Président de la République ou d'une collectivité territoriale à des fins électorales. M.-C. de Montecler, « La commission de contrôle de la présidentielle s'agace », *AJDA* 2022, p.251.

317 V. CE, 6 mai 2015, n° 382518, *M. Pagn*, T., p. 686

Si, contrairement aux États-Unis, les périodes électorales sont relativement protégées de la **publicité politique ciblée** grâce au RGPD et aux règles contraignantes sur le financement de la vie politique et l'interdiction de la publicité commerciale à des fins de propagande électorale six mois avant un scrutin (art. 52-1 du code électoral), nul n'est à l'abri de manipulations, notamment extérieures, par des *hackers* ou des *bots*. L'Union européenne devrait prochainement examiner un texte relatif à la « publicité politique » dont l'objectif serait d'imposer des obligations de transparence aux partis politiques qui devront déclarer leurs dépenses de publicité sur les réseaux. L'objectif est que les citoyens sachent qui a payé pour pousser un message politique, quel budget a été alloué, qui a été ciblé et comment[318].

• *Les actions de déstabilisation des campagnes électorales à travers les réseaux sociaux*

Le bon déroulement d'une campagne peut être affecté par la diffusion de fausses nouvelles ou de propos diffamatoires (*cf.* l'affaire des *Macron leaks*[319]), de manipulations par diffusion massive de messages ou d'ingérences étrangères par des fausses identités voire des *trolls*.

La « **guerre de l'information** » est même devenue une nouvelle forme de conflit considérée comme telle par le ministère des armées qui s'est doté d'une doctrine militaire de lutte informatique d'influence[320]. L'invasion du Capitole par les partisans de Donald Trump en témoigne. Cet épisode a montré que les États démocratiques peuvent être potentiellement déstabilisés par des campagnes de désinformation et souligne la vulnérabilité du processus démocratique.

Différentes initiatives ont été prises pour endiguer ces phénomènes mais la tâche est complexe. En 2016, un "*Code of conduct*" (Code de conduite) a été conclu afin de lutter contre la désinformation durant les élections entre la Commission européenne et les GAFAM qui ont mis plusieurs années à le mettre en œuvre. **Dans une résolution adoptée le 10 octobre 2019 le Parlement européen** a souligné la menace que représentent les ingérences électorales étrangères pour les sociétés démocratiques européennes[321]. Le 22 décembre 2018, la France a adopté la *loi dite anti-fake news*[322] visant à incriminer la diffusion de fausses nouvelles en période

318 Proposition de règlement relatif à la transparence et au ciblage de la publicité à caractère politique COM/2021/731. *Le Figaro*, 13 octobre 2021, « Bruxelles veut encadrer la publicité politique ciblée sur les réseaux sociaux ».

319 Le 5 mai 2017, un lien vers un dossier supposé contenir des courriels compromettants de l'équipe d'En Marche est posté sur internet, relayé par des sites complotistes américains (notamment *alt-right* et *4chan*). En quelques heures, l'affaire est évoquée près d'un demi million de fois et d'importantes rumeurs se mettent à circuler. L'information est particulièrement relayée par des suprématistes blancs américains. On sait qu'environ 18 000 bots ont amplifié la diffusion par des *retweets* automatiques. Très vite, on s'aperçoit qu'il n'y avait rien d'intéressant dans ces fichiers truqués et que le vol et la mise à disposition de ces fichiers provenaient de services russes.

320 https ://aeromorning.com/blog/doctrine-militaire-de-lutte-informatique-dinfluence/

321 Résolution du Parlement européen du 10 octobre 2019 sur l'ingérence électorale étrangère et la désinformation dans les processus démocratiques nationaux et européen (2019/2810(RSP),

322 Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information. En période électorale, un individu peut saisir le juge des référés pour exiger le retrait d'une « *allégations ou imputations inexactes ou trompeuses d'un fait de nature à altérer la sincérité du scrutin à venir diffusées de manière délibérée, artificielle ou automatisée et massive par le biais d'un service de communication au public en ligne* ». Puis le juge dispose d'un délai de 48 heures pour statuer sur le retrait du contenu en cause : l'obligation éventuelle de retrait d'un contenu est alors imposée par l'autorité judiciaire.

électorale et à créer une procédure spécifique de référé qui, à ce jour, n'a jamais conduit à une condamnation[323]. La loi prévoit également **l'obligation** pour les opérateurs de plateformes en ligne dont l'activité dépasse un seuil déterminé de nombre de connexions sur le territoire français (5 millions) pendant **les trois mois précédant le premier jour du mois d'élections générales** et jusqu'à la date du tour de scrutin où celles-ci sont acquises, de fournir à l'utilisateur **une information loyale** sur l'identité de la personne qui porte une information se rattachant à un débat d'intérêt général, de fournir à l'utilisateur une information loyale, claire et transparente sur l'utilisation de ses données personnelles dans le cadre de la promotion d'un contenu d'information se rattachant à un débat d'intérêt général et de rendre public le montant des rémunérations reçues en contrepartie de la promotion de tels contenus. Ces informations sont agrégées au sein d'un registre mis à la disposition du public par voie électronique, dans un format ouvert, et régulièrement mis à jour au cours de la période mentionnée au premier alinéa du présent article.

De manière plus générale et même hors des périodes électorales, un devoir de coopération des plateformes est prévu par le Titre III de la loi (*cf. infra* 2.4). L'ARCOM peut suspendre la diffusion de certains services[324] qui diffusent de façon délibérée des fausses informations de nature à altérer le scrutin (art. 6 de la loi) voire résilier de façon unilatérale la convention avec la personne morale contrôlée par un État étranger ou placée sous l'influence de cet État « *si le service ayant fait l'objet de ladite convention porte atteinte aux intérêts fondamentaux de la Nation, dont le fonctionnement régulier de ses institutions, notamment par la diffusion de fausses informations* » (art. 8).

Suite au bilan mitigé de la loi de 2018, le décret n° 2021-922 du 13 juillet 2021 a créé Viginum, pour lutter notamment contre la propagation de fausses informations visant à déstabiliser le processus électoral français lors des élections présidentielles et législatives de 2022.

Les réseaux sociaux : « splendeur ou misère » de l'expression citoyenne ?

Les réseaux sociaux, potentielles *agora* ouvertes à tous les citoyens, constituent un outil exceptionnellement puissant, dont l'utilisation peut aussi bien s'avérer positive pour la démocratie que négative, les effets pouvant être décuplés par la puissance même de cet outil.

- *Les réseaux sociaux, misère de l'expression citoyenne ?*

De l'avis de plusieurs auteurs et chercheurs[325], les réseaux sociaux joueraient depuis quelques années un rôle majeur dans la déstabilisation de la vie politique des États et favoriseraient la montée en puissance de l'illibéralisme dans le monde occidental. En effet, il apparaît que les réseaux sociaux, loin de promouvoir le pluralisme des idées politiques, ont tendance au contraire à favoriser la radicalisation des idées en enfermant leurs utilisateurs les plus actifs dans leurs certitudes et même dans une expression toujours plus maximaliste de ces certitudes.

323 Mis en œuvre une fois en 2019 au sujet d'un *tweet* de Christophe Castaner lors des élections européennes, le juge estime que les propos en cause n'étaient pas manifestement erronés et que la loi ne s'appliquait pas car la diffusion des propos n'était ni artificielle, ni automatisée.

324 D. Chavalarias, *Toxic Data,* Flammarion, 2022.

325 D. Chavalarias, *Toxic Data,* Flammarion, 2022.

Les algorithmes de recommandation des plateformes, en effet, favorisent la reproduction du semblable et partant, tendent paradoxalement à appauvrir le débat démocratique. Or, le **principe du pluralisme**[326], comme composante de la liberté d'expression, n'a pas seulement pour objet de permettre aux idées, même minoritaires, de pouvoir être exprimées, il permet aussi, par la confrontation d'idées différentes, l'expression éclairée du vote des citoyens et favorise l'acceptabilité du « verdict des urnes ».

Certaines décisions de modération prises par des réseaux sociaux peuvent avoir une réelle incidence sur l'expression des partis politiques et le pluralisme[327]**.**

L'affaire *Casapound* (Italie)

En Italie, plusieurs décisions ont été rendues par le tribunal romain dont l'**affaire *Facebook contre Casapound***[328]. Elle concerne la suppression par Facebook des pages du parti politique d'extrême droite *Casapound Italia*, que l'opérateur a estimées contraires à ses CGU en raison de l'incitation à la haine qu'elles comportaient. Par une *décision du 12 décembre 2019,* la juridiction, statuant à juge unique, a fait droit à la demande en référé du parti *Casapound* tendant à contraindre *Facebook* à réactiver ses comptes, au motif que *Facebook* occupe une « position spéciale» et que, en raison du nombre important de ses utilisateurs, ce service était devenu l'un des principaux médias du débat politique italien. Pour le juge italien, l'exclusion du parti politique de la plateforme ne doit pas être analysée sous l'angle d'une rupture des relations contractuelles entre l'entreprise et l'utilisateur, mais comme **une atteinte au principe constitutionnel du pluralisme politique**, protégé par l'article 49 de la Constitution italienne. La juridiction retient ainsi, certes par une décision provisoire, l'illégalité de la mesure prise par *Facebook* et renvoie, selon les règles de procédures de droit italien, l'affaire à la formation collégiale. La formation collégiale, par une *décision rendue le 29 avril 2020*, confirme que *Facebook* ne pouvait pas exclure *Casapound* de l'utilisation de la plateforme. Toutefois, le tribunal a cette fois-ci considéré que le comportement de *Facebook* avait porté atteinte, non au principe du pluralisme des partis politiques, mais à la liberté d'expression et à la liberté d'association, principes constitutionnellement protégés par les articles 21 et 18 de la Constitution. **Le Tribunal en conclut ainsi que la société privée n'était pas en mesure de désactiver la page du parti sur la base du règlement contractuel** sans porter nécessairement atteinte aux principes visés.

Certains défenseurs de la liberté d'information considèrent aussi que les nouvelles technologies numériques représentent un danger pour la démocratie, en raison de leur rôle déterminant dans la guerre informationnelle[329].

326 CC, n° 2004-497 DC du 1er juillet 2004 : la décision fait référence au « *pluralisme des courants de pensées et d'opinions* » et affirme que « *le respect de son expression est une condition de la démocratie* ».
327 P. Auriel, M. Unger, « La modération par les plateformes porte-t-elle atteinte à la liberté d'expression ? Réflexions à partir des approches états-unienne » *(Zhang v. Baidu.com*, 2014) et italienne (*Casapound contro Facebook*, 2019), *RDLF* 2020. Chron. 80.
328 *Facebook c. Casapound* : Tribunal de Rome, ordonnance du 12 décembre 2019, n° 59264 et Tribunal de Rome, ordonnance du 29 avril 2020, n° 37/XVII/20.
329 C. Deloire, *La Matrice*, éd. Calmann-Lévy, mars 2022.

• *Les réseaux sociaux : splendeur de l'expression citoyenne ?*

L'arrivée d'internet et des réseaux sociaux constitue à l'évidence une révolution dans les modes de communication des citoyens. Jamais ceux-ci n'avaient eu une tribune aussi puissante et aussi directe pour s'adresser aux responsables politiques, débattre avec d'autres concitoyens, manifester leurs opinions. Ce porte-voix si puissant, si direct et si nouveau galvanise de nombreuses personnes. Des Printemps arabes à *Me too*, les réseaux sociaux ont ainsi puissamment contribué à l'émergence de nombreux mouvements citoyens, notamment celui des gilets jaunes[330]. Les réseaux sociaux promettent en effet une **démocratie directe numérique**, résurgence inattendue des démocraties directes antiques, où le citoyen peut discuter directement avec la « magistrature ». Dans un environnement fracturé marqué par l'individualisme, ces nouvelles formes de participation à la vie de la cité peuvent apparaître comme bienvenues[331].

Si les grandes plateformes sont souvent utilisées par des collectivités territoriales comme forum de discussion, d'autres réseaux sociaux « citoyens », plus proches des « ***Civics techs*** »[332], ont également vu le jour. Certains réseaux sociaux permettent ainsi de faire vivre une vie de quartier, de participer aux actions locales[333]. Le réseau collaboratif *Confidens* a ainsi permis pendant plusieurs années à des petites villes de France (de moins de 50 000 habitants) de partager des informations locales et de faire vivre la démocratie locale. Modéré par des utilisateurs, son fonctionnement permettait de publier des informations vérifiées et lutter directement contre les fausses informations. Bien que le service rendu soit réel et comme de nombreux dispositifs de *civics techs*, la difficulté de trouver un modèle économique pérenne l'a contraint à s'interrompre.

Si certains se montrent très favorables à ces écosystèmes, d'autres les voient comme des dispositifs fragilisant la **démocratie représentative**[334]. Pourtant, certaines plateformes, comme *Make.org*, se révèlent complémentaires de la démocratie représentative et peuvent permettre au contraire de la renforcer. Lancée en 2016, la plateforme consiste à recueillir les suggestions citoyennes et à mettre en relation des opinions variées pour tenter d'en faire émerger un consensus. Ayant pour objectif de lutter contre l'impuissance politique des citoyens en permettant de mener des actions parallèles à celles du gouvernement, elle a lancé des consultations citoyennes comme par exemple « Comment construire des villes plus durables pour tous ? » (2021). Déjouant les biais traditionnels des réseaux sociaux classiques, tels que la modération algorithmique opaque, à laquelle est préférée une modération en *open source*, couplant l'IA et le contrôle humain, ou encore le financement par annonceurs au profit d'un système philanthropique, le dispositif apparaît fiable et protecteur des données personnelles.

330 D. Chavalarias, *Toxic Data,* Flammarion, 2022.

331 L. Blondiaux. *Le nouvel esprit de la démocratie. Actualité de la démocratie participative.* Seuil, 2008.

332 V. note 42.

333 *Nextdoor* est l'endroit où les quartiers se rassemblent pour accueillir les nouveaux voisins, échanger des recommandations et s'informer sur les dernières actualités locales, où les voisins soutiennent les commerces locaux et reçoivent les dernières nouvelles de la part des services publics, où les voisins empruntent des outils et vendent des canapés.

334 CNIL, site internet, 10 décembre 2019, « Évènement : les civic tech bouleversent-elles vraiment la démocratie ? ».

Reste qu'il n'est pas toujours aisé de donner une véritable légitimité à cette forme de « parole citoyenne », notamment en raison des modalités selon lesquelles elle est recueillie. L'utilisation des réseaux sociaux comme outils de participation citoyenne soulève des enjeux nouveaux : il s'agit d'élaborer des outils de participation capables de fournir des résultats clairs, représentatifs, transparents et infalsifiables tout en préservant l'accessibilité des dispositifs et la vie privée des citoyens[335]. L'enjeu des prochaines années sera de conserver les aspects positifs de ces réseaux sociaux et de ces *civics techs* afin de les envisager comme des compléments nécessaires mais non suffisants à la démocratie représentative.

-- *Les réseaux sociaux en période de crise : l'exemple de la guerre en Ukraine*

Les réseaux sociaux se sont révélés, en période de crise, des outils incontournables de propagande, de résistance voire de soutien logistique direct aux conflits[336] et leur maîtrise est de ce fait, au cœur d'enjeux stratégiques. Ce constat a d'ailleurs conduit le législateur européen à inscrire dans le DSA un article dédié aux protocoles de crise (art. 37).

Alors que l'épidémie de Covid-19 avait déjà montré combien les réseaux sociaux pouvaient servir de véhicule puissant aux thèses « conspirationnistes » mais aussi de relais efficace d'une forte politique de promotion vaccinale par les pouvoirs publics, la récente guerre en Ukraine a donné un tour nouveau à la question de l'utilisation des réseaux sociaux par les pouvoirs publics[337]. L'attaque russe contre l'Ukraine débutée le 24 février 2022 a posé rapidement la **question du contrôle des informations** accessibles, partie intégrante de la stratégie militaire. Les autorités russes ont ainsi rapidement pris les mesures nécessaires pour empêcher l'accès des Russes à Facebook et Instagram[338]. Face au risque de censure de Wikipédia par Moscou, de nombreux Russes ont téléchargé l'ensemble des articles présents sur Wikipédia, afin d'y avoir accès au cas où le site viendrait à être bloqué par la suite[339].

Les réseaux sociaux ou les sites qui comportent une fonction accessoire de discussion (notamment de géolocalisation) se révèlent par ailleurs très utiles aux forces combattantes, montrant ainsi que, au-delà de la maîtrise de l'information, les réseaux sociaux peuvent même constituer des **sources directes et opérationnelles de renseignement** pour les belligérants (les utilisateurs authentifient et géolocalisent des images de conflits qui deviennent des outils clés pour les opérations militaires voire pour la conduite d'enquêtes sur d'éventuels crimes de guerre[340]).

335 C. Mabi, « La « *civic tech* » et « la démocratie numérique » pour « ouvrir » la démocratie ? », *op.cit,* p. 244.
336 B. Campion, « La guerre en quasi-direct sur les réseaux sociaux : révolution et enjeux des sources ouvertes », *Association la nouvelle revue,* 2022/3 n° 11, consultable sur www.cairn.info.
337 *Philosophie magazine*, *site internet,* 18 mai 2022, « Vers une « ubérisation » de la guerre en Ukraine ».
338 *Le Monde*, *site internet,* 21 mars 2022, « La Russie interdit Facebook et Instagram pour 'extrémisme '».
339 *Le Monde,* site internet, 15 mars 2022, « Guerre en Ukraine : Wikipédia, menacée de blocage en Russie, poursuit sa documentation du conflit ». *Numerama*, site internet, 22 mars 2022, « En Russie, Wikipédia est de plus en plus téléchargé par crainte d'un blocage ».
340 B. Campion, *op. cit.*

Les réseaux sociaux ont également été utilisés par les ambassades occidentales à Kiev : l'Ambassadeur de France en Ukraine a ainsi souligné l'importance de cette nouvelle forme de communication, d'une part, pour informer en direct les Français expatriés des mesures de précaution à prendre ou pas, notamment s'agissant des évacuations, et, d'autre part, pour relayer auprès du public, notamment ukrainien, les positions et les actions conduites par la France. L'ambassadeur de France en Afghanistan lors de l'évacuation conduite au moment du retour des Talibans au pouvoir à Kaboul avait fait les mêmes remarques[341].

La maîtrise de l'information politique et stratégique est capitale pour les États, rendant d'autant plus délicate la place qu'occupent les réseaux sociaux en tant que nouvelle source d'information au sein des démocraties contemporaines.

-- Les réseaux sociaux, une nouvelle source d'information anomique ?

Dans une démocratie, les médias jouent un rôle crucial dans l'organisation du débat. Du fait de cette spécificité, ils sont, selon les temps démocratiques – période électorale ou non – et selon les pays, soumis à des règles plus ou moins contraignantes leur demandant de faciliter l'expression de toutes les voix afin de garantir un débat démocratique de qualité.

Aux États-Unis, pendant longtemps, la ***Fairness Doctrine***[342] imposait aux médias de présenter de manière impartiale des opinions plurielles. Elle avait été reconnue par la Cour Suprême des États-Unis dans un arrêt célèbre de 1969[343] : « *La parole concernant les questions publiques,* disait la Cour, *est plus qu'une affaire de libre expression, elle tient à l'essence même du gouvernement du peuple par lui-même.* » Le mouvement de dérégulation initié dans les années 1980, suivi d'une augmentation massive du nombre de médias, et l'essor du financement par la publicité ont largement ébranlé cette doctrine. Peu à peu, les médias se sont spécialisés et les points de vue se sont cloisonnés. La France, également touchée par ce phénomène d'éclatement et d'expansion médiatique (notamment avec les chaînes d'information en continu), a au contraire maintenu **l'obligation de pluralisme sur les chaînes de radio et de télévision** en confiant au CSA, désormais ARCOM, la mission de veiller à son respect.

Cependant l'apparition des réseaux sociaux dans la sphère informationnelle a d'autant plus renforcé la polarisation du débat que ces derniers, qui ne sont pas des médias au sens strict, revendiquent leur statut d'hébergeur et ne sont pas soumis au principe du pluralisme[344]. A l'heure où un nombre croissant de personnes ne s'informent plus qu'à travers les réseaux sociaux, où les fils d'actualités sont fortement déterminés par les algorithmes des plateformes, le maintien du pluralisme, indispensable à une démocratie vivante et solide, doit trouver de nouvelles formes.

341 *cf.* R. Le Goff, « La 'Tweet diplomacy' », *L'ADN,* 25 mai 2002.
342 Politique de la Commission fédérale des communications américaine (FCC) introduite en 1949.
343 *Red Lion Broadcasting Co. v. FCC*, 1969. L. Blondiaux, B. Manin, *Délibération politique et principe du contradictoire in le Tournant délibératif de la démocratie*, Presses de Sciences Po, 2021.
344 J.-L. Missika, H. Verdier, *Le business de la haine*, Calman Levy, 2022.

2.2. Les défis pour l'espace public et la vie en société

Les réseaux sociaux ont engendré de nombreux bouleversements. Le débat public a changé d'aspect, le rapport à l'identité et à la vie privée s'est complexifié, des mutations économiques, sociales et environnementales ont vu le jour, enfin de nouveaux dangers sont apparus.

2.2.1. La transformation du débat public comme lieu d'échanges et d'information

Le débat public a été transformé par les réseaux sociaux tant dans sa nature que dans son rythme. Son assise s'est élargie, son contenu s'est étoffé mais il est aussi devenu plus vulnérable et les discours de haine et les fausses informations y ont trouvé un terrain propice à leur déploiement. Dans un premier temps affaiblis, les médias traditionnels, contraints de s'adapter à ce nouveau paysage, retrouvent peu à peu leur place structurante. A l'aune de ce nouveau média, ils se sont transformés à la recherche de nouveaux équilibres.

Les apports indéniables des réseaux sociaux pour l'espace public : l'exceptionnelle multiplication des échanges individuels, l'enrichissement du débat public et la diminution de l'isolement

Même si la liberté d'expression est garantie en droit, son exercice effectif n'a, en pratique, que rarement été mis en œuvre de façon égalitaire. Pour profiter d'une réelle publicité, l'expression nécessitait auparavant l'utilisation d'intermédiaires tels que les médias audiovisuels, de radio ou de presse écrite. La notoriété ou des qualités particulières (experts, politiques, journalistes) conditionnaient donc l'accès au public. Ce type de fonctionnement, outre son caractère vertical et élitiste, présentait le risque de favoriser une pensée majoritaire au détriment de mouvements de pensées plus minoritaires ou dissonants. L'apparition d'internet puis des réseaux sociaux a changé ce mode de fonctionnement, permettant à tous les individus, malgré les frontières, les barrières sociales et culturelles, de faire valoir des opinions divergentes mais aussi de se rencontrer, de constituer des communautés, etc. **Les réseaux sociaux ont ainsi rompu des isolements, rassemblé des individus auparavant isolés autour de valeurs partagées, galvanisé des résistances et favorisé des actions citoyennes** (Printemps arabes, mouvement *metoo*, etc.).

Mais si internet et les réseaux sociaux sont devenus des outils incontournables et plébiscités, l'égalité dans l'accès au débat public s'est cependant révélée porteuse d'autres difficultés. En effet, ce mode de communication est aussi une aubaine pour les agitateurs et les prédicateurs de haine. Si la grande majorité des échanges se déroule sereinement, une minorité de contenus, par la nocivité qu'ils induisent, occupent une part démesurée du débat et affaiblissent voire remettent en cause les

bienfaits de ce nouveau mode de communication. A une communication verticale et balisée a succédé une profusion pleine de richesse mais aussi de désordre.

La multiplication des propos mensongers et violents

Un double phénomène peut être constaté. D'une part, les réseaux sociaux, par leur fonctionnement technique, accentuent la propagation des contenus polémiques, violents voire faux et confortent l'atomisation du débat ; d'autre part, les groupuscules les plus extrêmes ont trouvé dans cet outil de communication un moyen efficace de diffuser leurs idées et déstabiliser la société.

- *Le commerce de l'émotion et ses effets secondaires*

Parmi la multitude d'informations et de discussions échangées sur les réseaux sociaux les plus importants[345], un nouvel ordonnancement est apparu. A la sélection des contenus par des professionnels de l'information est venue se substituer une **sélection par l'émotion**. Au temps long du tri des contenus par les « personnes autorisées » a succédé la mise en avant immédiate des contenus les plus attirants. De nouvelles hiérarchisations du débat se sont ainsi formées. Plus le contenu est virulent, disruptif ou original quitte à être faux ou malveillant, plus il a de chance d'être transmis et vu.

Ce phénomène trouve notamment sa cause dans le modèle économique de ces réseaux qui repose sur l'*engagement* de l'utilisateur. Pour maximiser la rentabilité publicitaire, il est nécessaire que l'utilisateur passe le plus de temps possible sur le réseau et que l'opérateur recueille le plus grand nombre de données sur son comportement et ses goûts. Pour capter l'attention de l'internaute, différentes techniques sont utilisées. L'aléa de ce qui va apparaître crée une forte envie de rester sur le réseau – à l'instar du fonctionnement des machines à sous dans les casinos –, et l'apparition de contenus qui suscitent des sentiments forts, comme la colère ou l'indignation, qui agissent comme des *stimuli* sur les consciences, produisent de la dopamine et maintiennent sans cesse éveillés.

Les discussions sur les réseaux se sont révélées très souvent chaotiques et l'espace conversationnel a souvent davantage ressemblé à une **jungle** qu'à un espace délibératif[346]. Les attaques les plus violentes et les théories les plus excentriques ont tendance à être plus souvent mises en avant, les contenus les plus abscons voire les plus vils peuvent se trouver **propagés** au détriment de ceux basés sur la science et la raison. Pierre Bellanger déplore ainsi « *la privatisation de la vérité en micro-réalités alternatives portées par des factions rivales* » et la disparition progressive de la confiance collective[347]. Gérard Bronner dénonce « *la lazy thinking* »[348] (pensée paresseuse) qui conduit à favoriser les théories du complot et les fausses informations, à relativiser toute affirmation et à « **polariser** » le débat. Ces phénomènes présentent le risque d'accroître la défiance à l'égard des autorités et de nuire à la vie démocratique[349].

345 Les propos qui suivent ne concernent que les réseaux les plus puissants qui fonctionnent grâce à la publicité ciblée.

346 J.-L. Missika, H. Verdier, *op.cit.*

347 P. Bellanger, *Internet et le serpent arc-en ciel*, 18 avril 2010.

348 G.Bronner. *Apocalypse cognitive*, PUF 2021.

349 *Les lumières à l'ère numérique*, rapport de la commission présidée par G. Bronner

• *Un outil efficace aux mains des plus activistes*

Les individus et groupes les plus radicalisés ont trouvé un lieu d'expression idéal dans les réseaux sociaux (mais aussi dans les messageries cryptées, ce qui complique le travail des forces de police). Certains utilisateurs pratiquent aussi *l'astroturfing*, qui consiste à mobiliser d'autres internautes pour créer des mouvements d'indignation entièrement fabriqués visant à « simuler un mouvement spontané », à modifier des résultats de sondage en ligne, à tromper les algorithmes de recommandation ou encore à harceler une personne[350]. Les analyses de chercheurs démontrent que les relais de fausses informations ou de contenus radicaux proviennent souvent des mêmes comptes et participent de la montée des extrêmes[351]. Les réseaux sociaux sont devenus les meilleurs instruments de l'apologie de la violence, le paramétrage des algorithmes, qui met en avant les contenus qui suscitent le plus d'engagement, conduisant à **propager plus rapidement et plus loin** (hors du cercle premier) **les contenus violents ou haineux**[352]. L'épisode de l'attentat de Christchurch en est l'exemple le plus dramatique.

L'attentat de Christchurch (2019)

Le 15 mars 2019, l'attentat de Christchurch perpétré contre une mosquée néo-zélandaise et ayant fait 50 morts, est diffusé en direct par le terroriste pendant dix-sept minutes sur Facebook Live. Recopiée à de nombreuses reprises, la vidéo se répand sur les autres réseaux sociaux avant que les modérations ne puissent réagir. Dans un communiqué du 19 mars, le réseau social se défend en affirmant avoir supprimé 1,5 millions de copies de la vidéo en vingt-quatre heures. Il reconnaîtra par la suite que plus de 300 000 copies ont échappé à sa modération. Cette défense ne réussit pas à calmer les critiques émanant notamment des autorités néo-zélandaises qui appelaient à de véritables engagements des plateformes. En mai 2019, Facebook prend l'engagement d'investir 7,5 millions d'euros dans des partenariats de recherche afin d'améliorer les **techniques de modération** algorithmique et de bannir systématiquement de Facebook Live toute personne ne respectant pas les politiques de Facebook. En mai 2019 « l'appel de Christchurch », initié par la France et la Nouvelle-Zélande, signé entre plusieurs gouvernements et plateformes de réseaux sociaux avec pour objectif d'améliorer la lutte contre la diffusion de contenus terroristes en ligne est également signé par Facebook.

Il faut relever que, très récemment, deux minutes ont suffi à la plateforme Twitch pour interrompre la retransmission en direct de la fusillade de Buffalo en mai 2022[353].

350 J.-L. Missika, H. Verdier, *op.cit.*
351 *Cf.* travaux de D. Chavalarias, *Toxic Data,* Flammarion, 2022.
352 S. Vosoughi, D. Roy, S. Aral, *The spread of true and false news online*, Science, 2018.
353 RTBF, *Tuerie de Buffalo : la mort en direct, l'impossible défi des réseaux sociaux*, 19 mai 2022.

S'agissant **des fausses informations**, la difficulté est la même. La « **viralité** » des propos accentue leur portée et leur effet délétère. Ainsi sur Twitter, 6% des comptes sont des *bots* qui sont responsables de 33% des *tweets* relayant de fausses informations[354]. Les discours de haine et les fausses informations ne sont évidemment pas apparus au XXIe siècle mais internet et les réseaux sociaux leur ont conféré un portevoix inédit. De nombreux auteurs soulignent que ces effets ne sont pas voulus par les opérateurs mais sont consubstantiels à une entreprise qui fait commerce de l'influence sociale.

Les algorithmes, véritables nuisibles ou simples boucs émissaires ?

Les opérateurs, en mettant à disposition des internautes des outils permettant de réagir, de classer, de recommander certains contenus ou les mettre à l'écart, sont accusés d'être responsables de la déstructuration du débat public. Le *design* des interfaces est critiqué car les **fonctionnalités offertes** (*like*, *retweet*, etc.) qui permettent, sans aucune conséquence pour l'utilisateur, de « pousser » des contenus sans vérification de leur véracité ni débat contradictoire. Plus encore, ce sont les **algorithmes de recommandation** qui sont accusés de mesurer arbitrairement le niveau de pertinence d'un contenu et de favoriser ceux qui « capturent » le plus longtemps possible l'attention des internautes[355]. L'ombre de la manipulation des opinions semble ainsi planer sur les réseaux sociaux. Plusieurs expériences ont démontré que les fils d'actualité se modifient en fonction des réactions des utilisateurs[356] et que ne sont proposés aux internautes que des contenus qui correspondent à leurs goûts de sorte que se forment des effets de *clustering* ou « **des bulles de filtre** »[357] qui ont tendance à enfermer les utilisateurs dans des schémas de pensée et favorisent le phénomène de « **chambre d'écho** ». Les algorithmes dits de recommandation sont accusés de favoriser les contenus les plus « stimulants » qui seront aussi les plus viraux contribuant ainsi à accentuer la **polarisation** du débat public. Les algorithmes sont même accusés de **biaiser** les résultats en conduisant à discriminer parfois les personnes, volontairement ou involontairement, en fonction de leur genre, de leur origine ethnique, ou encore

354 Ch. Shao et al., « The spread of low-credibility content by social bots », *Nature Communications*, vol. 9, 2018.

355 F. Tarissan explique que d'un tri par popularité (nombre de références), par autorité (indicateurs de ceux qui créent les pages web) puis par notoriété (nombre de tweet, de *like*), les opérateurs sont passés à un tri par prédiction. Conscientes que les utilisateurs manipulent aussi les outils proposés, les plateformes se réfèrent à d'autres outils comme le *wachtime* (temps passé) pour comprendre ce qui intéresse réellement les internautes et affiner le tri. F. Tarissan, *Au cœur des réseaux. Des sciences aux citoyens*, Le Pommier, Paris, 2019.

356 D. Chavalarias. *Toxic Data*, Flammarion, 2022.

357 E. Pariser, *The Filter Bubble : What the Internet Is Hiding From You*, Londres, Penguin Press, 2011. Dans son ouvrage (ibid), F. Tarrissan explique cette expression : « *Parce qu'ils agissent en amont sur les informations à laquelle un utilisateur peut avoir accès et parce qu'ils filtrent celles-ci avant que l'utilisateur ne puisse décider par lui-même si elles sont pertinentes ou non, les algorithmes créent une bulle autour de chaque internaute, l'empêchant d'être exposé à l'ensemble des points de vue existants. Autrement dit, non seulement un utilisateur ne décide pas de l'information qui lui est proposée mais, et c'est ce qui rend le phénomène particulièrement pernicieux, il n'a surtout pas connaissance de ce qui est rejeté par l'algorithme* ».

de leur orientation sexuelle[358]. La défenseure des droits a consacré un rapport sur la difficile question de l'automatisation des discriminations par les algorithmes[359].

Si les chercheurs dénoncent un manque global d'accessibilité à ces algorithmes, que le *Digital Services Act* devrait améliorer, plusieurs études ont néanmoins pu être menées, qui ont démontré que les choix proposés par les algorithmes peuvent **influencer** les personnes ou **amplifier** des phénomènes[360], mais aussi qu'ils favorisent « l'auto-satisfaction » de l'utilisateur. Ainsi, quelle que soit l'efficacité du filtrage opéré par l'algorithme, il ne doit pas faire oublier le rôle du comportement de l'utilisateur lui-même[361]. De même, il a été démontré que les **biais algorithmiques**, qui sont réels, ne font que reproduire **les biais humains**. Ces derniers peuvent être le fruit de la mauvaise qualité des données d'apprentissage qui ont configuré l'algorithme, d'autres peuvent venir directement de représentations biaisées que les concepteurs ont transférées sans le vouloir à la machine, auxquels s'ajoutent des biais engendrés par les objectifs de rentabilité[362]. Certains opérateurs achètent des jeux de données pour entraîner leur algorithme et ne sont en pratique pas en mesure d'identifier d'éventuels biais. En réalité, la polarisation du débat public induite par les réseaux sociaux vient de ce que le mécanisme de filtre se conjugue **au biais de confirmation**, très analysé en sociologie, selon lequel l'être humain est attiré par des messages qui confirment sa vision des choses et que ce biais se renforce à mesure que lui sont transmis des messages auxquels il adhère. **Les réseaux sociaux renforcent donc ce biais et l'accentuent**[363]. Il est vrai qu'il n'est pas rare que des personnes soient inscrites dans plusieurs réseaux sociaux ce qui limite un peu l'effet de *chambre d'écho*[364].

Les règlements européens récemment adoptés tentent de prendre en compte la complexité de ces fonctionnements en sollicitant davantage de transparence ainsi que la mise en place par les opérateurs de solutions adaptées aux risques systémiques identifiés. Mais il reste encore du chemin à parcourir pour comprendre ces écosystèmes et adapter la régulation à ces paramètres. Une plus grande ouverture à la recherche, prévue en principe par le DMA et le DSA, est à cet égard indispensable.

---

358 Un algorithme entraîné avec des jeux de données biaisés peut donner des résultats discriminatoires. *Le Figaro,* « Un algorithme de Facebook confond des personnes noires avec des singes », 4 septembre.2021.

359 Des recherches ont montré que certains systèmes de reconnaissance faciale avaient plus de difficultés à identifier les femmes et les personnes non blanches à cause du manque de représentativité des données utilisées. Ces données étaient majoritairement nourries par des visages « masculins et blancs ». Le même problème a été constaté pour certaines technologies d'identification vocale, ces dispositifs ayant été construits sans avoir pensé aux femmes et à leurs voix. V. Défenseure des droits, site internet, l'article « algorithmes-prevenir-lautomatisation-des-discriminations ».

360 L'algorithme de Twitter a été accusé d'amplifier la paroles conservatrices. *Cf. Toxic Data op. cit.*, p. 88.

361 E. Bakshy, S. Messing, L. A. Adamic, « Exposure to ideologically diverse news and opinion on Facebook », *Science* 348 (6239), 2015.

362 T Grison, (T.), « IA et modération des réseaux sociaux : un cas d'école de 'discrimination algorithmique' », *The Conversation*, 9 septembre 2021.

363 D. Chavalarias, *Toxic Data,* Flammarion, 2022.

364 Il faut également prendre en compte dans ce débat le rôle de l'algorithme de recommandation des moteurs de recherche qui guide voire influence les recherches des internautes de manière significative.

Si la nature du débat public a été modifiée sous l'effet conjugué de l'usage et des fonctionnalités des réseaux sociaux, son rythme l'a également été.

L'atomisation par l'accélération du débat

Le fonctionnement des réseaux sociaux est fondé sur l'**alerte** et la **transmission** (notification/retweet). Poussés par l'effet de dépendance à ces réseaux et par les stimulations permanentes et instantanées des messages et de certains contenus (parfois éphémères, comme les *stories*), les utilisateurs ont tendance à accélérer sans cesse le rythme des échanges qui peut aller jusqu'à devenir frénétique. Ce « *réchauffement médiatique* » comme l'appelle Dominique Boullier n'est pas sans lien avec le processus d'engagement sur lequel repose l'écosystème des réseaux sociaux fondé sur la publicité ciblée[365]. Selon cet auteur, « *l'impératif d'expression* » et la « *tyrannie du buzz* » engendrent une effervescence et une pression incontrôlée sur le débat, incompatibles avec la qualité de discussions contradictoires et éclairées. Même dans le domaine de la recherche scientifique, on peut constater la multiplication des *preprint*[366]. Si les réseaux sociaux n'en sont évidemment pas la seule cause, leur rôle n'en est pas moins essentiel à cet égard et leur fonctionnement produit des effets au-delà de leurs utilisateurs. Les médias classiques reconnaissent que, outre le choix des sujets d'actualité, le rythme de l'information est de plus en plus dicté par des réseaux comme notamment Twitter. Il a été démontré que beaucoup des personnes qui retransmettent un message sur Twitter (*retweet*) ne l'ont même pas lu. **La réaction prend souvent la place de la réflexion critique** de sorte qu'il est permis de se demander s'il ne faut mettre en place des outils de décélération.

Les médias traditionnels au secours du débat public ?

L'apparition du numérique et plus spécifiquement des réseaux sociaux a profondément bouleversé le secteur des médias[367]. Les individus ne s'informent plus de la même façon, les marchés publicitaires se tournent désormais de plus en plus vers les réseaux sociaux et ont tendance à se détourner des médias traditionnels, aggravant la crise de ce secteur. Pour suivre l'actualité, une part croissante de personnes a recours aux réseaux sociaux, où l'information est accessible gratuitement *via* les fils d'actualités des réseaux. La proportion des Français s'informant *via* les médias sociaux est ainsi passée de 18% en 2013 à 38% en 2021 et cette proportion atteint même les 2/3 s'agissant des Français de moins de 35 ans.

Cette situation a d'abord contraint les médias traditionnels à chercher à s'aligner sur la vitesse du numérique et à fournir des articles de plus en plus courts et réactifs pour le web[368]. Il est vrai que l'on a assisté aussi à un retour des abonnements pour

365 D. Boullier, *Comment sortir de l'emprise des réseaux sociaux*. Le passeur. 2020.
366 Travaux provisoires, non finalisés.
367 D. Cardon, *Culture numérique*, *op. cit.*
368 J. Cagé, N. Hervé, M.-L. Viaud, *L'information à tout prix*, Paris INA Edition, 2017.

bénéficier des avantages du journalisme de qualité permettant d'authentifier des informations et de fournir des analyses de qualité nécessaires à la bonne tenue du débat public[369]. En outre, il faut relever que, s'agissant des supports d'information, les médias traditionnels qui sont aussi présents sur les réseaux sociaux conservent une part dominante.

Dans un contexte de multiplication des fausses informations, de nombreux médias se sont dotés d'un **service de *fact checking*** destiné à vérifier la véracité d'informations notamment les citations publiques de personnalités en remontant à la source. Outre les chartes éditoriales et la charte de Munich de 1971, qui guident le travail de journalisme, ces services respectent les principes de l'International Fact-Checking Network (IFCN)[370]. Ce mouvement a été accéléré suite à l'élection américaine de novembre 2016 durant laquelle de nombreuses *fakes news* ont circulé. Certains réseaux sociaux eux-mêmes ont mis en place des services collaboratifs de *fact cheking* comme Twitter aux États-Unis. Des médias se sont également dotés d'outils pédagogiques pour fournir un guide de compréhension de l'actualité[371]. En France, le journal 20 minutes a ainsi créé un partenariat avec Facebook qui lui demande de vérifier des informations. Quand l'information a été vérifiée (« *fact checkée* »), un « *pop-up* » informe le public. Dans certains cas, un bandeau peut apparaître signalant qu'il s'agit d'une fausse information et renvoyant vers l'article réalisé par le média.

Certains voient dans ces pratiques une forme de « police de la pensée », estimant qu'elles imposent une prétendue vérité, même dans les domaines qui relèvent de l'opinion[372]. Il est certain que la frontière peut parfois être floue entre ce qui relève du fait et de l'interprétation et la préservation de la liberté d'expression justifie que ces distinctions soient maniées avec la plus grande prudence. Le Conseil constitutionnel dans sa décision relative à la loi du 22 décembre 2018 a retenu une conception stricte de la fausse information. Celle-ci ne peut s'appliquer qu'à «*des allégations ou imputations inexactes ou trompeuses d'un fait de nature à altérer la sincérité du scrutin à venir. Ces allégations ne recouvrent ni les opinions, ni les parodies, ni les inexactitudes partielles ou les simples exagérations. Elles sont celles dont il est possible de démontrer la fausseté de manière objective. [...] Seule la diffusion de telles allégations ou imputations répondant à trois conditions cumulatives peut être mise en cause : elle doit être artificielle ou automatisée, massive et délibérée*»[373].

369 *Cf.* le succès du New York Times accessible par abonnement.

370 Il s'agit d'une fondation principalement financée par des dons privés et qui met à disposition des outils divers de *fact-checking*. L'organisme a été fondé par un italien qui faisait du fact-checking en Italie qui se rendait compte que certaines *fake news* traversaient les frontières, d'où le besoin de regrouper les différentes initiatives. Un correspondant français certifie la conformité des services à la charte de l'IFCN qui contient des exigences de transparence et d'impartialité.

371 Rubrique les décodeurs du journal *Le Monde*.

372 J.-P. Chazal, « Fact checking : une police de la pensée ? », *Dalloz*, 2022, p.65.

373 DC n° 2018-774 DC du 20 décembre 2018.

2.2.2. La transformation de l'identité sociale et de la vie privée

Au-delà des mots exprimés, c'est l'existence de l'homme comme « *animal social* »[374] qui se trouve modifiée par les réseaux sociaux. Confortant la thèse de Norbert Elias selon laquelle il faut cesser d'opposer l'individu et la société et que seules comptent les relations et les interdépendances qu'elles définissent[375], la vie privée des individus se trouve redessinée par les réseaux sociaux. De l'identité à la mort, de l'expression publique à l'expression privée, les réseaux sociaux transforment le rapport de l'individu au monde. Sa vie, parfois inlassablement exposée sur la toile, peut finir par lui échapper. Si dans le monde virtuel, l'homme ne peut laisser l'empreinte de ses pas, il laisse de nombreuses « traces numériques » qui nourrissent les immenses bases de données.

Les identités multiples et la redéfinition de la vie privée

Autrefois, seules les personnes publiques devaient « maîtriser leur image » et leur expression publique. Désormais chaque individu présent sur les réseaux sociaux construit son identité publique, peut choisir les informations qu'il souhaite divulguer et dans quel cercle il le fait. Il peut aussi user de pseudonymes pour s'exprimer plus librement. Ainsi se construisent différentes identités (identité professionnelle, identité amicale, identité liée à un centre d'intérêt, identité politique, etc.), autant de facettes qui souvent se complètent, parfois s'opposent voire s'entrechoquent. Des paroles dites dans un contexte non professionnel peuvent, ainsi avoir des conséquences sur la perte d'un emploi ou des sanctions disciplinaires[376], des images festives postées sur le net peuvent revenir en *boomerang* et dissuader un futur employeur d'embaucher une personne, des photos ou des vidéos peuvent être utilisées pour des vengeances (*revenge porn*). La maîtrise de ces nombreuses identités n'est pas toujours aisée même si certains adeptes des réseaux sociaux, souvent les plus jeunes, en sont devenus de véritables experts[377]. Par ailleurs, les réseaux sociaux encouragent une volonté parfois excessive d'affirmation de soi, laissant peu de place aux personnalités les plus réservées. Les enquêtes soulignent ainsi que les sentiments de tristesse et de mélancolie sont presque tabous sur les réseaux sociaux.

En réalité**, la fabrication de l'identité numérique consiste paradoxalement à donner l'illusion d'une image naturelle et authentique alors qu'elle est le plus souvent très travaillée.** La question n'est dès lors pas d' «être ou ne pas être » mais d'être ou de ne pas être visible. Le sociologue Dominique Cardon a théorisé ce phénomène qui s'appuie sur deux variables que sont « les identités multiples »[378] distinguées

374 Formule prêtée à Aristote.

375 N. Elias, *Qu'est-ce que la sociologie ?*, trad. de l'all. par Y. Hoffman, Aix-en-Provence, Pandora, 1981, La Tour-d'Aigues, L'Aube, 1991, p. 156-158.

376 *Cf.* 1.2.2.2

377 S. Livingstone et A. Third, Children and young people's rights in the digital age : an emerging agenda », *New media and Society*. 19, 2017

378 D. Cardon, *Culture numérique*, *op. cit.* : « *Nous ne sommes pas exactement la même personne quand nous interagissons avec notre famille, nos collègues et amis ou avec des inconnus. Ce que l'on dit et la manière dont on le dit ne cessent de varier selon la distance spatiale, le degré de retenue ou de familiarité souhaité* ».

selon le degré d'articulation entre la vie réelle et vie virtuelle et le degré de visibilité que les réseaux sociaux donnent aux profils des internautes pour distinguer, d'une part, quatre identités différentes sur les réseaux sociaux (civile, agissante, narrative, virtuelle) et, d'autre part, quatre catégories de réseaux sociaux (paravent, clair-obscur, phare, mondes virtuels). Il démontre combien les réseaux sociaux offrent **une nouvelle structure à la vie sociale** avec des gradations différentes.

Parfois l'instrument échappe à ses utilisateurs et l'enjeu devient alors **la protection de la réputation**. Si le droit à l'effacement a été consacré par le RGPD, sa mise en œuvre effective n'est pas aisée. La CNIL publie ainsi des recommandations sur son site[379] et suggère à cet égard d'utiliser des pseudonymes, de ne pas publier des photos gênantes « *car leur diffusion est incontrôlable* »[380].

Dans ces conditions, quel sens a désormais **la notion de vie privée** à l'heure des réseaux sociaux ? En réalité, les internautes ne disent pas « tout et n'importe quoi » sur le web et se livrent le plus souvent, avec plus ou moins d'habileté et de maîtrise, à un véritable travail de mise en scène. « *La vie privée n'est plus tant une question de frontière que de contexte*. (…) *Chaque individu réclame de fixer sa propre définition du privé et du public* » et sollicite une protection très forte de ce qu'il ne souhaite pas divulguer[381]. Ainsi, la nature des informations divulguées tend à devenir moins importante que le cadre dans lequel elles ont été divulguées. Le critère de la *communauté d'intérêt*, utilisé par les juridictions judiciaires pour distinguer les propos tenus dans un espace privé ou public, est à cet égard toujours pertinent. **L'approche subjective et casuistique de la notion de vie privée et d'espace privé est donc plus que jamais pertinente**.

La mort sur les réseaux sociaux : la promesse d'une vie éternelle ?

Chaque jour, de nombreuses personnes décèdent et de nombreuses pages des réseaux sont laissées à l'abandon de sorte qu'on peut avoir le sentiment que l'on ne meurt jamais vraiment sur les réseaux sociaux[382].

Si la loi pour une République numérique du 7 octobre 2016 puis le RGPD ont introduit dans la LIL des dispositions qui définissent **des droits des individus relatifs à l'organisation du traitement de leurs données *post-mortem***[383] et **les droits des héritiers sur les données numériques du défunt**[384], en l'absence de demandes des héritiers ou de directives laissées en ce sens, la page continue d'exister, les responsables de traitement n'étant pas en mesure de faire la différence entre un compte inactif et le compte d'une personne décédée. En pratique, nombreux sont

379 CNIL, site internet, « Le droit à l'effacement : supprimer vos données en ligne ».

380 CNIL, site internet, « 10 conseils pour rester net sur le web ».

381 D. Cardon, *op. cit.*, p.185-186.

382 On estime à près de 8 000 le nombre de personnes inscrites sur Facebook qui décèdent chaque jour dans le monde. « Mort numérique : peut-on demander l'effacement des informations d'une personne décédée ? », CNIL,.28 décembre 2020.

383 Les personnes peuvent dorénavant donner des directives générales ou particulières relatives à la conservation, à l'effacement et à la communication de leurs données après leur décès.

384 En l'absence de directives données de son vivant par la personne, les héritiers auront la possibilité d'exercer le droit d'accès, s'il est nécessaire pour le règlement de la succession du défunt et le droit d'opposition pour procéder à la clôture des comptes utilisateurs du défunt et s'opposer au traitement de leurs données.

les réseaux sociaux qui, à travers les conditions générales d'utilisation des réseaux, refusent aux héritiers le droit d'accéder aux comptes en les considérant comme attachés à la personne. D'autres ont mis en place des procédures spécifiques (depuis 2015, il existe sur Facebook par exemple une possibilité de paramétrage de page commémorative, de désignation d'un légataire ou encore de suppression des informations du compte une fois le décès annoncé). En réalité, aucun texte ne répond directement à la question de la protection des données *post-mortem* et la question du statut juridique des données personnelles ressurgit à cet égard. Sont-elles protégées au titre des droits extrapatrimoniaux attachés à la personne (les rendant inaliénables et insaisissables) ou sont-elles des biens patrimoniaux transmissibles aux héritiers?

Face à la profusion des données numériques qui persistent après le décès des individus, certains réclament **le droit à la mort numérique** mais son fondement ne va pas sans difficulté[385] car le droit au respect de la vie privée n'a plus de portée après la mort[386]. Pour autant, plusieurs pistes pourraient être explorées : estimer qu'il existe un droit à la protection de la vie privée par ricochet pour les héritiers[387] ; recourir au principe de dignité qui fonde déjà le principe de protection du cadavre[388] ; reconnaître un droit à la suppression des données personnelles à la mort du détenteur[389] ; étendre le droit à l'oubli dans ce cas de figure ou consacrer un droit à l'auto-détermination des données personnelles comme le Conseil d'État l'avait proposé dans son étude de 2014[390] et inciter les individus à prévoir des dispositions testamentaires sur ce point[391].

La question de la « mort numérique », au-delà de l'opportunité de reconnaître un droit à la protection des données personnelles, met en exergue celle des « traces numériques » que les individus disséminent sur les réseaux sociaux et à bien d'autres endroits, laissant craindre, dans un futur proche, des atteintes à la vie privée de grande ampleur ou des détournements d'utilisation à des fins stratégiques.

Quelle protection de la vie privée dans un environnement saturé de traces numériques ?

Actuellement, l'une des plus grandes vulnérabilités des individus vient de ce que circulent sur la toile et/ou sont détenues par des entreprises ou des États peu démocratiques, des milliers de données qui permettent de déceler non seulement leurs goûts et centres d'intérêts, mais aussi leurs convictions politiques

385 C. Bordes, « Prévoir sa mort numérique. Le devenir des données numériques post-mortem », *RDLF* 2020, Chron. n° 09.

386 CCass., 1e civ., n° 97-15.756, 14 décembre 1999 ; V. C. Caron, « Les morts n'ont pas de vie privée », *Recueil Dalloz*, 2000, p.266 et s.

387 L. Castex et al., « Défendre les vivants ou les morts ? Controverses sous-jacentes au droit des données *post mortem* à travers une perspective comparée franco-américaine », *Réseaux*, n° 210, 2018/4, p. 120.

388 M. Fabre-Magan, « La dignité en droit : un axiome », *R.I.E.J.*, vol.58, 2007/1, p.7, 13 et 23.

389 Proposition de loi, n° 93, 2009-2010, visant à mieux garantir la vie privée à l'heure du numérique, présentée par M.Y. Détraigne et Mme A.-M.Escoffier.

390 Étude annuelle du Conseil, *Le numérique et les droits fondamentaux*, 2014.

391 La décision CJUE *Google Spain* de 2014 n'accorde qu'un droit au déréférencement des moteurs de recherche.

ou religieuses, leurs relations amicales, leurs déplacements, etc. Si, au départ, les collectes de données sont justifiées par les opérateurs au nom de « *l'amélioration de l'expérience client* » et afin de répondre au mieux à la demande, ces collections d'informations constituent des sources de richesse très importantes et leur réutilisation à d'autres fins ne fait pas toujours l'objet d'information éclairée. Une amende de 150 millions de dollars vient d'être prononcée par la *Federal Trade Commission* (FTC) et le ministère de la Justice américain contre Twitter au motif que ce réseau n'a pas, entre 2013 et 2019, informé ses utilisateurs que leurs adresses e-mail et numéros de téléphone ne servaient pas uniquement à mieux protéger leurs comptes, mais aussi à des fins de ciblage publicitaire[392].

Les méthodes de pistage pour récolter les traces sont nombreuses et certaines sont de plus en plus critiquées (*cookies*, boutons de partage, *like*, outils d'authentification, pixels invisibles, etc.). Certains réseaux ont été condamnés par les autorités de régulation pour avoir utilisé abusivement ces traceurs notamment sans le consentement des internautes[393]. L'association *Exodus Privacy*, dont l'objet est de lister les traqueurs embarqués dans les applications, a mis en évidence l'omniprésence de ces traqueurs dans les applications mobiles. Si certains affichent leurs intentions (cibler les utilisateurs à des fins publicitaires), d'autres ont un fonctionnement plus opaque[394]. Certes, les réseaux sociaux ne sont pas les seuls pourvoyeurs de données, mais ils y tiennent une grande part et, en outre, détiennent des informations très sensibles. Utilisées de façon mal intentionnée, elles pourraient constituer des armes redoutables contre tel ou tel individu. C'est ce qu'a dénoncé Shoshana Zuboff dans son livre « *L'Age du capitalisme de surveillance : le combat pour un avenir humain face aux nouvelles frontières du pouvoir* »[395]. Dès lors, l'enjeu de protéger ces traces et données numériques, qui se vendent à prix d'or grâce aux courtiers en *data* (*data broker*), est crucial.

L'actualité fournit déjà quelques exemples d'usage secondaire de ces données qui peuvent servir à surveiller ou profiler les individus à des fins critiquables. Le 27 janvier 2022, l'autorité de protection des données belge (APD) a prononcé une amende à l'encontre de l'ONG EU DisinfoLab et de l'un de ses chercheurs, pour collecte massive et publications de données dans le cadre d'une étude visant à identifier l'orientation politique des personnes à l'origine des *tweets* portant sur l'affaire Benalla[396]. Les *Centers for disease control and prévention* aux États-Unis sont soupçonnés d'avoir acheté des données de géolocalisation de millions

392 En plus de cette amende, Twitter devra bien stopper cette pratique et proposer une authentification multifactorielle qui ne requière pas l'utilisation d'un numéro de téléphone. V. également « twitter-pay-150-million-penalty-allegedly-breaking-its-privacy-promises-again » sur www.ftc.gov.

393 Facebook a notamment été condamné plusieurs fois à ce titre par les autorités belges (Recommandation n° 04/2015 du 13 mai 2015, commission de protection de la vie privée Belge et Cour d'appel de Bruxelles, 29 juin 2016) ; par l'agence espagnole de protection des données (AEPD) en septembre 2017 ; par la CNIL (délibération SAN-2017-006 du 27 avril 2017 et délibération SAN-2021-024 du 31 décembre 2021).

394 Par ex., l'application Pregnancy + récolte les informations privées de l'enfant à naître (afin d'accompagner les parents dans la naissance) et les transmet à Facebook (semaine de grossesse et mois de naissance attendu).

395 Ed.Zulma, 2020. Les autorités sanitaires américaines ont suivi la géolocalisation de millions de personnes.

396 Derriennic, site internet, 21 février 2022, « Affaire Benalla : une ONG sanctionnée par la CNIL belge »..

d'Américains pour vérifier le respect des mesures de confinement[397]. Bien plus grave encore est le système de « crédit social » mis en place en Chine, pour noter les individus et leur accorder ou refuser des droits en fonction de leur score, lequel prend également en compte ce qui est dit sur les réseaux sociaux.

Souveraineté et données biométriques

Les États et les consommateurs ont pris conscience de la nécessité de freiner certaines activités privées dont le moteur est l'exploitation des données personnelles pour ne pas fragiliser davantage la vie privée des individus et indirectement les démocraties : c'est notamment le cas des **données biométriques.** Aux États-Unis, l'entreprise *Clearview AI* devenue experte dans la reconnaissance faciale grâce aux innombrables photos en libre accès sur les réseaux sociaux, a été contrainte dans le cadre d'une action en justice de l'association *American civil liberties union* (ACLU) dans l'État de l'Illinois, qui est doté d'une loi très stricte sur la confidentialité des données biométriques, d'accepter de ne plus vendre sa base de données à des entreprises privées et de ne fournir que les autorités fédérales et locales. La technologie de *Clearview* a été jugée illégale au Canada et en Australie. En novembre, le Royaume-Uni a infligé à l'entreprise une amende d'un montant de plus de 21 millions d'euros pour avoir récupéré les images sans consentement[398]. La Commission européenne enquête depuis plus d'un an sur l'entreprise et, en décembre 2021, la CNIL a donné deux mois à *Clearview* pour cesser d'utiliser les images accessibles sur internet. L'entreprise Méta, qui a annoncé publiquement renoncer à utiliser ce type de technologie, est actuellement poursuivie par le procureur général du Texas pour avoir collecté illégalement des données biométriques sans l'accord des utilisateurs[399]. Si les acteurs du système bancaire réfléchissent au déploiement de monnaies numériques en raison des avantages qu'ils pourraient en tirer[400], de nombreux obstacles restent à franchir pour répondre aux risques d'atteintes à la vie privée à travers les données collectées et pour assurer la cybersécurité des dispositifs.

En France, le RGPD encadre strictement la réutilisation des données et des équilibres doivent parfois être trouvés pour répondre à d'autres impératifs aussi importants que la préservation de l'ordre public.

Enfin, il faut bien être conscient que les données collectées sur les réseaux sociaux sont majoritairement détenues par des entreprises qui ne sont ni françaises ni même européennes, ce qui pose la question de leur potentielle **utilisation stratégique** pour déstabiliser l'État français.

397 SiecleDigital, 4 mai 2022. Au-delà de la surveillance du couvre-feu, le CDC avait également l'intention d'analyser les visites de voisins à voisins, les visites des lieux de culte, des écoles et des pharmacies, et aussi une variété d'analyses avec ces données spécifiquement axées sur la « *violence* ».

398 Décision rendue par l'ICO (information commissioner 's office, équivalent de la CNIL française), le 29 novembre 2021. Une nouvelle condamnation pour un montant avoisinant 9 millions d'euros a été rendue très récemment le 23 mai 2022.

399 SiecleDigital, site Internet, 15 février 2022, « Reconnaissance faciale : Meta inculpé par l'État du Texas ».

400 Amélioration de la perception de l'impôt, caractère programmable de la monnaie, de la lutte contre les trafics.

La recherche d'outils de certification des comptes et de l'identité

Si les identités sur les réseaux apparaissent multiples, des **outils d'authentification** seraient utiles pour répondre aux risques de manipulation et pour sécuriser les échanges sur internet et les réseaux sociaux. La liberté d'expression n'exclut pas la confiance. L'idée a émergé de certifier les comptes voire les identités derrière les comptes. Twitter dispose d'un **outil de certification de comptes de personnalités**. Facebook et Google proposent un service (Facebook connect et Google sign-in) qui transfère notamment des informations aux sites partenaires sur l'identité du titulaire de compte. En France, la Poste propose également une solution d'identité numérique dont la sécurité est attestée par l'ANSSI. Enfin il existe aussi des dispositifs libres (gratuits) et décentralisés comme « Entr'ouvert » qui permet cette authentification et qui est utilisé par plusieurs entreprises et réseaux sociaux.

Après la mise en œuvre de **France connect**, service public en ligne d'identification et d'authentification donnant accès aux services de l'administration publique française et d'entreprises privées en réutilisant les identifiant et mot de passe d'un compte choisi par l'utilisateur, est venue l'idée de donner une **identité numérique** prolongeant l'identité civile. Ce projet est actuellement en cours. Le service de garantie de l'identité numérique (SGIN) va être mis en œuvre sous l'égide du ministère de l'intérieur et de l'Agence nationale des titres sécurisés (ANTS). Ce traitement permettra aux titulaires d'une carte d'identité numérique de s'identifier et de s'authentifier auprès d'organismes publics ou privés grâce à une application installée.

2.2.3. Les mutations économiques, sociales et environnementales engendrées par les réseaux sociaux

Il serait vain de vouloir dresser une liste exhaustive de toutes les mutations engendrées par les réseaux sociaux mais on peut s'attacher aux plus saillantes.

Les mutations économiques et sociales

Les réseaux sociaux les plus importants figurent parmi **les acteurs les plus puissants de l'économie contemporaine**. Fondés sur l'économie de la donnée et la publicité ciblée, ils ont acquis des pouvoirs de marché considérables qui ont des répercussions sur l'équilibre des marchés (*cf.* 2.1) et ont fragilisé les industries traditionnelles comme les médias par l'attraction qu'ils exercent sur la publicité. Dotés d'une capacité d'innovation très importante, ils évoluent sans cesse à la recherche de nouveaux marchés. Les investissements sont réduits, les chambres d'écho importantes et les marges considérables. La « *datafication* » de la société grâce aux métadonnées, aux outils statistiques et d'analyses enrichissent et transforment de nombreux secteurs économiques, y compris culturels, qui voient se développer de nouvelles activités et de nouveaux métiers [401].

401 D. Frau-Meifs, *Les youtubeurs : les nouveaux influenceurs,* Ed. de l'attribut, n° 5, 2017/2 Cairn.info ; J. Toledano. : « Une ORTF décentralisée pour le XXIe siècle », *Les échos*, 27 avril 2022

• *L'économie de la donnée et la publicité ciblée*

Les réseaux sociaux sont, en raison de leurs caractéristiques (v. partie 1.1.3), un acteur essentiel de la nouvelle économie de la donnée, ou « *data driven economy* »[402], leur modèle économique étant fondé sur la collecte des données de leurs utilisateurs. Facebook génère à elle seule plus de 700 téraoctects de data par jour. Si cette « économie de la donnée » représente à l'évidence de formidables opportunités de profit[403] pour les réseaux sociaux, leur utilisation soulève, ainsi qu'il a été dit, des difficultés, en termes de régulation, de gouvernance[404] et même de santé (phénomènes d'addiction).

Le marché de la publicité ciblée en ligne est concentré sur très peu d'acteurs dont le pouvoir de marché est très important. En 2020, l'entreprise Meta a réalisé un chiffre d'affaires de 84 milliards de dollars, principalement grâce aux recettes issues des publicités. Selon un rapport du groupe d'experts pour l'économie des plateformes en ligne de 2021, une plateforme comme Google (mais la logique s'applique également à Facebook) domine le marché des publicités en ligne à **chaque étape de la chaîne d'intermédiation des publicités en ligne**. Ce quasi-monopole crée un système de « jardin clos » (*walled garden*), dans lequel la plateforme privilégie ses propres services pour la vente ou l'achat de publicité en ligne, puisqu'il est présent à toutes les étapes de la chaîne d'intermédiation (ce qui renforce indirectement les effets de réseau), lui permettant de subventionner « à perte » certains de ses services économiquement peu rentables sur certains niveaux de la chaîne grâce aux recettes des autres entités plus rentables. Par ailleurs, ce quasi-monopole sur la chaîne d'intermédiation lui permet d'imposer ses propres normes sur les données récoltées en réduisant leur lisibilité par les autres acteurs, et d'obtenir un avantage concurrentiel sur le marché (seuls ses services peuvent les utiliser pour vendre de la publicité). Par exemple, les espaces publicitaires de YouTube ne sont ouverts qu'aux DSP appartenant à Google, ce qui oblige les annonceurs à passer par ce service, **et pose question en termes de concurrence**.

Le mécanisme complexe de la publicité ciblée : « *Un processus typique de vente d'inventaire publicitaire fonctionne de la manière suivante. Lorsqu'un utilisateur ouvre une page web (ou utilise une application), le serveur publicitaire de l'éditeur (Publisher Ad Server[405]) envoie une demande d'offre aux Supply side Plateforms (SSP)*[406] *pour l'espace publicitaire disponible sur la page web. À leur tour, les SSP envoient des demandes d'enchères à plusieurs Demand Side Plateforms (DSP)*[407]*. Les DSP évaluent l'opportunité publicitaire en fonction des*

402 World Economic Forum, rapport, « Data-driven Economies : Foundations for Our Common Future, White Paper », Avril 2021.

403 OECD (2013-06-18), rapport, « Exploring Data-Driven Innovation as a New Source of Growth : Mapping the Policy Issues Raised by "Big Data" », OECD Digital Economy Papers, n° 222, OECD Publishing, Paris.

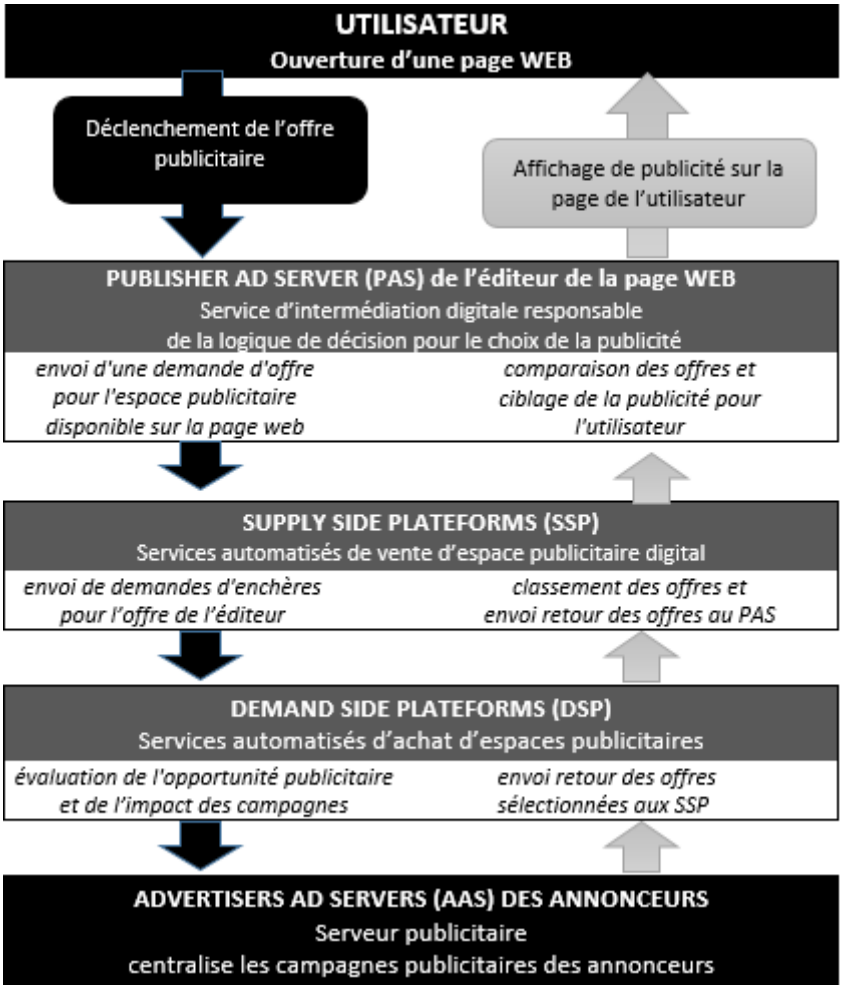
404 S. Duboc, D.-J. Noel, *Économie et gouvernance de la donnée*, Avis du CESE, février 2021

405 Le « Publisher Ad Server » joue un rôle central dans l'intermédiation digitale, en tant que responsable de la logique de décision qui détermine le choix de la publicité qui va apparaître à chaque endroit publicitaire disponible.

406 Le « Supply Side Platforms » (SSP) fournit la technologie pour automatiser la vente d'espace publicitaire digital.

407 Les « Demand Side Platforms » (DSP) sont des services qui permettent aux publicitaires et aux

objectifs des campagnes de leurs annonceurs [dont les publicités sont stockées sur les advertisers ad servers[408] et qui peuvent également vérifier l'impact d'une campagne publicitaire] et envoient des offres aux SSP. Les SSP classent ensuite les offres reçues en fonction du prix et des niveaux de priorité qui peuvent avoir été fixés par l'éditeur et envoient leurs offres gagnantes à l'éditeur. Enfin, le serveur publicitaire de l'éditeur compare les offres reçues des SSP, ainsi que tout accord direct préexistant entre l'éditeur et des annonceurs spécifiques, et décide de la publicité à diffuser sur la page web. »[409]



agences médias d'acheter des espaces publicitaires de la part des SSP.

408 Les « Advertiser Ad Servers » sont utilisés par les publicitaires et les agences médias pour stocker les publicités, les livrer aux éditeurs, garder une trace de cette activité et évaluer l'impact de leurs campagnes en suivant les conversions (d'achats à la suite de l'exposition à la publicité.

409 Rapport de la Commission Européenne relatif à la publicité en ligne. « Market Power and Transparency in Open Display Advertising – A Case Study », 2021.

Du côté des entreprises[410], la publicité ciblée permet d'accroître l'intérêt porté par les consommateurs à la publicité[411], augmentant ainsi le taux de conversion (acte d'achat du produit suite à l'exposition à la publicité) des consommateurs par rapport à la publicité traditionnelle. De plus, le coût des campagnes publicitaires est potentiellement moins élevé, puisqu'elles s'adressent à un nombre plus restreint d'utilisateurs pour un rendement économique plus favorable en termes d'acte d'achat. Du côté des consommateurs, certaines études démontrent que les utilisateurs sont plus satisfaits de la publicité ciblée que de la publicité traditionnelle, puisqu'elle leur permet de voir davantage de produits qui correspondent à leurs attentes[412].

Mais deux difficultés majeures demeurent : d'une part, les utilisateurs n'ont pas toujours consenti à la réutilisation de leurs données à des fins publicitaires ; d'autre part, ce financement des plateformes par la publicité nourrit l'économie de l'attention aux effets pervers déjà décrits. Face aux critiques concernant la réutilisation de données sensibles, Facebook a annoncé qu'à partir de janvier 2022, les annonceurs ne pourront plus utiliser de données sensibles afin de réaliser la publicité ciblée portant sur des sujets « sensibles »[413], comme l'orientation sexuelle[414].

Nombreuses sont les critiques qui visent la totale opacité du mécanisme d'enchère et les multiples conflits d'intérêts qui gangrènent le dispositif. Le DSA et le DMA devraient apporter des premiers éléments de transparence.

• *Les nouvelles activités et les nouveaux métiers engendrés par les réseaux sociaux*

-- *Social marketing, Social listening et Market place*

Le développement du digital a engendré de nombreux nouveaux métiers[415] **mais certains sont plus particulièrement liés aux réseaux sociaux. Ils sont souvent placés dans la catégorie du *web social*** ou du ***social marketing***. Ces derniers sont en effet un réservoir de données qui constituent autant d'informations sur les individus et les entreprises. L'utilisation des traces numériques par le biais du *scraping* soulève des questions de protection de la vie privée mais constitue une manne pour l'économie de marché. Jamais il n'a été aussi facile pour une marque, une entreprise ou une personnalité d'avoir accès à des informations

410 P. Vandenneucker, « Perceptions des utilisateurs quant à la publicité ciblée comportementale en ligne : Une étude qualitative », Louvain School of Management, Université catholique de Louvain, 2016. Prom., A.-C. Jeandrain. http ://hdl.handle.net/2078.1/thesis :7108.

411 D. Bergemann, A. Bonatti, Targeting in advertising markets : implications for offline versus online media, The RAND Journal of Economics, 42(3), 417-443.

412 D. S. Evans, « The online advertising industry : Economics, evolution, and privacy », *Journal of Economics Perspectives*, Forthcoming, 23(3), 37-60.

413 Numerama, site internet, 10 novembre 2021 « Facebook va arrêter la pub ciblée sur les sujets « sensibles » : une annonce en trompe-l'œil ».

414 Doh-Shin Jeon, Market power and transparency in open display advertising – a case study, Rapport final du groupe d'experts pour l'économie des plateformes en ligne, Commission Européenne, 2021.

415 Par ex., Data Scientist, Data Engineering, CISO (Chief Information Security Officer), développeur de logiciel de sécurité, l'analyste en sécurité, l'ingénieur en sécurité, l'architecte réseau, le cryptographe, le testeur d'intrusion.

sur sa réputation ou sur ses concurrents. Les informations sur les habitudes de consommation et les aspirations des consommateurs sont également précieuses.

Ces données qui permettent notamment la publicité ciblée ont engendré dans les années 2000 de nouvelles activités (comme le *marketing digital*) parmi lesquelles figure le ***social listening***, littéralement « écoute du consommateur sur les médias sociaux ». De nombreuses entreprises se sont lancées dans cette activité de veille et d'analyse des réseaux sociaux pour permettre ensuite de réaliser des actions de marketing. Le *social listening* permet la surveillance de l'*e-réputation*, de réaliser des remontées d'informations sur les produits (annonceur et concurrents), de détecter et analyser des tendances et l'activité des influenceurs, de comprendre les comportements des consommateurs, de mesurer l'efficacité publicitaire, mesurer l'engagement, etc. Du fait des réglementations, la *data* est devenue moins accessible et plus chère et les réseaux sociaux, en position de force, fixent des barrières de prix très élevés. Cette source de financement permet de ne pas dépendre entièrement de la publicité. Du fait de ce prix, on assiste à une forte concentration du marché mais des entreprises comme Brandwtach ou Ipsos sont toujours présentes[416].

Les réseaux sociaux ont également donné naissance à de nouveaux métiers. Le ***social media manager*** d'une entreprise est chargé de s'assurer de son bon positionnement sur les réseaux sociaux et de tisser une relation directe avec les clients. Les ***community managers*** ont vocation à créer, développer et gérer une communauté en ligne à l'aide d'outils et de stratégies. Facebook a récemment lancé une certification de ses *community managers*[417]. De plus en plus d'entreprises y recourent pour accroître leur notoriété, chercher de nouveaux clients et fidéliser les leurs[418].

Depuis quelques années, des *market places* (places de marché) se sont développées sur les réseaux sociaux. Elles permettent, d'une part, à des commerçants indépendants de commercialiser leurs produits à travers un site e-commerce multi vendeurs et, d'autre part, aux consommateurs de s'informer plus directement sur la qualité des produits. A travers les commentaires, les usagers contribuent désormais directement à l'e-réputation des marques. Près d'un tiers des Français a déjà acheté un produit *via* un réseau social, la proportion atteignant 38% chez les 18-34 ans.

-- *Les influenceurs*

La nouvelle activité la plus connue, en passe de devenir un métier pour certains, est celle d**'influenceur**. Ce dernier désigne la « *Personne qui, en raison de sa popularité et de son expertise dans un domaine donné (mode, par exemple), est capable d'influencer les pratiques de consommation des internautes par les idées qu'elle diffuse sur un blog ou tout autre support interactif (forum, réseau social, etc.)* »[419].

416 Siècle digital, site internet, 22 janvier 2019, « Quel avenir pour le Social Listening ? ».
417 Siècle digital, site internet, 10 octobre 2020, « Facebook : une certification bientôt disponible pour les community managers ».
418 Pôle emploi, dossier, « Le métier de Community manager (H/F) ».
419 Définition du dictionnaire Larousse

Son activité pourrait s'apparenter à celle du « *leader d'opinion* » dont l'influence personnelle oriente les comportements politiques ou économiques. Le succès est tel que de nombreux jeunes rêvent d'exercer ce « métier » au point qu'une école a même ouvert ses portes à Paris[420]. En créant des contenus photos et vidéos sur différents réseaux sociaux afin de fidéliser ses abonnés, l'objectif de l'influenceur est de susciter toujours plus d'engagement et d'avoir le plus de *followers.* Plus la communauté est importante, plus il est intéressant pour les marques de signer des partenariats avec les influenceurs qui sont rémunérés par celles-ci pour leur faire de la publicité.

Cette nouvelle manière de faire de la publicité soulève toutefois des questions, elles aussi nouvelles, liées notamment à l'absence de transparence du caractère publicitaire de certains messages avec des risques de comportement avoisinant l'abus de confiance ou la pratique commerciale trompeuse. La nouveauté tient en effet au fait que les influenceurs vont non seulement partager du contenu informatif ou de divertissement, mais vont également donner leurs avis et recommandations sur les produits pour lesquels ils ont été payés afin d'en faire la publicité, sans nécessairement faire état de ce lien commercial. **Les influenceurs les plus connus bénéficient ainsi d'un important pouvoir de prescription de nouvelles tendances.** Selon une étude effectuée en 2020, la France compterait ainsi environ 150 000 influenceurs sur les réseaux sociaux[421]. 60% d'entre eux ont moins de 30 ans et plus de 70% sont sur Instagram. Leur rémunération est difficile à estimer, en raison des nombreux paramètres qui entrent en compte (tarif prédéfini ou audience, etc.) mais certains d'entre eux gagneraient plusieurs centaines de milliers d'euros par an[422]. Certains sont des humoristes-généralistes (Cyprien, Norman, Squeezie, Seb la frite etc.), d'autres spécialisés (EnjoyPhoenix dans la mode et la beauté, Roxane dans la cuisine, Tibo Inshape dans la musculation, etc.).

Quel statut juridique pour les « influenceurs » ?

Lorsque les marques ont recours aux influenceurs pour la fourniture de contenus à caractère commercial, il existe un contrat prévoyant des obligations réciproques de publication d'un contenu, en échange d'une contrepartie. **Mais le cadre juridique des influenceurs n'est pas clairement défini.** Dans la majorité des cas, il n'existe pas de lien de subordination juridique entre les influenceurs et les marques et les contrats qui les lient sont des contrats de prestation de service. **La relation contractuelle est déterminée au cas par cas et prend souvent la forme d'un contrat d'artiste ou de mannequinat** (pour les mineurs : *cf. infra*).

420 La Croix. Influenceur, un vrai métier. 17 oct. 2021

421 *https ://fashionunited.fr/actualite/business/influenceurs-le-marketing-d-influence-a-fait-un-bond-en-2020/2020121125439*

422 https ://www.20minutes.fr/arts-stars/web/2427311-20190117-bfmtv-revele-salaires-youtubeurs-norman-cyprien

Aujourd'hui, le marché de l'influence représente 15 milliards d'euros[423] et présente de nombreux avantages pour les entreprises puisqu'elles peuvent ainsi contourner la méfiance et le désintérêt des jeunes vis-à-vis des campagnes publicitaires classiques, diffusées sur des supports traditionnels. Par ailleurs, le coût d'une campagne pour les entreprises est souvent moins élevé.

Certaines dérives consistant à faire de **la publicité déguisée** ont été constatées[424]. En France, selon la dernière étude menée par l'Autorité de régulation professionnelle de la publicité (ARPP), seuls 55% des *posts* sponsorisés étaient identifiés en 2019 comme publicité alors que l'ARPP oblige à apposer un *hashtag* ou « mot-dièse » sur un contenu sponsorisé. Une influenceuse a ainsi été condamnée à une amende de 20 000 € par la DGCCRF en 2018, pour pratiques commerciales trompeuses (elle avait notamment omis de mentionner qu'elle était rémunérée par les sociétés exploitant ce site pour en faire la promotion[425]). Pour communiquer sur les bonnes pratiques, l'ARPP (l'Autorité de Régulation Professionnelle de la Publicité) a lancé le « *certificat de l'influence responsable* », guide pédagogique à destination des influenceurs.

En Allemagne, la Cour suprême fédérale civile (BGH) a précisé dans plusieurs arrêts de septembre 2021 et de janvier 2022[426] les critères permettant de déterminer si une activité d'un influenceur sur les réseaux sociaux est considérée comme ayant « un but commercial ». Les juges allemands ont précisé notamment que les publications devaient toujours être signalées comme de la publicité lorsqu'elles présentent un caractère « excessivement promotionnel » (*ubertrieben werblicher Charakter*) ou si l'influenceur reçoit une rémunération ou une contrepartie similaire pour sa publication. Le 10 août 2021, le Bundestag a adopté la « *loi sur le renforcement de la protection des consommateurs en matière de droit de la concurrence et de droit industriel* » qui prévoit qu'une activité en faveur d'une entreprise tierce ne constitue pas une activité à but commercial (donc de la publicité) lorsque l'auteur de cette activité ne reçoit pas de rémunération ou de contrepartie similaire de la part de l'entreprise tierce ou ne se fait pas promettre une telle rémunération en contrepartie.

Par ailleurs, les influenceurs constituent un nouveau point d'entrée privilégié pour **les fraudes et les arnaques** comme le schéma commercial pyramidal basé sur le modèle dit de la « vente à la boule de neige »[427], ou de « dropshipping »[428]. En avril

423 France Inter, site internet, 18 juin 2021, « Influenceurs : peu de règles, beaucoup d'abus ».

424 *Le Figaro*, site internet, 13 septembre 2021, « Plus d'un quart des influenceurs font de la publicité déguisée sur les réseaux sociaux ».

425 « *Or, le défaut d'indication du caractère publicitaire de sa publication (par un logo ou une mention orale ou écrite par exemple) constitue une pratique commerciale trompeuse à l'encontre de ses abonnés qui peuvent croire à tort que la promotion de l'influenceuse résulte d'une expérience passée positive désintéressée* » Extrait du communique de presse de la DGCCRF relatif à l'affaire « Nabilla » de 2018.

426 Cour suprême fédérale : 9 septembre 2021, I ZR 90/20, *Influencer I* ; 9 septembre 2021, I ZR 125/20, *Influencer II* ; 9 septembre 2021, I ZR 126/20, *Cathy Hummels* ; 13 janvier 2022, I ZR 126/20, *Influencer III*.

427 La rémunération des recruteurs résulte principalement, voire exclusivement, du recrutement de nouveaux membres par les influenceurs, les produits ou services proposés servent uniquement de vitrine légale, et l'intérêt principal du vendeur, à la tête de la pyramide, réside dans la perspective de gains financiers substantiels qui résultent de la seule progression du nombre des affiliés.

428 Pratique de vente visant à supprimer une étape dans la chaîne commerciale, le vendeur attendant

2020, la DGCCRF a mise en place, avec d'autres services de l'État et des autorités de contrôle, une « task-force » pour lutter contre ce type d'arnaques ». A cette fin, un « *guide de prévention contre les arnaques visant à sensibiliser contre les pratiques frauduleuses qui existent dans le* « *dropshipping* »[429] a été publié. De plus en plus de comptes sur les réseaux sociaux font également de la prévention et du « *name and shame* »[430] des influenceurs peu scrupuleux[431].

Par ailleurs, le flou juridique dans lequel opèrent ces influenceurs a pu avoir des conséquences sur les finances publiques : la Commission Européenne estime ainsi que la pratique du « dropshipping » a constitué un manque à gagner fiscal d'environ 7 milliards d'euros au sein de l'Union Européenne[432]. Depuis le 1er juillet 2021[433], plusieurs directives européennes[434] ont été réformées afin de modifier le régime juridique de la TVA et le rendre applicable aux « *dropshippers* ».

-- Les créateurs de contenus (user generated content)

Les réseaux sociaux ont également permis l'émergence d'une nouvelle génération de **créateurs**, notamment sur des plateformes comme Youtube et Tiktok[435]. Le contenu généré par l'usager (*user generated content*) a pris dans tout le secteur culturel une importance majeure. L'industrie culturelle peut s'enrichir de la participation de nouveaux talents qui sont, dans un premier temps, adoubés par les autres utilisateurs et non par la profession. Certains, sans se voir comme des leaders d'opinion ou des influenceurs, se considèrent comme des intermédiaires et des personnes ressources. Les *booktubeurs* s'efforcent ainsi de rendre visibles des auteurs, animent des communautés d'écriture et de partage de savoir. Certaines maisons d'édition les ont intégrés dans leur stratégie de communication[436]. Pour soutenir cette « industrie créative » foisonnante, certains préconisent un dispositif

---

d'effectuer une vente avant de passer commande à son fournisseur, et faire livrer les produits directement au client – dont la qualité des produits proposé par les influenceurs pose question, puisqu'en pratique, il s'agit souvent de produits peu chers achetés à des géants de l'export chinois comme Aliexpress, et dont le principal intérêt est qu'ils peuvent être revendus par les influenceurs avec de confortables marges, et ce, au détriment de la qualité du produit proposé au consommateur Damien Leloup, Devenir riche sur internet sans rien faire : les mirages du « dropshipping ». V. *Le Monde*, site internet, 31 juillet 2019, « Devenir riche sur Internet sans rien faire : les mirages du 'dropshipping' ».

429 DGCCRF, publications, « guide-des-arnaques-task-force ».

430 Pratique visant à afficher publiquement les influenceurs peu scrupuleux sur les réseaux sociaux afin de leur faire perdre de la crédibilité.

431 *Le Monde*, site internet, 1er mars 2022, « Sur les réseaux sociaux, la traque aux arnaques d'influenceurs ».

432 Vendeur pratiquant le « dropshipping ». Jusqu'au 1er juillet 2021, sous l'empire du régime antérieur, un régime de franchise de TVA était prévu pour les biens dits de faible valeur (inférieur à 22 euros). Les opérateurs ont donc instrumentalisé cette règle et minorer le coût de leurs produits pour échapper au paiement de la TVA. Par ailleurs, les « dropshippers » n'ayant pas la qualité de destinataire réel (ils passent commande mais n'ont jamais physiquement la marchandise en leur possession) c'est le consommateur qui s'acquitte de la TVA et des droits de douanes prévus.

433 Lexbase, site internet, 13 juillet 2021, « [Focus] Réforme de la TVA et dropshipping : la fin de la récréation ? ».

434 Directive UE/2017/2455 et 2019/1995.

435 TikTok est d'ailleurs devenu partenaire officiel du festival de Cannes, ce qui a engendré quelques remous. *Le Monde*, site internet, 20 mai 2022, « Festival de Cannes 2022 : TikTok accusé de pression sur le jury du festival de courts-métrages, dont le président démissionne avant de se raviser ».

436 D. Frau Meigs, *op. cit.*

d'aide qui leur permette de réaliser leur activité sans dépendre de la plateforme[437]. Ce phénomène participe indéniablement à la **démocratisation de la culture**. On trouve aussi sur les réseaux sociaux des professeurs qui donnent des cours ou des conseils gratuits et sont suivis par des milliers de jeunes.

-- Le digital labor : modérateurs et « travailleurs du clic »

L'essor des réseaux sociaux s'est accompagné de la croissance du *digital labor*, terme qui désigne des **micro-tâches** qui accompagnent le développement de l'IA et de l'économie des plateformes.

On appelle **modérateurs** les individus qui, pour parfaire les sélections réalisées par les algorithmes de modération des contenus, trient les contenus problématiques sur les réseaux sociaux. Si leur travail est indispensable, leurs conditions de travail sont souvent particulièrement dégradées et régulièrement dénoncées[438] car ils sont exposés à des milliers d'images traumatisantes[439] et sont payés à la tâche. S'il existe quelques entreprises qui développent du micro-travail dit « propre »[440], les modérateurs sont souvent embauchés dans des pays en développement par des sous-traitants parfois peu scrupuleux[441]. Les grandes entreprises du numérique externalisent certaines tâches grâce au recours à des plateformes de micro-travail comme Amazon Mechanical Turk, fondée en 2005. Pour quelques centimes d'euros par tâche, les entreprises peuvent acheter le travail de centaines de personnes pour effectuer des micro tâches comme regarder une vidéo sur Youtube ou trier des tickets de caisse. Leur travail est « invisibilisé » : signature de clause de confidentialité interdisant aux modérateurs d'évoquer la nature de leurs missions, impossibilité pour chaque modérateur d'entrer en contact avec ses homologues et donc de créer des solidarités, etc. Le plus souvent les plateformes donnent des informations générales à leur sujet[442] et refusent de donner le nombre de modérateurs qui connaissent la langue et la culture des pays dans lesquels leur action est censée s'exercer au motif que ces derniers peuvent voir leur sécurité menacée. La lanceuse d'alerte Frances Haugen[443] a accusé Facebook lors de son audition au Sénat en novembre 2021 de ne pas avoir suffisamment de modérateurs francophones – 3/4 des modérateurs de Facebook seraient ainsi anglophones – **posant la question de la capacité de modération de Facebook dans les pays francophones**. Dans le monde arabophone (composé de 220 millions d'utilisateurs), les « Facebook Files » ont aussi révélé qu'en

437 J. Toledano. Les échos. 28 avril 2022

438 A. Casilli, P. Tubaro, C. Le Ludec, M. Coville, M. Besenval, T. Mouhtare, E. Wahal. « Le Micro-Travail en France. Derrière l'automatisation, de nouvelles précarités au travail ? », Projet de recherche DiPLab, mai 2019.

439 INA, site internet, 21 octobre 2020, entretien avec S.-T. Roberts, « Les réseaux sociaux hébergent les pires immondices dont sont capables des humains ».

440 Par ex., Accenture qui a créé une branche micro travail.

441 *Le Monde*, site internet, 11 mai 2022. « Meta, la maison mère de Facebook, accusée d'esclavage moderne au Kenya ».

442 En 2018, Facebook sous-traite sa modération à plus de 7 500 personnes, sous différents statuts (employés à plein temps, entrepreneurs ou sous-traité à des entreprises partenaires) répartis sur plusieurs continents et qui examinent près de 8 000 publications par jour.

443 ZDNet, site internet, 11 novembre 2021, « Il n'y a « pas suffisamment de modérateurs francophones chez Facebook », alerte Frances Haugen ».

2021 il n'y avait que 766 modérateurs[444] chargés de trier les contenus publiés[445]. Au total en 2020, on estimait à plus de 100 000, les personnes travaillant dans le monde au quotidien comme modérateurs. Les « nettoyeurs du web » souffrent souvent de stress post-traumatique suite au visionnage des contenus qu'ils doivent modérer. Malheureusement, il n'existe pas encore d'alternatives fiables d'outils automatisés ou informatiques permettant de remplacer la modération humaine, et il semble donc indispensable de réfléchir à des pistes d'amélioration visant notamment à sensibiliser les plateformes à la vérification des conditions d'emplois des salariés par les sous-traitants.

Les « travailleurs du clic » désignent tous les individus rémunérés pour commenter, pousser un contenu ou donner de faux avis sur les réseaux sociaux. Le plus souvent ces tâches sont externalisées par les plateformes et sont réalisées par des individus payés à la tâche et massivement localisés dans les pays en développement[446]. En 2019, les chercheurs estiment à 260 000 ces micro-travailleurs, dont une majorité de femmes (56%) qui sont les plus actives sur les plateformes de *crowdsourcing* françaises comme « *Foule Factory* ».

- *L'apparition des réseaux sociaux d'entreprises : outil de transformation des relations sociales*

Les réseaux sociaux d'entreprise sont des réseaux internes[447] auxquels seuls les salariés et dirigeants de l'entreprise peuvent avoir accès. Il y a sur le marché une offre très diversifiée de modèles de réseaux sociaux d'entreprise proposant des fonctionnalités différentes[448]. La sécurisation et la protection des données personnelles constituent de forts arguments commerciaux[449]. Dès 2015, 58% des grandes entreprises françaises avaient ainsi créé leur propre réseau social, pour

444 *Le Monde*, site internet, 16 novembre 2021, « Facebook emploi 766 modérateurs en langue arabe pour 220 millions d'utilisateurs arabophones ».

445 Siècle digital, site internet, 12 juillet 2018, « Les modérateurs Facebook examinent près de 8 000 publications par jour ».

446 A. Casilli, « De la classe virtuelle aux ouvriers du clic », *Esprit*, n° 5 (7 mai 2019) : 79-88 ; « Être présent en ligne : culture et structure des réseaux sociaux d'internet », *Idees economiques et sociales* 169, n° 3 (25 décembre 2012) : 16-29 ; A. Casilli, P. Tubaro, C. Le Ludec, M. Coville, M. Besenval, T. Mouhtare, E. Wahal. « Le Micro-Travail en France. Derrière l'automatisation, de nouvelles précarités au travail ? », *op. cit.*

447 On les appelle indifféremment réseaux sociaux d'entreprise (RSE) ou réseaux sociaux internes (RSI).

448 On peut citer Slack, Whaller, Azendoo, Yammer, Jamespot, Talkspirit (plateforme française) et Workplace.

449 Whaller est un RSE à destination des organisations (entreprises privées, administrations publiques, etc.), qui peuvent à la fois l'utiliser comme solution de communication (messagerie ou réseau social d'entreprise) mais également outil collaboratif (box de fichiers, coédition, événements, tâches, visio, audio, webinaires…) permettant de faciliter le travail et le télétravail, le tout dans un environnement très sécurisé (stockage des données sur des serveurs *cloud* locaux OVH certifié SecNumCloud par l'ANSSI). Whaller repose sur la création par les utilisateurs de "sphères", par défaut en mode "privé", dans lesquels les utilisateurs peuvent choisir soit de s'adresser à l'ensemble des membres du groupe, soit à certains utilisateurs. Ces sphères ne peuvent communiquer entre elles. Chaque "sphère" correspond à un réseau social propre. Whaller n'exploite pas les données personnelles de ses utilisateurs à des fins commerciales (autre que pour le bon fonctionnement du service), et est basé sur le principe de "neutralité algorithmique". Le réseau revendique aujourd'hui plus de 600 000 utilisateurs et est implanté dans plus de 25 000 organisations.

un coût moyen de cinq euros par salarié[450]. L'objectif premier est de faciliter la circulation de l'information, d'encourager les échanges ouverts et collaboratifs et de rompre le cloisonnement des tâches. Ils permettent aussi de renforcer l'engagement des salariés, en améliorant les processus de gestion de projet (accès en temps réel et transparence des informations). Les collaborateurs peuvent s'investir davantage sur les projets et valoriser leurs compétences, ce qui facilite la détection des talents et crée un levier de reconnaissance et de motivation individuelle. L'entreprise peut également utiliser le RSE pour diffuser sa culture d'entreprise (transparence des informations, *feedback*…). Outils mis au service de la transformation des entreprises, ils tendent à remplacer des outils de communication interne classique comme l'intranet, qui traduit une approche "*top-down*" (descendante) de l'information, au profit d'une approche plus collaborative de celle-ci[451].

La persistance d'une logique pyramidale difficilement compatible avec l'essor de la « culture 2.0 » au sein de l'entreprise expliquerait pourquoi l'usage des réseaux sociaux internes demeure limité[452]. Ainsi, selon une étude réalisée en 2017[453] dans le secteur privé, seuls 17% des salariés et 25% des dirigeants utiliseraient le réseau social de leur entreprise, même s'il y a des exemples de réussite[454]. Le constat est *mutatis mutandis* le même dans la sphère publique, en raison notamment des réticences de la hiérarchie craignant d'être contournée par le développement d'échanges directs entre les agents[455]. Il est vrai que la crise du covid a conduit à un développement spectaculaire du télétravail et donc la nécessité de développer de nouveaux outils de travail adaptés, tout en répondant aux nouvelles attentes des salariés (davantage de transparence, d'échanges[456]), ce qui pourrait faciliter le développement et l'usage de ces réseaux sociaux professionnels.

Un impact environnemental préoccupant

Longtemps, le numérique n'a été perçu que comme un formidable moyen de limiter la consommation de papier et d'économiser des transports. Plusieurs études ont démontré le rôle essentiel des technologies numériques pour lutter contre le changement climatique. Puis, certaines voix se sont élevées pour remettre en cause l'impartialité et le sérieux de ces travaux et, depuis lors, nombreux sont ceux qui tentent à l'inverse d'alerter l'opinion publique sur l'impact écologique majeur de ces technologies[457]. David Pitron, dans son ouvrage « *Enfer numérique, voyage au bout d'un like* », qui souligne les implications physiques et matérielles du numérique,

450 V. Lungu, *Réseau social d'entreprise*, Le Mans : Gereso édition, 2015.
451 M.-J. Scotto, H. Tiffon, « Les réseaux sociaux internes d'entreprise comme dispositifs ascendants de promotion de l'égalité professionnelle F/H : 2 exemples du secteur informatique », *Question(s) de management*, 2019/1 (n° 23), p. 67-87
452 *Ibid*.
453 IGS-RH Alumni, site internet, 27 novembre 2017, « L'IGS-RH s'allie à BDO pour explorer l'usage des data RH et la RSE ».
454 *Les échos*, site internet, 8 avril 2019, « Whaller, le réseau social français qui se débat face à Facebook ».
455 *La Gazette des communes*, site internet, 12 mars 2019, « Les réseaux sociaux internes en quête de clics ».
456 Welcome to the Jungle, site internet, 23 février 2021, « Ça marche vraiment les réseaux sociaux d'entreprise ? ».
457 F. Berthoud, « Numérique et écologie », *Annale des Mines – responsabilité et environnement*, n° 87, 2017/3.

rappelle qu'un simple *like*, pour parvenir à sa destination, traverse sept couches de fonctionnement d'internet[458] et que la transition numérique, contrairement au langage souvent éthéré volontairement choisi par les services marketing (*cloud*, dématérialisation, réalité virtuelle, etc.) a de réelles conséquences physiques et participe davantage au dérèglement climatique qu'elle n'aide à le prévenir.

On estime ainsi que le secteur numérique est responsable de 4% des gaz à effet de serre (contre 1,9% pour l'aviation), pour moitié en raison des équipements (ordinateurs, tablettes, smartphones, etc.) et pour moitié à raison des *data centers*, qui sont de gros consommateurs d'électricité pour faire fonctionner leurs puissants systèmes de refroidissement (25%) et leurs infrastructures de réseau (25%). **La forte augmentation des usages liés au numérique et notamment aux réseaux sociaux pourrait entraîner un doublement de l'empreinte carbone d'ici 2025**[459].

Outre ces impacts directs, l'écosystème numérique, qui valorise la donnée et biaise les prix en offrant de nombreuses prestations gratuites ou bon marché, participe d'un système qui pousse à la surconsommation de biens et au décuplement des données[460]. Chaque minute, 1,3 millions de personnes se connectent sur Facebook, 4,1 millions de recherches sont effectuées sur Google, 4,7 millions de vidéos sont consultées sur YouTube et 1,1 million de dollars sont dépensés sur les sites de vente en ligne. Les réseaux sociaux ont donc une large part de responsabilité à prendre. Si aucune politique publique de sobriété numérique n'est déployée, le numérique pourrait atteindre d'ici 2040 près de 7% (6,7%) des émissions de gaz à effet de serre de la France, niveau bien supérieur à celui actuellement du transport aérien. Cette croissance serait notamment portée par l'essor de l'internet des objets et des émissions des *data centers*. Le coût collectif de ces émissions pourrait passer de 1 à 12 milliards d'euros entre 2019 et 2040[461].

Si cet enjeu semble avoir été identifié par les pouvoirs publics, la difficulté à mesurer l'impact environnemental du numérique persiste, les efforts ayant à ce stade davantage porté sur la **mise en place d'outils de mesure de cet impact et d'évaluation**[462]. Dans son rapport publié en décembre 2020 *Pour un numérique soutenable*, l'ARCEP a ainsi souligné le besoin urgent d'une méthode d'analyse de l'empreinte environnementale du numérique. Celle-ci s'appuyait notamment sur une étude lancée par la Commission européenne à l'automne 2020 relative aux

458 Extrait : « *La septième couche correspond à votre terminal (un ordinateur, par exemple) puis votre notification amoureuse s'est enfoncée dans les strates intermédiaires du Net jusqu'à atteindre la première couche physique d'Internet, composé notamment de câbles sous-marins. Entre les deux, la notification a emprunté l'antenne 4G d'un opérateur mobile ou une box Internet, glissé le long des parties communes de l'immeuble pour atteindre des tuyaux de cuivre enfouis 80 centimètres sous les trottoirs. Puis elle a parcouru des câbles qui filent le long des grandes voies de communication (autoroutes, fleuves, chemins de halage, voies ferrées…) pour rejoindre d'autre Like dans les locaux techniques de l'opérateur. Il lui a ensuite fallu traverser les mers et transiter par un centre de données. Des tréfonds du Net, le Like a enfin pris le chemin inverse jusqu'à la septième couche : le téléphone du sujet de votre désir*. »

459 T. Mendés-France et Q. Leeds, *op. cit.*

460 D. Pitron *op. cit.*

461 ARCEP, rapport, *Pour un numérique soutenable,* 15 décembre 2020. Sénat, rapport d'information *Pour une transition numérique écologique,* n° 555 (2019-2020), 24 juin 2020.

462 La mesure de cet impact environnemental implique d'être en capacité d'appréhender un écosystème complexe et mondialisé d'opérateurs de communications électroniques, de centres de données, de fabricants d'équipements de réseaux, de composants électroniques et de terminaux, etc.

indicateurs et normes utilisés pour l'étude des centres de données et des réseaux de communications électroniques[463]. En janvier 2021, l'ARCEP et l'ADEME ont publié un rapport insistant sur l'importance de conduire une évaluation de l'empreinte environnementale complète et rigoureuse qui nécessite de collecter des données et d'en ouvrir l'accès[464]. L'empreinte carbone est donc loin d'être le seul impact sur l'environnement, ce qui justifie le recours à une approche multicritères[465]. Selon cette étude, l'essentiel de l'impact environnemental du numérique provient des terminaux, qui représenteraient au moins 65% des impacts et jusqu'à plus de 90% pour l'épuisement des ressources abiotiques naturelles (métaux et minéraux).

La **Commission européenne** a établi des critères applicables aux marchés publics écologiques s'agissant de l'efficacité énergétique dans les centres de données (critères MPE) et est également à l'origine du *Code of Conduct on Data Centres Energy efficiency*, programme européen indépendant qui promeut les meilleures pratiques en matière d'efficacité énergétique dans les centres de données et surveille la consommation d'énergie. La filière semble s'être enfin saisie du sujet et a lancé une initiative commune au niveau européen : *Climate Neutral Data Center*. Cet objectif a été repris à son compte par la Commission européenne au sein de sa stratégie digitale (*Shaping Europe's Digital Future*).

Un autre problème subsiste cependant, celui de l'efficacité énergétique des centres de données d'informatique en nuage (*cloud data centers*) qui représentaient 35% des données en 2018 et devraient atteindre 60% en 2025[466]. Le code de conduite de l'Union Européenne pour des centres de données, qui paraît efficace sur le plan énergétique, pourrait être utilisé comme une base pour le développement par étapes d'un code de conduite pour l'informatique en nuage.

Au niveau français, le Gouvernement a publié une feuille de route pour limiter l'empreinte écologique du numérique. Cette feuille de route envisage ainsi un soutien aux *data centers* écologiquement vertueux et un effort de réduction de la consommation énergétique des *data centers* français dans la continuité des objectifs fixés par le décret tertiaire et la Loi de transition énergétique pour la croissance verte (LTECV). D'autres propositions ont été formulées, notamment dans une étude réalisée par le Sénat ainsi que dans une étude du CNNUM, afin d'améliorer la

463 Commission européenne, *Study on greening cloud computing and electronic communications services and networks : toward climate neutrality by 2050*, 2022

464 Elle souligne ainsi l'importance de la base de données « IMPACTS » mise à disposition par l'ADEME qui représentera un outil précieux ; l'extension des pouvoirs de collecte de l'Arcep devrait permettre, par la mise en place d'un baromètre environnemental, d'ouvrir l'accès à certaines données nécessaires pour affiner la mesure de l'impact environnemental du numérique en France.L'étude souligne la nécessité de former les acteurs de l'écosystème pour les accompagner dans la mise en œuvre de la méthodologie de mesure des impacts environnementaux

465 L'impact environnemental du numérique s'évalue également par le biais de 12 indicateurs environnementaux tels que : épuisement des ressources abiotiques – (fossiles, minérales & métaux), acidification, éco-toxicité, empreinte carbone, radiations ionisantes, émissions de particules fines, création d'ozone, matières premières, production de déchets, consommation d'énergie primaire, consommation d'énergie finale.

466 Commission européenne, communication, février 2020, « Shaping europes digital future » ; stratégie, priorités 2019-2024, « *Shaping Europe Digital Future*» ; rapport, 9 novembre 2020, « Energy-efficient Cloud Computing Technologies and Policies for an Eco-friendly Cloud Market ».

soutenabilité écologique du numérique[467]. L'assemblée numérique européenne qui s'est réunie les 21 et 22 juin 2022 a notamment consacré ses débats à la transition numérique et verte[468]. Il s'agit à l'évidence d'un enjeu majeur.

2.2.4. Les nouveaux dangers

Les réseaux sociaux, à coté des avancées majeures auxquelles ils ont conduit, induisent aussi voire exacerbent des comportements nocifs. Outre les difficultés liées à la haine en ligne et aux atteintes à la vie privée, les réseaux sociaux, comme des catalyseurs, facilitent des comportements illicites, comme le harcèlement, ou moralement condamnables, comme la délation ou la vengeance. Ils génèrent aussi des addictions et peuvent affecter la santé mentale. Beaucoup de ces difficultés touchent davantage les plus jeunes. Les réseaux sociaux peuvent aussi se révéler des nouveaux vecteurs de trouble à la sécurité et à la tranquillité publiques.

Les dangers particulièrement prégnants pour les mineurs

On estime que 63% des moins de 13 ans ont au moins un compte sur un réseau social : Instagram rassemble 58% des 11-14 ans et 89% des 15-18 ans, Snapchat est plébiscité par 75% des 11-14 ans et 88% des 15-18 ans, Youtube est visité par 78% des 11-14 ans et 75% des 15-18 ans, Tiktok est passé d'environ 30% à presque 50% d'utilisateurs chez les 11-18 ans de 2020 à 2021 ; son utilisation a plus que doublé chez les 15-18 ans[469].

Pourtant, les réseaux sociaux comportent, en particulier pour les plus jeunes, des risques intrinsèques, liés à l'usage de l'outil lui-même, et des risques extrinsèques.

> • *Les risques intrinsèques : l'addiction aux écrans, la mésestime de soi, l'anxiété, l'isolement*

L'Autorité de régulation des communications[470] indique que 84% des jeunes âgés de 12 ans et plus utilisent un téléphone portable. Ce chiffre coïncide avec l'acquisition du premier téléphone portable, avant 12 ans pour 41% des filles, pour 30% des garçons. Les adolescents sont, pour la plupart, équipés d'un téléphone portable (99% selon la même autorité[471]).

Une enquête Ipsos a révélé que le temps d'écran moyen que les jeunes consacrent à internet est d'environ 15h et 11 mn par semaine en 2017 pour les 13-19 ans[472]. Chez les 7-12 ans, la moyenne s'élève à 6h et 10 mn. S'agissant des téléphones mobiles, les 7-12 ans sont surtout actifs sur les applications de jeux tandis que

467 Sénat, rapport, 24 juin 2020, « Pour une transition numérique écologique », n° 555 (2019-2020). CNNUM, rapport, 2020, « Feuille de route sur l'environnement et le numérique ».
468 Ministère de l'économie, des finances, et de la souveraineté industrielle et numérique, 21 juin 2022, [Vidéo] Conférence « Assemblée numérique européenne ».
469 Source : Enquête Génération numérique « les pratiques numériques des jeunes de 11 à 18 ans », mars 2021.
470 ARCEP, *Baromètre du numérique « équipement et usages* », 2021.
471 ARCEP, *Baromètre du numérique*, 2019.
472 Enquête Ipsos, Junior Connect 2017.

les 13-19 ans se concentrent sur les réseaux sociaux et les messageries[473]. Il est vrai que la question de la maîtrise des écrans ne se pose pas qu'aux jeunes (8 Français sur 10 sont conscients de ne pas parvenir à maîtriser parfaitement leur consommation d'écrans[474]) mais elle est susceptible d'être plus grave pour eux.

Cette difficulté à arrêter la consommation des réseaux sociaux est souvent liée à la peur de manquer une information importante (FoMO). Ce besoin de rester en permanence en contact nourrit la nomophobie (contraction de no mobile phobia), qui est la crainte de ne pas disposer de son smartphone en état de marche avec soi. Un projet de loi en Californie, adopté par la chambre des Représentants de cet État le 23 mai 2022, vise à permettre aux parents des enfants considérés comme « addicts » aux réseaux sociaux de poursuivre les plus importantes plateformes en justice. Celles-ci seraient alors contraintes de désactiver les comptes des enfants concernés et pourraient être redevables de dommages et intérêts allant jusqu'à 25 000 dollars, au titre du non-respect de l'obligation de ne pas engendrer une dépendance chez les utilisateurs de moins de 18 ans[475].

Les réseaux sociaux accentuent en outre la tendance à faire des comparaisons et à modifier la perception que les individus peuvent avoir de leur apparence physique et de leurs conditions de vie : les sentiments de jalousie et de frustration qu'ils génèrent peuvent fragiliser les utilisateurs, en particulier les adolescents et les jeunes adultes[476]. Une étude a montré que le sentiment « *compare and despair* » (se comparer et désespérer) baisse significativement lorsque l'usage des réseaux sociaux est réduit à environ 30 minutes par jour[477]. De fait, il semblerait que les jeunes qui utilisent beaucoup les réseaux sociaux ont une humeur davantage négative que ceux qui les utilisent avec parcimonie[478], ce qui fait craindre une augmentation du risque de dépression et de conduites addictives.

Une étude[479] a souligné que le désir des filles de changer leur apparence, y compris par la chirurgie esthétique, augmente après avoir passé du temps sur Facebook. Des réseaux sociaux ont été attaqués au motif qu'ils iraient jusqu'à contribuer à

473 Enquête Ipsos, Junior Connect' 2018.

474 Baromètre MILDECA/Harris Interactive 2021.

475 Dans ce projet de la loi, la définition de la dépendance donnée dans le projet de loi est la suivante : elle « désigne l'utilisation d'une ou plusieurs plateformes de réseaux sociaux qui présente les deux caractéristiques suivantes : (A) Indique une préoccupation ou une obsession pour une plateforme de réseaux sociaux, ou un retrait ou une difficulté à cesser ou à réduire l'utilisation de celle-ci, malgré le désir de l'utilisateur de cesser ou de réduire cette utilisation ; (B) Cause ou contribue à causer des préjudices physiques, mentaux, émotionnels, développementaux ou matériels à l'utilisateur. »

476 N. Haferkamp, N., Kramer, « Social Comparison 2.0 : Examining the Effects of Online Profiles on Social-Networking Sites », *Cyberpsychology, Behavior, and Social Networking*, 2010, 309-214.

477 M. Hunt, R. Marx, C. Lipson, J. Young, *No More FOMO : Limiting Social Media Decreases Loneliness and Depression*, décembre 2018.

478 C. Sagioglou, T. Greitemeyer, « Facebook's emotional consequences : Why Facebook causes a decrease in mood and why people still use it », *Computers in Human Behavior*, 2014, 359-363. K. Lup, L. Trub, L. Rosenthal, « Instagram #Instasad? : Exploring Associations Among Instagram Use, Depressive Symptoms, Negative Social Comparison, and Strangers Followed », *Cyberpsychology, Behavior, and Social Networking*, 2015, 247-252. G. O'Keeffe, K. Clarke-Pearson, « The Impact of Social Media on Children, Adolescents, and Families », *Pediatrics*, 2011, 800-804.

479 J. Fardouly, J. Diedrichs, P. C. Vartanian, L. Halliwell, « E. Social comparisons on social media : The impact of Facebook on young women's body image concerns and mood », *Body Image*, 2015, pp. 38-45.

promouvoir l'anorexie[480]. Pour certains chercheurs[481], derrière le *self branding* se cache un désir de ressembler aux autres qui efface les différences et leur richesse. Il compare ainsi Instagram à une « *chambre d'amplification d'un idéal tyrannique* », qui instaure une pression pour correspondre à un idéal type, ce qui induirait une « *narcissisation de la société* ». A un âge où l'estime de soi est souvent fragile, la comparaison par rapport aux autres est amplifiée par les réseaux sociaux. La culture du *like* renforce ce phénomène avec une intensification de l'importance de l'assentiment des pairs. De fait, un grand nombre de *likes* génère un niveau de satisfaction élevé, mais aussi des sentiments de jalousie ou de frustration[482].

Les effets négatifs des réseaux sociaux sur la santé mentale se répercutent souvent sur les résultats scolaires[483]. Une étude montre que les liens sociaux quotidiens, dans la vie réelle, sont également renforcés lorsque ces applications ne sont pas utilisées[484]. On peut aussi s'inquiéter de l'impact qu'ont les réseaux sociaux sur la maîtrise de la langue française et les capacités d'expression écrite.

Pour prévenir ces dangers, plusieurs actions sont menées, notamment par l'éducation nationale mais aussi par l'association e-Enfance (qui intervient dans les établissements scolaires afin d'informer les élèves sur ces dangers et leur transmettre les bons réflexes à acquérir). La CNIL accompagne aussi les mineurs et les parents à travers son site internet[485] : elle y rappelle notamment les droits numériques dont les mineurs disposent, propose aux parents des accompagnements dans l'éducation au numérique, invite les opérateurs à donner une information plus poussée par le *design* et les parents à installer des logiciels de contrôle parental.

> • *Les risques extrinsèques : l'exposition à la pornographie et le harcèlement en ligne*

-- *L'exposition à des contenus inappropriés : la pornographie*

Outre le cyber-harcèlement et la haine en ligne, l'exposition à la pornographie se trouve facilitée par l'usage des réseaux sociaux. La fondation Gabriel Péri et le fonds Actions Addictions ont, en 2018, publié les résultats d'une enquête confiée à Ipsos portant sur l'addiction à la pornographie chez les jeunes de 14-24 ans. Elle révèle que 21% d'entre eux regardaient des images à caractère pornographique au moins une fois par semaine, dont 15% chez les 14-17 ans[486]. Or, l'exposition prématurée des mineurs aux contenus pornographiques peut engendrer des

480 A. Casilli et P. Tubaro, *Le Phénomène «pro-ana» : Troubles alimentaires et réseaux sociaux*, Paris, Presses des Mines, 2016.

481 M. Stora, O. Duris, « Les réseaux sociaux sont-ils néfastes pour la santé mentale ? », *Fondation pour la recherche médicale*, 28 juin 2021.

482 A. Mayol, T. Pénard, « Facebook use and individual well-being : *Like* me to make me happier! » et « Usage de Facebook et satisfaction : les *Like*s font-ils notre bonheur ? », *Revue d'économie industrielle,* 2017.

483 L. Braghieri, R. Levy, A. Makarin, *Social Media and Mental Health*, août 2021.

484 H. Allcott, L. Braghieri, S. Eichmeyer, M. Gentzkow, « The welfare effects of social media », *American Economic Review*, vol. 110, mars 2020.

485 CNIL, site internet, 9 juin 2021, « Recommandation 1 : encadrer la capacité d'agir des mineurs en ligne ».

486 Sénat, question écrite n° 06068 sur l'exposition des mineurs à la pornographie.

chocs ou traumatismes, notamment lors d'une exposition involontaire[487]. Près d'un quart des jeunes déclarent que la pornographie a eu un impact négatif sur leur sexualité en leur donnant des complexes et 44% des jeunes ayant des rapports sexuels déclarent reproduire des pratiques qu'ils ont vues dans des vidéos pornographiques.

La lutte contre l'exposition des mineurs à la pornographie a été annoncée comme une priorité par le président de la République en 2019. Une nouvelle plateforme, https ://jeprotegemonenfant.gouv.fr a été créée pour informer, conseiller et accompagner la mise en place du contrôle parental. Certaines associations et l'ARCOM ont décidé d'assigner en justice les fournisseurs d'accès au motif qu'ils laissent les contenus pornographiques librement accessibles bien que la loi le réprime au niveau pénal[488]. Si ces affaires n'ont pu aboutir pour des raisons procédurales, les voies d'action existent et seront sans doute à nouveau utilisées[489]. La loi n° 2020-936 du 30 juillet 2020[490] prévoit également que le seul fait d'exiger de déclarer son âge pour accéder à des contenus pornographiques en ligne ne suffit pas à exonérer les sites pornographiques de leur responsabilité pénale[491]. Cette loi a également confié au président du CSA, devenu l'ARCOM, le pouvoir d'intervenir auprès des éditeurs ou hébergeurs de sites, pour leur demander d'agir en faveur de la protection des mineurs[492].

-- Le harcèlement en ligne

Le harcèlement est un phénomène malheureusement ancien mais il a pris un tel essor avec les réseaux sociaux, notamment chez les jeunes, que le terme cyber-harcèlement est apparu et qu'il a donné lieu à une incrimination pénale particulière[493]. Il est vrai que les adolescents ont généralement tendance à vouloir s'identifier à un groupe et ont trouvé dans les réseaux sociaux un outil idéal pour évoluer au sein de communautés. Aujourd'hui, pour la grande majorité d'entre eux, l'intégration dans la vie réelle passe par une activité numérique importante.

Le ministère de l'éducation nationale, particulièrement mobilisé à juste titre contre ce phénomène, en donne la définition suivante : « *un acte agressif, intentionnel perpétré par un individu ou un groupe d'individus au moyen de formes de communication électroniques, de façon répétée à l'encontre d'une victime qui ne peut facilement se défendre seule*[494].» La facilité avec laquelle il est possible de

487 Table ronde sur la régulation de l'accès aux contenus pornographiques en ligne, 8 juin 2022.

488 Infraction punie de 3 ans d'emprisonnement et de 75 000 euros d'amende (art. 227-24 du code pénal).

489 *Le Monde*, site internet, 24 mi 2022, « Blocage de sites pornographiques : l'ARCOM essuie un revers devant la justice ».

490 Loi du 30 juillet 2020 visant à protéger les victimes de violences conjugales.

491 Art. 22 de la loi.

492 Art. 23 : « *Lorsqu'il constate qu'une personne dont l'activité est d'éditer un service de communication au public en ligne permet à des mineurs d'avoir accès à un contenu pornographique en violation de l'article 227-24 du code pénal, le président du Conseil supérieur de l'audiovisuel adresse à cette personne, par tout moyen propre à en établir la date de réception, une mise en demeure lui enjoignant de prendre toute mesure de nature à empêcher l'accès des mineurs au contenu incriminé. La personne destinataire de l'injonction dispose d'un délai de quinze jours pour présenter ses observations*.»

493 Il s'agit d'un harcèlement moral aggravé par l'utilisation d'outils numériques, art. 222-33-2-2 du code pénal.

494 Ministère de l'éducation nationale, site internet, décembre 2021, « Qu'est-ce que le cyber-harcèlement ? ».

créer de fausses informations et des rumeurs, de les rendre massivement virales, accessibles au plus grand nombre sans espace de repli possible (le harcèlement se prolongeant partout dans la sphère de la vie de la victime, alors que le harcèlement scolaire classique s'arrête aux portes de l'établissement) et le risque important de voir les propos réapparaître malgré leur retrait caractérisent le cyber-harcèlement[495]. Il se pratique *via* les téléphones portables, messageries instantanées, forums, *chats*, jeux en ligne, courriers électroniques, réseaux sociaux, sites de partage de photographies, etc. Il peut revêtir plusieurs formes comme les intimidations, la propagation de rumeurs, les moqueries, le piratage, les menaces, le *revenge porn*, etc. Il est probable que l'outil numérique désinhibe certains et facilite les passages à l'acte. 20 % des jeunes disent avoir déjà été confrontés au cyber-harcèlement, ce qui s'expliquerait par l'augmentation du nombre de jeunes connectés, le rajeunissement de la première connexion et la multiplication des plateformes[496]. À la rentrée 2020, le confinement s'est traduit par une augmentation de 26% des cas par rapport à septembre 2019, selon l'association e-Enfance.

-- L'assistance mise en place contre le cyber-harcèlement

De nombreux dispositifs ont été mis en place pour venir en soutien des mineurs victimes de cyber-harcèlement et, en 2008, le programme européen "*Safer Internet*" a été mis en place afin d'inciter les États membres de l'UE à créer une « *helpline* » à destination des jeunes, des professionnels et des parents afin de les orienter et de les conseiller sur des difficultés concrètes rencontrées par les mineurs dans leur usage des réseaux sociaux. L'association e-Enfance, qui existe depuis 2005, a été retenue dans le cadre de l'appel à projet et a mis en place un numéro d'assistance, le 3018 en France[497]. Si un sondage mené par l'Institut Montaigne[498] révélait en 2020 que 61% des parents ne savaient pas vers quel interlocuteur se tourner en cas de cyber-harcèlement, la « *helpline* » a reçu 18 000 appels en 2021, soit 52% de plus qu'en 2020[499]. Les personnes chargées de cette « *helpline* » expliquent aux jeunes la procédure à suivre pour bloquer la personne menaçante et créer un autre compte mais aussi pour rassembler des preuves en vue d'une plainte. Lorsque le contenu semble illégal, un signalement est réalisé auprès de la plateforme Pharos (*cf. infra*). Elle peut demander aux hébergeurs d'arrêter la diffusion d'un contenu qui préjudicie à un mineur. Outre le numéro d'assistance, les associations mettent en place des actions préventives dans les écoles et parfois auprès des parents.

---

495 J. Atlan? K. Hendriks, *Plus facile, plus viral, impitoyable… L'école des parents*, 2021, 641, 35-37

496 Caisse d'épargne, site internet, 6 octobre 2021, étude réalisée par la Caisse d'épargne et l'association E-Enfance sur le cyberharcèlement des jeunes.

497 Ouvert 6 jours sur 7, le dispositif s'est professionnalisé et accueille des psychologues, juristes ou encore de nombreux experts du numérique. Le 3018 bénéficie d'un accès prioritaire auprès des services de police et de gendarmerie spécialisés de la plateforme Pharos et internet-signalement.gouv.fr, et est conventionné avec le 119-Enfance en Danger pour un transfert direct et prioritaire des appels. Les personnes chargées de la helpline vont expliquer aux jeunes en difficulté la procédure à suivre : prendre des captures d'écran, bloquer la personne menaçante, créer un autre compte, etc. Ensuite, elle qualifie juridiquement le contenu illégal pour ensuite procéder au signalement auprès de la plateforme. Elle peut demander aux hébergeurs d'arrêter la diffusion d'un contenu qui préjudicie à un mineur.,

498 Rapport de l'Institut Montaigne, « Internet : le péril jeune ? », avril 2020

499 Les chiffres sont donnés par l'association E-Enfance

En 2009, la Commission européenne a fait signer aux plateformes une charte sur la protection des mineurs en ligne dans laquelle elles s'engageaient à mettre en place des fonctionnalités spécifiques et notamment à créer un dispositif de signalement prioritaire concernant les mineurs. Progressivement, l'ensemble des plateformes ont intégré le dispositif (Facebook, Youtube, Tiktok…). Avec le DSA, il est probable que certaines associations obtiendront le titre de **signaleur de confiance**, ce qui leur permettra de voir traiter leurs signalements de manière prioritaire. Plusieurs pays européens ont pris des dispositions pour protéger les mineurs des réseaux sociaux[500].

Deux difficultés restent à ce stade non résolues : la multiplication des harcèlements sur les messageries privées, qui rendent plus complexes les signalements compte tenu de l'assimilation de ces messageries à de la correspondance, et la nécessité pour les mineurs d'être accompagnés par leurs parents pour déposer plainte.

Les atteintes générales à la sécurité et à la tranquillité publique

> • *Délation, atteinte à la réputation, vengeance privée, fraudes : l'effet catalyseur des réseaux sociaux*

Les réseaux sociaux engendrent une désinhibition, souvent aggravée par **l'anonymat,** qui ouvre la voie à de nombreux actes malveillants. Leur nocivité est accrue par la **difficulté à interrompre totalement leur diffusion.** L'effacement des données pourtant garanti par le RGPD reste en effet difficile à faire respecter (au point que des juridictions ont pu en tenir compte dans l'évaluation des préjudices subis par les victimes[501]).

Parmi ces actes, figurent toutes sortes de formes de vengeance, mise au pilori, atteinte à la réputation, délation. Récemment, une pratique sur les réseaux sociaux consistant à exposer certaines photos et des informations personnelles, le plus souvent sexuelles, pour humilier une personne et la soumettre à la vindicte populaire, s'est développée. Appelé « Fischa » verlan du mot affiche, cette pratique a pris de l'ampleur au point qu'une association « Stop Fischa » s'est constituée[502]. Elle n'est pas très éloignée du harcèlement et du *revenge porn*, qui a fait l'objet d'une nouvelle incrimination (jugée conforme à la Constitution par le Conseil Constitutionnel[503]).

Une autre forme de vengeance privée connue sous le nom de *doxing* consiste à révéler des informations sur une personne ou sa famille afin de l'exposer à un risque d'atteinte à sa personne[504]. Elle a été incriminée par la loi confortant

500 En Allemagne par exemple, l'accord sur la protection des mineurs dans les médias » uniformise les règles entre les landers (Jugendmedienschutz-Staatsvertrag, JMStV). L'accès à certains contenus est interdit aux mineurs et les opérateurs doivent mettre en place des dispositions de vérification d'âge. La loi sur la protection des données et de la vie privée dans le domaine des télécommunications et des télémédias (TTDSG), interdit l'utilisation des données personnelles es mineurs à des fins commerciales

501 Pour des dommages subis à la suite d'un r*evenge porn*, *cf.* l'arrêt de la chambre correctionnelle de la cour d'appel de Limoges, 20 mai 2022.

502 *Le Monde*, 24 mai 2022, « Les comptes « Fischa » sur les réseaux sociaux, la plaie du cybersexisme ».

503 Art. 226-2-1 du code pénal, créé par la loi n° 2016-1321 du 7 octobre 2016 *pour une République numérique*. Conseil constitutionnel, note sur CC, 30 septembre 2021, n° 2021-933 QPC, JoRf du 1er octobre 2021, RSC 2021.

504 Art. 223-1-1 du code pénal.

le respect des principes de la République[505] à la suite de l'attentat contre Samuel Paty. La spécificité de ce type d'infraction est qu'elle n'a pas besoin d'être suivie d'effet pour être caractérisée. D'autres comportements comme ceux dont a été victime la jeune Mila[506] souvent dénommés « harcèlements en meute » ou « raids numériques » ont fait l'objet de nouvelles incriminations dans la loi du 3 août 2018 contre les violences sexuelles et sexistes[507].

Certains internautes vont même jusqu'à se conduire comme de véritables justiciers, en n'hésitant pas à dénoncer publiquement des comportements qu'ils estiment condamnables voire à tendre des pièges à des personnes qu'ils soupçonnent de commettre des infractions, notamment de visionner des images pédopornographiques. Le mouvement des *Anonymous* qui pratiquent activement le *hacking* s'est ainsi spécialisé dans ce type d'agissement, posant la question de la légitimité d'actions par lesquelles des citoyens se substituent à la police et à la justice avec tous les risques de dérapages que cela comporte, notamment quant au respect de la présomption d'innocence sur le web[508].

On peut également se demander jusqu'à quel point le « tribunal du web » peut influencer la Justice elle-même. Il est parfois difficile pour l'institution judiciaire d'échapper aux controverses et au « venin de la vengeance »[509], elle-même médiatisée massivement sur les réseaux sociaux.

Par ailleurs, si certaines révélations sur les réseaux sociaux ont permis de confondre des criminels[510] et de libérer des paroles (*cf.* mouvement *Metoo*), ces succès se réalisent parfois au détriment du respect de la vie privée et de la présomption d'innocence, posant la question du juste équilibre à trouver entre les intérêts en présence, question classique mais que la caisse de résonnance des réseaux sociaux pose avec une acuité nouvelle. L'arrêt de la première chambre civile de la Cour de Cassation du 11 mai 2022[511] a privilégié l'intérêt général qui s'attache à la libération de la parole des victimes d'agression sexuelle sur la protection de la vie privée des personnes accusées. Il a ainsi reconnu le bénéfice de la bonne foi et refusé de condamner deux femmes – dont l'une qui a lancé le mouvement « balance ton porc » – pour les faits de diffamation pour avoir accusé sans preuve suffisante et publiquement deux personnalités pour des faits d'agression sexuelle. Cet arrêt,

505 Loi n° 2021-1109 du 24 août 2021 confortant le respect des principes de la République.

506 *Le Monde, 29 janvier 2020,* « L'affaire Mila expliquée : insultes contre l'islam, menaces contre une lycéenne et réaction politique 'maladroite' ». Le tribunal de Paris a prononcé le 24 mai 2022 des peines allant de 4 à 6 mois de prison avec sursis contre onze personnes reconnues coupables d'avoir participé au harcèlement en ligne de l'adolescente Mila. Sur les onze personnes reconnues coupables, une a été condamnée pour menaces de mort et les dix autres pour harcèlement suite à des messages envoyés sur les réseaux sociaux.

507 Art. 222-33-2-2 du code pénal, créé par la loi n° 2018-703 du 3 août 2018 renforçant la lutte contre les violences sexuelles et sexistes.

508 *Numerama*, 17 octobre 2012, « Amanda Todd : Des Anonymous dévoilent l'identité du harceleur présumé ».

509 G. Von der Weid, « La justice dans le débat démocratique - Quelle justice sur les réseaux sociaux? », *Les cahiers de la justice*, 2017, p. 523.

510 L'auteur de l'article précité raconte comment le compte Instagram Assault Police (police des agressions) a permis de confondre un ancien étudiant de l'Université américaine du Caire, ayant fait subir en toute impunité, des viols, harcèlements, agressions sexuelles plus de cinquante ans durant.

511 Première chambre civile de la Cour de cassation (n° 21-16.156 et 21-16.497).

rendu sur l'avis contraire de l'avocat général, qui estimait que le bénéfice de la bonne foi devait reposer sur la vraisemblance des faits rapportés et dont il faut relever qu'il n'a pas fait l'objet d'une publication, a été très discuté[512].

Dans un registre différent, les réseaux sociaux apparaissent comme des outils très utiles aux mains des **fraudeurs** et délinquants en tout genre. De nombreuses affaires liées à la vente de faux passes sanitaires sur Snapchat sont par exemple actuellement en cours d'instruction. D'autres sont liées à des piratages de comptes sur Twitter dans le but de diffuser des messages malveillants. Plusieurs trafics de drogue sur des réseaux sociaux ont été démantelés[513], mais l'on voit se développer les cas d'escroqueries ou des *ransomwares* sur internet. Le ministère des finances s'efforce à juste titre de sensibiliser les internautes aux risques d'arnaques sur les réseaux sociaux[514]. Certaines ont même été facilitées par des influenceurs.

- *Les nouvelles discriminations*

Les personnes qui ne possèdent pas de comptes sur les réseaux sociaux peuvent subir une certaine forme d'ostracisme. Comme l'illectronisme, ne pas évoluer sur un réseau social peut engendrer une mise à l'écart. Cette absence peut être volontaire mais aussi involontaire lorsqu'elle est due à des **difficultés d'accès à internet** (fracture numérique dans les zones blanches, souvent rurales ou difficultés liées à des conditions matérielles défavorables) ou de maîtrise de l'outil (illectronisme).

Surtout, cette divergence d'usage atteste et creuse la **fracture générationnelle qui se manifeste tant dans l'absence de présence sur les réseaux que dans le choix du type de réseau**. Si 84% des jeunes de 18 à 24 ans ont participé à des réseaux sociaux en 2021, seulement 38% des personnes âgées de plus de 70 ans les utilisent, par manque de maîtrise ou d'envie. Quant au choix du réseau, un fossé important est relevé entre les générations : aux États-Unis, si 71% des jeunes entre 18 et 29 ans utilisent Instagram, ils ne sont que 13% parmi les personnes entre 65 ans et plus en 2021 (l'écart dans l'usage de Facebook est moins fort, puisque 70% des jeunes entre 18 et 29 ans l'utilisent, comme 50% des personnes entre 65 ans et plus). Par ailleurs, une nouvelle forme de discrimination générée par les **systèmes d'IA** a vu le jour. La Défenseure des droits s'en est fait l'écho du rapport Equinet sur l'IA et l'égalité[515] et a demandé que le principe de non-discrimination soit placé au cœur du projet de règlement européen sur l'IA[516].

512 *Le club des juristes,* 17 mai 2022, Ch. Bigot, « Balance ton porc : liberté d'expression ou diffamation. La Cour de cassation fait prévaloir l'intérêt général qui s'attache à la libération de la parole collective » ; *Marianne*, 11 mai 2022, S. Prokhoris, « Collectif 50/50 : Allons-nous vers une révision drastique du logiciel Metoo/intersectionnalité ? ».

513 *Le Parisien* avec AFP, 27 juillet 2020, « Bretagne : un réseau de trafic de drogue sur les réseaux sociaux démantelé ». *01net*, 7 février 2021, « Telegram, WhatsApp, quand la vente de drogue migre vers les réseaux sociaux ». *Atlantico*, 24 septembre 2013, « Délinquance 2.0 : quand les réseaux sociaux jouent les assistants du crime ».

514 *Bercy Infos*, 26 janvier 2022, « Arnaques sur les réseaux sociaux : à quoi devez-vous faire attention ? ».

515 *Equinet*, réseau européen des organismes de promotion de l'égalité, 2022, « Pour une IA européenne protectrice et garante du principe de non-discrimination. Avis établissant des recommandations et des principes essentiels pour la future législation européenne portant sur l'intelligence artificielle ».

516 Défenseure des droits, *communiqué de presse*, 21 juin 2022, « Pour une IA européenne protectrice et garante du principe de non-discrimination ».

2.3. Les réseaux sociaux au service de l'action publique

Pour répondre à ses missions plus efficacement, l'administration a trouvé dans les réseaux sociaux un outil pertinent à plusieurs égards. Que ce soit pour informer les usagers, promouvoir les actions d'intérêt public ou améliorer les performances de l'administration, les réseaux sociaux constituent, utilisés à bon escient, une aide précieuse pour l'administration. Leur utilisation par les agents publics dans leur sphère privée soulève par ailleurs des questions déontologiques nouvelles mais présente aussi des opportunités notamment en termes de gestion des carrières.

2.3.1. L'information et la promotion de l'action publique sur les réseaux sociaux

Il n'est pas toujours aisé pour l'administration de faire connaître ses actions et de les mettre en valeur auprès du public dans un contexte dans lequel son image demeure souvent négative (une majorité de Français estimerait que l'accueil qui leur est réservé dans les administrations n'est pas satisfaisant et qu'elles ne font pas assez d'efforts pour faciliter les démarches des usagers[517]).

Les réseaux sociaux, nouvel outil d'information et de promotion

Les réseaux sociaux sont devenus un **outil d'information, de mise en œuvre et de promotion de l'action publique**, notamment pour toucher des publics plus jeunes. Les collectivités territoriales font de plus en plus souvent appel à des « *community managers* »[518] en charge de suivre en temps réel l'ensemble des réseaux sociaux en pratiquant une veille constante. Les ministères et les administrations déconcentrées de l'État font également appel aux réseaux sociaux, à la fois pour surveiller leur **e.réputation**[519] et pour faire connaître leurs actions. Le service d'information au Gouvernement (SIG) a développé au cours des dernières années une communication spécifique aux réseaux sociaux et s'efforce d'assurer une mise en cohérence de la communication gouvernementale sur ces réseaux[520]. Le Conseil d'État y recourt également.

La **police nationale** a ainsi ouvert, dès septembre 2012 au niveau central, des comptes Facebook et Twitter, progressivement suivis de comptes départementaux visant à favoriser « *le rapprochement entre la police et la population, et, en particulier, les publics juvéniles ; la valorisation de la police et de son action ; le recrutement ;*

517 *Challenges*, 7 octobre 2021, « Administration : pourquoi les Français sont de plus en plus insatisfaits ».

518 *Cf. 2.2. Les nouveaux métiers*.

519 *20minutes*, 17 avril 2021, « Réseaux sociaux : Le gouvernement va dépenser 2,8 millions d'euros pour surveiller sa « réputation » en ligne ». Site internet du Gouvernement, « Respect de l'identité visuelle de la marque de l'État ».

520 Une charte des réseaux sociaux de l'État a été élaborée à cette fin.

la diffusion de campagnes de prévention ; et, de plus en plus, l'information du public dans les situations de crise »[521]. Les autorités gouvernementales ont pu utiliser les réseaux sociaux pour diffuser des informations officielles liées à la pandémie et notamment diffuser les gestes et précautions à prendre pour lutter contre la propagation du virus. Le **porte-parole du Gouvernement** a multiplié sa présence sur les plateformes (Twitch, Instagram, etc.) afin de sensibiliser davantage de personnes[522]. Les **agences de santé ainsi que le ministère de la santé et des solidarités** ont publié sur les plateformes les informations nécessaires à la gestion de la crise par les autorités mais aussi les gestes et précautions au niveau individuel[523]. Durant **la présidence française de l'Union européenne**, les internautes ont été invités à suivre son actualité sur les réseaux sociaux[524]. L'armée dispose d'un espace dédié aux jeunes sur Facebook « Parlons Défense ».

Nombreuses sont les **collectivités territoriales** qui utilisent les réseaux sociaux pour informer les habitants des actions locales, faciliter certaines démarches et la communication avec les administrés. Un observatoire a été créé qui permet de fournir une analyse comparative de leur présence sur les réseaux sociaux[525]. Il propose aussi des instruments d'analyse pour les classer en fonction de critères notamment écologiques et a lancé récemment ResponsiWeb. L'observatoire socialmédia des territoires fournit un palmarès des collectivités territoriales les plus présentes sur les réseaux sociaux. Mais l'utilisation des réseaux sociaux les plus « grand public » expose aussi ces collectivités à certains risques comme les fausses informations et les *trolls*[526].

En cas de **crise**, cet outil se révèle précieux pour transmettre des informations rapidement et son usage est encouragé par l'association des maires de France[527]. Les réseaux sociaux peuvent aussi, en sens inverse, permettre aux administrés de signaler des difficultés à leur collectivité ou poser des questions. Ils favorisent ainsi le **rapprochement de la collectivité et de ses habitants** et peuvent faciliter, à terme, l'identification des besoins des usagers. Le ministère de l'intérieur a ainsi mis en place une veille opérationnelle des médias sociaux pour améliorer les performances en situation d'urgence (MSGU), en s'appuyant sur un réseau de bénévoles et d'associations comme celle qui regroupe les volontaires internationaux en soutien opérationnel virtuel (VISOV)[528].

---

521 I. Huré, G. Le Saulnier, « Le discours institutionnel de la force publique sur les réseaux sociaux numériques », *OpenEdition Journals*, 17 décembre 2020.

522 *20minutes*, 20 novembre 2020, « Coronavirus : Comment le gouvernement tente de sensibiliser les jeunes à la crise sanitaire ».

523 Exemple de *tweet* du ministère de la santé et des solidarités sur https://twitter.com/Sante_Gouv.

524 France diplomatie, site internet, « Ouverture du site internet, des réseaux sociaux et de la plateforme d'accréditation de la présidence française du Conseil de l'Union européenne (10 décembre 2021) ».

525 https ://myobservatoire.com/

526 *La Gazette des communes*, 4 mai 2020, n° 2518, « Communication territoriale : la chasse aux *fake news* est ouverte ». CNFPT, dossier documentaire, 26 septembre 2012, « Réseaux sociaux et collectivités locales ».

527 AMF, site internet, « La communication locale plus que jamais essentielle à l'heure de la crise sanitaire ».

528 Organisation et équipe bénévole de VISOV

La nécessité de prendre en compte l'illectronisme

Une réelle attention doit être prêtée aux personnes qui ne maîtrisent pas l'outil informatique et qui se trouvent discriminées par cette méconnaissance[529]. Selon l'INSEE, 17% de la population française est concernée par l'illectronisme[530].

Malgré les efforts pour réduire l'illectronisme (le Gouvernement a ainsi récemment mis en place une politique d'inclusion numérique pour lutter contre ce phénomène[531]), l'usage des réseaux sociaux ne peut aujourd'hui pas être le mode exclusif de communication et d'échange avec les administrés. L'utilisation de cet outil pour informer les usagers, outre la dépendance à des réseaux sociaux étrangers qu'elle engendre (cf 2.1), doit donc faire l'objet d'une particulière vigilance. Une vigilance encore plus grande doit être portée lorsqu'une administration décide d'imposer aux administrés d'avoir recours à un téléservice pour l'accomplissement de démarches administratives, comme vient de le juger la section du contentieux du Conseil d'État (3 juin 2022, *CNB*, n° 452798 et autres) : une telle obligation ne peut être imposée que si l'accès normal des usagers au service public et l'exercice effectif de leurs droits sont garantis, l'administration devant tenir compte à cet égard de la nature de la démarche qui est dématérialisée, de son degré de complexité, des caractéristiques de l'outil numérique proposé, ainsi que de celles du public concerné.

2.3.2. L'amélioration des performances de la puissance publique et des services publics par l'utilisation des réseaux sociaux et des messageries

Tant les réseaux sociaux grand public que les réseaux sociaux internes peuvent améliorer les performances de l'administration et contribuer à renforcer la confiance du citoyen dans les affaires publiques. Dans une note de 2019, le CNNUM a d'ailleurs préconisé l'utilisation des réseaux sociaux pour permettre aux usagers de **faire valoir leurs attentes** et de participer à la détermination des politiques publiques dans un processus de co-construction[532]. A cet égard, les réseaux sociaux sont devenus partie prenante de « l'accélérateur d'initiatives citoyennes »[533], projet conçu par la direction interministérielle de la fonction publique (DITP), ou encore des initiatives de la Direction interministérielle du numérique (DINUM)[534].

Les réseaux sociaux grand public, appui des politiques publiques

Les réseaux sociaux grand public présentent l'intérêt de rassembler de nombreuses personnes et de faciliter des actions de consultation, autrefois lourdes et complexes. Les consultations pratiquées par les personnes publiques

529 Livre blanc contre l'illectronisme.
530 INSEE, site internet, « Une personne sur six n'utilise pas Internet, plus d'un usager sur trois manque de compétences numériques de base ».
531 Gouvernement, site internet, « Comment agir contre l'illectronisme ».
532 Rapport du Conseil national du numérique : « Transformation de l'État, dépasser la norme par la pensée design », 2019.
533 Gouvernement, site internet, www.modernisation.gouv, « Accélérateur d'initiatives citoyennes ».
534 https ://numerique.gouv.nc/actualites/27-04-2018/liberte-dexpression-et-reseaux-sociaux

en direction de la population en général passent de plus en plus souvent par une forme numérique qui peut emprunter le vecteur des réseaux sociaux grand public. Le **ministère de l'intérieur** a également mis en place une veille opérationnelle en s'appuyant sur les témoignages directs des témoins de **catastrophes** pour améliorer les performances en situation d'urgence et faciliter l'intervention des services de secours[535]. La Mission interministérielle de lutte contre les drogues et les conduites addictives (MILTD) utilise la puissance de diffusion des réseaux sociaux pour mener des campagnes de prévention digitale : avec le *hashtag* #PreventionMDMA[536], elle a ainsi pu prévenir de la consommation de drogues en diffusant des messages de prévention sur les risques liés à la consommation de la MDMA/ecstasy.

Les réseaux sociaux permettent aussi d'améliorer les prestations offertes par les services publics. Pour des **services publics de transport** comme SNCF Transilien, c'est un outil précieux pour informer les voyageurs en temps réel du trafic et gérer les imprévus. Les *community managers* des centres opérationnels répondent ainsi aux questions des usagers posées sur les réseaux sociaux.

Les réseaux sociaux, un outil devenu incontournable pour Pôle Emploi

Pour Pôle Emploi, les réseaux sociaux sont incontournables pour identifier les demandeurs d'emploi, accéder aux jeunes et diffuser des informations[537]. En 2019, plus de 75% des demandeurs d'emploi inscrits à Pôle Emploi étaient actifs sur les réseaux sociaux notamment pour y rechercher un travail. Présent sur plusieurs réseaux sociaux, Pôle Emploi s'est fixé des lignes éditoriales différentes selon le type de réseau et des règles de fonctionnement protégeant la vie privée des demandeurs d'emploi et exigeant de ses agents un strict respect des obligations de réserve et de neutralité pour ne pas entacher sa réputation. En 2022, son compte Facebook comptait 800 000 abonnés (contre 84 000 pour son homologue anglais). Au niveau local, Pôle Emploi utilise les réseaux pour diffuser des informations de proximité sur le marché de l'emploi. Il s'appuie sur un réseau de collaborateurs dénommés les *ambassadeurs* qui, avec leurs 1 500 comptes, valorisent l'action de Pôle Emploi et font connaître ses services. Ils génèrent plus de 8 millions de vues par an et entre 10 et 15 000 *retweets*.

Pôle Emploi travaille même avec certains influenceurs qui peuvent, dans leur domaine, relayer des informations capitales pour les demandeurs d'emploi. C'est ainsi que Kelly Cruz, l'une des influenceuses les plus connues dans le secteur du BTP, a transmis des informations sur les fausses idées sur les recrutements dans ce secteur.

Les informations recueillies grâce aux réseaux sociaux ont permis à Pôle Emploi d'évoluer en proposant des formations à l'usage des réseaux sociaux (afin de valoriser son image) et un suivi différencié selon les besoins des demandeurs d'emploi. A cette fin, un réseau social fermé appelé SPHERE a été créé. Il offre aussi un espace d'entraide et de partage d'informations entre demandeurs.

535 Gouvernement, site internet, sur l'utilisation des Médias sociaux associés à la gestion de l'urgence (MGSU) par les services d'incendie et de secours.

536 #PreventionMDMA : la nouvelle campagne de prévention digitale pour informer sur la MDMA | Mildeca

537 Rapport public annuel de la Cour des Comptes 2020, p. 188.

Les réseaux sociaux sont aussi un relais puissant pour les **opérateurs culturels français**, notamment dans le champ de l'audiovisuel public. En effet, les six groupes de l'audiovisuel public (France Télévisions, Radio France, France Médias Monde, l'INA, Arte et TV5 Monde) sont tous présents sur les réseaux sociaux et diffusent massivement leurs contenus. Culture Prime[538], qui produit et poste des contenus culturels tous les jours sur Facebook, Youtube et les sites des chaînes publiques, annonce en moyenne 1,4 millions de personnes chaque jour qui voient au moins une de ses publications sur Facebook et une communauté de plus de 240 000 abonnés.

Les réseaux sociaux et messageries internes, outils sécurisés de l'action publique

S'agissant des réseaux sociaux ou messageries internes, leur usage s'inscrit dans le mouvement global de numérisation des services de l'État et de sa « **plateformisation** » que la direction interministérielle chargée de la transformation numérique (DINUM) met en œuvre depuis plusieurs années[539]. Il vise à moderniser les services de l'État et ceux offerts aux administrés dans le cadre d'un « service public augmenté »[540]. Il n'existe pas à proprement parler de réseau social interne à l'État, mais l'idée de permettre aux agents de disposer de moyens de communications confidentiels pour améliorer le fonctionnement de l'administration a émergé au début des années 2000. Depuis 2018, l'ensemble des agents des trois fonctions publiques peuvent utiliser la **messagerie Tchap**, conçue par la DINUM. Dédiée aux agents des ministères qui ont besoin d'utiliser une messagerie instantanée pour collaborer directement, elle est hébergée sur des serveurs français. En 2022, elle comptait 235 000 utilisateurs[541]. Une expérimentation pour l'ouvrir aux collectivités territoriales est en cours car ces dernières, en utilisant des plateformes destinées au grand public, ne disposent pas des garanties liées à la sécurité et la confidentialité des échanges.

Si le **Groupe d'intervention de la gendarmerie nationale** (GIGN) a développé un réseau social interne, sur lequel il est possible de réaliser des tchats, des envois de vidéos et photos, et même une géolocalisation en temps réel sur les lieux de la crise[542], l'usage de ce type de dispositif demeure exceptionnel.

Si l'outil que constituent les réseaux sociaux pourrait permettre de renforcer l'horizontalité des relations entre fonctionnaires, son maniement pourrait s'avérer

538 En 2018, les six groupes de l'audiovisuel public ont lancé Culture Prime, le premier média social culturel à destination des plus jeunes.

539 L'État plateforme, concept initialement proposé par l'ingénieur informaticien et entrepreneur américain Tim O'Reilly, puis développé en France par Nicolas Colin et Henri Verdier, entrepreneurs et hauts fonctionnaires spécialistes des technologies numériques, consiste à réinventer les modes de gouvernement en se fondant sur la créativité et les technologies collaboratives connues des plateformes numériques. L'objectif est de mieux résoudre les problèmes collectifs au niveau local et national et d'améliorer les services proposés par l'État. Cette ambition repose sur plusieurs axes mis en place par le Gouvernement français depuis quelques années : le partage des données publiques (avec la création du portail interministériel data.gouv.fr en 2011), le développement de nouveaux services conçus à partir des ressources partagées, l'adoption d'une stratégie globale avec la dématérialisation de l'ensemble des démarches administratives en 2022 et l'expérimentation d'une plateforme numérique d'État.

540 ENA, « E-administration et transition numérique de l'État », 2019 ; J. Le Bolzer, « Henri Verdier : La transformation de l'État doit surtout être organisationnelle et managériale », *Les Echos*, 22 juillet 2019.

541 Tchap, Site de Beta Gouv, consulté en mai 2022.

542 Ministère de l'intérieur et des outre-mer, reportage, « Le ministère de l'intérieur à l'heure du numérique ».

plus délicat dans le cadre hiérarchique. C'est d'ailleurs pour cette raison que certains réseaux sociaux d'entreprises parviennent difficilement à susciter l'adhésion des salariés. C'est aussi pour cette raison que la mise en place d'un réseau social interne à la police nationale n'a pas fonctionné. Une complémentarité des axes de communication pourrait utilement être recherchée afin de renforcer la cohésion interne et de faire vivre des administrations de façon moins cloisonnée. L'armée américaine utilise ainsi un social web sécurisé pour mener des projets collaboratifs et permettre aux jeunes officiers d'échanger sur certains sujets[543].

En une quinzaine d'années, les réseaux sociaux ont ainsi profondément transformé le travail et les modes de fonctionnement des acteurs publics, pour lesquels ils représentent à la fois une opportunité et une contrainte. D'un côté, ils permettent une communication en temps réel entre les acteurs publics eux-mêmes et avec les usagers du service public, source d'efficacité et de transparence ; de l'autre, plus leur usage se développe, plus les administrations et les pouvoirs publics doivent s'adapter à leur rythme et à leurs codes, ce qui peut aussi être en facteur de modernisation et d'efficacité accrues.

Les réseaux sociaux, sources d'information pour l'administration

Les données accessibles sur les réseaux sociaux peuvent constituer des informations précieuses pour l'administration.

Dans le cadre de la stratégie nationale de **prévention et de lutte contre la pauvreté**, ont été mises en place des « maraudes numériques » qui permettent de repérer sur les réseaux sociaux les jeunes plus vulnérables à l'aide des réseaux sociaux et d'entrer en contact avec eux[544].

Outre cette utilisation dans le cadre des politiques sociales, les informations sur les réseaux sociaux peuvent aussi intéresser la puissance publique dans le cadre de ses missions de **préservation de l'ordre public**. La loi de finances pour 2020 a autorisé, à titre expérimental et pour une durée de trois ans, les **administrations fiscale et douanière** à collecter et à traiter de manière automatisée les données personnelles accessibles publiquement sur les sites internet de certains opérateurs de plateformes, aux fins de recherche de manquements et d'infractions en matière fiscale et douanière.

La décision du Conseil Constitutionnel du 27 décembre 2019 relative à la loi de finances pour 2020 (n° 2019-796 DC).

A l'occasion de l'examen du recours formé contre ce texte, le Conseil constitutionnel a rappelé **l'équilibre à trouver entre protection de la vie privée et préservation de l'ordre public** pour fixer le cadre légal de ces pratiques. Il juge que les données susceptibles d'être collectées et exploitées doivent répondre à certaines conditions cumulatives : d'une part, il doit s'agir de **contenus librement accessibles** sur un service de communication au public en ligne d'une des plateformes précitées, à l'exclusion donc des contenus accessibles seulement

543 *Huffington post*, site internet, 30 juillet 2012, « Les armées face aux réseaux sociaux ».

544 Bilan d'étape de la stratégie pauvreté de la Délégation interministérielle à la prévention et à la lutte contre la pauvreté, octobre 2021, p. 40.

après saisie d'un mot de passe ou après inscription sur le site en cause ; d'autre part, ces contenus doivent être **manifestement rendus publics par les utilisateurs de ces sites**. Il en résulte que ne peuvent être collectés et exploités que les contenus se rapportant à la personne qui les a, délibérément, divulgués. Ne peuvent également faire l'objet d'aucune exploitation à des fins de recherche de manquements ou d'infractions, les données qui révèlent la prétendue origine raciale ou l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne, les données génétiques et biométriques et celles concernant la santé et la vie ou l'orientation sexuelles. Le Conseil constitutionnel relève enfin que les personnes intéressées par ces saisies de données bénéficient, notamment, des garanties relatives à l'accès aux données, à la rectification et à l'effacement de ces données ainsi qu'à la limitation de leur traitement, ce qui renforce d'autant plus la protection de leurs données personnelles[545]. En l'espèce, s'il précise que les dispositions légales en cause sont de nature à porter atteinte au droit au respect de la vie privée ainsi qu'à l'exercice de la liberté d'expression et de communication, il juge cependant que, ayant pour finalité de répondre à l'objectif de valeur constitutionnelle de lutte contre la fraude et l'évasion fiscales, elles peuvent être autorisées à condition d'être entourées de garanties suffisantes, notamment s'agissant du type de données susceptibles d'être collectées et exploitées[546].

Pour lutter contre l'utilisation de *trolls*[547], la manipulation des informations et la diffusion de *fake news* massives qui peuvent avoir des conséquences très nocives particulièrement en période électorale, durant des crises majeures ou dans le cadre d'opérations engageant l'armée française, l'État a créé l**e service de vigilance et de protection contre les ingérences numériques étrangères (VIGINUM)**. Placé auprès du secrétariat général de la défense et de la sécurité nationale (SGDSN), il a pour mission de détecter et de caractériser les opérations **d'ingérence numérique étrangères** portant atteinte aux intérêts fondamentaux de la Nation à partir de l'analyse des contenus accessibles publiquement sur les plateformes en ligne[548]. Il est autorisé à mettre en œuvre une collecte automatisée de **données manifestement rendues publiques** sur les réseaux sociaux pour identifier les menaces.

Les informations disponibles sur les réseaux sociaux sont aussi utiles pour contribuer à résoudre **des enquêtes pénales**. Aux traditionnelles enquêtes de voisinage, il faut maintenant ajouter le recueil d'informations publiques sur les réseaux sociaux. Les réseaux sociaux ne sont plus seulement utilisés par les « cyber-patrouilles », qui recherchent des infractions en lien avec la cyber-criminalité. A travers la plateforme *Moncommissariat.fr,* les habitants

545 CC, 27 décembre 2019, *Loi de finances pour 2020*, *n° 2019-796 DC*.

546 Celles-ci doivent répondre à deux conditions cumulatives : il doit s'agir de contenus librement accessibles sur un service de communication au public en ligne d'une des plateformes précitées, à l'exclusion donc des contenus accessibles seulement après saisie d'un mot de passe ou après inscription sur le site en cause et ces contenus doivent être manifestement rendus publics par les utilisateurs de ces sites. Ainsi ne peuvent être collectés et exploités que les contenus se rapportant à la personne qui les a, délibérément, divulgués.

547 Faux comptes derrière lesquels se cachent des robots.

548 Décret n° 2021-1587 du 7 décembre 2021 portant création d'un traitement automatisé de données à caractère personnel dans le but d'identifier les ingérences numériques étrangères.

peuvent aussi signaler des infractions notamment les lieux de points de vente de drogue. Par ailleurs, certains enquêteurs se forment aux enquêtes sur *opensource*, ce qui peut permettre d'obtenir des résultats très positifs.

Le suivi des réseaux sociaux est surtout devenu un élément central dans la **lutte contre le terrorisme**, tant leur rôle dans la propagande djihadiste est important, à travers notamment la diffusion massive de vidéos de propagande[549]. Selon une enquête récente menée sur les profils de détenus incarcérés pour terrorisme, les deux tiers auraient basculé à la suite d'échanges virtuels[550]. La direction générale de la sécurité intérieure (DGSI)[551] et la direction générale de la sécurité extérieure (DGSE)[552] ont d'ailleurs massivement investi dans l'observation et la surveillance d'internet et des réseaux sociaux, évolution qui n'est pas sans créer des inquiétudes chez les défenseurs des libertés[553] et appelle certainement à une vigilance particulière des instances de contrôle comme, le cas échéant, du juge administratif.

2.3.3. L'usage des réseaux sociaux par les fonctionnaires dans leur sphère privée ou dans le cadre de leur gestion de carrière

L'obligation de réserve à l'ère des réseaux sociaux

Si les fonctionnaires jouissent de la liberté d'expression et d'opinion, ils sont tenus de respecter l'obligation de discrétion professionnelle[554] (voire de secret professionnel pour certains d'entre eux[555]) et le devoir de réserve dégagé par la jurisprudence[556]. Ce dernier principe, qui désigne « *l'obligation faite à tout agent public de faire preuve de réserve et de retenue dans l'expression écrite et orale de ses opinions personnelles* [557]**», est d'un usage délicat lorsque l'expression a lieu sur un compte public de réseau social**[558]. L'application de ce principe aux réseaux sociaux a donné lieu à plusieurs décisions juridictionnelles.

549 *France culture*, émission, 6 juin 2017, « Pourquoi trouve-t-on encore des vidéos de propagande terroriste sur YouTube ? ».

550 *Le Monde,* site internet, 29 décembre 2021, « Djihadisme en France : « Deux tiers des détenus pour terrorisme ont vécu un choc moral sur Internet ».

551 *Planet.fr*, site internet, 8 juillet 2021, « Cybersécurité : les 10 conseils de la DGSI à appliquer dès à présent ».

552 *Le Figaro*, site internet, 4 juillet 2013, « La France espionne aussi les réseaux sociaux ».

553 *Le Figaro*, site internet, «La France surveille elle aussi internet ».

554 Art. 26, al.2 de la loi du 12 juillet 1983 dite Le Pors.

555 Art. 26, al.1 de la loi du 12 juillet 1983 dite Le Pors.

556 Conseil d'État (section), 11 janvier 1935, *Bouzanquet*, n° 40842. *Le Monde,* site internet, 11 octobre 2018, « Réseaux sociaux : quand les fonctionnaires se prennent les pieds dans le devoir de réserve ».

557 Le manquement ne s'apprécie pas au regard du contenu mais du mode de l'expression : il est déterminé au regard du caractère public de l'espace sur lequel le propos a été porté. L'obligation s'applique pendant et en dehors du temps de travail. Elle est évaluée selon plusieurs critères notamment la situation hiérarchique, les circonstances de l'expression, le degré de publicité. Ils doivent en particulier s'abstenir de divulguer des informations pouvant nuire à des collègues ou porter atteinte au bon fonctionnement du service.

558 *Le Monde*, site internet, 11 octobre 2018, « Réseaux sociaux : quand les fonctionnaires se prennent les pieds dans le devoir de réserve ».

Pour éviter de trop nombreux écarts, de nombreuses administrations se sont dotées de **chartes de déontologie. Les ministères des finances et des comptes publics ont publié en 2018 une charte d'utilisation des outils numériques qui prévoit que, si les agents peuvent utiliser les réseaux sociaux « grand public »**[559], ils sont responsables des contenus et commentaires qu'ils y publient et doivent en assumer les conséquences ; ils sont appelés à prendre en considération un contexte caractérisé par la perméabilité de la frontière entre cadre professionnel et vie privée et le risque que les contenus soient repris ou relayés par des tiers. Les collectivités territoriales ont pu elles aussi élaborer des chartes destinées à leurs agents dans une démarche pédagogique.

Dans **l'armée**, les militaires, soumis à une obligation de réserve particulièrement stricte[560], sont sensibilisés aux risques que représentent les communications sur les réseaux sociaux. Le premier risque identifié est celui de la fuite «involontaire», au sens où des soldats peuvent mettre en ligne des informations sans se rendre compte ni de leur caractère sensible, ni de l'impact qu'elles peuvent avoir en termes de sécurité. En 2010, une opération de l'armée israélienne aurait ainsi été annulée suite à sa révélation involontaire sur Facebook par un soldat[561]. Le deuxième risque est politique : des images choquantes peuvent être publiées malencontreusement et soulever des difficultés[562].

S'agissant des **magistrats**, la question est d'autant plus cruciale que les décisions rendues ne doivent être entachées d'aucun soupçon de partialité ou de conflit d'intérêt.

S'agissant des magistrats administratifs, la **charte de déontologie de la juridiction administrative** a été complétée pour prendre en compte les problématiques nouvelles liées à l'usage des réseaux sociaux[563]. Elle recommande de faire preuve de retenue dans l'utilisation des réseaux lorsque ces derniers ne restreignent pas l'accès à un cercle privé d'utilisateurs, notamment lorsque le partage d'opinions privées est susceptible de faire naître un doute sur l'impartialité du juge (article 47 de la Charte). Elle considère que le compte d'un réseau social doit être regardé comme étant public sauf si les paramètres ont eu pour effet de restreindre la portée des informations diffusées (article 47-1). Elle recommande également de s'abstenir de mentionner sur les réseaux sociaux la qualité de magistrat administratif ou de membre du Conseil d'État ou de prendre part à une polémique qui serait de nature à rejaillir sur l'institution (article 47-2). Aussi, il est demandé de s'abstenir de diffuser sous un pseudonyme des propos qui ne seraient pas assumés si divulgués sous

559 Facebook, Twitter, Snapchat, LinkedIn, Viadeo, Google+, Instagram...

560 L'art. L. 4121-2 du code de la défense indique que « *les opinions ou croyances, notamment philosophiques, religieuses ou politiques, sont libres* », mais ne peuvent être exprimées « *qu'en dehors du service et avec la réserve exigée par l'état militaire* ». Il impose une obligation de discrétion, « *les militaires doivent faire preuve de discrétion pour tous les faits, informations ou documents dont ils ont eu connaissance dans l'exercice de leurs fonctions* ». En outre, l'art. L. 4121-3 interdit aux militaires en activité « *d'adhérer à des groupements ou associations à caractère politique* », mais cela n'empêche pas qu'ils se présentent à des élections. Plus généralement, l'art. L. 4111-1 stipule que « *l'état militaire exige en toute circonstance esprit de sacrifice, pouvant aller jusqu'au sacrifice suprême, discipline, disponibilité, loyalisme et neutralité* ».

561 *Huffington post*, site internet, 30 juillet 2012, « Les armées face aux réseaux sociaux ».

562 *ibid*.

563 Décision du 16 mars 2018 complétant la Charte de déontologie de la juridiction administrative.

l'identité réelle (article 47-3). Enfin, elle demande à la fois de ne pas commenter l'actualité politique et sociale (article 47-4) et de faire preuve de prudence autant dans le partage de contenu que dans l'adhésion à d'autres contenus (article 45-5).

Les services publics aussi se sont dotés de **guides d'usage des réseaux sociaux** pour sensibiliser leurs agents. **Radio France** recommande à ses collaborateurs dans un guide de bonne pratique de s'exprimer en respectant « *les valeurs de véracité, de rigueur, de complétude, d'honnêteté, de mesure et d'impartialité* », de ne « *pas participer à la diffusion de rumeurs ou fausses informations* », « *de ne pas porter atteinte au principe de neutralité du service public* » et d'être prudent et vigilant. Ils sont informés que leurs publications peuvent engager la crédibilité de l'ensemble du service.

Les réseaux sociaux comme outil de gestion de carrière

Outre l'usage privé qui peut parfois être en délicatesse avec les obligations professionnelles des fonctionnaires, ceux-ci sont de plus en plus nombreux à utiliser les réseaux sociaux, notamment professionnels, pour faire connaître leurs compétences et promouvoir l'action de leurs services[564]. La place prise en quelques années par LinkedIn dans la gestion des ressources humaines de la fonction publique en est une illustration emblématique[565]. Les cadres ont été les premiers à en utiliser les fonctionnalités pour enrichir leur réseau, faire évoluer leur carrière et échanger avec leurs pairs[566]. Progressivement, ce réseau social s'est imposé comme un outil de travail partagé par l'ensemble de la fonction publique, facilitant le développement des échanges au sein d'une communauté de travail[567]. Il n'est pas exclu que les réseaux sociaux deviennent à terme un nouvel espace de gestion de carrière.

2.4. Un défi pour les régulations et les cadres d'intervention

Comme on l'a vu, les réseaux sociaux ont modifié le cadre des débats publics, le paysage économique et social, les relations entre l'État et ses administrés voire l'exercice de la souveraineté des États. Si les utilisateurs ont rendu cet outil incontournable, la question de sa **régulation** est apparue, après quelques années de flottement, indispensable. Il s'agit en effet de **garantir un marché économique libre qui reste équitable pour tous les opérateurs de marché, de préserver la vie privée de l'usager et de lutter contre l'ensemble des comportements qui mettent en péril la démocratie et l'ordre public tout en sauvegardant la liberté d'expression et de communication**. L'objectif est, certes, exigeant et difficile à

564 La Gazette des communes, site internet, 23 septembre 2020, « Les agents montrent leur meilleur profil sur les réseaux sociaux ».

565 Pour une analyse des facteurs expliquant la pénétration spectaculaire de LinkedIn dans le monde du travail, v. la conférence du Conseil d'État du 15 décembre 2021 sur «Les réseaux sociaux, vecteurs de la transformation de l'économie et du travail ».

566 A titre d'exemple : *Employés de EHESP - École des hautes études... - LinkedIn*

567 V. LinkedIn, *post*, « Post de Fonction Publique du XXIe siècle ».

atteindre, mais conforme aux libertés et aux droits fondamentaux auxquels notre pays est légitimement attaché. Les **méthodes et moyens utilisés** pour y parvenir varient. Sans cesse mis à l'épreuve, ils doivent s'ajuster. Cet exercice est d'autant plus difficile que le monde du numérique change constamment.

Si le droit s'est considérablement enrichi pour répondre à ces objectifs (*cf.* première partie), d'autres leviers d'action complémentaires ou autonomes sont utilisés. La palette est large et il faut peser au trébuchet l'intérêt de chacune de ces voies par rapport à l'objectif recherché pour ne pas porter atteinte de façon excessive à certains droits ou libertés. Il faut aussi articuler ces différents outils de régulation. C'est le **principe de proportionnalité** qui doit toujours guider l'action de la puissance publique. Ce principe est d'ailleurs un fil conducteur du DSA et du DMA.

Avant d'envisager les propositions qui pourraient être faites pour mieux répondre aux innombrables enjeux posés par les réseaux sociaux (troisième partie), plusieurs étapes doivent être franchies. La première consiste à examiner les atouts et limites de l'autorégulation qui s'est considérablement développée au fil du temps, la deuxième à faire le point sur l'ensemble des instruments mis en œuvre ces dernières années par la puissance publique pour réguler les réseaux sociaux, la troisième à écarter les pistes qui semblent inadéquates et la quatrième à esquisser, en tenant compte des arbitrages déjà effectués (notamment par le DSA et le DMA), les contours des prochaines régulations et des défis auxquelles elles vont être confrontées.

2.4.1. Les avantages et les limites de l'auto-régulation

La modération : miracle ou mirage ?

Face à la multiplication des contenus problématiques et outre la procédure de signalement par les utilisateurs que les normes en vigueur leur imposent de mettre en place, les plateformes se sont dotées de **règles internes de fonctionnement** qui sont, pour certaines, exposées dans les conditions générales d'utilisation et visent à lutter contre les contenus illicites. Si la suppression des contenus manifestement illicites (terrorisme et pédopornographie) est peu à peu maîtrisée par les grands réseaux sociaux, il est en revanche beaucoup plus difficile de lutter contre la désinformation (*fake news*) ou les contenus haineux dont la définition n'est pas toujours aisée.

- *Les différents types de modération*

Ce qu'on a appelé pudiquement « **modération** » est tantôt réalisée par l'internaute lui-même sur demande de la plateforme, par des personnes appelées modérateurs (ou patrouilleurs chez Wikipédia), tantôt par des algorithmes, tantôt par les deux. La mesure la plus emblématique de régulation consiste à supprimer ou rendre **invisibles** des contenus. Cette invisibilisation sous la forme du « shadowban » permet de neutraliser la diffusion sans que l'internaute s'en rende forcément compte. Face à la masse de données échangées – Twitter par exemple qui voit à peu près 500 millions de *tweets* par jour, Youtube 500 heures de vidéo par minute[568] – la plupart des plateformes ont en effet recours à des **algorithmes** qui effectuent ce tri soit au moyen de mots ou images clefs soit en mobilisant d'autres données. Twitter

568 Estimation chiffrée en 2022 transmise par les opérateurs

parviendrait ainsi à bloquer environ 90% des contenus pédopornographiques de sa propre initiative, ce qui est à la fois beaucoup et pas assez. Elles ont aussi recours à titre principal ou complémentaire à des **contrôleurs humains** qui vérifient le tri opéré par l'algorithme ou effectuent ce tri dans certains cas. Au fil des années, les procédures internes se sont enrichies et ont tenu compte de la nécessité de **graduer les réactions**. Ainsi Twitter peut réduire simplement la visibilité d'un contenu désagréable, demander à l'utilisateur de retirer son contenu pour pouvoir retweeter ou suspendre un compte temporairement. Suite à plusieurs rappels à l'ordre un compte peut être définitivement suspendu. Youtube dispose également d'une procédure assez normée (au bout de trois récidives, la chaîne Youtube en cause est fermée).

• *Entre « sur-modérer » et « sous-modérer », un tamis difficile à configurer*

Trier du contenu sans tomber dans l'atteinte à la liberté d'expression est délicat. Les plateformes sont accusées d'en faire trop ou pas assez. Même LinkedIn a été montré du doigt comme lieu de désinformation sur les vaccins contre la covid 19. Les plateformes se prêtent de plus ou moins bonne grâce à l'exercice de modération mais elles revendiquent, pour la plupart, le droit de ne pas devenir des « administrateurs de la vérité »[569], ce qui est compréhensible.

S'agissant des modérations humaines, outre les questions de respect des droits sociaux des intéressés qu'elles soulèvent, leur qualité suppose d'être réalisée par des personnes en nombre suffisant et maitrisant la langue et la culture des pays dans lesquels les contenus sont visibles. Officiellement pour des raisons de sécurité, les opérateurs rechignent à transmettre des informations sur ce point de sorte qu'il est bien difficile d'évaluer son niveau d'efficacité. S'agissant des algorithmes, leur paramétrage peut conduire à des résultats iniques. Le tri par mots-clefs conduit à une sélection parfois grossière car le contexte des propos n'est pas pris en compte (humour, ironie) ; de même celui par images conduit à des suppressions injustifiées ou absurdes (comme la censure du célèbre tableau *L'origine du Monde* de Gustave Courbet). La difficulté tient également au fait que les algorithmes ne tiennent pas compte de la culture du pays. Certains contenus pourraient être illicites dans certains pays et pas dans d'autres, mais l'intelligence artificielle – qui ne porte pas toujours bien son nom – ne procède le plus souvent à aucune contextualisation[570]. Compte tenu du faible accès aux données des opérateurs, la puissance publique peine à évaluer le nombre de contenus non illicites qui sont rejetés par les algorithmes.

Les juridictions ont été saisies de difficultés s'agissant des tris opérés par les algorithmes et ont rendu des décisions qui permettent peu à peu de constituer des lignes directrices. Ainsi, la CJUE, dans un arrêt du 6 octobre 2020 (aff. C-511/18), rendu à propos d'un algorithme mis en place pour détecter automatiquement les contenus terroristes, a précisé les conditions auxquelles doivent répondre les algorithmes. Elle énonce ainsi que « *les modèles et critères préétablis sur lesquels se fonde ce type de traitement de données doivent être, d'une part, spécifiques et fiables, permettant d'aboutir à des résultats identifiant des individus à l'égard*

569 *Le Monde*, site internet, 18 février 2022, « Sur LinkedIn, la désinformation en toute tranquillité ».
570 *France Culture*, site internet, 28 octobre 2020, « Réseaux sociaux : la régulation face aux libertés, 28/10/20, avec Romain Badouard et Joëlle Toledano ».

desquels pourrait peser un soupçon raisonnable de participation à des infractions *terroristes, et d'autre part, non-discriminatoires* ». Elle évoque également la nécessité **d'une intervention humaine** en raison d'inévitables erreurs dans ce type d'algorithmes. Enfin, elle demande l'information des personnes par la publication des renseignements de nature générale sur le traitement et, dans certains cas, l'intervention humaine. S'agissant des **algorithmes utilisés par l'administration,** le Conseil constitutionnel, à l'occasion de l'examen de la procédure Parcoursup fondé sur un traitement algorithmique, a consacré par une décision du 3 avril 2020[571] l'existence d'un droit constitutionnel à l'accès aux documents administratifs, renforçant ainsi l'exigence « d'explicabilité » des algorithmes.

Un moyen de limiter les effets nocifs des réseaux sociaux est aussi d'identifier les contenus les plus viraux et de se concentrer sur leur analyse et leur modération. Certains opérateurs, comme Twitter, prônent une approche *safety by design* pour « dissuader à la viralité » par exemple en sollicitant l'internaute et lui demandant s'il a lu le contenu avant de le retweeter. Des mécanismes d'authentification des comptes sont aussi proposés pour les personnes jouissant d'une notoriété publique.

Les réseaux sociaux ont été critiqués pour avoir « sur-modéré » des contenus et ainsi « privatisé » la censure[572]. D'un autre côté, une **sous-modération** est aussi critiquable. L'affaire des Facebook Files en constitue un bon exemple.

Les *Facebook files* (2021) suite aux révélations de Frances Haugen

En septembre 2021, le Wall Street Journal publie une série d'articles prenant appui sur des milliers de documents internes à Facebook (Facebook files) révélés par une ancienne employée, Frances Haugen. Selon ces documents, l'entreprise privilégierait le profit par rapport à la sécurité des données et à la protection des utilisateurs et utilisatrices. La modération serait plus souple pour certaines célébrités ou personnels politiques qui seraient traités différemment de l'utilisateur classique et la société, Instagram, bien que consciente de la nocivité de certains contenus sur **la santé mentale des jeunes** notamment, n'aurait rien fait pour pallier ces dysfonctionnements et aurait volontairement laissé travailler depuis 2018 des algorithmes mettant en avant des contenus violents et toxiques et accélérant la propagation de fausses nouvelles, sans que les ingénieurs de la plateforme ne réussissent à l'endiguer. D'autres révélations ont suivi notamment celles liées à la **mauvaise qualité de la modération** effectuée sur les contenus dans des langues autres que l'anglais, comme l'arabe et ses nombreux dialectes. Cette sous-modération encouragerait la propagation de contenus violents dans des pays déjà en proie aux crises géopolitiques (comme l'Irak ou le Yémen). Frances Haugen a également déposé plainte auprès de la SEC accusant Facebook de mentir à ses investisseurs. Auditionnée par le Sénat américain en octobre 2021, elle a également été entendue par plusieurs instances européennes et françaises.

571 Décision n° 2020-834 QPC du 3 avril 2020 *Union nationale des étudiants de France [Communicabilité et publicité des algorithmes mis en œuvre par les établissements d'enseignement supérieur pour l'examen des demandes d'inscription en premier cycle].*

572 R. Badouard, « Les plateformes, nouveaux censeurs », *Esprit,* mars 2021.

Devant ces difficultés, les plateformes testent régulièrement de nouveaux dispositifs. Twitter a annoncé la mise en place de communautés fermées avec des **modérateurs bénévoles**. De très nombreux réseaux sociaux ont recours à la **modération communautaire**[573]. Elle fonctionne très bien pour l'encyclopédie Wikipédia qui est déjà fondée sur un modèle collaboratif et compte sur ses patrouilleurs[574]. Elle est également utilisée sur les groupes privés de Facebook.

L'Oversight Board de Meta : exemple ou contre-exemple ?

L'*Oversight Board* (littéralement Conseil de surveillance) encore appelé « **Cour suprême de Facebook** », a été imaginé par Marc Zuckerberg sur la suggestion d'un professeur de droit de Harvard en novembre 2018, préfiguré en 2019[575] et a vu le jour en 2020. Il se veut **indépendant** (il est financé par Méta mais *via* un trust séparé), **accessible** et **transparent**. Sa mission est de confirmer ou d'infirmer les décisions de modération de Facebook[576] (et d'Instagram) après avoir examiné leur conformité avec les règles de contenus et les valeurs édictées par Meta. Ses décisions s'imposent à toutes les instances internes et aux utilisateurs de Méta (sauf contrariété avec la loi). Elles sont rendues publiques et accompagnées d'une note. Les membres de cet organe disposent notamment du pouvoir de demander des informations complémentaires à la plateforme, d'interpréter les standards de la communauté Facebook[577], de demander à autoriser ou supprimer un contenu. Cet organe peut également publier des avis consultatifs en matière de politiques conduites par Meta et formuler des recommandations en vue de les amender[578]. L'*Oversight Board* est donc une forme d'**instance d'appel** interne à l'entreprise et organisée par elle, qui a en outre la particularité de pouvoir **sélectionner,** dans un délai de 90 jours, les affaires qui présentent une complexité, une importance et une pertinence particulières à l'échelle mondiale qui pourraient contribuer à élaborer de futures règles. Il est composé de **20 membres,** nommés pour 3 ans renouvelable 2 fois, recrutés parmi des personnalités reconnues[579], soumis à des règles de confidentialité et d'impartialité, qui peuvent s'adjoindre ponctuellement les éclairages **d'experts externes**.

573 *Le Monde*, site internet, 6 novembre 2021, « La modération communautaire est-elle l'avenir des réseaux sociaux ? ».

574 La modération est très active sur Wikipédia. Il existe un filtre pour empêcher les modifications de l'encyclopédie trop grossières. Les communautés de Wikipédia par pays ont le pouvoir de poser des filtres qui sont en partie régis par des algorithmes. Ils repèrent certains mots clés ou motifs repérés dans le texte (« expressions régulières ») et selon la nature du problème, être signalés. Les patrouilleurs (bénévoles) sont chargés de vérifier que la modification est censée. La sanction est le blocage de la personne.

575 Rapport d'expertise et de contribution international, sur le fondement des experts internationaux interrogés par l'entreprise (issus de 88 pays différents) et charte de fonctionnement.

576 Les sanctions ordinaires de Facebook sont la suppression de contenus en infraction, la suspension de comptes ou de pages avec un délai précis, ou la désactivation permanente du compte

577 Ces standards sont la liberté d'expression, l'authenticité, la sécurité, la confidentialité, la dignité.

578 Le premier avis consultatif relatif au partage d'informations privées sur le lieu de résidence, a été publié par le Conseil en février 2022.

579 Not. Helle Thorning-Schmidt, ancienne première ministre du Danemark, Catalina Botero Marino, ancienne rapporteure spéciale pour la liberté d'expression auprès de la Commission interaméricaine des droits de l'homme, Alan Rusbridger, ancien rédacteur en chef du *Guardian*, ou Tawakkol Karman, militante qui a reçu le prix Nobel de la paix en 2011 pour son rôle dans les manifestations du printemps arabe au Yémen, ou encore Julie Owono, avocate franco-camerounaise, directrice d'Internet sans frontière. Cinq membres sur vingt sont américains.

Quelques décisions et rapports de l'Oversight Board

Saisi du dossier relatif à l'exclusion de Donald Trump du réseau social, l'Oversight board a confirmé la décision d'exclusion mais a demandé à Facebook de revoir dans le délai de 6 mois si le compte devait être définitivement supprimé ou seulement temporairement suspendu. Suite à cette décision, Meta a suspendu les comptes du président Trump jusqu'en janvier 2023. D'autres décisions **ont annulé** des suppressions de publications ou de comptes par Facebook en estimant, après expertise, que les standards n'avaient pas été enfreints. Il en est ainsi de le la décision de suppression d'une publication d'août 2019 d'un utilisateur suédois sur sa page Facebook, décrivant des violences sexuelles sur deux mineures alors qu'il s'agissait de signaler une question d'intérêt général et de condamner l'exploitation sexuelle des mineurs[580], de la suppression d'une publication discutant d'une infusion à base de plantes diffusée par le compte Instagram d'une école spirituelle au Brésil en estimant que les utilisateurs doivent pouvoir discuter positivement d'utilisations traditionnelles ou religieuses de substances qui ne sont pas médicales[581], de la décision de Meta de supprimer une publication d'un artiste autochtone d'Amérique du Nord qui visait à sensibiliser le public aux massacres historiques perpétrés contre ces peuples d'Amérique du Nord[582]. L'Oversight Board a aussi confirmé certaines décisions[583]. Il publie aussi des **rapports** dont celui de 2021 qui a demandé à Facebook de renforcer sa politique de transparence, notamment concernant le système de régulation de comptes détenus par des personnalités politiques[584]. Les derniers rapports d'activité notaient une croissance constante du nombre d'appels (339 000 cas au troisième trimestre 2021) alors que seulement 6 décisions avaient été rendues pendant la même période. Le scandale des *Facebook files* a mis à mal la crédibilité de cette instance dont les règles de fonctionnement originales (empruntant seulement partiellement au système arbitral) suscitent la polémique[585].

Si la mise en place de cette instance (qui a conduit Facebook à accepter davantage de transparence) peut constituer une avancée en permettant de contester les décisions de modération devant un organe dont les premières décisions semblent pouvoir être regardées comme impartiales, son existence ne peut suffire à répondre à toutes les questions que soulèvent les décisions de modération et,

580 Décision sur le cas 2021-016-FB-FBR (1er février 2022).

581 Décision sur le cas 2021-013-IG-UA (9 décembre 2021).

582 Décision sur le cas 2021-012-FB-UA (9 décembre 2021).

583 Décision sur le cas 2021-011-FB-UA (28 septembre 2021), dans laquelle le Conseil a confirmé la décision de Facebook de supprimer une publication d'un utilisateur anglais d'Afrique du Sud sur la société sud-africaine qui comportait des termes insultants pour les personnes ciblées.

584 Le Conseil dénonce le manque de clarté dans les règles de modération de contenu appliquées par la plateforme ainsi que le système de régulation des comptes « VIP » par le système de « cross-check » (XCheck), dévoilé par la lanceuse d'alerte Frances Haugen au Wall Street Journal en septembre 2021. Ce système, bénéficiant à des millions de comptes de personnalités ou de responsables politiques, permet de les soustraire à la modération commune appliquée aux comptes ordinaires. Le Monde avec AFP, « Le conseil de surveillance de Facebook critique les règles du réseau social concernant la modération des contenus de célébrités », 21 octobre 2021

585 *CNN Business,* site internet*,* 12 octobre 2021, « Whistleblower Frances Haugen will meet with Facebook Oversight Board ».

plus fondamentalement, ses conditions de mise en place et d'exercice soulèvent des questions nouvelles tenant à une forme de « privatisation » de la justice, qui plus est dans un domaine particulièrement sensible. En outre, elle n'est saisie que d'un nombre infime de dossiers par rapport à la masse de contentieux, elle décide des dossiers sur lesquels elle se prononcera et exerce son contrôle en se fondant essentiellement sur les règles fixées contractuellement par le réseau social en cause même si parmi ses principes directeurs figurent des normes internationales[586]. La création de cette instance soulève donc au moins autant de questions que celles auxquelles elle prétend répondre et cette voie peut difficilement être envisagée comme un modèle, sauf à s'engager dans une véritable privatisation de la justice et de la liberté d'expression sur internet.

L'auto-régulation : un outil nécessaire qui n'est pas suffisant et qui doit être supervisé

L'auto-régulation ne constitue pas un outil suffisant pour assurer la régulation des réseaux sociaux. D'une part, la crédibilité de la démarche peine à s'accommoder du manque d'informations données par les opérateurs de réseaux sociaux ; d'autre part, chaque plateforme adopte ses règles de régulation rendant de fait impossible une réelle régulation du secteur par les pairs, enfin, pour l'instant, l'autorégulation semble plus un outil pour limiter l'intrusion des acteurs publics que pour internaliser les exigences normatives[587]. L'auto-régulation constitue un **outil peut-être utile mais certainement pas suffisant**. Elle doit aussi se réaliser **sous étroite surveillance du régulateur** : il est primordial que les décisions de modération soient transparentes et contestables par l'utilisateur devant une instance indépendante extérieure au réseau social en cause. C'est d'ailleurs un objectif du DSA.

2.4.2. La diversité des instruments mis en place par la puissance publique

Pour tenter de parvenir à une régulation plus efficace, la France a d'ores et déjà recours à des instruments permettant d'expertiser et d'analyser les problématiques posées, à des instruments de régulation et des politiques publiques visant à éduquer et sensibiliser les individus pour leur permettre de tirer le meilleur des réseaux sociaux et de se prémunir contre les risques qu'ils présentent.

Les instruments d'évaluation et d'expertise

Pour qu'une régulation soit effective dans un secteur aussi technique que le numérique, l'État doit plus que jamais s'appuyer sur des outils d'analyse et d'évaluation.

586 Blog de F. Gsell, 6 mai 2021, « facebook-et-la-suspension-de-trump-le-facebook-oversight-board-est-il-au-rendez-vous» .

587 Mission « Régulation des réseaux sociaux-Experimentation Facebook », mai 2019.

• *L'observatoire de la haine en ligne*

Les pouvoirs publics ont mis en place un instrument spécifique pour lutter contre la haine en ligne : l'observatoire de la haine en ligne, crée par la loi du 24 juin 2000 dite loi Avia. Sa mission est triple : analyser et quantifier les contenus haineux en ligne, suivre l'évolution de la haine en ligne pour mieux comprendre son fonctionnement et partager les informations des différents acteurs concernés, publics et privés. Il regroupe des représentants des grands opérateurs, des associations, des administrations et des chercheurs. Il a institué en son sein plusieurs groupes de travail[588] pour avoir un suivi plus précis du phénomène. En pratique, cette instance apparaît comme un outil précieux de **discussion et de concertation avec les acteurs du marché pour la mise en œuvre de la régulation.**

• *Le pôle d'expertise de la régulation numérique : le PeRen*

Le manque de compétence technique de l'administration française pour apporter un contre-point aux plateformes des réseaux sociaux a rapidement été identifié comme une lacune invalidante. Le décret n° 2020-1102 du 31 août 2020 a ainsi instauré un service à compétence nationale, le pôle d'expertise de la régulation numérique (PEReN), rattaché au Directeur Général des Entreprises (DGE) pour sa gestion administrative et financière, et placé sous l'autorité conjointe des ministres chargés de l'économie, de la culture et du numérique. Il a pour objet de venir en aide à l'État et aux diverses AAI concernées (Autorité de la concurrence, CSA/ARCOM, ARCEP, CNIL, etc.) et pour mission d'étudier les plateformes numériques afin de mettre en place ou d'adapter leur régulation. Il peut intervenir **pour apporter aux services de l'État une expertise et une assistance technique générale sur les données** (notamment en matière d'analyses de données, de codes sources, de programmes informatiques, de traitements algorithmiques et d'audit des algorithmes utilisés par les plateformes numériques) **et pour fournir une contribution et une expertise techniques sur les plateformes numériques** dans le cadre de contrôles, enquêtes ou études menées sur elles. Sa mission est de vérifier que les plateformes respectent bien la réglementation et les garanties qu'elles offrent aux utilisateurs dans leurs règlements[589]. Le PeRen entretient des échanges réguliers avec les services de l'État intéressés. Enfin il anime un réseau d'experts publics en sciences des données et des traitements algorithmiques, en associant des représentants de la recherche (en lien, notamment, avec la direction interministérielle du numérique, chargée de l'informatisation des services de l'État).

Le PEReN réalise des «preuves de concept» c'est-à-dire des études qui permettent de voir ce qu'il est réellement possible de faire pour créer un cadre réglementaire efficace. Il travaille ainsi sur une méthode novatrice d'audit dite en transparence « faible », qui permet de solliciter des algorithmes sans disposer du code source afin de comprendre les paramètres pris en compte. Il peut ainsi trouver les critères

588 Un pour réfléchir à la notion de contenus haineux et proposer une définition, un pour étudier la pratique des contenus haineux, un chargé d'analyser les mécanismes de diffusion et de propagation des discours haineux et de réfléchir à la façon de les détecter et les combattre et le dernier consacré à la prévention, à l'éducation et à l'accompagnement des publics.

589 *Le Monde*, site internet, 22 janvier 2021, « A Bercy, une cellule d'informaticiens pour aider l'État à réguler les GAFA ».

d'un algorithme de recommandation. Il a publié le 6 mai 2021, une étude sur les méthodologies d'audit des algorithmes de recommandation de contenus, dans laquelle il dresse un état des lieux des méthodes qui peuvent être utilisées, suivant le coût pour la plateforme et le régulateur, ainsi que la granularité de l'audit[590]. Aux côtés de l'INRIA, il a lancé un projet, appelé Regalia, qui vise identifier les outils permettant de vérifier que les plateformes respectent le principe de loyauté[591]. Outil précieux pour développer des politiques publiques pertinentes dans un domaine hautement technique, il a notamment publié des notes d'expertise sur l'interopérabilité[592], sur les enjeux de sécurité pour la distribution des applications mobiles hors des magasins des OS[593] et plus récemment sur les outils de vérification d'identité des mineurs[594].

Pour pouvoir assurer ses missions, la loi[595] lui a confié à titre expérimental la possibilité de collecter des données dans le but « *d'expérimenter des outils liés à la régulation de ces opérateurs de plateforme* », sans que les opérateurs des plateformes puissent lui opposer un refus d'accès aux services existants de mise à disposition de ces données ou une interdiction de collecte automatisée par les CGU. Un décret d'application encadre cette collecte et la durée de conservation. Le succès du PeRen fait consensus et il est souhaitable que son dimensionnement soit désormais à la hauteur des enjeux actuels.

Les instruments de régulation existants

Pour mettre en œuvre l'ensemble des règles déjà existantes, la France s'est dotée de très nombreuses structures et d'outils de coopération qui sont désormais bien implantés dans le paysage institutionnel. Outre le rôle majeur des régulateurs (autorités administratives indépendantes et services de l'État), plusieurs dispositifs spécifiques doivent être mentionnés.

- *Les structures centrales permettant d'améliorer l'efficacité des politiques publiques en matière numérique*

Avec l'avènement du numérique, de multiples structures ont vu le jour au sein des administrations pour adapter les politiques publiques à ces nouveaux enjeux. Aucune n'est spécifiquement dédiée aux réseaux sociaux car les problématiques posées sont plus larges. Les ministères se sont dotés, pour la plupart, d'une agence ou d'un service chargé du numérique[596]. La **direction interministérielle du numérique** (DINUM) qui est en charge de la transformation numérique de

590 PEReN, rapport, « Méthodes d'évaluation des algorithmes de recommandation de contenus », 6 mai 2021.

591 INRIA, site internet, 8 décembre 2020, « Le projet-pilote REGALIA au service de la régulation des algorithmes ».

592 PEReN, site internet, 8 octobre 2021, « Éclairage sur : l'interopérabilité ».

593 PEReN, rapport, 18 février 2022, « Applications mobiles : quels enjeux de sécurité pour leur distribution hors des magasins des OS ? ».

594 PEReN, rapport, 20 mai 2022, « Éclairage sur…no 4 - Détection des mineurs en ligne : peut-on concilier efficacité, commodité et anonymat ? ».

595 Art. 36 de la loi n° 2021-1382 du 25 octobre 2021.

596 Parmi les multiples services, il faut citer également l'agence du numérique, service à compétence nationale chargé d'impulser et de soutenir des actions préparant la société française aux révolutions numériques rattaché au ministère de l'économie.

l'État (modernisation du système d'information de l'État, qualité des services publics numériques, création de services innovants pour les citoyens et outils numériques de travail collaboratif pour les agents) existe sous des appellations différentes depuis 2011 ; mais, s'agissant des réseaux sociaux, c'est la **direction des plateformes de la direction générale des entreprises** rattachée au ministère des finances et de l'économie qui pilote notamment les évolutions réglementaires sur le sujet (en lien avec le ministère de la culture).

> • *Les plateformes de signalement au soutien de la lutte contre les comportements illicites sur les réseaux sociaux et la protection de la cybersécurité (Pharos, Thésée, cyber malveillance.gouv.fr)*

Les réseaux sociaux sont le lieu d'actes cybercriminels ou cybermalveillants (harcèlements, hameçonnage ou *phishing*, piratage de comptes, rançongiciels ou ransomwares, prise d'otage de données personnelles, arnaques, etc.). Des instruments visant à lutter contre ces différents types de malveillance voire de délinquance ont été instaurés.

S'agissant du volet cyber-sécurité, **l'agence nationale de sécurité des systèmes d'information** (ANSSI), service à compétence nationale rattaché au secrétariat général de la défense et de la sécurité nationale (SGDSN), a vu le jour en 2009. Elle assure une mission **de défense** des systèmes d'information de l'État mais elle est aussi chargée d'une mission de conseil et de soutien aux administrations et aux opérateurs d'importance vitale. Une plateforme intitulée **cybermalveillance.gouv.fr** a été créée en 2017 à l'initiative du ministère de l'Intérieur et de l'ANSSI pour prévenir et sensibiliser les internautes à la cybersécurité, assister les victimes d'actes de cybermalveillance et accompagner les professionnels dans la sécurisation de leur système d'information[597].

Sur le volet répressif, a été mis en place dès 2009[598], au sein de l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), un portail de signalement des contenus illicites de l'internet dénommé **Pharos**[599], qui permet de signaler en ligne les contenus et comportements illicites de l'internet. Cette plateforme permet à chaque internaute de signaler les contenus illicites dans une variété de domaines[600]. Une fois le contenu signalé, des policiers et gendarmes affectés vérifient que les contenus et comportements signalés constituent bien une infraction à la loi française. Leur mission est de les traiter et d'alerter les services compétents tels la Police nationale, la Gendarmerie nationale,

597 Dans l'optique de renforcer la cybersécurité des internautes et des organisations, le projet de loi d'orientation et de programmation du ministère de l'intérieur (LOPMI), présenté en conseil des ministres le 16 mars 2022 entend moderniser et augmenter les outils dont disposent l'État pour renforcer cette cybersécurité, notamment sur les réseaux-sociaux par la création d'une agence numérique des forces de sécurité, d'une école «cyber» au sein du ministère, la création du numéro 17 Cyber, pour signaler en direct une cyberattaque ou une escroquerie en ligne, recrutement de 1 500 cyber-patrouilleurs, sensibilisation.

598 Arrêté du 16 juin 2009 portant création d'un système dénommé « Pharos » (plate-forme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements).

599 Plateforme d'Harmonisation, d'Analyse, de Recoupement et d'Orientation des Signalements

600 Pédocriminalité et pédopornographie, expression du racisme, de l'antisémitisme et de la xénophobie, incitation à la haine raciale, ethnique et religieuse, terrorisme et apologie du terrorisme, escroquerie et arnaque financières utilisant internet)

les Douanes, la Direction générale de la concurrence, de la consommation et de la répression des fraudes. Une enquête est alors ouverte sous l'autorité du procureur de la République. De nombreux signalements sont transmis à la justice afin de voir supprimer les contenus illicites.

Cette plateforme qui emploie une cinquantaine d'agents (policiers et gendarmes) est **un succès** dans la mesure où elle est à la fois relativement bien connue des internautes et bien investie par ces derniers. En 2021, il y a eu environ 264 000 signalements sur Pharos (qui se ventilent ainsi : 53,7% pour escroqueries, 11,3% pour atteintes aux mineur, 5,7% pour discrimination et 3% pour terrorisme). Les grandes plateformes de réseaux sociaux se montrent assez coopératives pour identifier les auteurs de contenus illicites qu'elles retirent à la demande des autorités de police ; la coopération est toutefois plus délicate s'agissant des contenus haineux, plus difficiles à caractériser. La difficulté est souvent d'obtenir, pour permettre l'enquête, les données pertinentes. Par exemple, à la suite de l'assassinat de Samuel Paty, certains des opérateurs sollicités n'ont pas pu fournir aux autorités françaises les contenus précédemment signalés dans la mesure où ils avaient été supprimés par la plateforme.

Le 15 mars 2022 a été mis en place, toujours au sein de l'OCLCTIC le dispositif **Thésée**[601] qui permet de **déposer plainte en ligne** – *via* "France Connect" – pour des actes de cybermalveillance. Les plaintes et signalements sont traités par une équipe de 17 policiers et gendarmes affectés. Le délai de réponse estimé est d'environ huit jours, pour un volume de dossiers quotidiens évalué à 500. Les actes les plus problématiques pourront être aussi transférés à Pharos puis réorientés. Un dispositif devrait faciliter les recoupements de plainte et l'identification de phénomènes de masse comme la circulation de faux passes sanitaires sur Snapchat en 2021.

Il faut noter aussi l'existence d'une plateforme dénommée **pointdecontact.net**, mise en place par l'association des fournisseurs d'accès et de services internet (AFA). Grâce à des outils de signalements des contenus illicites (application mobile, formulaire en ligne, extension de navigateur internet, etc.), les signalements sont recueillis puis analysés avant que soient entreprises des démarches de retrait de contenu auprès des opérateurs et d'être transmis à Pharos. En 2020, *Point de Contact* a reçu 60 307 signalements, représentant une augmentation de plus de 98% par rapport au nombre de signalements reçus en 2019.

- *Les dispositifs de police administrative de retrait et de blocage*

Dans le cadre des dispositifs de lutte contre les contenus illicites, des instruments administratifs et judiciaires ont été mis en place pour permettre le retrait ou le blocage rapide de ces contenus[602].

Outre les mécanismes de référé ou de procédure accélérée au fond, la loi du 13 novembre 2014 relative à la lutte contre le terrorisme permet le **blocage** par une **autorité administrative** désignée, en l'occurrence l'OCLCTIC, des sites web

601 Traitement Harmonisé des Enquêtes et des Signalements pour les E-escroqueries.
602 Des demandes de déréférencement peuvent aussi être faites auprès des moteurs de recherche.

provoquant à des actes de terrorisme ou en faisant l'apologie ainsi que des sites contenant des représentations de mineurs à caractère pornographique. Elle permet également des mesures administratives de **retrait** et de déréférencement de ces mêmes contenus, adressées par l'autorité administrative aux éditeurs, hébergeurs et moteurs de recherche[603]. Ces derniers sont passibles de sanctions pénales en cas de refus[604]. Afin d'éviter toute mesure qui serait disproportionnée ou abusive, la loi soumet le dispositif au contrôle d'une **personnalité qualifiée** désignée, en son sein, par l'autorité compétente. La personnalité qualifiée vérifie le bien-fondé des demandes de retrait de contenus et de blocage. Si elle estime que ces demandes n'étaient pas conformes aux textes en vigueur, elle émet des recommandations aux fins de levée de la mesure de blocage ou de retrait. Elle peut saisir le juge administratif en cas de difficulté. À compter du 7 juin 2022, le contrôle en matière de blocage, de retrait et de déréférencement administratifs de contenus des sites terroristes et pédopornographiques sera opéré par la personnalité qualifiée désignée par l'ARCOM, alors qu'auparavant cette personne était désignée par la CNIL. En 2021, 137 953 mesures administratives ont été prononcées[605].

C'est également à cette date que sera applicable le **règlement TCO**[606], entré en vigueur le 6 juin 2021 qui permet de faire **retirer** dans un délai d'une heure les contenus à caractère terroriste sur internet par les plateformes ayant leur siège principal en France[607]. Il sera également possible de solliciter ce retrait d'autres États membres si besoin. Une proposition de loi visant à adapter le droit français à ce nouveau dispositif a été déposée devant l'Assemblée Nationale le 11 janvier 2022[608]. Il est envisagé de conférer à l'ARCOM un pouvoir de sanction pécuniaire à l'encontre des opérateurs qui ne se conformeraient pas aux injonctions de suppression des contenus.

Le rapport d'activité de la personnalité qualifiée pour l'année 2021 fait apparaître un accroissement considérable du nombre de contenus illicites ayant fait l'objet d'une intervention de l'OCLCTIC et donc d'une vérification par la personnalité qualifiée. 137 953 demandes de l'OCLCTIC visant à restreindre l'accès à des contenus à caractère terroriste ou pédopornographique ont été vérifiées en 2021 par la personnalité qualifiée, soit une augmentation de 250% par rapport à 2020. La majorité des demandes sont suivies d'effet[609].

---

603 Sont visés les contenus contraires aux art. 227-23 et 421-2-5 du code pénal.

604 Est puni d'un an d'emprisonnement et de 75 000 € d'amende le fait, pour une personne physique ou le dirigeant de droit ou de fait d'une personne morale exerçant l'activité de fournisseur d'hébergement ou d'accès, de ne pas satisfaire aux obligations définies à l'art. 6, I, 7., alinéas 4 et 5 de la LCEN, ni à celles prévues à l'art. 6-1 LCEN, de ne pas avoir conservé les éléments d'information visés à l'art. 6, II, LCEN ou de ne pas déférer à la demande d'une autorité judiciaire d'obtenir communication desdits éléments.

605 118 407 retraits, 420 blocage et 2 568 déréférencement s'agissant des contenus pédopornographiques ; 14 888 retraits, 19 blocage et 1 651 déférencement s'agissant des contenus terroristes.

606 Règlement du Parlement européen et du Conseil du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne.

607 Il reviendra au législateur de désigner la personnalité qualifiée qui sera amenée à vérifier les mesures prises dans ce nouveau cadre et à adapter la LCEN à ce nouveau dispositif.

608 Proposition de loi portant diverses dispositions d'adaptation au droit de l'Union européenne en matière de prévention de la diffusion de contenus à caractère terroriste en ligne, n° 4883.

609 CNIL, rapport d'activité de la personnalité qualifiée.

• *L'adaptation des services et techniques d'enquêtes ainsi que de l'institution judiciaire*

-- Les services d'enquête

En France, plusieurs services spécialisés dans la délinquance sur internet existent : ce sont le département informatique et électronique de l'Institut de recherches criminelles (IRCGN), la Brigade d'enquête sur les fraudes aux technologies de l'information (BEFTI) et surtout **l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC)** structure interministérielle, à compétence nationale, centralisée et opérationnelle placé auprès de la direction Centrale de la Police Judiciaire (DCPJ)[610]. Il comporte en son sein la plateforme Pharos, une section opérationnelle chargée de la répression des infractions, une section d'assistance technique de recherche et de développement, une section des relations internationales chargée de la coopération avec Europol, Interpol et les pays signataires de la Convention de Budapest[611] et une section de formation des investigateurs en cybercriminalité. Il anime le réseau que ces derniers constituent avec les Laboratoires de l'investigation opérationnelle du numérique (LION) déployés depuis 2015 sur le territoire. Par ailleurs, en février 2021, a été créé un pôle cyberespace dénommé **ComCyberGend** relevant directement du directeur général de la gendarmerie nationale ayant pour mission de piloter, conduire et animer le dispositif de la gendarmerie nationale dans la lutte contre les cyber-menaces[612]. Il est en mesure de réaliser des investigations dans l'ensemble des espaces numériques, mais également de développer de nouvelles méthodes criminalistiques d'investigation numérique.

-- Les techniques d'enquêtes propres à la cyber-criminalité

Afin de simplifier la mission confiée aux enquêteurs, des outils spécifiques tels que la réquisition informatique[613] ont été mis en place. Ils peuvent être accompagnés d'une procédure de mise au clair des données cryptées nécessaires à la manifestation de la vérité, de saisie, de géolocalisation[614] voire parfois de la mise en œuvre d'une enquête sous pseudonyme ou d'une infiltration. La loi du 21 juin 2004 punit de

610 L'Office coordonne, au niveau national, la mise en œuvre des opérations de lutte contre les auteurs d'infractions liées aux technologies de l'information et de la communication. Dans ce cadre, il diligente des enquêtes spécialisées, et il procède, à la demande de l'autorité judiciaire, à des actes d'enquête et à des travaux techniques d'investigation. L'OCLCTIC détient une base de sites pédopornographiques dénommée GESSIP (gestion des sites pédophiles), et il gère le point de contact national des signalements dans le cadre de la lutte contre la pédophilie (www.internet.mineurs.gouv.fr).

611 Concernant toutes les infractions qui relèvent de sa compétence, l'office constitue, pour la France, le point de contact central dans les échanges internationaux par l'intermédiaire du Bureau central national d'Interpol, de l'unité nationale d'Europol ou du Groupe d'alerte « G8-cybercrime ». Il est également le point de contact pour l'ensemble des pays ayant signé la convention sur la cybercriminalité.

612 Il connaît des problématiques liées aux virus informatiques sur les serveurs français, mène des enquêtes sur les espaces numériques, les problèmes liés aux *cloud* et à la récupération des données, analyse des scellés (disques-durs, téléphones et ordinateurs) dans le cadre des enquêtes, problèmes de *phishing* mais aussi trafic d'animaux, stupéfiants, apologie du terrorisme, proxénétisme ou pédo-pornographie. Il y a environ 250 enquêteurs en technologies numériques et 50 cyberinfiltreurs.

613 Les officiers de police judiciaire peuvent agir par voie télématique ou informatique dans le cadre des enquêtes préliminaires (C. pr. pén., art. 77-1-1 et 77-1-2) et de flagrance (C. pr. pén., art. 60-1, art. 60-2), ainsi que sur commission rogatoire (C. pr. pén., art. 99-3 à 99-5).

614 Art. 230-32 à 230-44 du code de procédure pénale.

3 ans d'emprisonnement le refus de donner les clés de chiffrement aux autorités judiciaires[615]. Dans tous les cas, ils impliquent la conservation des données de connexion par les personnes habilitées par la loi[616]. La loi n° 2019-222 du 23 mars 2019 portant réforme de la justice a remplacé les dispositions spéciales relatives à l'infiltration numérique pour faire de **l'enquête sur pseudonyme sur internet une procédure de droit commun** désormais prévue à l'article 230-46 du code de procédure pénale et dont le champ d'application n'est plus défini au regard de la nature de l'infraction mais uniquement au regard de la peine encourue. En revanche, seuls des agents spécialement habilités peuvent les réaliser, sous le contrôle du Procureur de la République ou du juge d'instruction. C'est important car l'enquête sous pseudonyme peut être particulièrement utile sur les réseaux sociaux.

-- La spécialisation des services judiciaires

La justice s'est aussi organisée pour faire face à ces nouveaux contentieux. Au tribunal judiciaire de Paris, une **section spécialisée dans la lutte contre la cybercriminalité**, qui existe depuis 2014, dispose d'une compétence exclusive pour des infractions spécifiques[617]. Le **pôle national de la haine en ligne**, crée par la loi Avia[618], dispose d'une compétence nationale, **concurrente**[619] à celle résultant du droit commun pour certaines infractions limitativement énumérées[620]. En 2021, la plateforme Pharos lui a transmis 102 signalements. Les principales difficultés sont liées à l'obtention, sur réquisition, de l'historique des échanges (contenus). Souvent, le parquet saisit le tribunal selon la procédure accélérée prévue par la

615 La loi pour la sécurité quotidienne du 15 novembre 2001 a inséré, dans le code de procédure pénale, un titre IV relatif au déchiffrement des données cryptées et l'art. 434-15-2 du code pénal. Cet article a été jugé conforme par le Conseil Constitutionnel dans une décision QPC n° 2018-696 du 30 mars 2018.

616 Afin de permettre la réalisation de ces opérations, a été créée par la loi du 3 juin 2016, la plateforme nationale des interceptions judiciaires, et en 2017 l'agence nationale des techniques d'enquête numériques judiciaires a été chargée de la mettre en œuvre.

617 D'une part, pour les faits de cybercriminalité très sensibles tels que ceux visant des systèmes informatiques étatiques, institutionnels ou des opérateurs nécessaires au bon fonctionnement de l'État (ex. Énergie), d'autre part, les affaires pour lesquelles les victimes de phénomènes massifs et sériels (ex. rançongiciels) se trouvent sur l'ensemble du territoire national et enfin, lorsque les informations sont transmises par des autorités policières ou judiciaires étrangères (V. A. CHÉRIF, D. 2019. 1536).

618 Art. 15-3-3 du code de procédure pénale, décret n° 2020-1444 du 24 novembre 2020 désignant le tribunal judiciaire de Paris et circulaire en date du 24 novembre 2020 du ministre de la Justice (NOR : JUSD2032620C).

619 Les critères de saisine du parquet de Paris, sous réserve de son appréciation pour chaque procédure, sont la complexité de la procédure, résultant de la technicité de l'enquête, de vérifications internationales, de la multiplicité d'auteurs et notamment lorsqu'ils sont localisés en de multiples points du territoire et le fort trouble à l'ordre public engendré par les faits, notamment en cas de retentissement médiatique important, ou la sensibilité particulière de l'affaire au regard de la personnalité de la victime ou de celle de l'auteur ou du contexte des faits.

620 Lorsque les propos diffusés sur internet visibles depuis n'importe quel point du territoire national seront susceptibles de constituer les infractions de provocation directe non suivie d'effet à la commission d'un crime ou d'un délit (L. 29 juill. 188 art. 24 alinéas 1 et 2), les délits de provocation publique à la discrimination, à la haine ou à la violence (art. 24 alinéas 7 et 8) et d'injure publique (art. 29 alinéa 2, 33 alinéas 2 et 3), de diffamation publique à raison de l'appartenance ou de la non-appartenance, réelle ou supposée, à une ethnie, une nation, une prétendue race ou une religion déterminée ou à raison du sexe, de l'orientation sexuelle ou identité de genre ou du handicap ou le harcèlement moral dès lors que les messages sont publics et comportent des éléments permettant de retenir une circonstance aggravante des art. 132-76 et 132-77 du code pénal (art. 29 alinéa 1 et 32 alinéas 2 et 3)

LCEN pour faire retirer un contenu[621]. Un des sujets majeurs est actuellement celui de l'absence quasi-totale de possibilité d'agir lorsque les contenus sont diffusés sur des messageries, notamment les messageries cryptées, ainsi que sur des petites plateformes, vers lesquelles risquent de se reporter des comportements criminels qui, actuellement, prospèrent sur les grandes plateformes.

• *La coopération des plateformes pour lutter contre les contenus terroristes*

Pour lutter contre les contenus terroristes, les plus grandes plateformes ont mis en place le **Global Internet Forum to Counter Terrorism (GIFCT**) auquel participent plusieurs gouvernements[622] afin de partager les informations les plus importantes et les moyens de lutte contre les comptes terroristes notamment en analysant leur ramification. Concrètement il s'agit d'une base de données à laquelle ont accès les États et certaines entreprises privées. Après l'attentat de Christchurch, le groupe a renforcé son indépendance et mis en place un protocole partagé de gestion de crise commun aux États et aux entreprises mis en place en lien avec les travaux menés par Europol et la Commission européenne afin de répondre le plus efficacement et le plus rapidement possible en cas d'attaque terroriste et/ou de propagation virale de contenus terroristes en ligne[623]. Cette approche est efficace mais ne permet pas de lutter contre la propagation des contenus illicites auprès des réseaux de taille moyenne ou petite ainsi que sur les messageries, notamment cryptées.

Par ailleurs, l'article 14.5 du **règlement TCO** dispose que les hébergeurs doivent informer immédiatement les autorités chargées des enquêtes et des poursuites pénales dès qu'ils prennent connaissance d'un contenu à caractère terroriste présentant une menace imminente pour la vie. Europol doit aussi être informé. L'article 6 du règlement oblige aussi les hébergeurs à conserver pendant six mois les contenus à caractère terroriste retirés ou auxquels l'accès a été bloqué, ainsi que les données connexes afin de permettre leur utilisation dans le cadre des procédures de réexamen administratif, de contrôle judiciaire ou de traitement des réclamations, et aux fins de prévention et de détection d'infractions terroristes. La durée de conservation de six mois peut être prolongée, à la demande de l'autorité ou de la juridiction compétente, « *en cas de nécessité et aussi longtemps que nécessaire, aux fins de procédures de réexamen administratif ou de contrôle juridictionnel en cours* ».

-- Les obligations de coopération des plateformes dans la lutte contre les fausses informations et les contenus haineux

Concernant la lutte contre les contenus haineux, l'article 6-4 de la LCEN impose notamment aux opérateurs de **coopérer** avec les autorités publiques, en mettant en place des moyens humains et technologiques proportionnés et en désignant en leur sein un interlocuteur (un « point de contact ») pour ces mêmes autorités. Ces dispositions ont vocation à être remplacées à compter du 31 décembre 2023 par le DSA.

621 Site internet du TJ précité, onglet "parquet", "communiqués de presse", TJ Paris 25 janvier 2022, Numéro JurisData : 2022-000919 et 2022-000832

622 Notamment les États Unis, France, Royaume-Uni, Canada, Japon, Ghana.

623 Ministère de l'Europe et des affaires étrangères, site internet, « L'Appel de Christchurch, quelles avancées ? (12 mai 2021) ».

Contre la diffusion de fausses informations, outre l'adoption de dispositions contraignantes applicables durant les périodes électorales, la loi du 22 décembre 2018 relative à la lutte contre la manipulation de l'information a mis à la charge des opérateurs de plateformes des obligations (dont l'articulation avec le DSA est discutable). Il s'agit, pour les plateformes en ligne dépassant un certain seuil de connexion, d'imposer un **devoir de coopération** qui oblige les plateformes à mettre en œuvre un dispositif de **signalement** ainsi que des mesures complémentaires (lutte contre les comptes qui propagent massivement des fausses informations, transparence des algorithmes d'information des utilisateurs sur les contenus sponsorisés d'information se rattachant à un débat d'intérêt général et d'éducation aux médias). Suivant cette mesure, Facebook a ajouté une catégorie « fausse information », et Youtube une catégorie « contenu trompeur » aux motifs de signalement proposés à l'utilisateur sur son interface. Le CSA, désormais ARCOM, est chargé de sa mise en œuvre[624]. Dans sa recommandation n° 2019-03 du 15 mai 2019, il a fixé des **lignes directrices** pour la mise en œuvre de ces dispositifs. Le rapport de synthèse de 2020 souligne la qualité des échanges avec les plateformes mais regrette l'insuffisance d'informations fournies sur les moyens humains et financiers déployés pour lutter contre la manipulation de l'information et sur l'intelligibilité des algorithmes.

S'agissant de la promotion des contenus fiables, certains opérateurs pourraient accepter de faire remonter de façon algorithmique ces derniers ou de dégrader la visibilité des contenus non fiables. Le recours aux partenariats avec les ***fact checkeurs*** est promu et l'ARCOM encourage la démarche de **labellisation** des entreprises et agences de presse et des services de communication audiovisuelle.

Les instruments pédagogiques, éducatifs ou incitatifs

Pour lutter contre les effets indésirables des réseaux sociaux ou promouvoir des utilisations vertueuses, une multitude d'actions, de différentes natures, peuvent être mobilisées. Il est indispensable d'apprendre à se servir de l'outil pour mieux en maitriser les fonctionnalités, il faut aussi sensibiliser les plus jeunes à la nécessité de se comporter sur les réseaux comme dans la « vraie vie ». Enfin, l'éducation aux médias est nécessaire pour permettre aux internautes, confrontés à un océan d'informations, de sélectionner les plus pertinentes et d'aiguiser leur sens critique. Démontrant la défiance envers la science et la confiance accordée aux propos des stars ou influenceurs, une étude récente a montré que les *tweets* des célébrités sont particulièrement efficaces pour informer leurs *followers* sur les vaccins contre la Covid-19 et que, paradoxalement, leurs messages portent moins quand elles citent des sources scientifiques[625].

- *Les actions pédagogiques et de sensibilisation*

Maîtriser l'outil numérique, et plus particulièrement les réseaux sociaux, s'apprend. Le ministère de l'éducation nationale, pour faciliter l'apprentissage du numérique, a développé de nombreux outils et, notamment depuis 2016, **Pix** (qui est un service public développé en logiciel libre pour "évaluer, développer et certifier

624 CSA, rapport *Lutte contre la diffusion des fausses informations sur les plateformes en ligne*, 2020.
625 *Le Monde*, site internet, 26 janvier 2022, « Novak Djokovic, Twitter et les antivax ».

ses compétences numériques" tout au long de la vie). Structure à but non lucratif constituée en groupement d'intérêt public[626], elle a pour mission d'accompagner **l'élévation du niveau général de compétences numériques**. Des cours en ligne sont proposés mais les méthodologies utilisées (défis, mises en situation, jeu, etc.) permettent à la personne de participer à la construction de son apprentissage afin d'acquérir une véritable culture numérique. Des tests de certification des compétences dans 5 grandes thématiques[627] sont proposés. La certification du niveau acquis au sein d'un centre agréé en France est valable trois ans, reconnue par l'État et le monde professionnel. Elle sert de nouvelle certification des compétences numériques de tous les élèves et étudiants de France depuis septembre 2019.

Outre cet apprentissage technique, la puissance publique a mis en œuvre des mesures pour sensibiliser chacun à l'importance de se comporter avec civisme sur les réseaux sociaux et apprendre à choisir, comprendre et critiquer les contenus proposés.

La **CNIL** a réalisé un **kit pédagogique du citoyen numérique** qui regroupe l'ensemble des ressources conçues pour l'éducation d'un citoyen numérique, à destination des adultes et des formateurs. Accessible également sur les sites de l'ARCOM et du Défenseur des droits, il offre de nombreuses ressources pédagogiques pour expliquer les enjeux du numérique à toute personne et aider les formateurs et les parents dans leur rôle. La CNIL anime également le collectif EDUCNUM qui regroupe différents acteurs (70) du monde de l'éducation, de la recherche, de l'économie numérique, de la société civile, de fondations d'entreprise et d'autres institutions pour promouvoir la culture numérique à travers de nombreuses actions pédagogiques[628].

L'éducation nationale s'est aussi fortement mobilisée sur les questions de numérique depuis plusieurs années[629] et a mis en œuvre différentes actions à destination des enseignants et des élèves permettant de répondre plus précisément aux difficultés liées à l'usage des réseaux sociaux. L'enjeu est d'apprendre aux élèves « **à communiquer par le biais des réseaux sociaux dans le respect de soi et des autres** »[630] et «*faire prendre conscience des enjeux civiques de l'usage du numérique et des réseaux sociaux* **»**[631]. La plupart des dispositifs sont coordonnés par le **Centre de liaison de l'enseignement et des médias d'information** (**CLEMI**) qui est chargé de l'éducation aux médias dans l'ensemble du système éducatif car l'éducation aux réseaux sociaux s'inscrit plus largement dans la politique ministérielle **d'éducation**

626 Selon l'arrêté du 27 avril 2017 portant approbation de la convention constitutive de PIX, le GIP est constitué par l'État (Ministère chargé de l'éducation nationale et par le ministère de l'enseignement supérieur), le centre national d'enseignement à distance (CNED) et l'Université de Strasbourg (Université ouverte des humanités).

627 Information et données, communication et collaboration, création de contenu, protection et sécurité, environnement numérique.

628 https ://www.educnum.fr/

629 Ministère de l'éducation nationale et de la jeunesse, site internet, « L'utilisation du numérique à l'école ».

630 Extrait du Socle commun de connaissances, de compétences et de culture, domaine 2.

631 B.O. n° 31 du 30 juillet 2020.

aux médias et à l'information (EMI) qui est affichée comme priorité[632]. Le ministère entend "*permettre aux élèves d'exercer leur citoyenneté dans une société de l'information et de la communication, de former des citoyens éclairés et responsables, capables de s'informer de manière autonome en exerçant leur esprit critique*". Le CLEMI élabore un **guide de référence** de l'utilisation des réseaux sociaux en classe, en collaboration avec la Délégation académique au numérique. Il doit permettre aux enseignants d'utiliser les réseaux sociaux avec leurs élèves en classe de façon sécurisée et fiable. Il s'efforce d'apporter des solutions concrètes aux enseignants qui souhaitent appuyer le projet pédagogique sur les réseaux sociaux, tout en rappelant les précautions nécessaires pour respecter les règles de droit (liberté d'expression, droit à l'image et de diffusion de contenus, données à caractère personnel). Les académies se sont aussi saisies de la difficulté[633].

De nombreuses initiatives, parfois appuyées et financées par les pouvoirs publics, sont aussi le fruit de la société civile ou des plateformes. C'est par exemple le cas de l'école TUMO, soutenue par la mairie de Paris, qui propose des formations numériques entièrement gratuites, notamment en programmation, à un public entre 12 et 18 ans. La *Facebook data valuation tool (FDVT)* est un outil développé par des chercheurs de l'université de Madrid depuis 2016, dans le cadre du du projet européen TYPES (Towards transparencY and Privacy in the onlinE advertising business), du programme Horizon 2020. L'objectif de FDVT est de développer un outil qui informe en temps réel les utilisateurs de la valeur économique de leurs données personnelles qui est générée puis captée par Facebook.

- *Les actions d'information, de responsabilisation, d'incitation*

Les pouvoirs publics multiplient les actions d'information et d'incitation, selon la théorie du *nudge* (du « coup de pouce » en français) pour aider les internautes à maîtriser les outils numériques. La **certification** par la CNIL ou le CEPD (comité européen de protection des données), qui permet d'attester du niveau de conformité d'un organisme aux règles relatives à la protection des données, est un outil efficace d'information et de valorisation auprès des tiers. Réalisée selon des référentiels établis par la CNIL ou le CEPD, la certification peut porter sur un produit, un service, un processus ou un système de données. Elle est réalisée par un tiers certificateur agréé.

Par ailleurs, le **cyber-score** a été mis en place par la loi n° 2022-309 du 3 mars 2022 et devra être affiché par les entreprises à partir du 1er octobre 2023, notamment les réseaux sociaux. Il s'agit d'un dispositif d'audit de sécurité réalisé par un prestataire qualifié par l'ANSSI et la saisine de la CNIL permettra d'intégrer les facteurs de conformité à la loi informatique et libertés. La méthodologie du dispositif sera précisée par un arrêté des ministres chargés du numérique et de la consommation après avis de la CNIL. Il clarifiera les critères d'évaluation de l'audit, ses conditions de validité et ses modalités de présentation.

632 Circulaire du 24 janvier 2022, NOR : MENE2202370C sur la généralisation de l'éducation aux médias et à l'information Bulletin officiel n° 4 du 27 janvier 2022

633 L'académie de Paris a distribué un guide d'utilisation des réseaux sociaux.

Ce tour d'horizon non exhaustif des instruments existants démontre la richesse et la complexité d'un secteur qui mobilise des actions de la puissance publique très diverses. D'ailleurs, le droit applicable comme les autorités de régulation compétentes sont également multiples et un des principaux défis pour les prochaines années est celui de leur coordination.

2.4.3. Le défi des inter-régulations organiques et matérielles

Face à la multiplicité des problématiques posées par les plateformes et à l'enchevêtrement des normes qui s'appliquent à elles, les enjeux d'articulation et d'inter-régulation sont d'une importance cruciale. Si les règlements européens *Platform to business*, *DSA* et *DMA* ont désormais vocation à constituer le droit commun des services en ligne et du marché des plateformes, il reste encore à les rendre compatibles avec les autres réglementations en vigueur et, surtout, à mettre en œuvre ces nouveaux outils de manière efficace et volontariste.

L'enchevêtrement des régimes juridiques

L'approche sectorielle des régulations des plateformes et plus largement des services de communication électronique pose certaines difficultés notamment car les plateformes sont des « caméléons » ou mieux des « chauves-souris » comme dans la fable de La Fontaine (des réseaux sociaux sont aussi des « *market places* », des messageries privées proposent aussi des fonctionnalités de réseaux sociaux, des plateformes de géolocalisation comportent des lieux de discussion, etc.), de sorte que les frontières posées par les réglementations compliquent souvent leur mise en œuvre. A cet égard, **l'approche fonctionnelle** choisie par la plupart des textes européens semble appropriée : ce n'est pas tant à un opérateur ou à une plateforme prise dans son ensemble qu'au **service en cause** que la norme s'adresse. Pour déterminer le régime juridique sectoriel applicable, la question sera alors de savoir si le service en question est une activité principale ou accessoire de la plateforme (ce qui ne sera pas toujours simple il est vrai). C'est ce que propose le DSA pour déterminer l'application ou non du règlement à un service de diffusion d'information.

En outre, les **droits interagissent et sont perméables**. Comme il a été dit dans la première partie, une clause de CGU pourra être déclarée abusive au motif qu'elle méconnaît le RGPD, de même qu'un opérateur pourra être considéré comme abusant de sa position dominante en raison de l'ampleur des données personnelles qu'il collecte. En effet, la question des données personnelles est souvent liée à celle de la concurrence : la captation des usagers et la possession de données donnent de puissants avantages concurrentiels (comme en témoigne l'affaire du rachat de WhatsApp). La question préjudicielle posée dans l'affaire *Meta Platforms* (C-252/21) actuellement pendante devant la Cour de justice de l'Union européenne devrait permettre de préciser les conditions dans lesquelles les autorités nationales de la concurrence peuvent s'appuyer sur le droit des données personnelles ou le

prendre en compte pour caractériser des manquements au droit de la concurrence. En sens inverse – et bien plus exceptionnellement –, le droit de la protection des données peut donner un avantage concurrentiel aux opérateurs de réseaux sociaux par rapport à d'autres acteurs du numérique[634], posant la question de savoir s'il ne faut pas injecter une dose d'asymétrie dans cette réglementation exigeante.

La nécessaire inter-régulation

Si des instances existent au niveau européen pour coordonner les différents acteurs nationaux dans un secteur déterminé comme l'ORECE (ou BEREC) s'agissant des télécommunications, le CEPD s'agissant des données personnelles et le REC s'agissant de la concurrence, ce qui est d'autant plus opportun que les questions apparaissent inter-sectorielles, **il existe un besoin accru de coordination matérielle s'agissant de certains sujets transversaux**. Quelques dispositifs de convergence inter-sectorielle, plus ou moins structurés, ont été timidement créés ces dernières années, la plupart des rapprochements se faisant de façon informelle et bilatérale.

Le 2 mars 2020, **le pôle numérique ARCEP-ARCOM**, qui a pour objectif d'approfondir les analyses techniques, économiques et environnementales des marchés du numérique et d'accompagner les deux régulateurs dans la mise en place de leurs nouvelles missions dans le domaine du numérique, a vu le jour. Il vise également à mettre à disposition du grand public des données de référence communes sur ces sujets. Le **référentiel des usages numériques** contribue à la réalisation de ces objectifs. En agrégeant des données issues de différentes sources établies, il fournit des éléments chiffrés et centralisés sur les déploiements des réseaux fixes, la couverture des réseaux mobiles, l'accès à internet, l'équipement des foyers, les usages internet et audiovisuel. Pour sa deuxième édition, le référentiel intègre de nouvelles thématiques, telles que la prise en compte des enjeux environnementaux du numérique au travers de l'équipement en smartphones, ou encore l'utilisation des outils de contrôle parental sur internet.

Des coopérations informelles peuvent aussi avoir lieu. L'Autorité de la concurrence française a récemment pris en compte la question de la protection des données personnelles dans son analyse concurrentielle et a pu bénéficier du soutien de la CNIL pour expertiser la question[635]. Il reste que les deux approches peuvent entrer en tension et, dans certains cas, les règles de protection de données peuvent entrainer des distorsions de concurrence[636]. Ainsi lorsque Google met en œuvre la « *Privacy Sandbox* » qui vise à supprimer tous les *cookies* tiers au nom de la

634 Comme le soulignait le rapport précité d'Anne Perrot, Mathias Emmerich, Quentin Jagorel, Publicité en ligne : pour un marché à armes égales, novembre 2020) l'exigence de consentement en matière de cookies, peut aboutir soit à des « cookies walls » limitant l'audience des sites soit à une perte de valeur économique liée au refus des cookies, peut favoriser les réseaux sociaux qui peuvent recueillir des données sur leurs utilisateurs sans recourir aux cookies, dans le cadre d'un « environnement logué ».

635 Apple ATT : *Décision 21-D-07* du 17 mars 2021 relative à une demande de mesures conservatoires présentée par les associations Interactive Advertising Bureau France, Mobile Marketing Association France, Union Des Entreprises de Conseil et Achat Media, et Syndicat des Régies Internet dans le secteur de la publicité sur applications mobiles sur iOS.

636 Par ex., les politiques de minimisation des données peuvent augmenter les coûts d'accès aux données pour des concurrents potentiels. De même, le non partage de données personnelles peut empêcher des entreprises de proposer des produits compétitifs à des clients. V. M. E. Stucke, « The Relationship Between Privacy and Antitrust », *Notre Dame Law Review*, 23 février 2022.

protection des données personnelles : cette approche risque d'avoir une incidence très importante sur le marché de la publicité en ligne pour les annonceurs qui n'auront plus de moyens de savoir si les publicités affichées correspondent au profil de l'utilisateur. Cela a conduit la Commission européenne a ouvrir une enquête sur cette pratique pour en évaluer la conformité avec les règles de la concurrence[637].

Les enjeux d'articulation des normes

En parcourant les vingt dernières années d'activité normative en lien avec les réseaux sociaux et en s'en tenant aux textes majeurs, on ne peut qu'être frappé par le nombre de textes adoptés et par la multiplicité des notions mobilisées, y compris au niveau européen, par chaque règlement ou directive. Mais le maniement articulé de ces textes n'est aisé ni pour les opérateurs ni même pour les juristes. La polysémie de la notion de plateforme, tantôt service de la société d'information, service d'hébergement, prestataire de service intermédiaire, fournisseur de service intermédiaire, opérateur de plateforme en ligne, est à cet égard exemplaire[638]. Certes il n'est pas toujours aisé de s'accorder sur les notions, surtout lorsque la réalité des pratiques est complexe et multiforme, comme on l'a vu, et que les normes répondent à des finalités différentes. Les plateformes sont protéiformes, interviennent dans des domaines parfois très différents, mettent en relation des structures et des individus qui, eux-mêmes peuvent interagir pour des finalités variées et dans des cadres différents. Mais s'il est difficile de trouver une notion qui embrasse toutes les spécificités, il n'est pas souhaitable de continuer à édicter des normes sans les articuler entre elles, la formule « *sans préjudice de* » souvent retenue n'étant bien souvent qu'un paravent commode, le juge devant, in fine, trouver la bonne articulation entre ces réglementations à l'occasion des affaires dont il est saisi.

2.4.4. L'office du juge

Le rôle du juge dans la régulation des réseaux sociaux est à la fois déterminant et nécessairement circonscrit en ce sens qu'il ne peut intervenir qu'*in fine* et pour les cas dont il est finalement saisi, ce qui n'est évidemment pas propre aux réseaux sociaux mais qui doit être rapporté à la masse considérable de l'activité de ces réseaux et à leurs rôles multiples. Il reste que c'est le juge, dans son rôle d'application du droit aux faits, qui précise les frontières à ne pas dépasser[639], tranche les questions juridiques les plus complexes, qui ne trouvent pas de réponse évidente dans les normes, interprète à la lumière de l'évolution de la technique et des enjeux

637 Commission, AT.40670 Google - Adtech and Data-related practices.

638 J. Rochfeld, C. Zolynski, *La loyauté de plateformes. Quelles Plateformes ? Quelle loyauté ?*, Dalloz IP/IT 2016, 520 ; Chronique droit européen du numérique, « La rationalisation des catégories juridiques relatives aux services numériques », *RTD Europ*, 2021 p. 188 ; F. Sabrini, « La notion de plateforme au cœur des nouvelles relations entre professionnels, regards croisés entre deux réglementations : P2B vs Loi pour une République numérique », *RDT Com*, 2020, p. 215.

639 La CJUE a exclu à une reprise la mise en œuvre d'une obligation de filtrage généralisée et préventive par un intermédiaire technique (CJUE, 24 novembre 2011, *Scarlet c/ SABAM*, aff. C-70/10 ; CJUE, 16 février 2012, aff. C-360/10). Elle a en revanche déjà considéré dans un cas que des injonctions visant à prévenir la réapparition d'un contenu illicite déjà signalé étaient compatibles avec le droit de l'Union (E. Glawischnig-Piesczek, CJUE, 3 octobre 2019, aff. C-18/18).

les concepts fondateurs et ancestraux du droit[640]. Son rôle demeure néanmoins circonscrit : la régulation des réseaux sociaux est et sera, avec la mise en œuvre du DMA et du DSA, en très grande partie ce qu'en feront les régulateurs (européens et nationaux), le juge ne pouvant intervenir *in fine* qu'en cas de contestation et sur la base des partis qui auront été pris ou pas par le régulateur. Les amendes records prononcées par les autorités de régulation comme la Commission européenne sont maintenant plus nombreuses[641] et beaucoup ne sont pas contestées devant le juge.

Compte tenu de la sphère d'influence des réseaux sociaux, de multiples juridictions sont potentiellement concernées[642], ce qui ne facilite pas la tâche du requérant. Or, les décisions de jurisprudence sont essentielles, comme en témoignent celles rendues au sujet du transfert des données personnelles[643] ou de la portée du consentement en droit des données personnelles[644]. Parfois, seul le juge est en mesure de préciser le cadre juridique applicable au litige : ainsi dès lors qu'un internaute modère des messages ou exclut certains personnes de son blog, il peut être appréhendé comme un éditeur de contenu et se voir reconnaître responsable de propos tenus par un autre participant au forum[645].

Le **contrôle des abus d'expression** a toujours été le domaine par excellence du juge car cette matière nécessite toujours *in fine* une approche casuistique[646]. Si le DSA instaure un contrôle *ex ante* de l'activité de modération des plateformes dans une approche systémique, il n'a pas évidemment entendu modifier la place du juge à cet égard qui conserve une **compétence exclusive dans la qualification finale des contenus**. Il est d'ailleurs le seul à même d'apprécier les propos dans le contexte culturel et juridique dans lequel ils ont été tenus. Il reviendra donc au juge, en France le juge judiciaire compétent, de vérifier l'illicéité du contenu (les éléments constitutifs de l'infraction sont réunis) et l'adéquation de la réponse apportée par l'opérateur. Le contrôle de la pertinence de la décision de retrait ou de blocage par l'autorité administrative (OCLCTIC) en dehors des dispositions spécifiques mentionnées dans le règlement TCO au sujet des contenus terroristes, relèvera, lui, du juge administratif. Concernant les contenus illicites qui n'auraient

640 V. les jurisprudences appliquant la loi de 1881 aux propos tenus sur les réseaux sociaux (Première partie).

641 Par ex., décision du 20 mars 2019 dans laquelle la Commission a sanctionné Google d'une troisième amende de 1,49 milliards d'euros pour abus de position dominante. La Commission reproche à Google d'avoir cherché à étouffer la concurrence d'AdSense for Search, son système de publicité contextuelle. La Commission accuse Google d'avoir limité artificiellement la possibilité, pour les utilisateurs d'AdSense for search, d'utiliser des services d'affichage de publicités contextuelles concurrents de Google.

642 Le juge constitutionnel pour fixer les points d'équilibre lorsque plusieurs libertés et droits constitutionnellement garantis entrent en confrontation, le juge civil pour vérifier notamment le caractère abusif des clauses dans les conditions générales d'utilisation, le juge pénal pour caractériser l'infraction de diffamation ou condamner l'harceleur, le juge prud'hommal pour juger du caractère abusif du licenciement prononcé pour des propos tenus sur les réseaux sociaux, le juge administratif pour apprécier la méconnaissance de l'obligation de réserve du fonctionnaire ou le retrait administratif abusif d'un contenu, sans oublier les juge européens qui s'assurent de la cohérence de l'application du droit européen par les juges des États membres ou les États parties de la Convention européenne des droits de l'homme.

643 CJUE, gr. ch., 6 octobre 2015, *Schrems*, aff. C-362/14 ; CJUE, gr. ch., 16 juillet 2020, *Data Protection Commissionner c/ Facebook et Schrems*, aff. C-311/18).

644 CE, 19 juin 2020, *Sté Google LLC*, n° 430810, Rec.

645 CEDH, 16 juin 2015, *Delfi c/ Estonie*, n° 64569/09, Légicom 2016, n° 57, p. 35, note N. Verly.

646 La même approche est prônée s'agissant du contrôle des mécanismes de modération. CEDH, 2 février 2016, *Magyar Tartalomszolgáltatók Egyesülete et Index.hu Zrt c/ Hongrie*, n° 22947/13.

pas été supprimés, le juge judiciaire pourra être saisi soit d'une demande fondée sur la LCEN de retrait de contenu soit d'une demande de condamnation d'une plateforme qui n'aurait pas retiré un contenu malgré le signalement effectué par un utilisateur ou le Procureur de la République. *In fine*, c'est donc bien au juge d'apprécier au cas par cas la licéité du contenu.

Ce rôle indispensable du juge a été mis en avant notamment par le rapport de la CNCDH sur la haine en ligne qui réclame également des moyens supplémentaires pour renforcer les capacités des juridictions judiciaires[647]. Ce rapport, comme celui élaboré par la commission Bronner[648], propose cependant, pour ne pas laisser les plateformes opérer seules leur modération et parce que le contrôle du juge sur les contenus intervient souvent trop tard (même si la loi du 24 août 2021 a prévu le recours à la comparution immédiate utilisée pour certaines infractions de la loi de 1881), la mise en place d'une **instance d'expertise indépendante chargée de donner un avis aux plateformes sur la qualification du contenu sans préjudice d'un recours au juge**. Cette proposition, qui comporte des risques (notamment celui d'allonger inutilement les délais de traitement des signalements, les plateformes pouvant avoir tendance à saisir systématiquement cette instance) pourrait être mise en œuvre dans le cadre du DSA, qui prévoit la possibilité pour les États membres d'instaurer un règlement extra-judiciaire des litiges afin de résoudre les litiges liés aux décisions de modération des plateformes. Une réflexion pourrait être conduite sur ce point avec la personne qualifiée par l'ARCOM, chargée de vérifier la licéité des décisions de retrait et de blocage des contenus, l'association pointdecontact.fr et les autorités compétentes (ARCOM, juge judiciaire). Il faudrait également vérifier l'articulation d'un tel dispositif avec les outils qui seront mis en place en application du DSA (*cf. infra*).

2.4.5. Les leviers controversés ou à approfondir

La prise de conscience des dangers qui émanent des réseaux sociaux ou sont amplifiés par eux a entrainé une multiplication des propositions de régulation ces dernières années qu'il convient d'analyser, notamment au regard de leur faisabilité juridique et technique[649]. Toutes répondent à des objectifs légitimes mais certaines semblent, à ce stade, prématurées, inabouties ou inadéquates. Une réévaluation fréquente de leur pertinence pourrait cependant opportunément être réalisée.

Les leviers controversés

- *Interdire l'utilisation de pseudonymes sur les réseaux sociaux ?*

Face à la multiplication des discours de haine en ligne, du cyber-harcèlement voire d'encouragement au terrorisme, de nombreuses voix réclament l'interdiction de l'utilisation de pseudonymes pour s'exprimer sur les réseaux sociaux et l'obligation corrélative de s'exprimer avec sa véritable identité civile. Il est vrai que la possibilité de se cacher derrière un pseudonyme peut engendrer un sentiment d'impunité qui

647 CNCDH, *Avis sur la lutte contre la haine en ligne*, 8 juillet 2021.
648 *Les lumières à l'ère numérique*, janvier 2022.
649 S. Abiteboul, J. Cattan, *op. cit.*

conduit certains à s'affranchir de règles habituelles de vie en société, à commencer par le respect d'autrui. L'usage des pseudonymes rend par ailleurs l'action de la justice pénale plus complexe et donc plus lente lorsqu'il s'agit de poursuivre les auteurs d'infractions sur les réseaux sociaux.

Pourtant cette option, même si elle peut être séduisante à première vue, se révèle, à l'examen, très discutable. La possibilité de s'exprimer sous un autre nom que le sien, qui a toujours été admise dans la vie réelle, est, comme l'a d'ailleurs rappelé par exemple la CNIL, « *une condition essentielle du fonctionnement des sociétés démocratiques* » qui permet « *l'exercice de plusieurs libertés fondamentales essentielles, en particulier la liberté d'information et le droit à la vie privée* ». Elle peut faciliter la prise de parole de personnes qui craignent la discrimination ou souhaitent contester les positions acquises. En outre, cette forme d'anonymat n'est que relative. Il est en effet relativement facile, en cas de nécessité, d'identifier une personne compte tenu des nombreuses traces numériques qu'elle laisse (adresse IP, données de géolocalisation, etc.). La LCEN prévoit l'obligation de fournir à la justice les adresses IP authentifiantes des auteurs de message haineux et plusieurs dispositifs normatifs, dont la directive dite « Police-Justice », obligent les opérateurs à conserver de telles données : en pratique, les opérateurs répondent généralement sans difficulté aux réquisitions judiciaires pour communiquer l'adresse IP. Les obstacles rencontrés existent mais apparaissent finalement assez limités : la possibilité de s'exprimer sur internet sans laisser aucune trace paraît donc à ce jour réservée aux « *geeks* » les plus aguerris[650].

L'idée selon laquelle la haine serait plus facilement proférée sous le couvert d'un pseudonyme n'est pas non plus clairement étayée par les faits et les études sur ce point font plutôt défaut[651]. Surtout, « *être incapable d'identifier immédiatement ses interlocuteurs est une situation parfaitement banale, aussi bien en ligne que hors ligne. (…) Le chauffard qui refuse une priorité laisse bien apparaître un identifiant unique sur sa plaque minéralogique, mais un particulier ne pourra le relier à une personne dénommée. Ainsi, le processus visant à identifier un individu contre son gré nécessite toujours un effort (…)* »[652]. Plus encore, la mise en œuvre de l'interdiction du « pseudonymat » engendrerait de nombreux risques tout aussi problématiques pour la société. Obliger à afficher en toute circonstance son identité, c'est garantir la possibilité pour tous de savoir mille choses sur un individu, y compris ses données les plus sensibles (convictions religieuses, politiques, orientation sexuelle) en tapant simplement son nom dans le moteur de recherche. Pour toutes ces raisons, la suppression de l'anonymat, qui n'a été adoptée par aucune démocratie occidentale et n'est pas envisagée au sein de l'Union européenne, ne paraît pas constituer une solution raisonnable conforme à notre cadre juridique le plus fondamental.

650 Le ministère de l'intérieur a constaté une augmentation des outils d'anonymisation depuis 2013, avec un nombre moyen d'utilisateurs directs quotidiens de TOR en France ayant doublé en quelques années, passant de 50 000 à près de 100 000 en 2017 (Ministère de l'intérieur, *État de la menace liée au numérique*, mai 2019).

651 Par ex., les menaces de morts qui avaient précédé l'assassinat de Samuel Paty avaient été proférées sous la réelle identité des auteurs, comme dans l'affaire Mila, celle de la Ligue du LOL ou encore l'affaire des *tweets* antisémites à l'encontre de April Benayoun.

652 *Les Echos*, site internet, 12 février 2019, « Point de vue - Contre la levée de l'anonymat en ligne ».

• *Interdire les réseaux sociaux aux enfants ?*

En France les enfants ne peuvent consentir seuls à l'exploitation de leurs données personnelles qu'à partir de l'âge de 15 ans. Ils peuvent consentir seuls aux CGU s'il s'agit d'un contrat d'usage et que l'âge fixé par la plateforme est respecté. En pratique, de nombreux parents ouvrent des comptes à leurs enfants, parfois très jeunes, voire dès leur naissance. La question peut se poser de savoir s'il ne faudrait pas, à l'instar des jeux d'argent en ligne ou de l'alcool, interdire les réseaux sociaux en-dessous d'un certain âge. Certains prônent des restrictions, déjà à l'œuvre dans certains pays comme la Chine[653] (qui limite drastiquement les temps d'écran), pour éviter les risques de dépendance et ne pas exposer les enfants à des contenus inadaptés[654]. Outre les questions très délicates que cela pose en termes de libertés publiques, puisque de telles propositions aboutissent à ce que l'État fixe les règles d'usage des réseaux sociaux à la place des parents, on peut douter de l'efficacité de telles règles qui pourraient être aisément détournées et qui pourraient souligner des difficultés qui ne sont pas uniquement dues aux réseaux sociaux eux-mêmes[655].

• *Démanteler les GAFAM ?*

Le constat de l'hyperpuissance politico-économique des GAFAM fait la quasi-unanimité. Certains experts, y compris américains, préconisent l'adoption de lois anti-trust et le démantèlement des GAFAM pour mettre fin à leur hégémonie. Plusieurs économistes et sociologues français[656] soutiennent cette idée et certains considèrent même que les récents règlements européens vont être contre-productifs s'ils ne s'accompagnent pas du démantèlement de ces géants[657].

Si une prise de conscience de l'effet systémique et dangereux des très grands réseaux sociaux semble voir le jour aux États-Unis (*cf.*, par exemple, la récente nomination de Lina Khan à la tête de l'anti-trust américain[658]), les récents évènements mondiaux et notamment la guerre en Ukraine, qui rebat les cartes des équilibres stratégiques, pourraient avoir changé la donne. Le contexte de forte concurrence avec la Chine, la vive opposition entre les deux grands partis politiques aux États-Unis et l'absence

653 La Chine interdit le *streaming* aux mineurs de moins de 16 ans, limite les jeux en ligne à 3 heures par semaine, et à 40 minutes par jour le temps d'utilisation du tiktok chinois (Douyin), rendu également inaccessible la nuit, aux moins de 14 ans.

654 C'est ce que préconise Gaspard Koenig, fondateur du Think Tank Générations Libres.

655 *Le Monde*, 25 septembre 2021, « Faut-il interdire les réseaux sociaux aux adolescents ? ».

656 Partant du constat que la taille de ces firmes vient concurrencer les États, à l'image de la compagnie des Indes au XIX[e] siècle et que plusieurs évènements comme Cambridge Analytica, les *hacking* des russes durant la campagne présidentielle de 2016 aux États-Unis et l'adoption du RGPD ont révélé la nécessité de changer la gouvernance du numérique, Dominique Boulier propose quatre démantèlements de nature différente : un de nature industrielle visant à séparer les activités des plus grosses entreprises pour mettre fin à leur position dominante, un de nature économique visant notamment à mettre fin à la confusion des rôles dans le domaine de la publicité en autonomisant les régies publicitaires, en mettant en place un moteur de recherche de service public (nationalisation) dépourvu de publicité et à lutter contre leurs pratiques d'optimisation fiscale, un concernant le modèle de captation des traces qui ne doit pas concerner que les données personnelles mais également les métadonnées (données agrégées) en accroissant l'encadrement des algorithmes et en évitant les collectes à visée de profilage et enfin un visant les mécanismes de « réchauffement médiatique » par la mise en place d'une autorité de régulation chargée de la protection de notre écosystème attentionnel et de la mise en œuvre des mesures de ralentissement.

657 *Le Monde*, site internet, 21 avril 2022, « Vouloir limiter les abus des grandes plates-formes numériques sans toucher à la structure des entreprises va faire plus de mal que de bien ».

658 *Le Monde*, site internet, 16 juin 2021, « Lina Khan, une farouche critique des GAFA, nommée à la tête de l'antitrust américain ».

de consensus de l'ensemble des acteurs institutionnels sur ce qu'il conviendrait de démanteler et comment procéder rendent ces projets illusoires. Surtout, et même si les abus de positions dominantes et les concentrations sont dangereux, il ne faut pas sous-estimer les autres difficultés que pourraient entraîner de telles décisions, notamment celle de rompre la coopération avec ces acteurs et de rencontrer des difficultés à réguler un secteur aux mains d'opérateurs dispersés. Enfin, les expériences passées peu concluantes font douter de l'efficacité[659].

A ce stade et sachant qu'un démantèlement ne pourrait, en tout état de cause, être mis en œuvre qu'au niveau de la Commission européenne et que les responsables politiques français et européens privilégient la voie de la régulation et des actions moins agressives visant à rétablir les conditions d'un marché équitable, cela ne paraît donc envisageable, du moins à court ou même moyen terme[660]. Il ne faut cependant pas exclure, dans l'hypothèse où le DSA et le DMA se révéleraient inefficaces, que cette opinion majoritaire ne change. Par ailleurs, on remarque que la piste du démantèlement outre-Atlantique crée une pression positive sur les opérateurs qui, sur certains sujets, nuancent leurs positions ou, à l'inverse, multiplient les dépenses de *lobbying*, preuve d'un sentiment de danger.

Les leviers à approfondir

- *Freiner le rythme des échanges ?*

Face au rythme effréné des échanges sur les réseaux sociaux, qui transforme la tonalité du débat public lui-même, des propositions visant à ralentir le débit des échanges et à les apaiser ont vu le jour. Certains auteurs proposent des solutions radicales, estimant que seules des mesures fortes peuvent lutter contre la forte addiction engendrée par les réseaux sociaux. Au-delà des mesures incitant à la totale déconnexion agissant comme « cure de désintoxication », il a été proposé **d'imposer des ralentissements à la circulation des réactions** sur les réseaux sociaux. Pour organiser « le refroidissement médiatique », Dominique Boulier propose ainsi que les interfaces tiennent compte de seuils au-delà desquels il ne serait plus possible de réagir. Si cette solution n'est pas sans intérêt, sa compatibilité avec la liberté d'expression n'est pas évidente dans la mesure où elle reviendrait à contingenter le nombre de réactions qu'un utilisateur serait autorisé à faire dans un laps de temps donné. Une formule moins radicale consisterait à prévoir un temps de latence avant l'envoi d'une réaction afin de ralentir le rythme des réactions sur les réseaux : l'effet positif à en attendre serait évidemment plus limité mais le risque de contrariété avec la liberté d'expression également.

A ce stade, il semble préférable de promouvoir de simples mesures d'incitation pour pousser les utilisateurs à agir de façon plus réfléchie ou à auto-limiter leurs réactions en proposant des paramétrages ou des fonctionnalités plus adaptées

659 En 1998, le DoJ (Département de la justice américain) et 20 États ont déposé une plainte contre Microsoft, soupçonné d'abuser de sa position monopolistique. En 2000, le tribunal fédéral saisi de l'affaire a ordonné le démantèlement de l'entreprise. Le géant a fait appel et l'arrivée de George W. Bush à la Maison-Blanche en 2001 a favorisé l'adoption d'un accord avec le DoJ. La menace d'un démantèlement des GAFAM est donc bien réelle, mais demeure liée aux contingences de la politique américaine. V. www.vie-publique.fr, parole d'expert, 12 octobre 2021, « Les GAFAM : vers une régulation ou un démantèlement ? ».

660 *Cf.* not. Assemblée nationale, rapport n° 3127, *Les plateformes numériques*, 24 juin 2020.

plutôt que d'imposer un nombre maximal de réactions par heure ou par jour qui semble restreindre significativement la liberté d'expression. La nécessité d'imposer de tels freins pourra cependant être utilement reconsidérée au regard des futures recherches et audits réalisés dans le cadre du DSA qui pourraient révéler des risques systémiques afférents et démontrer l'opportunité d'une telle mesure pour minimiser ces risques.

• *Aller plus loin dans le contrôle des fausses informations ?*

Au vu des risques que comporte la propagation sur internet en général et sur les réseaux sociaux en particulier des rumeurs et des fausses nouvelles, des propositions ont été faites pour améliorer leur prévention et leur répression. Le rapport dirigé par Gérald Bronner propose ainsi la mise en place d'un dispositif complémentaire à l'article 27 de la loi de 1881[661] permettant d'**engager la responsabilité civile du diffuseur de mauvaise foi d'une fausse nouvelle qui porte préjudice à autrui**, ce préjudice devant être apprécié notamment à l'aune de la viralité de la diffusion et de l'influence relative de celui qui diffuse ou relaye la diffusion fautive. Il s'agirait de permettre à la juridiction de prendre en compte l'influence ou la popularité numérique de celui qui a diffusé sciemment la fausse nouvelle pour évaluer le montant des dommages et intérêts. Si la proposition est intéressante sur son principe, on peut s'interroger sur sa réelle portée tant le volume et la rapidité de partage des fausses nouvelles rendent illusoire la perspective d'attraire les diffuseurs devant un juge, sachant qu'il faudra au demeurant établir leur mauvaise foi[662]. La commission Bronner propose également d'imposer aux plateformes une obligation de modération des fausses nouvelles susceptibles de troubler l'ordre public. Si l'on peut comprendre l'objectif recherché, laisser les plateformes définir ce que sont des fausses nouvelles susceptibles de causer un trouble à l'ordre public présente un risque sérieux, d'autant que dire des choses fausses n'est pas interdit en soi ! Par ailleurs, il faut relativiser la portée des fausses informations qui concernent moins de 0,1% des contenus et proviennent presque toujours des mêmes comptes (72% des fausses informations sont relayées par deux communautés politiques)[663].

En réalité, dans le domaine de la lutte contre les fausses nouvelles, tant le contrôle *ex ante* que le contrôle *ex post* semblent délicats à manier. En effet, ne constituant pas par elles-mêmes des contenus illicites et nécessitant un important effort d'interprétation avant de recevoir une telle qualification, toute action visant à renforcer leur contrôle induit un risque d'atteinte à la liberté d'expression. Comme le soutient d'ailleurs le rapport Bronner, les actions pédagogiques et d'accompagnement paraissent en définitive les mieux à même d'aider chacun à faire preuve de clairvoyance et toute action trop intrusive dans le contrôle de la véracité des contenus présente le risque pour l'État d'être soupçonné de mettre en place une police de la pensée.

661 « *La publication, la diffusion ou la reproduction, par quelque moyen que ce soit, de nouvelles fausses, de pièces fabriquées, falsifiées ou mensongèrement attribuées à des tiers lorsque, faite de mauvaise foi, elle aura troublé la paix publique, ou aura été susceptible de la troubler, sera punie d'une amende de 45 000 euros. / Les mêmes faits seront punis de 135 000 euros d'amende, lorsque la publication, la diffusion ou la reproduction faite de mauvaise foi sera de nature à ébranler la discipline ou le moral des armées ou à entraver l'effort de guerre de la Nation.* ».

662 S. Merabet, « Les lumières à l'ère numérique, les aspects juridiques de la Commission Bronner », *JCP,* 14 février 2022, n° 6.

663 D. Chavalarias, *Toxic Data,* Flammarion, 2022.

• *Imposer une interopérabilité totale ?*

L**'interopérabilité** est la capacité d'un système informatique à fonctionner avec d'autres systèmes informatiques, sans restriction d'accès, *via* des API (interfaces de programmation) librement utilisables pour véhiculer des métadonnées. Contrairement à la communication humaine qui n'est pas impossible si chacun utilise ses propres expressions et « codes » linguistiques, la communication informatique n'est possible que s'il existe un protocole identique entre l'émetteur et le récepteur c'est-à-dire un unique code[664], par exemple le protocole d'internet « http » permet à des logiciels différents de communiquer. Ce sont donc les protocoles qui permettent l'interopérabilité.

L'interopérabilité recouvre une **diversité de niveaux possibles**. Elle peut se décliner sous des formes minimales, intermédiaires ou maximales :

- le niveau le plus faible est la portabilité des données, pour fluidifier les migrations entre les plateformes qui ne porte que sur les données ;

- le niveau intermédiaire encore appelé compatibilité consiste en l'ouverture technique permettant la communication des machines entre elles mais sans protocole partagé : l'interface exposée peut être spécifique à la plateforme et pose la question de savoir si c'est la plus grande plateforme ou la plus petite qui va ouvrir les connecteurs et se calquer sur l'autre ;

- le niveau le plus fort comporte des standards ou des protocoles qui peuvent être acceptés par tout le monde[665]. Les emails et les communications téléphoniques bénéficient d'une telle interopérabilité. Chacun peut se contacter selon le même protocole technique.

Certains serveurs communiquent selon un nouveau protocole commun et libre appelé *ActivityPub* et sont regroupés sous le terme de *fédiverse*. Des réseaux sociaux comme Mastodon communiquent selon ce protocole et sont donc interopérables. Mais les plus grands réseaux sociaux ont chacun leur protocole. L'obligation d'interopérabilité existe déjà dans de nombreux secteurs mais est toujours délicate dans sa mise en œuvre. Elle a été imposée en matière de téléphonie mobile et, malgré la complexité technique de l'opération et le temps qu'il a fallu aux opérateurs pour y parvenir, elle a été un succès, chaque personne conservant désormais son numéro de téléphone s'il change d'opérateur. Le RGPD impose aux opérateurs la portabilité des données mais celle-ci demeure à ce jour insuffisamment mise en œuvre : elle impose en effet qu'une table de correspondance soit réalisée entre les données afin qu'elles se comprennent mutuellement ce qui est lourd et coûteux. Le DMA imposera l'interopérabilité entre messageries : elle devra être mise en œuvre dans les prochaines années mais concernera davantage le partage d'information à des fins commerciales que la véritable interopérabilité au sens technique du terme[666].

664 La Quadrature du net, site internet, 13 juin 2019, « C'est quoi l'interopérabilité et pourquoi est-ce beau et bien ? ».

665 L'interopérabilité est assurée par une norme technique (= un référentiel établi par un organisme de normalisation officiellement agréé par un État *via* une organisation nationale de standardisation (comme Afnor pour la France), agréé au niveau Européen (comme le CEN ou le ETSI), ou encore issu d'un traité international (comme ISO)).

666 Le DMA définit l'interopérabilité comme « *la capacité d'échanger des informations et d'utiliser*

L'association La Quadrature du Net milite depuis des années en faveur de l'interopérabilité, estimant qu'elle permettrait à l'utilisateur de passer d'un réseau à un autre sans difficulté et ainsi de lutter contre les effets de réseaux et la position dominante de certains acteurs. Plusieurs rapports dont celui de la *Competition Policy for the Digital Area* de 2019[667] ont promu cette interopérabilité pour rendre la concurrence plus équilibrée et loyale. Certains estiment aussi qu'elle permettrait aux internautes de ne plus se trouver captifs de contenus haineux[668].

Plusieurs éléments incitent toutefois à la prudence. Outre qu'il n'est d'abord pas évident que les utilisateurs souhaitent une telle interopérabilité (la migration vers Signal d'une partie des abonnés de WhatsApp en réaction au rachat de ce dernier par Facebook en donne une indication), l'interopérabilité totale parait juridiquement compliquée, chaque réseau ayant ses propres CGU et certaines personnes ayant justement fait le choix d'être sur des réseaux sociaux alternatifs pour ne pas accepter les CGU d'autres réseaux. Par ailleurs, certains modèles économiques sont par nature difficilement compatibles (modèle de l'abonnement par rapport au modèle fondé sur la gratuité) et certains réseaux sociaux alternatifs souhaitent, pour protéger leur modèle, être préservés d'une immixtion des autres réseaux sociaux[669]. Un tel dispositif pourrait également avoir l'effet paradoxal de renforcer les positions dominantes des réseaux sociaux en leur fournissant davantage de graphes sociaux. La multiplication des responsables de traitements et la dissémination des données personnelles des utilisateurs pourraient également accroître les risques d'atteintes à la vie privée et à la sécurité des données, sauf à mettre en place une interopérabilité entièrement à la main de l'utilisateur. Par ailleurs, le bilan écologique de la démultiplication de lieux de conservation de données pourrait aussi être un inconvénient majeur. Enfin, l'interopérabilité totale n'incite pas à l'innovation. C'est d'ailleurs ce qui est constaté concernant les e-mails.

Le CNNUM qui a expertisé cette question a une approche nuancée. Il suggère de n'imposer l'interopérabilité qu'aux plus grosses plateformes et propose de distinguer l'*interopérabilité des graphes sociaux*[670], *l'interopérabilité des*

---

mutuellement les informations qui ont été échangées via *des interfaces ou d'autres solutions, de sorte que tous les éléments matériels ou logiciels fonctionnent avec d'autres matériels et logiciels et avec les utilisateurs de toutes les manières pour lesquelles ils sont censés fonctionner* ».

667 J. Crémer, Y.-A. de Montjoye, H Schweitzer, *Competition Policy for the digital era : Final report,* Publications Office of the European Union, Luxembourg, (2019).

668 La Quadrature du Net, *Pour l'interopérabilité des géants du web*, Lettre commune de 75 organisations, 21 mai 2019.

669 Une telle fonctionnalité pourrait mettre en danger Wikipédia car si la rapidité du débat des autres RS débarque sur la plate-forme qui est basée sur un temps long, cela pourrait briser la sérénité.

670 Le graphe social dessine la carte des liens entre les utilisateurs et des modalités de leurs connexions. Par l'ouverture d'API des plateformes, les nouveaux réseaux sociaux pourraient avoir accès aux données des graphes sociaux existants et les utilisateurs pourraient conserver les relations acquises sur le précédent RS. L'exportation des listes de contacts avec une actualisation en temps réel serait facilitée par l'API. Aujourd'hui, il n'est possible que de récupérer sa liste de contacts à un instant sur les RS existants sur le fondement du droit à la portabilité des données.

messageries instantanées[671] et *l'interopérabilité des contenus*[672], la dernière étant la plus difficile à mettre en œuvre[673]. Plus fondamentalement, l'interopérabilité ne semble réaliste que si elle préserve le modèle de chacun des réseaux sociaux en se fondant sur un standard commun minimal et en préservant les spécificités des différents réseaux sociaux. Poussée à l'extrême, l'interopérabilité parait assez antinomique avec l'idée des réseaux sociaux qui existent à travers des communautés fermées et protégées. L'option d'une interopérabilité totale imposée aux opérateurs semble donc, à ce stade, difficile et discutable. Cela n'enlève rien à l'intérêt de promouvoir des solutions moins absolues.

- *Créer un réseau social public ?*

Face à la nécessité de préserver le pluralisme des opinons et d'offrir un espace sécurisé au débat public, l'idée d'un réseau social public a été évoquée[674]. Ethan Zuckerman, universitaire et activiste réputé de l'internet américain, promeut la création de réseaux sociaux de service public, à l'image de médias comme PBS[675] ou de la BBC[676] qui bénéficient d'une forte réputation d'excellence, qui seraient financés par la puissance publique et proposeraient un média social alternatif plus respectueux des principes démocratiques[677]. Un tel réseau a été mis en place aux Pays-Bas, où les diffuseurs publics se sont regroupés pour créer « *Public spaces* », leur propre réseau social non lucratif qui n'utilise que des logiciels libres, ne conserve pas les données personnelles et dispose d'un statut qui garantit son indépendance politique et économique[678]. Séduisante, la piste paraît toutefois, à ce stade, peu réaliste du moins en France. Outre l'investissement que cela pourrait représenter sachant qu'aucun acteur public du secteur ne semble disposer d'un savoir-faire suffisant à cet égard, un tel réseau public risquerait de se heurter à la méfiance de nombreux utilisateurs et de ne pas être suffisamment attractif pour réussir à créer l'effet de réseau recherché[679]. A ce stade, le rôle des acteurs publics semble devoir se concentrer sur celui de régulateur voire de tiers de confiance (à l'instar de la Poste, qui dans le cadre du virage numérique propose des coffres-forts numériques[680]). Une autre solution serait de prévoir un soutien financier public à des réseaux répondant à des cahiers des charges strictes.

---

671 Elle vient d'être adopté par le DMA et devrait être assez aisée car il existe déjà un protocole standard pour la messagerie instantanée, la norme XMPP (Extensible Messaging and Presence Protocol) de l'Internet Engineering Task Force (IETF).

672 De façon graduelle, elle pourrait aller de la consultation de contenus, à la publication puis, en dernier lieu à l'interaction vis-à-vis des contenus. Le premier est déjà faisable grâce au standard RSS, utilisé par YouTube. Le deuxième consiste en la pratique du cross-posting (publication au-delà du RS initial). Le troisième pose des difficultés techniques importantes, car il s'agirait d'accepter les CGU de chaque plateforme et de lisser les modalités d'interaction (*like*s, etc.) ce qui n'est pas souhaitable du point de vue de la concurrence.

673 Avis du CNNum, Concurrence et régulation des plateformes. Étude de cas sur l'interopérabilité des réseaux sociaux, juillet 2020, p. 17.

674 H. Verdier *op. cit.*

675 Journal télévisé américain.

676 Radiodiffuseur britannique de service public.

677 B. Patino. *Tempête dans le bocal*, *op. cit,* p.140 et s.

678 https ://publicspaces.net/tag/english/

679 *Cf.* le réseau social « Truth social » crée par Donald Trump. *Le Monde*, 21 février 2022, « Pourquoi D.Trump lance son propre réseau social ».

680 Espace sécurisé de stockage de données hébergées en France

2.4.6. Les nouveaux équilibres du paysage de la régulation des réseaux sociaux à l'aune du DSA et du DMA

Le DSA et le DMA, s'ils ne régissent pas tous les domaines juridiques concernés par les réseaux sociaux, ont procédé à des arbitrages importants qui déterminent pour les années à venir les nouveaux équilibres de la régulation des plateformes.

Ces deux textes font le choix d'un encadrement des réseaux sociaux fondé sur **la logique de proportionnalité, la responsabilisation des acteurs et une supervision renforcée**. Jusqu'alors, outre les dispositifs d'autorégulation, les contrôles des contenus et du marché s'effectuaient uniquement *ex post* sous la houlette des autorités administratives et/ou du juge. Les deux règlements européens, surtout le DSA, introduisent des mécanismes de régulation *ex ante*, en faisant reposer sur les grands acteurs, notamment les très grands réseaux sociaux, la mise en place des instruments techniques permettant d'assurer effectivement le respect du principe de base selon lequel « *ce qui est légal hors ligne doit être légal en ligne et ce qui est illégal hors ligne doit être illégal en ligne* », selon les mots du commissaire Thierry Breton.

Les sanctions, confiées à la Commission européenne s'agissant des très grandes plateformes, qui sont évidemment indispensables pour assurer l'effectivité du dispositif ne pourront intervenir qu'en cas de manquement systémique de l'opérateur. Un effort est donc demandé en amont aux professionnels les plus importants du secteur (opérateurs cruciaux) dans le but d'équilibrer le marché et de mieux protéger les utilisateurs, à l'instar des mécanismes qui sont à l'œuvre dans le domaine bancaire ou financier. On retrouve là les principes directeurs de la *compliance*[681] dont la professeure Marie-Anne Frison-Roche avait souligné qu'ils étaient particulièrement adaptés au domaine du numérique[682]. Un tel dispositif repose sur la **confiance raisonnable** dans les acteurs : c'est pourquoi, les règlements accroissent significativement les obligations de **transparence** et **d'accessibilité aux informations**[683] et prévoient des **sanctions** potentiellement dissuasives[684].

681 Ce mot emprunté de l'anglais se dit, selon G. Cornu, de la conformité aux objectifs d'une réglementation prudentielle : préservation du système bancaire ou de gouvernance de la société. (*Vocabulaire juridique*, 13e éd., PUF, 2020). Selon M.-A. Frison-Roche, il désigne le fait de demander à certains opérateurs privés dits « cruciaux » d'internaliser des objectifs d'intérêt général, en raison de leur position et des moyens dont ils disposent, pour satisfaire ces objectifs (information, activité transnationale, technologie, etc.).

682 M.-A. Frison-Roche, *Internet, espace d'inter régulation*, Dalloz, 2016 ; *Régulation, Supervision, Compliance*, Dalloz, 2017 ; *L'apport du droit de la compliance à la gouvernance d'internet*, rapport commandé par le ministre en charge du numérique, avril 2019.

683 L'art. 31 du DSA prévoit notamment que « *Les très grandes plateformes en ligne fournissent au coordinateur de l'État membre d'établissement pour les services numériques ou à la Commission [...] l'accès aux données nécessaires pour contrôler et évaluer le respect du présent règlement*. »

684 S'agissant du DMA, en cas de non-respect de ses obligations ou des injonctions imposées par la Commission, un *gatekeeper* pourra être sanctionné par une amende pouvant aller jusqu'à 10% de son chiffre d'affaires mondial, et jusqu'à 20% en cas de récidive. Dans le cas où un contrôleur d'accès adopte un comportement de non-respect systématique du DMA, c'est-à-dire qu'il enfreint les règles au moins 3 fois en 8 ans, la Commission européenne peut ouvrir une enquête de marché et, si nécessaire, imposer des mesures correctives comportementales ou structurelles. Le DSA prévoit aussi des sanctions dissuasives (jusqu'à 6% du chiffre d'affaires annuel mondial de l'opérateur) en cas de non-respect de ses obligations.

Ces textes sont le produit des **arbitrages** qui ont été rendus par les co-législateurs européens, c'est-à-dire le Parlement européen et les représentants des gouvernements des 27 États membres réunis au sein du Conseil. Dans une économie numérique mondialisée, l'Union européenne est certainement le niveau pertinent pour créer les conditions d'un marché régulé, en mesure de faire le poids face aux géants américains et chinois et de faire des standards européens des éléments de référence au plan international.

Cette nouvelle législation place donc volontairement à un **niveau européen** ces nouveaux dispositifs de contrôle, conférant à la Commission européenne vis-à-vis de ces *gatekeepers* un rôle de régulateur tout à fait novateur et s'agissant des autres plateformes, un rôle de coordination pour éviter les incohérences entre les régulateurs nationaux[685]. Le choix a donc été fait d'une **régulation centralisée et cohérente** sur le territoire des 27, choix qui s'est notamment traduit par l'adoption de règlements et non de directives. A une réglementation stricte du marché risquant de freiner l'innovation et la libre circulation des produits et des services et sans doute peu réaliste techniquement, l'Union européenne a préféré un **dispositif souple de régulation partagée** pour lequel beaucoup dépendra de la mise en œuvre effective. Le dispositif repose sur un mécanisme proportionné qui fait peser des obligations plus lourdes sur les plus grosses plateformes afin de ne pas pénaliser au passage les petites structures, l'objectif étant de ne pas nuire à l'émergence, souhaitable, de nouveaux acteurs.

Le DSA et le DMA définissent également un équilibre entre la **responsabilité individuelle des utilisateurs finaux**, qui restent logiquement les premiers responsables de leurs propos comme de leurs comportements sur les réseaux sociaux, et leur **protection**, en imposant aux opérateurs une série de mesure comme l'interdiction des *darks patterns* (présentations mensongères), l'interopérabilité des messageries ou encore le droit à la contestation des décisions de modération des plateformes.

Le DSA et le DMA, en instaurant des obligations *ex ante* sur les ***gatekeepers,*** visent à renforcer la **sécurité juridique** des dispositifs sans porter une atteinte disproportionnée à la **liberté d'entreprendre et la liberté contractuelle**.

Ainsi, le DMA impose-t-il des obligations qui visent à lutter contre les environnements fermés et à favoriser le libre choix des utilisateurs finaux, à interdire les comportements déloyaux vis-à-vis des entreprises utilisatrices et à améliorer la transparence ainsi que l'accès aux données pour les professionnels, notamment en matière publicitaire. Les *gatekeepers* devront également notifier leurs acquisitions afin de prévenir d'éventuels comportements de prédation. La **supervision** de ces obligations est confiée à la Commission européenne, qui se voit attribuer de larges pouvoirs d'accès aux données et aux algorithmes. Elle engagera un dialogue avec les *gatekeepers* sur les mesures techniques à prendre afin de s'assurer de leur bonne compréhension des règles à respecter, quitte à en préciser l'application si nécessaire.

S'agissant de la **lutte contre les contenus illicites**, l'Union européenne a retenu, avec l'adoption du DSA, un **modèle nouveau.**

685 Ce dispositif présente l'avantage d'éviter le mécanisme d'autorité chef de file qui pose de nombreuses difficultés dans le cadre de la mise en œuvre du RGPD (*cf. supra*).

En effet, jusqu'à présent, la meilleure façon de garantir la liberté d'expression a consisté, pour les démocraties libérales, à ne confier le contrôle de ses abus qu'à une intervention *ex post* du juge, tournant la page à des siècles de censure. C'est l'équilibre mis en place par la loi sur la presse de 1881, qui demeure l'un des piliers de la démocratie française. Cependant, face à la multiplication exponentielle des échanges rendue possible par internet et les réseaux sociaux, ce seul contrôle juridictionnel *ex post* s'est avéré vain et les opérateurs se sont trouvés obligés de rétablir une nouvelle forme de contrôle *ex ante*, appelée *modération*, afin de freiner le déferlement de contenus contraires à l'ordre public. Chaque plateforme a donc opéré son tri selon ses propres critères. L'idée de confier un dispositif de régulation *ex ante* pour lutter contre les contenus illicites et se prémunir de modérations excessives a été retenue dans le DSA. **Une des originalités du dispositif est qu'il ne confie pas à la Commission européenne ou aux régulateurs nationaux le soin de dire au cas par cas si un contenu est contraire à l'ordre public** : le règlement contraint les très grandes plateformes à identifier les risques systémiques engendrés par les algorithmes de modération (soit qu'ils laissent passer des contenus illicites soit qu'ils censurent abusivement) et à mettre en place des mesures d'atténuation pour mieux les limiter. Le contrôle ainsi effectué est essentiellement statistique et s'opère à grosse maille. Si la détermination des contenus manifestement illicites ne fait pas difficulté, ceux situés *dans la zone grise* sont plus difficiles à réguler et des instruments de droit souple pourront être pris par la Commission en lien avec les régulateurs nationaux pour orienter les politiques de modération comme le code de conduite de lutte contre les contenus haineux[686]. **Le DSA laisse le dernier mot au juge national**, qui pourra toujours être saisi par l'utilisateur d'un recours contre une modération abusive (ou un refus de modérer).

Parmi tous les défis énumérés dans cette seconde partie, certains ont déjà été traités par la puissance publique. Celle-ci s'est concentrée sur les dispositifs visant à lutter contre les troubles à l'ordre public et sur l'arsenal pénal, tant procédural que de fond, qui a été significativement renforcé. Si l'efficacité de ces outils est sans doute perfectible, il ne paraît *a priori* pas opportun d'en créer de nouveaux. En outre, de nombreuses questions devraient à moyen terme être réglées par le DMA et le DSA qui n'appellent pas de textes nationaux supplémentaires (sauf de manière ponctuelle, par exemple pour désigner l'autorité coordinatrice pour le DSA ou pour permettre à l'Autorité de la concurrence d'utiliser les nouveaux outils établis par le DMA). Les propositions que le Conseil d'État a choisi de faire dans la présente étude ne portent donc pas principalement sur l'édiction de nouvelles normes. Elles s'attachent à définir des actions et des modalités d'organisation de la puissance publique permettant d'améliorer l'efficacité et l'effectivité du nouveau cadre de régulation qui vient d'être mis en place et de favoriser un usage mieux raisonné et plus équilibré des réseaux sociaux. Elles auront tout à gagner d'un renforcement de la recherche académique et notamment juridique sur les notions fondamentales remises en cause par le phénomène des réseaux sociaux, du consentement à l'identité en passant par la protection de la vie privée. Il s'agit, dans un contexte en permanente évolution, d'essayer de tirer le meilleur parti des opportunités incontestables qu'offrent les réseaux sociaux, tout en limitant autant que possible les risques de dépendance, d'addiction voire d'asservissement.

686 https ://ec.europa.eu/commission/presscorner/detail/en/fs_21_5106

3. Pour un usage maîtrisé et optimisé des réseaux sociaux

Les réseaux sociaux, par leur puissance, leur diversité, leur capacité à se transformer constamment posent une difficulté particulière à l'effort de régulation. Ils invitent aussi la puissance publique à se réinventer dans ses modes d'actions internes et externes. Celle-ci doit agir au moins sur ces deux fronts. D'une part, répondre aux enjeux majeurs qu'ils posent. D'autre part, saisir l'ensemble des chances qu'ils offrent et utiliser ses leviers pour moderniser l'action publique.

Les enjeux

Au terme de cette étude, trois enjeux majeurs se dessinent, qui dépassent d'ailleurs pour la plupart le seul cadre des réseaux sociaux, et dont beaucoup sont liés au développement plus global du numérique. Le premier est **l'enjeu politique et démocratique**. Les réseaux sociaux s'imposant toujours davantage comme le forum ou l'agora de notre époque, c'est-à-dire non seulement comme un nouveau lieu de rencontres et d'échanges entre individus mais aussi comme l'espace privilégié de la liberté d'expression et du débat public. Les réseaux sociaux ont un impact évident sur les modalités d'exercice de la liberté d'expression mais aussi sur le respect effectif des droits individuels comme celui au respect de la vie privée : leur rôle central et leur concentration entre les mains de quelques très puissants acteurs impliqueraient, en contrepartie, de renforcer les utilisateurs dans leurs droits et leurs moyens d'action. Le deuxième est **l'enjeu économique et stratégique**. Outre le fait que les entreprises européennes parviennent difficilement à trouver leur place sur un marché dominé par les géants américains et chinois, cette situation engendre une importante dépendance de l'économie française et européenne à l'égard de ces acteurs dominants et qui tendent à l'être toujours davantage, notamment grâce à la monétisation des données de leurs utilisateurs européens. La régulation de ce marché pour permettre une concurrence équitable et garantir une meilleure protection des données personnelles des Européens sans préjudicier à l'innovation se révèle donc un défi prioritaire pour les politiques publiques. Le troisième, trop souvent oublié, **est l'enjeu écologique**. L'utilisation exponentielle des réseaux sociaux a un coût environnemental massif. Il risque d'augmenter plus encore si les usages continuent à se développer sans limite comme c'est le cas actuellement. Cet enjeu doit être porté à la connaissance des utilisateurs beaucoup plus qu'il ne l'est aujourd'hui et pris en considération dans l'ensemble des décisions prises par la puissance publique.

Les priorités et les outils de régulation

Face à ces enjeux, l'action de la puissance publique est légitime mais elle doit trouver le bon niveau d'intervention auprès d'opérateurs évoluant dans une économie de marché libre. Deux questions principales se posent : d'une part, celle de définir les objectifs prioritaires que doivent poursuivre les politiques publiques ; d'autre part, celle de déterminer les moyens les plus pertinents pour y parvenir. La place majeure qu'occupent actuellement dans le monde les réseaux sociaux – et le rôle dominant que tiennent quelques-uns d'entre eux – appellerait dans l'idéal une régulation à l'échelle mondiale. Force est de constater que cette perspective idéale s'avère peu réaliste à court et même moyen terme, tant les enjeux sont délicats et importantes les différences d'approche et d'intérêt des principaux acteurs. D'ailleurs, leur développement s'est improvisé dans un cadre juridique longtemps incertain, en tirant partie des vides qui existaient et en bousculant les réglementations et législations traditionnelles susceptibles de l'entraver. Dans ces conditions, **l'échelle la plus pertinente pour la France paraît être celle de l'Union européenne** : son cadre institutionnel est bien adapté à la mise en place d'une régulation, les intérêts de ses États membres apparaissent largement convergents sur cette question et le marché européen constitue un niveau pertinent compte tenu du poids qu'il représente pour les réseaux sociaux.

La présente étude intervient à cet égard à un moment crucial. L'Union européenne vient justement, avec l'adoption des règlements DMA et DSA, de se doter pour la première fois, en un temps record, d'un dispositif de régulation qui, bien que non spécifiques aux réseaux sociaux, les intéresse au premier chef. Ce cadre juridique et ces outils de supervision devraient être mis en place, selon le type de dispositions, entre 2023 et 2024[687]. Mais, en pratique, beaucoup dépendra de la manière dont ils seront interprétés et utilisés. **Il apparaît indispensable que les autorités françaises, qui ont joué un rôle moteur dans l'adoption de ces textes, jouent également un rôle moteur dans leur mise en œuvre**. Les années qui viennent seront décisives.

Les opportunités

Le Conseil d'État invite par ailleurs la puissance publique à **se saisir encore davantage de l'outil** exceptionnel que constituent les réseaux sociaux. Jamais l'administration n'a eu à sa disposition un instrument permettant d'entrer aussi facilement au contact des administrés, de manière aussi large et aussi directe, mais aussi de modifier de façon aussi radicale la gestion des emplois publics.

Au regard de l'ensemble de ces éléments, le Conseil d'État estime que l'action des pouvoirs publics dans ce domaine devrait se concentrer autour de quelques objectifs clairs et structurants.

Le Conseil d'État estime d'abord que **l'objectif premier**, qui devrait guider l'action des pouvoirs publics tant dans la mise en œuvre des normes européennes que dans les recours éventuels à des instruments de droit interne, est celui d'un

687 Le DSA sera applicable en deux temps : pour les «très grandes plateformes» désignées comme telles par la Commission, 4 mois après son entrée en vigueur et, pour les autres plateformes, 15 mois après son entrée en vigueur ou au 1er janvier 2024, la date la plus tardive étant retenue. Concernant le DMA, il sera applicable 6 mois après son entrée en vigueur (date prévisionnelle : mars 2023).

rééquilibrage des forces en faveur des utilisateurs, y compris par la promotion d'instruments garantissant l'autonomie stratégique et la préservation effective des droits fondamentaux des citoyens européens. Les textes que vient d'adopter l'Union européenne rendent possible un tel rééquilibrage. Mais il faudra sans doute aller plus loin. S'agissant des questions qu'ils ne règlent pas, une approche purement nationale peut demeurer pertinente, y compris pour préparer la voie à de futures initiatives au niveau européen : le cadre juridique doit en effet rester dynamique pour s'adapter au développement des techniques et des usages.

Le Conseil d'État considère ensuite qu'il est indispensable à cette fin **que les différents acteurs de la puissance publique se mettent rapidement en ordre de marche**. D'une part, pour donner à la réglementation européenne et aux outils de régulation qu'elle institue leur pleine efficacité, en favorisant notamment une montée en puissance des compétences techniques et un fonctionnement en réseau des différents acteurs publics concernés. D'autre part, pour se saisir, davantage encore qu'aujourd'hui, de l'outil exceptionnel que constituent les réseaux sociaux pour en utiliser pleinement les potentialités pour l'action publique comme pour le fonctionnement de la sphère publique elle-même.

Le Conseil d'État est enfin d'avis que la puissance publique devrait conduire dès maintenant une **réflexion approfondie permettant d'anticiper efficacement les enjeux des évolutions qui se profilent.** Certaines sont déjà en cours et doivent dès maintenant faire l'objet d'une attention particulière au regard des enjeux majeurs qu'elles représentent pour l'avenir. D'autres sont encore à un stade préliminaire, comme celui du ou des métavers, mais risquent de poser des questions juridiques, économiques et sociales majeures au cours des prochaines années.

Agir en faveur d'un rééquilibrage des forces au profit de l'utilisateur et du citoyen, équiper la puissance publique pour réguler les réseaux sociaux mais aussi optimiser leur usage et penser les réseaux sociaux de demain : tels sont les trois principaux chantiers que le Conseil d'État recommande de mettre en œuvre dans les mois et les années qui viennent.

3.1. Rééquilibrer les forces au profit de l'utilisateur et du citoyen

Rééquilibrer les forces entre les utilisateurs et les grandes plateformes, dont certaines ont la puissance économique et la taille d'États, est ambitieux et ne peut être atteint facilement ni rapidement. La plupart des textes européens et français intervenus ces vingt dernières années et qui ont mis en œuvre le **principe de loyauté et de transparence** poursuivent déjà cet objectif mais il semble important de fixer à l'ensemble des politiques publiques relatives aux réseaux sociaux cet objectif principal. Le *Digital services Act* et le *Digital markets Act* imposent déjà des obligations aux opérateurs qui visent à rééquilibrer les forces au profit des

utilisateurs. Le DSA comporte de nombreuses obligations d'information et de transparence au profit de l'utilisateur. Quant au DMA, en prévoyant notamment que les contrôleurs d'accès doivent permettre aux utilisateurs finaux d'exercer la portabilité de leurs données et de choisir leurs logiciels, en interdisant les *dark patterns* (interfaces trompeuses) et en imposant le recueil du consentement des utilisateurs pour se servir des données à des fins publicitaires ou pour les combiner avec d'autres services, il contribue également à cet objectif. Toutefois, il apparaît nécessaire d'aller plus loin encore pour réaliser un rééquilibrage effectif, plusieurs propositions pouvant ainsi y contribuer, depuis la formation du contrat entre l'utilisateur et la plateforme jusqu'aux actions d'information et de pédagogie en passant par une meilleure maîtrise des paramétrages techniques.

3.1.1. Le rééquilibrage des relations contractuelles

Au fondement de la relation entre l'utilisateur et la plateforme se trouve un contrat, dont l'équilibre est aujourd'hui très favorable à la plateforme. Des efforts doivent être menés, tant au stade de la formation de ce contrat ou de sa modification, notamment en redonnant une réelle place aux utilisateurs ou aux associations qui les représentent, qu'aux différents stades de la vie du contrat, notamment en reconnaissant des droits subjectifs spécifiques aux utilisateurs.

Rééquilibrer la détermination des conditions générales d'utilisation et des politiques de confidentialité

Les réseaux sociaux sont avant tout des sociétés privées qui établissent **un lien contractuel** avec chacun de leurs utilisateurs. Chaque utilisateur est seul face à cet opérateur d'une puissance économique considérable. Le lien contractuel est donc très déséquilibré puisqu'au lieu d'une négociation sur les points sensibles du contrat, l'usager n'a d'autre choix que de consentir, d'une part, à toutes les **conditions générales d'utilisation** et, d'autre part, au traitement de ses données personnelles et à la politique de confidentialité des données définis par la plateforme, consentement qu'il peut d'ailleurs donner sans même les avoir lues en cliquant sur un onglet. On peut donc dire sans exagération que l'individu qui souhaite utiliser un service de réseau social est à la merci de l'opérateur, tributaire d'un **contrat d'adhésion** et d'un consentement au traitement des données largement biaisé par la volonté d'accéder avant tout au service. S'il est, pour l'instant, inenvisageable que chaque demande de service fasse l'objet d'une offre individualisée[688], ce déséquilibre n'est pas une fatalité et on ne doit pas s'en satisfaire[689]. Le rétablissement d'un meilleur équilibre s'agissant d'un contrat dont l'objet est de permettre aux individus de s'exprimer n'est pas sans lien avec une démocratie en bonne santé. Au-delà du « consentement » à des conditions unilatéralement fixées par l'opérateur comme du « consentement » à l'utilisation

688 On ne peut cependant exclure que l'IA permettra un jour ce tour de force

689 Dans le même esprit, H. Isaac et L.-V. de Franssu (Renaissance numérique) proposent d'intégrer une représentation des utilisateurs dans les instances de gouvernance des plateformes ou de permettre aux représentants des utilisateurs de participer directement à la régulation *via* une API (V. E. Marzolf, « Les utilisateurs doivent être intégrés à la régulation numérique », Acteurs publics, 18 mars 2022)

des données personnelles, dont il faut considérer avec précaution la portée[690], il faut, dès l'amont, chercher à terme à donner une véritable place aux utilisateurs afin qu'ils puissent, par l'intermédiaire des associations de consommateurs, participer à la détermination de ces conditions et faire valoir leurs priorités (protection de la santé, de l'environnement, des données personnelles, etc.). Ces actions, de nature contractuelle, conforteraient les objectifs poursuivis par les textes européens. Il faut souligner que dans un cadre différent, les actions des collectifs d'auteurs ont eu un poids considérable dans la détermination des équilibres de la directive 2019/790. Ce rééquilibrage *ex ante* pourrait compléter utilement les actions contentieuses *ex post* qui sont déjà exercées sur le terrain du droit de la consommation ou du droit des données personnelles.

Compte tenu du poids des grandes plateformes, le niveau le plus utile pour de telles actions paraît être le niveau européen. Le terrain n'est pas vierge. Le **bureau européen des unions de consommateurs** (BEUC), fédération de 41 associations de consommateurs issues de 31 pays d'Europe créée en 1962, qui représente les intérêts des consommateurs au niveau de l'Union européenne, est déjà très mobilisé sur les questions numériques. Il gagnerait à être soutenu, avec d'autres, dans cette optique[691]. Pour que les négociations aient un réel contenu, les associations pourraient étoffer leur expertise et renforcer leur représentativité : les rapprochements ponctuels qui ont déjà eu lieu entre les associations de consommateurs et des associations environnementales ou de protection des données personnelles pourraient se pérenniser, se renforcer, voire s'élargir à des associations de protection de la santé afin de créer des synergies et de constituer des fédérations d'utilisateurs plus puissantes.

La puissance publique, au niveau européen comme au niveau national, aurait intérêt à faciliter de telles actions par **une politique volontariste d'encouragement et d'accompagnement à la négociation** (qui pourrait s'inspirer du droit du travail). Des discussions informelles ont déjà lieu entre les plateformes et les associations de consommateurs mais, compte tenu du déséquilibre actuel des forces, elles sont difficilement fructueuses. Pour donner une assise à ces négociations, la **Commission européenne** pourrait prendre l'initiative de réunir les grandes plateformes relevant désormais de son nouveau rôle de régulateur et le BEUC ainsi que d'autres associations intéressées, le cas échéant en mettant en place une instance pérenne du type du **Conseil national de la consommation** (CNC) français[692]. En France, des négociations ont par exemple été menées sous l'égide

690 M. Fabre-Magnan, « Le consentement, ce n'est pas la liberté », *Le Figaro*, 9 novembre 2018.

691 *Le Monde*, 1er juillet 2022, « Données personnelles : des associations européennes de consommateurs portent plainte contre Google ». Selon elles, Google, au moment de proposer la création d'un compte, compliquerait volontairement le refus de la collecte des données personnelles.

692 Présidé par le ministre chargé de la consommation, il a pour objet d'instaurer la concertation entre les représentants des intérêts collectifs des consommateurs, des professionnels et des entreprises assurant des missions de service public, pour tout ce qui se rapporte à la consommation. Ce conseil est consulté par les pouvoirs publics sur les grandes orientations de leur politique consumériste, et donne son avis sur les problèmes de consommation et sur les textes législatifs et réglementaires qui lui sont présentés. Il peut aussi s'exprimer de sa propre initiative (sans saisine du ministre) sur les projets ou les propositions de lois et de règlements susceptibles d'avoir des incidences sur la consommation. Il est composé : d'un collège constitué des associations de défense des consommateurs agréées, d'un collège comprenant des organisations professionnelles les plus représentatives des activités industrielles,

du CNC sur les contrats-type d'enseignement à la conduite qui ont porté leurs fruits[693]. En rassemblant autour d'une même table l'ensemble des partenaires, la puissance publique pourrait impulser un processus moins informel et veiller au bon déroulement des discussions. Une jurisprudence récente de la CJUE permet de penser que la réglementation européenne sur les services de l'information est tout à fait compatible avec de telles évolutions nationales ou européennes[694].

Au niveau français, ce soutien pourrait également se traduire par le renforcement de la **DGCCRF** et des **instances placées auprès du ministre chargé de la consommation**, qui participent de la protection des consommateurs et qui pourraient voir leur expertise renforcée s'agissant des utilisateurs des réseaux sociaux grâce à l'appui des associations spécialisées dans ce secteur (*cf. infra*. 3.2.3). Les autres régulateurs compétents dans le domaine des réseaux sociaux pourraient aussi apporter leur appui.

Un tel renforcement pourrait, à terme, rétroagir sur les capacités des associations à davantage utiliser les dispositifs **d'action dans l'intérêt collectif des consommateurs**[695] ou **d'actions de groupe**[696] qui seraient très utiles dans ce secteur pour favoriser un rééquilibrage effectif au profit des utilisateurs. La transposition de la directive 2020/1828/UE sur les actions de groupe qui devrait prochainement intervenir pourrait permettre d'envisager d'assouplir les conditions pour lancer de telles actions.

En tout état de cause, il apparaît souhaitable que, **dans un premier temps**, avant de parvenir à négocier certaines clauses des CGU ou des politiques de confidentialité, les demandes des associations de consommateurs aux grandes plateformes soient prises en compte dans le cadre de **l'identification des risques systémiques**, la mise en place des mesures d'atténuation et les contrôles des audits organisés par les régulateurs.

---

commerciales, artisanales et agricoles et de services privés ainsi que d'entreprises assurant des missions de service public, de membres de droit, dont l'Institut national de la consommation (pour la liste complète v. arrêté du 15 février 2021).

693 Négociations qui ont abouti à l'adoption du décret n° 2020-142 du 20 fevrier 2020 et de l'arrêté du 29 mai 2020 définissant le modèle de contrat type pour l'enseignement de la conduite pour la catégorie B du permis de conduire.

694 Dans une affaire C-319/20 du 28 avril 2022 la CJUE a jugé que le RGPD ne s'oppose pas à une réglementation nationale qui permet à une association de défense des intérêts des consommateurs d'agir en justice, en l'absence d'un mandat qui lui a été conféré à cette fin et indépendamment de la violation de droits concrets des personnes concernées, contre l'auteur présumé d'une atteinte à la protection des données à caractère personnel, en invoquant la violation de l'interdiction des pratiques commerciales déloyales, d'une loi en matière de protection des consommateurs ou de l'interdiction de l'utilisation de conditions générales nulles, dès lors que le traitement des données concernées est susceptible d'affecter les droits que des personnes physiques identifiées ou identifiables tirent de ce règlement

695 Les art. L.621-1 et L.627-7 du code de la consommation autorisent les associations agrées ayant pour objet statutaire explicite la défense des intérêts des consommateurs à « *exercer les droits reconnus à la partie civile relativement aux faits portant un préjudice direct ou indirect à l'intérêt collectif des consommateurs* » et d'agir pour faire cesser ou interdire tout agissement illicite au regard du droit européen de la consommation (directive 2009/22/CE du 23 avril 2009 relative aux actions en cessation en matière de protection des intérêts des consommateurs. L'art. 38 de la LIL permet aussi ce type d'actions en matière de données personnelles.

696 Actions de groupe fondées sur les art. L. 623-1 et suivants du code de la consommation ou sur la protection du droit des données personnelles (art. 7 de la LIL modifiée par la loi du 20 juin 2018 relative à la protection des données personnelles et la loi du 10 novembre 2016 de modernisation de la justice du XXIe siècle.

Si le DSA prévoit que certaines informations minimales soient prévues dans les CGU et exige qu'elles soient claires et lisibles, y compris pour les mineurs (informations sur les modalités de la modération des contenus, le recours aux algorithmes et à l'examen humain ainsi que sur le système interne de réclamation[697]), la mise en place d'un lieu de négociation entre les associations et les grandes plateformes permettrait à terme, au moins sur les points les plus importants, d'élaborer des **standards minimums** des conditions générales d'utilisation et des politiques de confidentialité des données et de rééquilibrer ainsi les relations contractuelles entre utilisateurs et opérateurs.

Proposition n° 1

Afin de créer au niveau européen et national les conditions d'une « négociation collective » des conditions générales d'utilisation et des politiques de confidentialité, une politique ambitieuse de rééquilibrage de la relation contractuelle pourrait être menée, avec les autorités de régulation compétentes, selon les axes suivants :

- identifier des associations et regroupement d'associations susceptibles d'entrer en négociation avec les plateformes et les soutenir à cette fin ;

- créer, idéalement au niveau de la Commission européenne, une instance de concertation ayant pour objet d'asseoir à la même table l'ensemble des partenaires, d'identifier les clauses ou questions devant faire l'objet de discussions et de fixer conjointement l'ordre du jour des négociations et leur calendrier ;

- au fil des négociations, parvenir à l'élaboration conjointe de standards minimums pour les CGU et les politiques de confidentialité ;

- instaurer, à terme, un véritable « droit à la participation » des utilisateurs ou de leurs représentants à l'élaboration des conditions générales d'utilisation et des politiques de confidentialité des données des grandes plateformes.

Rééquilibrer la relation contractuelle par une meilleure protection des utilisateurs mineurs et le renforcement des garanties d'identité

Une des difficultés les plus importantes sur les réseaux sociaux est la participation des **mineurs** à des réseaux inadaptés à eux ou leur exposition à des contenus non autorisés à leur âge. 44% des 11-18 ans déclarent avoir déjà menti sur leur âge sur les réseaux sociaux[698]. Le DSA contient des dispositifs spécifiques pour les protéger[699] mais la **vérification de la** « **majorité numérique** », qui n'y figure pas et n'est qu'une simple obligation de moyen dans le RGPD, apparaît pourtant comme un verrou essentiel.

697 Futur art. 12 du DSA.

698 Source : Enquête Génération numérique « les pratiques numériques des jeunes de 11 à 18 ans », mars 2021.

699 L'art. 24 *ter* exige des plateformes qu'elles mettent en place des mesures appropriées et proportionnées pour garantir un niveau élevé de confidentialité, de sûreté et de sécurité des mineurs et interdit la publicité ciblée à leur endroit.

Une autre difficulté importante tient à l'**identification des auteurs d'infractions** qui constituent également une menace pour les internautes – notamment les mineurs – voire de déceler les *bots* qui participent à la diffusion rapide de contenus illicites ou dangereux. Sans remettre en cause la possibilité de s'exprimer sous pseudonyme sur les réseaux sociaux et sans porter atteinte à la vie privée des utilisateurs en leur demandant des informations sensibles lors de leur inscription sur les réseaux sociaux (notamment des photos et carte d'identités), des solutions techniques comme les **logiciels d'identité numérique** ou le SGIN (développé en ce moment par l'État) ou des recours à des tiers de confiance[700] pour l'authentification de l'âge[701] pourraient, à terme, assurer une meilleure protection des utilisateurs, responsabiliser davantage les internautes et les opérateurs et faciliter le travail des enquêteurs.

Au niveau européen, les conditions d'âge pour consentir au traitement de données personnelles découlent notamment du RGPD, et en particulier de son article 8 qui interdit l'utilisation de données personnelles d'utilisateurs âgés de moins de 13 à 16 ans suivant les États membres, la France ayant fixé cet âge à 15 ans. Avant cet âge limite, un consentement conjoint de l'enfant et du titulaire de l'autorité parentale est nécessaire : des lignes directrices du CEPD ont été réalisées sur ce point[702]. Elles rappellent que les responsables de traitement doivent s'efforcer de vérifier que l'utilisateur a dépassé l'âge minimum de « consentement numérique ». A cette question, il faut distinguer celle de la capacité contractuelle à consentir aux CGU qui, en France, débute à la majorité sauf pour *les actes courants* qui peuvent être réalisés par le mineur seul, en application de l'article 1149 du code civil[703]. S'agissant du contrôle de l'âge, certaines règles particulières existent notamment pour les jeux d'argent et les paris en ligne pour lesquels le processus de vérification de l'âge d'un utilisateur est régi par le décret n° 2010-518 du 19 mai 2010 relatif à l'offre de jeux et de paris des opérateurs de jeux et à la mise à disposition de l'Autorité nationale des jeux des données de jeux. **Les sites présentant du contenu à caractère pornographique** sont, quant à eux, régis par les nouvelles dispositions de l'article 227-24 du code pénal modifié par la *loi n° 2020-936 du 30 juillet 2020* visant à protéger les victimes de violences conjugales qui mentionne explicitement que les systèmes de vérification de l'âge basés sur une auto-déclaration ne constituent pas des systèmes valides sur de tels sites. À ces mesures contraignantes s'ajoutent des avis ou des lignes directrices d'autorités indépendantes ou encore de publications par des consortiums[704]. Pour répondre aux obligations légales, les grandes plateformes, et en particulier les réseaux sociaux, ont développé et mis en place sur leurs services en ligne des solutions de vérification de l'âge qui sont souvent purement déclaratives et peu efficaces. Pour établir la minorité d'un

700 Organisme indépendant qui certifie de la majorité d'une personne afin d'éviter la dissémination d'éléments d'identité chez les opérateurs sans pour autant avoir accès à des informations sur le type de site consulté par l'internaute afin de préserver sa vie privée dans les deux sens.

701 PeRen, rapport, *Détection des mineurs en ligne : peut-on concilier efficacité, commodité et anonymat ?,* mai 2022.

702 Lignes directrices 5/2020 sur le consentement au sens du RGPD, p. 31-32.

703 Cette qualification s'apprécie au cas par cas en fonction de l'âge, du type de contrat et du contexte familial. A défaut de pouvoir être considéré comme un contrat d'usage, la plateforme doit recueillir l'accord des titulaires de l'autorité parentale.

704 Recommandations de la CNIL, août 2021.

utilisateur, certaines plateformes ont recours à des mots clés prédéfinis estimant que le type de contenu consulté est un indice sur son âge, mais les fausses alertes sont très fréquentes et la précision dépend de la quantité de contenus publiés par l'utilisateur. Il est vrai que, en principe, plus la plateforme est grande, plus elle utilise des signaux faibles et améliore sa détection. Le PeRen, après avoir analysé différentes méthodes, a répertorié les moins contraignantes et intrusives pour l'utilisateur (vérification par carte bancaire, par base de données nationales, par recours à une solution d'identité numérique, par contrôle parental par défaut avec activation par les parents).

Afin d'éviter que les plateformes ne recueillent toujours plus de données personnelles sur leurs utilisateurs, il est proposé de recourir au **mécanisme de double tiers** qui permet de faire vérifier l'âge par un tiers de confiance tout en empêchant ce dernier de savoir quel site le sollicite (mécanisme de tiers de confiance renforcé)[705]. Ainsi aucune partie n'a accès à la fois aux données d'identification et de vérification. Les solutions tierces interviennent comme des coffres-forts numériques. Le déploiement de cette solution technique et des logiciels d'identité numérique pourrait conduire à imposer à brève échéance un **principe de « transparence intermédiée » des identités et des âges,** consistant à rendre systématiquement possible, au moins pour les autorités judiciaires, l'accès à l'identité ou à l'âge d'un utilisateur par le recours à un intermédiaire qui soit un procédé technique ou un tiers de confiance. Une telle obligation permettrait à la fois à la société de mieux protéger les plus jeunes et aux autorités compétentes de disposer d'un outil d'identification des auteurs d'infraction afin d'éviter toute impunité. Les internautes pourraient donc continuer à librement converser avec des pseudonymes voire à donner une liste très réduite de données d'identification auprès d'un opérateur, mais il serait possible voire nécessaire pour l'opérateur d'obtenir une vérification de l'âge ou l'authenticité de l'identité auprès d'un tiers (notamment, par exemple, en cas de paiement ou d'accès à des sites ou contenus réservés aux personnes dépassant un âge minimum) ou pour les forces de l'ordre d'identifier l'auteur de faits répréhensibles. La mise en place **d'une obligation de « transparence intermédiée » au niveau des opérateurs** garantirait déjà l'existence d'interlocuteurs responsables et contribuerait à davantage responsabiliser les utilisateurs. Elle devrait s'accompagner d'une **information des utilisateurs** afin de garantir la loyauté des échanges et de mettre fin au sentiment d'impunité.

Le recours à ces solutions pourrait, dans un premier temps, être promu **dans le cadre de l'application du DSA** pour les très grandes plateformes pour minimiser des risques systémiques identifiés, notamment la présence de mineurs sur les plateformes en méconnaissance des CGU ou l'existence de trop nombreux *bots* sur les plateformes. Il faut rappeler que le DSA interdit la publicité ciblée à destination des mineurs et toute publicité ciblée sur la base de données sensibles au sens du RPGD.

La France pourrait expertiser la possibilité de mettre en place un tel dispositif pour les plateformes établies sur son territoire ou recommander l'ouverture d'un chantier sur la généralisation de ces solutions à toutes les plateformes auprès de la Commission européenne à l'occasion de la mise en œuvre du DSA voire d'une

705 Les lignes directrices du CEPD recommandent un tel recours.

prochaine révision. En effet, un des effets secondaires du DSA risque d'être le déport de contenus haineux sur les moyennes et petites plateformes : ce dispositif permettrait d'accélérer l'identification des auteurs. Il faut noter qu'il existe des dispositifs d'identité numérique libres de droits et donc gratuits.

Proposition n° 2

Promouvoir la généralisation des recours aux solutions d'identité numérique et à des tiers de confiance afin de mieux protéger les mineurs, de vérifier la majorité numérique et de garantir la fiabilité des échanges sur les réseaux sociaux, en en informant les internautes.

Envisager de rendre son recours obligatoire au niveau européen dans une version révisée du DSA.

3.1.2. Le rééquilibrage par l'appropriation de l'outil et l'exercice des droits

Le rééquilibrage des forces entre utilisateurs et grandes plateformes ne passe pas que par le droit. Il passe aussi par la technique, précisément par le paramétrage d'une application grâce à des fonctionnalités qui permettent aux utilisateurs de connaître et d'exercer effectivement leurs préférences et donc leurs droits. La technique doit être mise au service de l'utilisateur.

Faciliter le paramétrage[706] des réseaux sociaux et mieux assurer la protection de l'utilisateur par le design attentionnel

Le DMA comporte des dispositions visant à favoriser le libre choix des utilisateurs en leur permettant notamment d'exercer leur droit à la portabilité des données, en leur permettant de choisir les logiciels utilisés (navigateur web notamment) et en interdisant les interfaces trompeuses (*dark patterns*). En agissant en faveur de l'équilibre du marché, il permet également d'offrir plus de choix aux utilisateurs. Le DSA oblige les très grandes plateformes à publier les conditions générales des principaux paramètres utilisés dans les systèmes de recommandation et des options dont disposent les utilisateurs pour les modifier. Ces textes européens visent donc à permettre à l'utilisateur d'être davantage maître de son usage des

706 Les interfaces des réseaux sociaux offrent aux utilisateurs la possibilité de modifier ou réaliser eux-mêmes certains réglages (encore appelés « préférences » ou « paramètres » selon les opérateurs) pour que l'outil réponde mieux à leurs aspirations : choisir si le compte est public ou fermé (paramètres de confidentialité) bloquer certains contenus ou personnes sans que celles-ci ne le sachent, voir qui consultent le compte (paramètres de visibilité) bloquer certaines publicités (paramètre de contrôle de la publicité), ajouter des mots de passe d'authentification (paramètres de sécurité) régler les fonctionnalités et les interactions avec d'autres utilisateurs (refuser les *like* sur une publication, refuser l'appropriation par un tiers d'un contenu, contrôler les notifications, etc.) permettre la surveillance des comptes des adolescents (paramètres de surveillance) gérer les données personnelles (obtenir une copie de ses données, etc.). Lorsqu'on évoque le paramétrage par défaut, cela signifie qu'un réglage est défini, faute de consigne différente de l'utilisateur. Ainsi les comptes sont souvent paramétrés « public » par défaut c'est-à-dire visibles par tous les membres du réseau alors qu'ils peuvent l'être aussi en mode « privé » et n'être visibles que par les personnes acceptées comme membre de sa communauté par l'utilisateur.

réseaux sociaux. C'est une démarche qu'il convient d'encourager et de renforcer, afin que les réseaux sociaux restent ou deviennent effectivement un simple outil de communication à la disposition des utilisateurs et non l'inverse. C'est, au demeurant, l'intérêt bien compris des réseaux eux-mêmes, comme l'a reconnu le créateur de Twitter, Jack Dorsey, qui a souligné que l'avenir des réseaux sociaux résidait dans un paramétrage individualisé des fonctionnalités (ce réseau offre ainsi par exemple la possibilité de choisir entre un fil d'actualité faisant appel à des algorithmes de recommandation et un fil d'actualité purement chronologique). L'internaute peut également, au sein de certains réseaux sociaux, bloquer des publicités ou des accès à des comptes malveillants.

L'ensemble des plateformes devraient être incitées à réaliser des efforts effectifs pour :

- améliorer le ***design attentionnel*** des interfaces en sensibilisant notamment l'utilisateur sur son mode de consommation (temps d'écran, valorisation de la lecture des contenus avant de les transférer, signal lorsque des propos sont virulents pour demander à l'utilisateur s'il tiendrait les mêmes propos dans la vie réelle, etc.) ;
- permettre à l'utilisateur de garder à sa main un ensemble de paramètres de configuration portant sur la recommandation des contenus, sur les systèmes de notification, et de bloquer des contenus pour créer des « *safe spaces* » ;
- améliorer l'ergonomie et l'accessibilité des **boutons de signalement** présents sur les réseaux sociaux. Dans son bilan de l'application des dispositions de lutte contre les fausses informations de 2020, le CSA avait formulé plusieurs recommandations en ce sens qui pourraient être généralisées à tous les types de signalement[707]. L'amélioration des conditions de signalement devrait aussi permettre de collecter des données chiffrées sur les conditions de traitement de ces signalements ainsi que des suites qui leur sont réservées par les plateformes et les autorités compétentes pour évaluer l'efficacité du dispositif. C'est un élément important pour assurer le succès effectif de la régulation ;
- favoriser des design d'application moins gourmands en énergie[708] et encourager l'éco-conception et l'allégement des lignes de code (écocoding)[709].

Parmi ces paramètres, pourraient aussi figurer la mise en œuvre des obligations de **portabilité des données**, la simplification de la demande d'effacement des données et la possibilité de **rendre interopérables certains graphes sociaux**, ce qui permettrait aux utilisateurs de changer de services tout en conservant les liens

707 Recommandation n° 2019-03 du 15 mai 2019 du Conseil supérieur de l'audiovisuel aux opérateurs de plateforme en ligne dans le cadre du devoir de coopération en matière de lutte contre la diffusion de fausses informations.

708 Par ex., la consommation de bande passante induite par le visionnage d'une vidéo est beaucoup plus importante que celle de la simple écoute audio. Ainsi, l'utilisation de Youtube, comme simple lecteur mp3 sans besoin de la dimension mp4 est un véritable "mauvais usage" et gaspillage de ressources.

709 Rapport d'information du Sénat, *Pour une transition numérique écologique*, 9 juin 2020 p. 7, Au-delà de l'allégement des fonctionnalités des plateformes, c'est la structure même de celles-ci et de leurs applications qui pourraient être revues. En effet, dans la mesure où la capacité des ordinateurs à traiter de l'information rapidement croît sans cesse, les développeurs et les codeurs ne sont pas forcément encouragés à "alléger" les lignes de code.

précédemment tissés. S'agissant de l'interopérabilité des réseaux sociaux, une mise en œuvre progressive apparaît préférable, l'interopérabilité totale paraissant pour l'instant trop complexe voire problématique (*cf.* 2.4), même s'il ne faut pas exclure par principe sa généralisation à terme.

Des tutoriels, à l'instar de ce que fait la CNIL[710], pourraient être mis à disposition des utilisateurs pour apprendre à utiliser au mieux les fonctionnalités des plus grands réseaux et s'en protéger.

Les plateformes devraient être incitées à réaliser sur chacune de leur interface un **tableau de bord** résumant en permanence un certain nombre de données et les présentant de façon conviviale (le cas échéant standardisée grâce à une approche commune), à l'instar du tableau de bord d'une voiture, afin de permettre à l'utilisateur d'être mieux conscient de son mode d'utilisation de l'outil et de pouvoir, le cas échéant, le modifier :

- l'information sur les publicités reçues, leurs critères d'affichage (en vertu du DSA article 30), sur les données et traces personnelles recueillies et celles utilisées pour le profilage ;
- les choix de paramétrage permettant de réduire l'exposition aux publicités ainsi qu'aux calculs des algorithmes en contrôlant l'utilisation des données et traces personnelles (dans la prolongation du RGPD vers le traitement des traces), avec un bouton d'alerte (signalement) simple d'accès en cas d'exposition à des contenus indésirables ;
- le retour d'information sur l'activité de l'utilisateur concernant la durée d'utilisation, le volume, la fréquence et les délais de réactions (j'aime, partage, commentaires), la durée de lecture des *posts*, les thèmes, groupes et correspondants en contact les plus fréquents ;
- les choix de paramétrage permettant de contrôler sa propre réactivité (avec fixation de seuils et alertes, et le cas échéant avec des mécanismes de « ralentissement » à l'instar des limiteurs de vitesse dans une voiture) : ces actions devraient même pouvoir être testées voire jouées pour vérifier les effets de ses choix.

Dans la mesure du possible, la mention d'informations concrètes sur **l'impact environnemental**, notamment l'empreinte carbone liée à l'utilisation du réseau (notamment la durée d'utilisation, la fréquence des réactions et le type de contenu visionné) serait également très utile.

Ce tableau de bord devrait idéalement figurer dans **le code de bonne conduite** qui va s'élaborer sous l'égide de la **Commission européenne** (art. 35 du DSA). A terme, si les opérateurs n'amélioraient pas le design de leurs interfaces, il devrait être envisagé d'imposer la réalisation d'un tel tableau de bord ou de consacrer un droit au paramétrage : cela devrait être envisagé en étroite coopération avec la Commission européenne dans le respect du DSA, voire en le modifiant sur ce point si cela apparaissait indispensable.

710 CNIL, site internet, « configurer ses outils ».

A ce stade, la promotion de ces outils de paramétrage semble pouvoir être réalisée dans le cadre de la mise en œuvre du DSA. En effet, il est probable que l'analyse des risques par les très grandes plateformes, si elle est réalisée honnêtement, les conduise à découvrir des difficultés liées à la méconnaissance des fonctionnalités offertes par les interfaces, à leur mésusage voire à leur nocivité (*cf.* 2e partie). Or parmi les risques systémiques identifiés par le DSA figurent les effets négatifs sur les droits fondamentaux (dont le droit au respect de la vie privée), le discours civique et la santé. C'est ainsi que le paramétrage de certaines fonctionnalités par défaut peut se révéler très nocif notamment pour le respect de la vie privée des utilisateurs (compte paramétré ouvert par défaut). Il est possible également que les audits révèlent de telles difficultés. Aussi, dans le cadre de l'appui qui devrait être proposé par la France à la Commission européenne pour identifier les questions les plus sensibles et procéder à l'analyse des rapports de recommandation d'audit, **la question du paramétrage des interfaces et de leur design devrait figurer comme un point clé**.

Des lignes directrices établissant les exigences minimales de paramétrage pourraient être réalisées dans le cadre de la mise en œuvre du DSA. En attendant, le CEPD a publié le 14 mars 2022 des lignes directrices sur *les dark patterns* (littéralement « modèles sombres ») qui en identifient différents types (*overloading*[711], *skipping*[712], *stirring*[713], *hindering*[714], *fickle*[715], *left in the dark*[716]) et promeuvent des bonnes pratiques à destination des plateformes (utiliser les mêmes formulations sur l'ensemble du site, inclure un bouton retour pour faciliter la navigation, etc.[717]).

Une réflexion sur les mesures mises en œuvre par les opérateurs pour **limiter** « **la viralité** » **des contenus illicites ou préjudiciables** devrait aussi figurer dans la liste des sujets à expertiser. La « viralité » a un lien étroit avec les effets délétères sur le discours civique mais aussi sur la santé mentale des utilisateurs les plus exposés

711 Signifie que les utilisateurs sont confrontés à une avalanche/une grande quantité de demandes, d'informations, d'options ou de possibilités afin de les inciter à partager davantage de données ou à autoriser involontairement le traitement de données personnelles contre les attentes de la personne concernée.

712 Concevoir l'interface ou l'expérience utilisateur de manière à ce que les utilisateurs oublient ou ne pensent pas à tout ou partie des aspects liés à la protection des données. Les deux types de *dark patterns* suivants entrent dans cette catégorie : *Deceptive Snugness* (confort ou facilité trompeurs), *Look over there* (regarde par là)

713 Affecte le choix des utilisateurs en faisant appel à leurs émotions ou en utilisant des stimuli visuels. Les deux types de *dark patterns* suivants entrent dans cette catégorie : *Emotional Steering* (orientation émotionnelle), *Hidden in plain sight* (caché en plein jour)

714 Signifie que les utilisateurs sont entravés ou bloqués dans leur recherche d'information ou de gestion de leurs données ce qui rend l'action difficile ou impossible à réaliser.

715 Signifie que la conception de l'interface est incohérente et peu claire, ce qui rend difficile pour l'utilisateur de naviguer dans les différents outils de contrôle de la protection des données et de comprendre la finalité du traitement.

716 Signifie qu'une interface est conçue de manière à cacher des informations ou des outils de contrôle de la protection des données ou à laisser les utilisateurs dans l'incertitude quant à la manière dont leurs données sont traitées et au type de contrôle qu'ils pourraient avoir sur celles-ci en ce qui concerne l'exercice de leurs droits.

717 European Data Protection Board, « Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them », mai 2022.

et paraît donc bien rentrer dans les risques systémiques contre lesquels les très grandes plateformes vont devoir lutter en application du DSA. De tels dispositifs devraient en effet être liés au paramétrage des applications.

La promotion de ces instruments devrait être facilitée par la mise en œuvre d'outils d'information du grand public par les plateformes.

Proposition n° 3

Permettre à l'utilisateur d'opérer différents paramétrages ou réglages sur la plateforme afin de mieux se protéger des dangers des réseaux sociaux.

Promouvoir la réalisation de tableaux de bord informatifs pour améliorer la connaissance par l'utilisateur de ses modes de consommation.

Favoriser l'émergence de paramétrages par défaut qui protègent les droits des utilisateurs et respectent certaines conditions minimales de sécurité.

S'assurer que la mise en œuvre du DSA conduit à une attention particulière portée au design et au paramétrage des applications, notamment sur ceux qui permettent de limiter la « viralité » des contenus.

Faciliter l'information sur la plateforme utilisée pour mieux maîtriser son usage

L'utilisateur doit être en mesure de disposer d'éléments d'information sur les réseaux qu'il utilise. Une étude réalisée par Odoxa en février 2022, explique que seulement 21% des Français feraient confiance aux réseaux sociaux et 76% s'inquiéteraient pour la protection de leurs données personnelles. Il existe déjà des dispositifs intéressants comme le **cyber-score** et la **certification CNIL** qui permettent d'informer l'utilisateur sur le site, la plateforme ou le réseau social utilisés. L'ARCOM a également mis en place un dispositif intitulé **EOL** qui permet de vérifier très rapidement si les sites et les œuvres consultés sur les réseaux sont respectueux du droit d'auteur[718]. Le règlement DSA encourage en outre les très grandes plateformes à avoir recours à des **normes sectorielles volontaires sur des points particuliers**[719]. Il faut noter que, pour mettre en place ces normes sectorielles volontaires, les organismes certificateurs devront se tourner notamment vers les régulateurs. Les autorités françaises devraient donc, à la lumière des informations récoltées sur le terrain et des travaux de recherches réalisés, disposer de suffisamment d'éléments pour être en mesure de proposer à la Commission européenne des critères d'appréciation pertinents pour ces certifications.

La difficulté pourrait venir du **manque de lisibilité de ces nombreuses informations**. La puissance publique ou les régulateurs pourraient opportunément réfléchir à un dispositif d'information aisément accessible qui permette de **centraliser** l'ensemble des informations objectives sur les opérateurs. Un dispositif permettant à

718 ARCOM, site internet, Avec EOL, l'offre légale culturelle en un clin d'œil ».

719 Sur : « *la soumission électronique des notifications au titre de l'article 14 ; la soumission électronique des notifications par les signaleurs de confiance au titre de l'article 19, y compris par l'intermédiaire d'interfaces de programme d'application ; les interfaces spécifiques, y compris les interfaces de programme d'application, visant à faciliter le respect des obligations établies aux articles 30 et 31; l'audit des très grandes plateformes en ligne au titre de l'article 28 ; l'interopérabilité des registres de la publicité visé à l'article 30, paragraphe 2 ; la transmission de données entre les intermédiaires de publicité aux fins des obligations de transparence en vertu de l'article 24, points b) et c)* ».

l'utilisateur de rapidement saisir les fonctionnalités et critères principaux du réseau social de son choix pourrait être utile. Plusieurs types de dispositifs d'information du public (label, norme, score, certification), plus ou moins contraignants, peuvent être envisagés :

- un dispositif facultatif mis en place par un organisme certificateur privé qui établit un référentiel à l'aide des professionnels du secteur, des associations de consommateur, voire de la puissance publique ;
- un dispositif fondé sur un référentiel établi par les autorités compétentes, qui demeure toutefois facultatif et dont l'efficacité repose sur la logique « *name and shame* » ;
- un dispositif fondé sur un référentiel établi par les autorités compétentes et ayant un caractère obligatoire.

Il pourrait être utile de mettre en place un dispositif fondé sur un référentiel établi par une autorité compétente dotée d'un degré suffisant d'indépendance et présentant un caractère facultatif, permettant d'établir une forme de **diagnostic** d'un réseau social qui en ferait la demande. Un décret pourrait ainsi fixer le cadre de référence (les indicateurs) ainsi que l'autorité publique compétente pour délivrer ce label. A l'instar des tableaux qui figurent sur les emballages alimentaires et qui permettent de connaître le taux de glucides, de lipides, de conservateurs des aliments, **l'utilisateur serait ainsi informé du type de réseau qu'il utilise.** Le référentiel pourrait rassembler des **critères objectifs** comme la certification CNIL, la certification à d'autres normes notamment celles concernant le RSE (responsabilité sociétale des entreprises) ou les normes environnementales, l'hébergement des données au sein de l'Union européenne, le recours à des modérateurs maîtrisant la langue française, la possibilité pour l'utilisateur de supprimer la publicité, l'absence d'utilisation de *cookies* tiers, la possibilité de classer ses contenus par ordre chronologique et non par le biais d'algorithmes de recommandation, le recours à la publicité ciblée, etc.

Il pourrait aussi être établi en fonction d'indicateurs de performance : la contribution à la politique de réduction de l'impact carbone, la qualité du *design* du réseau, l'accessibilité du bouton de signalement des contenus, la qualité du service client pour l'exercice des recours, le nombre de modérateurs parlant la langue française proportionnellement à la quantité d'utilisateurs parlant le français, l'ouverture de négociation des CGU avec les associations, l'absence de cession des données à des tiers, etc.

A ce stade, il parait raisonnable de s'en tenir à un **dispositif facultatif fondé exclusivement sur des critères objectifs**. Ce chantier pourrait être mené sous l'égide de la DGCCRF. A moyen terme, lorsque l'Union européenne et la France auront suffisamment de recul sur la mise en œuvre du DMA et du DSA, une réflexion pourrait être menée sur la nécessité d'enrichir les dispositifs **de certification** d'autres critères ou de définir des indicateurs de performance. Dans la logique du *Ranking*[720] mis en œuvre dans les domaines financiers et environnementaux, une

720 Classement, notation, qui peut porter sur les résultats d'entreprises, d'institutions, de salariés en entreprise, en matière de performance, de fiabilité financière, énergétique, de durabilité

telle démarche nécessiterait, au niveau européen, une définition des paramètres précisant les éléments à prendre en compte et ceux qui ne doivent pas l'être[721].

Proposition n° 4 - Créer un dispositif facultatif d'information sur les réseaux sociaux maniable et facilement accessible pour les utilisateurs sous forme de label, de score ou de flash info à partir d'un référentiel commun.

Faciliter les signalements, l'accès et l'exercice effectif des droits et l'accompagnement des victimes en ligne

Les utilisateurs peuvent être victimes de comportements malveillants sur les réseaux sociaux ou constater des pratiques illégales sans savoir vers qui se tourner, comment porter plainte ou aider les victimes. Par ailleurs, les utilisateurs détiennent des droits consacrés par des normes, telles que le RGPD (droit à l'effacement et à la portabilité des données), qui, en pratique, sont très insuffisamment respectées par les plateformes tout en faisant l'objet de peu de plaintes des intéressés. La question de l'accessibilité des dispositifs de plainte ou de signalement apparaît donc très importante. Le DSA impose aux plateformes une obligation de signalement aux autorités répressives ou judiciaires de l'État membre ou des États membres concernés (art. 15 du DSA). Ainsi, dès lors qu'une plateforme sera informée qu'une personne est victime d'un harcèlement susceptible de la mettre en danger, le signalement à la plateforme l'obligera à agir et, le cas échéant, à saisir les autorités compétentes de l'État concerné.

Comme il a été rappelé dans la première partie de la présente étude, le **signalement** est un élément central dans l'ensemble du dispositif pour éviter que les plateformes ne se réfugient derrière leur statut d'hébergeur. Il est un point d'appui majeur pour rendre effectives les obligations de régulation. Leur nombre permet aussi d'identifier les risques systémiques et de faire intervenir le régulateur établi par le DSA. Il est donc essentiel que, tant les victimes que les témoins de faits illicites sur les réseaux sociaux, connaissent les dispositifs existants et soient orientés vers eux.

Or, **la lisibilité actuelle du dispositif de plainte et de signalement n'est pas satisfaisante**. En effet, il comprend de nombreuses portes d'entrée. L'utilisateur peut signaler des faits auprès de la CNIL, en principe lorsque la législation sur les données personnelles est méconnue ; il peut saisir la plateforme Pharos ou *pointdecontact.net* pour signaler un contenu illicite ; il peut se rendre sur le site de la DGCCRF ou utiliser *Signal conso* pour signaler une fraude ou un comportement relevant du contrôle de la DGCCRF (voire de l'ANSSI s'il s'agit d'une entreprise victime de cyberattaques) et, bientôt, il pourra opérer un signalement auprès de l'ARCOM si une plateforme ne remplit pas ses obligations issues du DSA, notamment si de fausses informations susceptibles de troubler l'ordre public ou d'altérer la sincérité du scrutin sont suspectées ou qu'elle laisse prospérer des contenus contrefaits ; s'il est victime de malveillances, il peut se rendre sur le site *cybermalveillance.*

721 Directive n° 2003/125/CE de la Commission du 22 décembre 2003 et règlement (CE) n° 1060/2009 du Parlement européen et du Conseil sur les agences de notation de crédit du 16 septembre 2009 (« CRA 1 »), modifié par le règlement (UE) n° 513/2011 du 11 mai 2011 (« CRA 2 ») et le règlement (UE) n° 462/2013 du 21 mai 2013 (« CRA 3 »).

gouv.fr qui informe sur les menaces numériques et les moyens de s'en protéger et peut réaliser un diagnostic en ligne permettant en principe de le conseiller et de l'orienter (des kits de communication et des bonnes pratiques notamment sur l'usage des réseaux sociaux sont également proposés[722]) : ce dispositif est géré par le GIP Action contre la cybermalveillance (ACYMA[723]) mis en place dans le cadre de la stratégie numérique du Gouvernement.

Dans **ce qui ressemble un peu à un labyrinthe**, l'accompagnement de l'utilisateur et sa familiarisation avec un **guichet unique apparaît souhaitable**. Même si la qualité de chacune de ces différentes plateformes n'est pas en cause, force est de constater qu'elles offrent aux utilisateurs un paysage trop fragmenté et que la **coordination** entre elles demeure perfectible. De nombreux acteurs du numérique déplorent d'ailleurs une perte de temps dans les réorientations des signalements. Si *cybermalveillance.gouv.fr* a été conçu comme une forme d'assistant central aux victimes et offre un dispositif plutôt performant, il n'est pas suffisamment identifié par les utilisateurs et ne fait pas le lien avec l'ensemble des dispositifs. Il conviendrait soit de le ré-agencer pour en faire un véritable guichet unique et lui assurer une publicité suffisante auprès des internautes soit de créer un véritable point d'entrée unique, disponible sous la forme **d'une application** ayant une appellation commune (*Alerte.Net* par exemple) permettant **de recueillir les signalements et de les aiguiller**. Ce guichet unique pourrait aussi centraliser les informations sur les différentes plateformes et les dispositifs d'accompagnement des victimes de harcèlements ou de propos haineux en ligne. Ce dispositif n'empêcherait pas les utilisateurs de signaler directement les faits aux administrations concernées ni de déposer des plaintes pour faire valoir leurs droits s'ils le souhaitent.

Par ailleurs il serait souhaitable de faire figurer dans les audits les mesures de minimisation des risques mises en place par les plateformes, les solutions mises en œuvre par les plateformes pour rendre effectif l'exercice des droits des usagers reconnus par les normes européennes, notamment celui à **l'effacement des données.**

Proposition n° 5

Repenser la coordination entre les différentes plateformes de signalement et créer un point d'entrée unique pour faciliter l'exercice des droits et mieux accompagner les victimes.

Développer une application à télécharger sur les smartphones.

722 Gouvernement, site internet cybermalveillance.gouv.fr, « La sécurité sur les réseaux sociaux ».

723 Le groupement d'intérêt public ACYMA regroupe des acteurs étatiques impliqués tels que l'Agence nationale de la sécurité des systèmes d'information (ANSSI) qui relève des services du Premier ministre, le ministère de l'intérieur, le ministère de la justice, le ministère de l'économie et des finances, le secrétariat d'État en charge du numérique et le ministère des armées. À leurs côtés sont également rassemblés de nombreux acteurs de la société civile comme des associations de consommateurs ou d'aides aux victimes, des représentations professionnelles de type fédération ou syndicat, des assureurs, des opérateurs, des éditeurs. En 2022, ACYMA est fort d'une cinquantaine de membres.

3.1.3. Le rééquilibrage par la connaissance : accès, information et éducation aux réseaux sociaux

S'assurer d'un accès effectif des chercheurs aux données et aux algorithmes

Si les algorithmes sont au cœur du modèle des réseaux sociaux et doivent donc être compris des régulateurs, l'idée que les dangers des réseaux sociaux viennent davantage des paramétrages humains que de la technologie fait désormais consensus auprès des chercheurs[724]. Partant, le débat autour de la transparence des algorithmes a été affiné et dorénavant c'est d'abord « **l'explicabilité** » (pendant et après l'apprentissage) et **l'accessibilité aux données d'apprentissage** qui apparaissent utiles. En effet, les concepteurs d'algorithmes utilisent des jeux de données annotées pour donner une information à la machine et lui dire ce qu'il convient de comprendre. La compréhension devient plus complexe avec l'*e-learning* et la question se pose alors du niveau d'explicabilité des inventions techniques à exiger au sein d'une société démocratique[725]. Si réguler un algorithme n'a guère de sens, réguler les pratiques algorithmiques et responsabiliser les concepteurs est au contraire souhaitable.

Pour cette raison et parce que l'accès à ces données est une clé de la réussite de la régulation des plateformes, le DMA et le DSA comportent plusieurs dispositions qui obligent les très grandes plateformes à donner accès à certaines données. L'article 6 (i) du DMA prévoit notamment l'obligation pour les *gatekeepers* de fournir gratuitement aux entreprises utilisatrices un accès aux données agrégées et non agrégées, y compris les données personnelles, qui sont fournies ou générées dans le cadre de l'utilisation des services offerts, moyennant certaines conditions. La voie vers l'accessibilité totale n'est cependant pas d'actualité, les plateformes ayant avec succès opposé la nécessité de ne pas porter atteinte au secret des affaires (mais l'on peut s'étonner que le législateur ait admis qu'une telle objection puisse être opposée à un régulateur, généralement habitué à préserver la confidentialité de données dans des domaines très sensibles comme les produits de santé). Un consensus a néanmoins été trouvé pour ouvrir le plus largement possible l'accès aux données pour les chercheurs agréés, dans des conditions sécurisées.

Le DSA est construit sur une logique de responsabilisation des opérateurs et de supervision par des régulateurs. Il impose aux opérateurs des obligations de résultat, à charge pour eux de prendre les mesures qu'ils estiment adéquates pour les atteindre, le régulateur ayant la charge de vérifier que tel est bien le cas. De nombreuses **obligations de transparences** sont fixées[726] et l**'accès aux données**

724 A. Jean, *Les algorithmes font-ils la loi*, Édition de l'observatoire, 2021.

725 Aurélie Jean plaide pour l'élaboration d'algorithmes hybrides, qui intègrent le sujet de l'explicabilité dès la conception voire au sein même du modèle, et la mise en place de tests massifs de manière continue.

726 Ces obligations portent notamment sur les activités de modération de contenu (art. 13) et, s'agissant des plus grandes plateformes, sur la mise en œuvre du rapport d'audit (art. 33), sur les principaux paramètres utilisés dans les systèmes de recommandation (art. 29) et de façon plus générale, sur les données nécessaires pour contrôler et respecter le DSA (art. 31). Il conviendra de s'assurer que les informations sollicitées permettent réellement d'exercer un contrôle pertinent Des obligations de transparence visent également la publicité en ligne puisque l'art. 24 impose à toutes les plateformes de permettre aux utilisateurs d'identifier l'annonceur et les paramétrages utilisés dans le

des plateformes sur leurs pratiques de recommandation des contenus, d'une part, et de modération des contenus, d'autre part, apparaît comme **un élément essentiel de la réussite du DSA.** S'agissant **des très grandes plateformes**, c'est à la Commission européenne qu'il appartiendra *in fine* de les évaluer et d'engager le cas échéant des procédures de sanctions si elles n'étaient pas respectées. L'article 31 du DSA oblige les très grandes plateformes à transmettre au coordinateur des services numérique (CSN) de l'État de leur établissement ou à la Commission, sur demande motivée, les données nécessaires pour « *contrôler et évaluer le respect* » du DSA. Ce même article prévoit que les plateformes devront permettre aux chercheurs agréés par les autorités de l'État dans lequel elles ont leur établissement d'accéder aux données « *aux seules fins de mener des recherches qui contribuent à la détection, l'identification et la compréhension des risques systémiques* ». Il faut préciser que le DSA prévoit que les chercheurs pourront soumettre leur demande d'agrément au CSN de l'État membre de l'organisme de recherche auquel ils sont affiliés, lequel vérifiera les critères et transmettra le cas échéant la demande au CSN de l'établissement de la plateforme. Ces accès devront être facilitées par la mise en place d'interfaces appropriées.

Il serait souhaitable que des chercheurs appartenant à des organismes français soient agréés par les CSN des États d'établissement des très grandes plateformes, c'est-à-dire celui du Luxembourg et surtout celui de l'Irlande. L'accès à ces données de chercheurs qualifiés et indépendants est en effet un élément clé de la réussite du DSA. Les États membres pourront apporter leur concours à la Commission pour identifier les données à solliciter et pour mettre en place les organisations qui permettront aux chercheurs agréés d'accéder aux données dans des conditions sécurisées. Les autorités françaises devraient mettre en œuvre une politique volontariste dans ce domaine clé pour la réussite du DSA. Une coopération entre les chercheurs, voire certaines ONG[727], et les régulateurs devrait être réalisée pour affiner les critères d'évaluation et faire remonter à la Commission les informations qui lui permettront de jouer efficacement son rôle de régulateur des très grandes plateformes.

L'accès des chercheurs agréés aux données des très grandes plateformes n'épuise pas le sujet concernant les autres plateformes. A cet égard, **une politique volontariste** devrait être mise en place au niveau national en lien avec les universités et le CASD[728] afin d'offrir un cadre sécurisé à ces travaux. Le monde universitaire déplore l'insuffisant accès aux données des plateformes pour permettre de fournir des travaux d'évaluation, de prospection et d'analyse des réseaux sociaux. Il est en effet indispensable que la recherche soit en mesure d'étudier ces nouvelles dynamiques et de développer des outils et approches indépendants afin de les éclairer. Afin de promouvoir cette ouverture à la recherche, l'ARCOM vient de lancer une **grande consultation publique sur l'accès aux données des plateformes en ligne pour la recherche**. L'idée est de « *mener une réflexion sur le rôle que peut jouer la puissance publique pour aider le monde de la recherche à se saisir pleinement de ces problématiques.* » Ce rôle de facilitateur doit plus particulièrement s'exprimer dans

ciblage, et, pour les plus grandes plateformes, de tenir un registre contenant les informations sur les publicités et les annonceurs (art. 30).

727 Les ONG peuvent par exemple être la quadrature du net, Algorithm Watch, Algo transparency.

728 Centre d'Accès Sécurisé aux Données.

l'exploitation et l'analyse des données issues des réseaux sociaux ou des services de plateformes en ligne et qui conditionnent le développement des connaissances propres aux environnements numériques. « *L'enjeu de la bonne exploitation de ces données est double : il s'agit à la fois de pérenniser un écosystème de recherche dynamique, effectif et durable, capable de générer de la connaissance au bénéfice de tous (production scientifique), mais également de contribuer à l'expertise du régulateur dans son évaluation des dispositifs mis en œuvre par les opérateurs de plateformes pour satisfaire à leurs obligations telles que de la modération des contenus haineux (régulation de la transparence).* »[729]. **Cette initiative devrait être soutenue et promue**. Elle semble très complémentaire des dispositions contraignantes prévues par le DSA. A terme, en cas de difficulté d'accès aux données des plateformes non concernées par l'article 31 du DSA, il ne faut pas exclure d'envisager que le DSA soit complété sur ce point pour garantir cet accès aux informations.

Proposition n° 6

Soutenir l'agrément de chercheurs issus de la recherche française par les coordonnateurs des services numériques des États d'établissement des très grandes plateformes ainsi que leur accès effectif aux données de ces plateformes.

Apporter une assistance à la Commission européenne pour identifier les données à solliciter pour s'assurer du respect effectif du DSA.

Améliorer l'accessibilité et la lisibilité du droit

Comme cela a été souligné dans la première partie de la présente étude, le droit des plateformes et notamment des réseaux sociaux est à la fois riche et divers. Mais au fil des années, cette accumulation de normes (*cf.* le nombre de textes actuellement en cours d'élaboration dans les institutions de l'Union) le rend difficile d'accès voire illisible, même pour des professionnels du droit. Mobilisant de façon transversale de nombreuses règles sectorielles, sa construction en silos engendre des effets négatifs (risque de redondances ou contradictions des normes) et dessert sa lisibilité et son effectivité. En effet, certains problèmes soulevés dans un domaine peuvent trouver des réponses dans des règles d'un autre secteur et vice versa.

A moyen terme, un travail de **codification du droit européen des plateformes** devrait être engagé, afin de mettre à plat les normes applicables et de régler les incohérences, la codification au niveau européen se faisant généralement dans une logique de refonte. Ce projet ambitieux serait très utile. A court terme, une première étape devrait être **la réalisation d'une compilation des règles applicables**, qui faciliterait l'accessibilité de ces normes et leur donnerait une meilleure lisibilité et permettrait en outre de mieux identifier les complémentarités, les incohérences voire les vides. Cette compilation pourrait être réalisée à tout le moins au niveau national : elle aurait le mérite de réunir dans un même document, facilement accessible, l'ensemble des normes applicables, ce qui faciliterait leur appropriation par les différents acteurs comme leur compréhension et finalement leur application

729 ARCOM, site internet, « Consultation publique sur l'accès aux données des plateformes en ligne pour la recherche ».

effective. La réalisation d'un tel exercice au niveau européen aurait également le mérite de faire le point sur la législation abondante existante et de faciliter le partage de savoir entre les acteurs des différents champs concernés.

Par ailleurs, de nombreuses administrations ou entreprises se sont dotées de documents internes relatifs à l'utilisation d'internet en général et des réseaux sociaux en particulier par leurs agents et leurs personnels. Pour favoriser une certaine harmonisation notamment en promouvant les meilleures pratiques, l'élaboration **de lignes directrices** par le ministère chargé du travail, d'une part, et par le ministère chargé de la fonction publique, d'autre part, pourrait fournir un guide utile pour les entreprises et les administrations. Cela permettrait d'éviter les règlements intérieurs ou chartes trop contraignants, d'harmoniser les pratiques et de proposer un seuil minimal de protection de la vie privée. Cela permettrait également d'améliorer la connaissance par les utilisateurs de leurs droits et devoirs, notamment eu égard à **l'articulation entre leur vie professionnelle et leur vie privée**.

Proposition n° 7

Réaliser au niveau national une compilation des textes européens et nationaux applicables aux plateformes afin de rendre le droit des plateformes plus accessible et d'améliorer la qualité des futures normes. A terme, au niveau européen, engager un travail de compilation puis de codification de ces textes.

Au niveau national, adopter des lignes directrices sur l'usage des réseaux sociaux dans la vie professionnelle afin d'offrir aux administrations et aux entreprises ainsi qu'aux utilisateurs qui y travaillent un guide des pratiques relatives notamment à l'articulation vie privée-vie professionnelle.

Favoriser les contenus ayant fait l'objet de vérification et garantir une assise citoyenne à la question de la qualité du débat public

Il parait difficile d'imposer aux plateformes le respect du principe du pluralisme dès lors qu'elles ne sont pas des médias et parce que cela pourrait être assimilé à une forme de censure puisque la grande majorité des contenus est produite par les utilisateurs eux-mêmes. Reste que le phénomène de polarisation que facilite l'effet de bulle produit par les réseaux sociaux inquiète de nombreux observateurs et l'addiction au *like* peut entrer en contradiction avec la logique de confrontation d'idées différentes que suppose une société ouverte fondée sur le débat.

La Commission européenne a d'ailleurs récemment publié un code de conduite contre la désinformation qui promeut la lutte contre les faux comptes ainsi que les moyens technologiques permettant de « *privilégier les informations pertinentes, authentiques et faisant autorité dans les recherches, les flux ou d'autres canaux de distribution faisant l'objet d'un classement automatique* »[730]. L'application de ce code commence à permettre le recueil de données mais elles sont encore très générales. C'est ainsi que l'on sait qu'en 2021 les opérateurs ont supprimé 62,5% des contenus signalés contre 71% en 2020 et 2019[731].

730 Commission européenne, *Le Code de pratiques de 2022 sur la désinformation*, 16 juin 2022.

731 Commission européenne, « *Code de conduite de l'UE contre les discours de haine en ligne: les résultats restent positifs mais les progrès ralentissent* », 7 octobre 2021.

Dans les suite des réflexions menées notamment par le CNNUM[732], la commission Bronner et l'ARCOM dans le cadre du *Médium Freedom Act*, deux types de pistes peuvent être explorées.

D'une part, il faut souligner que des **actions concrètes** permettent d'ores et déjà **de modérer de façon adaptée des discussions pour faciliter des débats éclairés et constructifs et de promouvoir des contenus vérifiés.** S'agissant des actions qui visent à éprouver la véracité de l'information, on pourrait également s'inspirer des pratiques des *fact checkers* ou de la charte de fonctionnement de l'encyclopédie en ligne Wikipédia. En effet, celle-ci, afin d'assurer un bon niveau de qualité, exige que les sources soient renseignées et le cas échéant informe le lecteur de leurs insuffisances. La validation par les membres des réseaux sociaux des contenus répondant à des critères de qualité pourrait donc être expertisée (sources citées, liens d'intérêts signalés, etc.). Il pourrait aussi être utile de réfléchir à la façon de mettre en valeur des contenus provenant d'éditeurs professionnels ou d'organismes de documentation publics (la DILA, la BNF, etc.) sans pour autant créer de concurrence déloyale. Ces réflexions devraient associer les plateformes qui testent régulièrement des dispositifs. Twitter vient ainsi d'annoncer qu'il allait afficher des avertissements sur des *tweets* jugés trompeurs dans le cadre de sa politique de lutte contre la désinformation[733].

Des organismes privés se sont d'ores et déjà lancés dans la voie de la **certification de certains médias** (et non des contenus). Par exemple, la *Journalism trust initiative* (JTI) lancée par Reporters sans frontières en 2020 est « un label »[734] conçu sur le modèle des normes ISO, en faveur de la transparence et contre la désinformation. Il prend notamment en compte des critères tels que l'application d'une ligne éditoriale ou encore l'existence de mécanismes de correction, ou de garanties professionnelles au sein du média. Ce label se présente sous forme d'un rapport de transparence que remettent les médias et par un audit externe. Cette forme d'auto-régulation est prometteuse dans la mesure où elle s'attache au processus interne d'élaboration de l'information délivrée par les médias, c'est-à-dire à leur organisation interne et aux garanties qu'elle offre en termes de sérieux de l'information délivrée, et non aux contenus publiés au cas par cas.

En 2020, le Forum pour l'information et la démocratie lancé à l'initiative de Reporters sans frontières dans l'esprit de transposer l'action du GIEC en matière climatique aux enjeux de pluralisme et d'accès à l'information, proposait de lancer un groupe de travail sur les possibilités d'élargir et de consolider un dispositif de certification dans le prolongement de la JTI. L'échelon européen apparaît comme le plus à même de porter de telles réflexions sur une potentielle labellisation des réseaux sociaux. Le *media freedom act* ou « loi européenne sur la liberté des

732 CNNUM, site internet, « Pour un numérique au service du savoir ».

733 *Le siècle digital*, 20 mai 2022. Twitter annonce sa nouvelle politique pour lutter contre la désinformation. « *Pour prévenir ses utilisateurs, le géant des réseaux sociaux va mettre en place un système similaire au signalement d'images à caractère explicite. Un message d'avertissement s'affichera avant le tweet indiquant que ce dernier a enfreint les règles de Twitter concernant la propagation de fausses informations. L'utilisateur aura quand même la possibilité de lire le tweet en cliquant sur un bouton pour y accéder. Les retweets, les likes et les commentaires seront désactivés afin de ne pas pouvoir le partager. De plus, ces publications ne seront pas mises en valeur par l'algorithme.* »

734 Reporters sans frontières, site internet, « Journalism Trust Initiative ».

médias », initiée fin 2021 par la Commission européenne[735], apparaît un cadre intéressant pour ce chantier. Dans la mesure où ce projet de réglementation vise à renforcer la liberté, l'indépendance éditoriale et le pluralisme des médias, permettant aux citoyens de se forger une opinion libre et éclairée à même de contribuer à un débat démocratique riche et respectueux des opinions de chacun, il apparaît opportun d'intégrer les réseaux sociaux dans le champ d'application du texte et d'y inscrire le débat sur une potentielle certification (selon quels critères, quelle évaluation, quelle publicisation auprès des européens et européennes, etc.).

D'autre part, **une consultation citoyenne** sur le type de débat public que les citoyens souhaitent avoir en France à l'heure du numérique et des réseaux sociaux pourrait être organisée. La question de l'opportunité de disposer de réseaux sociaux reconnus comme participant d'une mission de service public pourrait lui être soumise (au sens de l'article 7 *bis* de la directive SMA, qui permet l'identification des médias qui promeuvent le pluralisme, la liberté d'expression et la diversité culturelle : « *Les États membres peuvent prendre des mesures afin d'assurer une visibilité appropriée pour les services de médias audiovisuels d'intérêt général.* »). Si l'idée d'un réseau social public ne semble à ce stade pas réaliste, la question de reconnaître un ou plusieurs réseaux sociaux participant de la mission d'intérêt général de pluralisme et de garantie d'un débat public de qualité se pose : une certification, le cas échéant avec un référentiel établi au niveau de l'Union européenne dans le cadre d'un DSA phase 2, permettant de garantir aux utilisateurs le sérieux et la qualité de l'information, sans préjudice de la ligne éditoriale de chacun, pourrait être envisagée.

S'il existe des structures spécifiques, comme le Comité national pilote d'éthique du numérique (CNPEN[736]), la *Commission supérieure du numérique et des postes* ou l'observatoire de la haine en ligne placé auprès de l'ARCOM (dédié, comme son nom l'indique, à la lutte contre la haine en ligne) ainsi que des acteurs de la société civile (Renaissance numérique, La Quadrature du Net, etc.) qui fournissent de façon habituelle une regard précieux sur les problématiques soulevées par les réseaux sociaux, le **Conseil national du numérique** dispose d'une place particulière dans le paysage institutionnel puisque, mêlant des spécialistes du numérique de tous horizons, il participe au débat public par ses réflexions et se fait l'écho de la société civile. Afin de mieux associer les citoyens et la société toute entière à l'encadrement des usages des réseaux sociaux, le rôle du Conseil national du numérique (CNNUM) pourrait être renforcé et davantage envisagé comme **lieu permanent de confrontation des idées de la société civile et de la recherche** et comme contre-point aux actions administratives du Gouvernement et des AAI. Cela permettrait l'animation d'un véritable dialogue démocratique permanent sur le numérique et les réseaux sociaux. Sorte d'États généraux permanents du numérique, il conviendrait de renforcer, d'une part, ses moyens pour lui

735 V. not. le discours d'Ursula Von der Leyen, présidente de la Commission européenne, sur l'état de l'Union (septembre 2021)

736 Placé sous l'égide du Comité consultatif national d'éthique (CCNE), son objectif est « *à la fois de remettre des premières contributions sur l'éthique du numérique et de l'intelligence artificielle et de déterminer les équilibres pertinents pour l'organisation du débat sur l'éthique des sciences et technologies du numérique et de l'intelligence artificielle* ».

permettre de fournir, de façon pérenne, des expertises de qualité et, d'autre part, son indépendance en prévoyant par exemple que ses membres soient nommés par plusieurs autorités (Parlement, Gouvernement, AAI, société civile, syndicats, universités, etc.). Une concertation pourrait rapidement être organisée sur la qualité du débat public à l'heure des réseaux sociaux.

Proposition n° 8

Soutenir les labels permettant de promouvoir des contenus fiables, de qualité et vérifiés.

Renforcer le rôle du CNNUM pour animer la concertation citoyenne sur les questions relatives aux usages des réseaux sociaux et initier une concertation sur la question de la qualité du débat public à l'heure des réseaux sociaux.

Renforcer les actions éducatives et de formation tout au long de la vie pour mieux maîtriser l'usage des réseaux sociaux

La meilleure arme pour utiliser à plein les effets positifs des réseaux sociaux et lutter contre leurs effets négatifs, qui est aussi la plus longue à porter ses fruits, demeure celle de **l'éducation et de la formation.** De nombreuses actions sont d'ores et déjà menées, notamment par les services du ministère de l'éducation nationale et les autorités de régulation, qui mettent à disposition des ressources pédagogiques[737] voire se sont dotées de pôles dédiés (la CNIL, par exemple, dispose d'un pôle éducation au numérique). Des actions de sensibilisation à l'utilisation des données personnelles sont également conduites. Ces actions sont indispensables et doivent être poursuivies voire renforcées et élargies.

• *Développer les actions pédagogiques à destination de tout public*

Si d'excellentes préconisations faites par de récents rapports méritent d'être reprises comme par exemple celles de la commission « Les Lumières à l'ère du numérique » (dite Commission Bronner), ou celles de la Commission nationale consultative des droits de l'homme (CNCDH), et que de nombreux acteurs, comme l'éducation nationale ou certains régulateurs, sont très actifs sur ces sujets, il faut encore aller plus loin.

Il conviendrait tout d'abord d'accentuer les mesures concernant **l'éducation à l'information et à la communication**. Aiguiser le sens critique, distinguer ce qui relève de l'opinion et du fait, prendre du recul par rapport à l'immense miroir déformant des réseaux sociaux, ne pas se laisser abuser par les *fake news*, être en mesure de se référer à des sources d'informations sûres, savoir réagir face à des contenus haineux, tout cela suppose un apprentissage.

Les connaissances en matière **d'éducation aux médias et à l'information (EMI)** et de pédagogie de l'esprit critique existent mais il faut correctement les mobiliser. La commission Les lumières à l'ère numérique sous la présidence de Gérald Bronner

737 L'Hadopi dorénavant ARCOM explique comment sécuriser ses accès à internet, utiliser un logiciel de contrôle parental, et met à disposition des personnels enseignants un kit pédagogique. V. ARCOM, site internet, rubrique « securiser-ses-acces-internet » et rubrique « education-et-sensibilisation ».

a demandé à ce que cette question soit déclarée « Grande cause nationale ». Apporter aux enseignants une formation adéquate à l'instar de ce qu'est en train de préparer le ministère de l'éducation nationale (PIX enseignant), faire venir des intervenants extérieurs, établir des kits pédagogiques, impliquer les jeunes en organisant des ateliers de co-création, leur apprendre à créer des réseaux sociaux internes aux écoles à l'instar des webradios[738] sont autant d'actions qui méritent d'être poursuivies et menées. A l'instar des présentations ludiques retenues par la CNIL pour sensibiliser les individus à la réutilisation des données personnelles ou de ce qui est proposé par le site cybermalveillance.gouv.fr pour sensibiliser les jeunes en fonction de leurs âges aux risques que comporte un usage mal maîtrisé d'internet[739], un jeu vidéo à vocation pédagogique (*serious game*) pourrait être réalisé pour montrer toutes les fonctionnalités qui existent sur les réseaux sociaux, comment s'en saisir pour se protéger au mieux. Il pourrait être aisément accessible sur la plateforme et l'application dédiée aux signalements et à l'information des individus (*cf.* proposition n° 3). Les actions de formation envers les enseignants devraient aussi avoir pour objectif de les sensibiliser à l'orientation des élèves vers des contenus de qualité, par exemple en promouvant la plateforme CulturPrime, crée en 2018 par les six groupes de l'audiovisuel public ayant pour objectif de rendre la culture accessible à un jeune public[740].

S'agissant de la **détection des fausses informations et de l'éducation aux médias**, le CSA avait répertorié, dans son rapport relatif à la lutte contre la diffusion des fausses informations de 2020, **les mesures prises par les opérateurs pour aider les internautes à identifier les contenus pertinents et fiables** (mise en avant d'informations « *fact checkées* », système d'évaluation des contenus par des codes couleurs), pour former les usagers à l'usage des plateformes et à l'identification des contenus (campagnes pour l'EMI, soutien financier, campagnes pendant les élections pour sensibiliser les jeunes) et pour apporter des aides à la recherche. Il avait cependant noté que les plateformes étaient encore trop peu nombreuses à s'investir sur les questions d'information et de bon usage, que beaucoup n'agissaient que vers les jeunes, que très peu de données lui étaient fournies sur l'impact des usages sur les comportements des utilisateurs et que les rapports avec le secteur de la recherche étaient insuffisants s'agissant de l'exploitation des données. Au terme de son analyse, il invitait les opérateurs à développer des approches multidimensionnelles en matière d'EMI, à nouer des partenariats pluriannuels, à évaluer l'impact de leurs actions et à bâtir avec le monde de la recherche des protocoles opérationnels de partage des données et d'exploitation transparentes de ces dernières.

738 Centre pour l'éducation aux medias et à l'information (CLEMI), site internet, « Carte-des-medias-scolaires-recensant-les-webradios ».

739 Gouvernement, site internet www.cybermalveillance.gouv.fr, « Accompagnement et sensibilisation des jeunes ».

740 Chaque jour sont produites et postées par chacun des partenaires, dans l'univers numérique et sous une même identité graphique, des vidéos culturelles et de connaissances, éditorialisées au fil de l'actualité. Ce réseau de production et de partage fédère également des programmes issus de plusieurs institutions culturelles telles que La Bibliothèque nationale de France, la Comédie-Française, le Centre Pompidou, le Louvre, l'Opéra de Paris, le Festival d'Avignon etc. La plateforme annonce en moyenne 1,4 million de personnes chaque jour qui voient au moins une de ses publications sur Facebook et une communauté de plus de 240 000 abonnés qui lui sont fidèles.

A cet égard, il faut souligner la pertinence **du dispositif EDMO**, projet lancé en 2020, financé par l'Union européenne, qui vise à analyser et lutter contre la désinformation en ligne. Consortium dirigé par l'Institut universitaire européen de Florence (Italie), il comprend la société *Athens Technology Center* de Grèce, l'Université Aahrus du Danemark, et l'organisation de vérification des faits *Pagella Politica* d'Italie. Il se décline ensuite sous forme de *hub* nationaux, notamment en France sous le nom de Defacto[741] qui rassemble l'AFP, le médialab Sciences po Paris, le centre pour l'éducation aux médias et à l'information (CLEMI) et XwikiSAS (une entreprise européenne indépendante éditant des solutions en *open source*).

D'autres actions peuvent être menées pour sensibiliser les utilisateurs à leur statut de victime potentielle afin de les conduire à mieux faire valoir leurs droits, notamment à la protection de leurs données personnelles[742]. Des actions d'information pourraient également être menées pour apprendre à mieux utiliser toutes les fonctionnalités offertes par les interfaces, dont certaines permettent de se protéger efficacement (bloquer des comptes, supprimer la publicité, etc.) Des actions de sensibilisation doivent aussi être menées dans les écoles pour apprendre aux enfants à se comporter de la même façon dans la vie « virtuelle » que dans la vie réelle. Les propositions faites plus haut concernant la lisibilité des informations sur les réseaux sociaux et le débat citoyen sur le pluralisme participent aussi de la politique d'éducation et de sensibilisation des citoyens aux réseaux sociaux.

Par ailleurs, **un travail d'initiation** à ces nouveaux modes de communication doit pouvoir être offert auprès des **personnes les plus vulnérables et des personnes âgées qui risquent l'isolement.**

- *Mettre en place un pilotage unifié*

Comme l'a souligné la commission Bronner, les initiatives sont multiples mais dispersées et peu articulées entre elles : elle préconise ainsi la création d'une cellule interministérielle dédiée. Pour une mobilisation générale et transversale impliquant tous les ministères (notamment éducation, culture, recherche) et tous les acteurs (ARCOM, CNIL, etc.), il serait souhaitable d'identifier et de **confier son pilotage à un service ministériel voire interministériel** qui pourra exercer la fonction **d'interpellation et d'impulsion** indispensable à toute politique publique (v. proposition 12).

Sensibiliser au coût environnemental des réseaux sociaux

Outre la question du coût environnemental des conditions de fabrication des outils numériques, l'idée de faire un usage écologiquement plus responsable du numérique fait son chemin. Récemment la *LCEN* a été modifiée pour prévoir que les personnes, dont l'activité est d'offrir un accès à des services de communication au public en ligne, informent également leurs abonnés de la quantité **de données consommées** dans le cadre de la fourniture d'accès au réseau et indiquent l'équivalent des émissions de gaz à effet de serre correspondant[743].

741 https ://defacto-observatoire.fr/Main/#.

742 CNIL, LINC, *Scènes de la vie numérique*, Cahier n° 8, 12 avril 2021.

743 Art. 6 1. bis de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique modifiée par la loi n° 2022-299 du 2 mars 2022.

Compte tenu de l'impact écologique des réseaux sociaux et de la méconnaissance qui entoure encore trop souvent cette problématique – alors qu'il est très connu s'agissant d'autres secteurs comme le transport, l'élevage ou le textile – il semble indispensable de poursuivre dans cette voie et de sensibiliser à grande échelle les utilisateurs. La nécessité de mener à bien de telles actions est notamment prévue par le chapitre 1er de la *loi du 15 novembre 2021 visant à réduire l'empreinte environnementale du numérique en France*. Cette loi vise, dans ses trois premiers articles, à user le **levier de l'éducation et de la formation des ingénieurs** pour mener à bien cette sensibilisation. Cette loi a également créé **un observatoire des impacts environnementaux du numérique** chargé d'analyser et quantifier les impacts directs et indirects du numérique sur l'environnement, de même que la contribution apportée par le numérique, notamment l'intelligence artificielle, à la transition écologique et solidaire (article 4). L'ARCEP va prochainement mettre à disposition du public un "baromètre environnemental" s'appuyant sur la plateforme de travail "pour un numérique soutenable". Quant à l'ARCOM, en lien avec l'ARCEP et l'ADEME (Agence de l'environnement et de la maîtrise de l'énergie), elle devra, à compter du 1er janvier 2023, publier une recommandation sur l'information des consommateurs par les services de télévision, les services de médias audiovisuels à la demande et les services de plateforme de partage de vidéos, en matière de consommation d'énergie et d'équivalents d'émissions de gaz à effet de serre de la consommation de données liée à l'utilisation de ces services[744].

Si toutes ces actions méritent d'être saluées, il parait aussi nécessaire de sensibiliser le grand public par **une campagne de communication grand public** permettant de faire prendre conscience de l'empreinte écologique ou carbone d'une activité typique des réseaux sociaux telle que le **visionnage de vidéos** (l'une des activités dont l'impact est le plus fort[745]). Des sondages indiquent en effet que la méconnaissance de cet enjeu semble être très élevée[746]. A terme il pourrait être utile de réfléchir à encadrer le *streaming* vidéo[747] ou promouvoir des messages d'alertes du type "*Réduire son temps d'écran de XX minutes, c'est économiser XX émissions de CO^2*".

A l'instar de tout usage qui a un impact environnemental significatif, la question va rapidement se poser de savoir si l'on peut se contenter d'actions d'information et de sensibilisation ou si des mesures plus contraignantes ne doivent pas être envisagées. Le Sénat, dans un important rapport sur le numérique soutenable[748], a ouvert des pistes prometteuses[749].

744 Art. 26 de la loi n° 2021-1485 du 15 novembre 2021.

745 ARCEP, site internet, rapport, décembre 2020, « Pour un numérique soutenable ».

746 Dans un sondage mené par YouGov pour Business Insider en 2020, il a été demandé à un panel représentatif de la population française de nommer, parmi une liste de marques d'électronique connues du public, celles qui étaient le plus écoresponsables selon eux. 76% des sondés ont répondu "je ne sais pas".

747 V. Rapport d'information du Sénat, *Pour une transition numérique écologique*, 9 juin 2020, p. 7.

748 Rapport d'information du Sénat, Pour une transition numérique écologique, 9 juin 2020 p. 7.

749 Notamment d'encadrer le *streaming* vidéo, d'interdire le *scroll* à l'infini et le lancement automatique des vidéos, de mettre en place une obligation de *reporting* des fournisseurs de contenus sur les stratégies cognitives utilisées pour accroître les usages, d'encourager les plateformes qui auront revu leur design pour limiter la consommation énergétique des utilisateurs et de prévoir l'installation d'un design "vert" par défaut et, de façon plus générale, d'envisager des actions visant à limiter l'impact écologique des centres de données, dont la consommation est importante et croissante (par rapport à

Proposition n° 9

Établir un plan ambitieux d'éducation et de formation relatif à l'usage des réseaux sociaux destiné à tous les publics et mettre en place un pilotage unifié.

Diffuser les outils existants et en créer de nouveaux notamment un jeu vidéo à vocation pédagogique qui sensibilise aux dangers des réseaux sociaux et informe les utilisateurs.

Lancer une campagne de communication grand public permettant de faire prendre conscience de l'empreinte écologique ou carbone des réseaux sociaux notamment le visionnage de vidéos ou le livestream.

3.1.4. Le rééquilibrage stratégique : stimuler une offre vertueuse, souveraine et sécurisée

La construction d'un « avenir numérique de l'Europe » est à l'œuvre, en France comme en Europe. Au sein de l'État, la DINUM met déjà de nombreux outils de travail collaboratif à disposition, qui répondent à l'objectif de renforcer l'autonomie stratégique française. Ils méritent d'être davantage connus et utilisés. En ce qui concerne l'encouragement **d'une offre européenne** conforme à nos valeurs et à nos intérêts stratégiques, des projets existent, dont certains sont en cours de déploiement comme le projet de *SecNum Cloud* qui va permettre de garantir un hébergement sécurisé des données en Europe mais ne sont souvent pas assez visibles. En effet, il existe des réseaux sociaux comme *Mastodon*[750] qui offrent des services payants ou gratuits sans réutiliser les données personnelles des internautes ni les exposer à de la publicité. La plupart de ces réseaux fonctionnent de façon **décentralisée**, avec des **logiciels libres** selon les valeurs premières du Net portées par Tim Berners-Lee. Ce dernier a d'ailleurs lancé un projet intitulé *Solid* pour « *un web décentralisé et une meilleure confidentialité des données* », estimant indispensable de redonner aux utilisateurs le pouvoir de contrôle sur leurs données. Plusieurs voix françaises se sont aussi élevées en ce sens. Dès janvier 2014, Pierre Bellanger[751], condamnant le fait que la France fasse « *partie des premiers exportateurs mondiaux de vie privée* », a préconisé la préservation d'un internet libre et ouvert. Henri Verdier, ambassadeur du numérique, promeut également l'utilisation des « *communs numériques* [752] » (tel que Wikipédia, Linux, OpenStreetMap). À l'occasion de l'Assemblée numérique de juin 2022 co-organisée par la présidence française du Conseil de l'Union européenne et la Commission européenne, un groupe de travail regroupant 19 États membres et la Commission européenne a rendu **un rapport sur les communs numériques** qui formule quatre

2018, la consommation énergétique des centres de données devrait augmenter de 21% pour atteindre 92,6 TWh/an en 2025).

750 V. *supra* les fiches d'identité des réseaux sociaux.

751 P. Bellanger, PDG de Skyrock, fondateur de skyblog, a publié de nombreux ouvrages sur le numérique. Il est membre du comité scientifique du Centre des hautes études du cyberespace.

752 H. Verdier utilise le terme "commun" (Ostrom) et non pas "bien commun", car il recouvre une réalité moins large, à savoir une ressource produite collectivement et gouvernée par ceux qui la produisent.

propositions[753] : la création d'un guichet unique européen pour orienter les communautés vers les financements et aides publiques adéquats ; le lancement d'un appel à projets pour déployer rapidement une aide financière aux communs les plus stratégiques ; la création d'une fondation européenne pour les communs numériques, avec une gouvernance partagée entre les États, la Commission européenne et les communautés des communs numériques et la mise en place du principe « communs numériques par défaut » dans le développement des outils numériques des administrations publiques. Cette initiative mérite d'être poursuivie et prolongée par un **soutien aux entreprises européennes qui développent des solutions alternatives respectueuses du modèle européen.**

Afin de donner l'exemple et de créer un effet de réseau, **l'administration et les collectivités locales** pourraient impulser un **changement de pratiques** en utilisant les réseaux sociaux dits « alternatifs », au moins pour accomplir leurs missions les plus sensibles, par exemple pour certaines consultations impliquant de faire connaître des données à caractère personnel et plus encore lorsqu'il s'agit de mettre en place des discussions internes. Pour ce faire, il conviendrait de les sensibiliser notamment aux risques de perte ou de transfert de données que représente l'utilisation de réseaux extra-européens. Pour faire vivre la démocratie locale et utiliser des *civics techs*, seuls les réseaux sociaux alternatifs sont, pour l'instant, à même de proposer **un espace suffisamment sécurisé et serein**. L'usage de réseaux comme *Mastodon ou Whaller*[754] devrait être promu auprès de tous les partenaires publics en l'accompagnant de mesures permettant de prendre en compte les individus les moins familiers avec les outils numériques. Ils pourraient contribuer à faire vivre la démocratie à l'ère du numérique et à retrouver le rôle d'internet comme *bien commun*. S'agissant **des outils à la disposition de l'État et de ses agents**, la DINUM met déjà de nombreux outils de travail collaboratif qui répondent aux objectifs de cybersécurité et de protection de la souveraineté à disposition[755], notamment la messagerie sécurisée de l'État français Tchap qui gagnerait à être connue et davantage utilisée. Ces outils devraient être promus et développés y compris en s'appuyant sur des consortiums public/privé en tant que de besoin.

L'utilisation des réseaux sociaux alternatifs pourrait aussi être encouragée auprès **de l'ensemble des corps intermédiaires** pour contribuer à renouveler le débat social et favoriser la réconciliation de la démocratie représentative et de la démocratie participative. A terme, on peut espérer que le secteur privé français et européen privilégie également ces dispositifs sécurisés (on peut ainsi relever que la Cour de Justice de l'Union européenne vient de créer sa propre instance sur Mastodon, où elle publie du contenu, accessible en français).

753 Ministère de l'Europe et des affaires étrangères, site internet, juin 2022, « Report of the European working team on digital commons ».

754 Whaller est une plateforme sociale et collaborative complète française à destination des organisations (entreprises privées, administrations publiques…) qui peuvent à la fois l'utiliser comme solution de communication (messagerie ou réseau social d'entreprise) mais également outil collaboratif (box de fichiers, coédition, événements, tâches, visio, audio, webinaires…) permettant de faciliter le travail et le télétravail, le tout dans un environnement très sécurisé (stockage des données sur des serveurs *cloud* locaux OVH certifié SecNumCloud par l'ANSSI). Elle est utilisée par Pôle emploi notamment.

755 Gouvernement, site internet numerique.gouv.fr, « Outils de travail collaboratif pour les agents : Webconférence d'État, France Transfert, Audioconférence de l'État, Osmose etc. »

Cette promotion impose un **effort important de communication** de l'État auprès des administrations, des collectivités territoriales, des établissements publics et des corps intermédiaires comme de leurs agents et membres. L'administration devrait, à cet égard, chercher à donner l'exemple. Sont en jeu la sécurisation de multiples données stratégiques et la conservation d'une certaine autonomie.

Proposition n° 10

Mettre en œuvre les propositions du groupe de travail européen sur les communs numériques.

Encourager les personnes publiques à utiliser les réseaux sociaux alternatifs ainsi que l'utilisation des communs numériques. Favoriser le recours aux réseaux sociaux alternatifs par l'administration et les collectivités locales pour accomplir leurs missions, au moins les plus sensibles (consultation des administrés ou citoyens sur des politiques publiques, remontée des difficultés, traitement des réclamations, échanges de données sensibles, etc.).

Mettre en œuvre une politique de soutien à l'industrie numérique européenne pour préserver l'autonomie stratégique.

3.2. Armer la puissance publique pour réguler et optimiser l'usage des réseaux sociaux

La puissance publique doit, d'une part, se mobiliser pour mettre en œuvre au mieux les cadres de régulation instaurés par l'Union européenne et, d'autre part, utiliser à plein le potentiel que représente l'usage des réseaux sociaux pour une administration efficace.

3.2.1. Le renforcement et la réorganisation de la puissance publique

L'adoption très récente par l'Union européenne des deux textes majeurs que sont le DMA et plus encore, pour les réseaux sociaux, le DSA, sans parler de la prochaine adoption de l'IA Act, font de la réussite de leur mise en œuvre – qui interviendra de façon échelonnée à compter de l'entrée en vigueur prévue à l'automne 2022 –, un enjeu décisif pour la mise en place effective d'une véritable régulation des réseaux sociaux.

La difficulté est double. D'une part, tant pour le DSA que pour le DMA, le régulateur premier est la **Commission européenne** et les régulateurs des États membres ne conserveront qu'une compétence seconde. Mais la Commission ne pourra jouer pleinement son rôle si elle n'est pas correctement informée des difficultés de terrain, si elle n'est pas en mesure d'identifier les risques et de vérifier que les analyses réalisées par les plateformes sont pertinentes. **Les autorités françaises seront donc dans une position originale** dans la mesure où l'essentiel des pouvoirs de régulation seront entre les mains de la Commission mais que cette dernière ne pourra correctement les exercer sans l'assistance concrète des autorités nationales en mesure de collecter les données et de les faire remonter vers elle. D'autre part, le DSA met en œuvre une forme de dispositif de *compliance* dans le domaine de la liberté d'expression, ce qui est très novateur et a pour conséquence de n'apporter **qu'une visibilité relative au dispositif**. En effet, comme tout dispositif de régulation où l'opérateur choisit, dans une certaine mesure, les moyens qu'il décide d'employer pour parvenir aux buts que lui a fixés le législateur, la réussite du dispositif dépend de sa correcte appropriation par les acteurs ainsi que de la vigilance et de l'efficacité du superviseur. Dans ces conditions, il apparait crucial que l'ensemble des acteurs concernés s'organisent rapidement pour permettre une mise en œuvre effective des règlements européens et, le moment venu, pour évaluer leur pertinence à l'épreuve du temps. Plusieurs actions visant à renforcer, au niveau national, l'efficience de la régulation et de l'expertise sur le numérique peuvent être mises en œuvre.

Favoriser une bonne articulation entre les régulateurs nationaux et la Commission européenne

Les changements portés par les règlements européens en cours sont ambitieux (notamment la portabilité des messageries, la mise en place d'audits et l'accessibilité aux algorithmes) mais peuvent se révéler insuffisants s'ils ne sont pas correctement mis en œuvre notamment en s'assurant du respect des obligations fixées aux opérateurs. Garantir leur bonne application est donc crucial.

Face à des acteurs très puissants, il est donc indispensable que la Commission européenne dispose rapidement **des moyens effectifs** (juridiques, financiers, humains, techniques) de contrôler la correcte application des textes, de disposer d'informations détaillées et d'exercer une supervision sur des processus de modération reposant essentiellement sur des algorithmes particulièrement

complexes. Le principe d'une compensation financière versée par les très grands acteurs à la Commission pour financer leur propre supervision a été à juste titre prévu dans le *Digital Services Act*. Celle-ci doit aussi pouvoir s'appuyer sur les États membres et les régulateurs nationaux qui doivent eux aussi disposer des moyens nécessaires à cette mission. Le succès de la mise en œuvre du DSA et du DMA va donc reposer sur **un partage efficace d'informations, d'expériences et de compétences entre la Commission et les autorités nationales compétentes**. Même si le DSA ne l'a pas explicité, le bon fonctionnement de la régulation des très grandes plateformes pourrait être rapproché de celui qui prévaut dans le domaine bancaire, dans lequel les banques centrales nationales jouent un rôle essentiel notamment pour collecter l'information dont la BCE a besoin pour assurer sa mission de supervision des banques systémiques.

La mise en œuvre du DSA impliquera tout d'abord que soient désignés dans les 27 États membres de l'Union les **coordonnateurs des services numériques** (CSN ou DSC : *digital services coordinator*) répondant aux exigences de l'article 39. En effet, aux côtés de la Commission, chargée de l'essentiel de la surveillance des très grandes plateformes, les autres plateformes seront placées sous la surveillance du CSN de leur lieu d'établissement. L'article 38 du règlement prévoit que l'État membre « *désigne une ou plusieurs autorités compétentes comme responsables de la surveillance des prestataires de services intermédiaires et de l'application du présent règlement* » et parmi ses autorités, le CSN. La **bonne coordination** entre les CSN et la Commission sera essentielle pour la réussite du DSA (si les compétences sont clairement réparties entre la Commission et les CSN, de nombreuses dispositions prévoient différentes formes de coopération).

Relèvera du contrôle de la Commission la mise en œuvre des obligations d'évaluation et de mesures d'atténuation des risques, de transparence des systèmes de recommandation, d'audit et d'accessibilité des coordonnateurs aux données pour les très grandes plateformes[756]. Aucune des très grandes plateformes n'ayant à ce stade son siège en France, le CSN français ne se verra confier aucune mission en lien direct avec elles (notamment l'agrément des chercheurs habilités à accéder à leurs données).

Le CSN sera chargé, pour les plateformes qui relèvent de son contrôle, de vérifier la bonne application des obligations figurant dans le DSA[757] et disposera à cette

756 C'est notamment à la Commission qu'il revient de vérifier l'obligation mise à la charge des plateformes les plus grandes, de donner accès aux données aux chercheurs agréés en conformité avec les actes délégués qui seront adoptés par la Commission et qui établiront les conditions techniques dans lesquelles les partages de données auront lieu. Ces conditions vont notamment prendre en compte la nécessité de respecter la confidentialité des informations soumises au secret des affaires. (futur art. 31 du DSA). En France, il sera sans doute opportun de s'inspirer du CASD pour bénéficier d'un environnement sécurisé.

757 Notamment les obligations d'informer sur la modération des contenus, le nombre de litiges transmis aux organes de règlement extrajudiciaires; d'adopter des conditions d'utilisation respectant les droits des usagers ; de déterminer un point de contact ; de mettre en place un mécanisme de signalement des contenus illicites, une information sur l'éventuelle décision de retrait ou de blocage, de fournir une motivation sur cette décision et les voies de recours possible ; de signaler des infractions pénales aux autorités lorsque les contenus illicites mettent en danger la vie ; de mettre en place un système interne de traitement des réclamations et de recours à des règlements extra-judiciaires ; de mettre en place un dispositif permettant de lutter contre les notifications abusives ou réclamations

fin de nombreuses prérogatives d'enquête et de sanction (art. 41). Il devra traiter les plaintes des utilisateurs dans ce cadre (art. 43). Il devra aussi attribuer le statut de **signaleurs de confiance**[758] aux entités établies dans son ressort (associations de protection des utilisateurs, collectivités publiques ou entreprises chargées d'une mission de service public répondant aux critères fixées par le DSA) afin de permettre la mise en place de **circuits prioritaires de signalement**. Le DSA prévoit également la possibilité pour des **organismes de règlement extrajudiciaire de litiges** d'être agréés par le coordinateur des services numérique de l'État dans lequel ils sont établis sous réserve de répondre à un certain nombre de critères[759].

Si le CSN français ne sera pas chargé de surveiller les très grandes plateformes, il devra pleinement **coopérer et participer** à cette mission en mettant à disposition de la Commission les informations dont il dispose (art. 44 ter), ses capacités techniques et d'expertise (art. 49 bis). Le CSN devra informer la Commission et les CSN de destination de toute ouverture d'enquête à l'égard d'un prestataire technique. Il pourra également solliciter l'ouverture d'une enquête auprès du CSN compétent (art. 45). Dans le cadre de cette coopération, le CSN français pourra notamment aider la Commission à bien identifier les informations pertinentes à auditer, à tenir à disposition des auditeurs des critères de recommandation autres que quantitatifs, à identifier dans le cadre de l'analyse des risques systémiques instaurée par le DSA non seulement **les risques extrinsèques** relevant de leur utilisation (atteinte à la vie privée) mais aussi les **risques intrinsèques** véhiculés par la structure même des réseaux sociaux (captation de l'attention, addiction), leurs modèles d'affaire et designs.

Un volet **environnemental** pourrait aussi être intégré aux audits et au pouvoir d'enquête donné à la commission par le DSA car il s'agit bien d'un risque systémique. La responsabilisation des plateformes sur le volet environnemental, avec un pouvoir de contrôle et d'inspection à l'échelon européen, sur des critères précis et des indicateurs fiables pourrait être une piste intéressante pour réduire l'impact environnemental des réseaux sociaux.

Il faut souligner que l'article 50 du DSA prévoit que, lorsqu'un CSN a des raisons de soupçonner qu'un fournisseur d'une très grande plateforme en ligne ou un moteur de recherche a enfreint les obligations à leur charge d'une manière « *qui affecte gravement les destinataires de service de son État membre* », il peut, par l'intermédiaire du système de partage d'informations, **demander à la Commission de se saisir de la question dans le cadre de son rôle de régulateur systémique**. C'est

manifestement infondées ; de faire apparaître les publicités en ligne de façon claire et non ambiguë, de permettre l'identification de la personne pour laquelle la publicité est affichée, de transmettre les informations utiles concernant les principaux paramètres utilisés pour déterminer le bénéficiaire auquel la publicité est présentée.

758 Art. 19 du DSA : « *Le statut de signaleur de confiance est attribué, sur demande présentée par une entité, quelle qu'elle soit, par le coordinateur pour les services numériques de l'État membre dans lequel l'entité présentant la demande est établie, dès lors que l'entité a démontré qu'elle satisfait à l'ensemble des conditions suivantes : (a) elle dispose d'une expertise et de compétences particulières aux fins de la détection, de l'identification et de la notification des contenus illicites; (b) elle représente des intérêts collectifs et est indépendante de toute plateforme en ligne; (c) elle s'acquitte de ses tâches aux fins de la soumission des notifications en temps voulu, de manière diligente et objective* ».

759 Futur art. 18 du DSA.

un élément très important pour la réussite effective du DSA : les CSN disposeront en effet de manière directe des remontées des difficultés concrètes rencontrées par les utilisateurs, difficultés individuelles qu'il n'appartient pas à la Commission européenne de traiter mais qui peuvent révéler, par leur nombre, leur fréquence, leur gravité, un manquement systémique de la plateforme aux obligations résultant du DSA, dont il appartient à la Commission de se saisir. En cas de difficultés susceptibles de révéler un manquement systémique, la Commission pourra mettre en œuvre ses pouvoirs d'enquête (inspection, demande d'informations) et, le cas échéant, en cas de manquement constaté, faire usage des pouvoirs coercitifs que lui attribue le DSA (mesures provisoires, surveillance renforcée) jusqu'au prononcé éventuel de sanctions qui peuvent être des amendes allant jusqu'à 6% de son chiffre d'affaire annuel mondial de l'exercice précédent. De plus, si la Commission décide d'engager une procédure à l'encontre d'une plateforme, elle en informe tous les CSN qui doivent, dans les meilleurs délais, lui transmettre toute information qu'ils détiennent sur le manquement en cause (art. 51). Le DSA prévoit aussi que la Commission doit pouvoir s'appuyer sur **les coordinateurs nationaux pour les services numériques**, qui pourront fournir des experts pour la conduite des enquêtes (art. 51.3). Ainsi une véritable coopération et mutualisation des forces est-elle prévue par le DSA. Il faut d'ailleurs souligner que le DSA institue formellement un **comité européen des services numériques**, groupe consultatif indépendant regroupant les coordinateurs des services numériques nationaux, qui sera chargé d'assurer la surveillance des fournisseurs de service intermédiaires, qui pourra conseiller la Commission et les autres autorités compétentes sur les questions émergentes dans l'ensemble du marché intérieur relatives aux matières régies par le DSA (art. 47).

S'agissant du *Digital Markets Act,* sa mise en œuvre incombe essentiellement à la **Commission européenne** qui est dotée de la capacité de demander des renseignements, de mener des inspections, d'adopter des mesures provisoires, de rendre les mesures volontaires obligatoires pour les contrôleurs d'accès et de contrôler la conformité au règlement. Elle pourra constater les manquements et les sanctionner. Le règlement prévoit **un plan de mise en œuvre et des modalités de suivi, d'évaluation et d'information**[760]. Des actions de **coopération et de coordination** entre la Commission et les autorités compétentes sont prévues s'agissant de la désignation des contrôleurs d'accès (art. 33) et s'agissant de l'application des règles de concurrence (art. 31). La Commission peut consulter les autorités nationales sur toute question relative à l'application du DMA. La Commission est assistée d'un **comité consultatif et d'un** « ***High-level Group*** » à vocation transversale puisque composé des différentes autorités de régulation compétentes au niveau européen (BEREC, CEPD et leurs équivalents pour la concurrence, protection des consommateurs et régulation des médias), chargés de la conseiller et de lui fournir une expertise[761]. Mais si la supervision des obligations est confiée à la Commission,

760 Le suivi sera divisé en deux parties : i) le suivi continu, qui rendra compte, tous les deux ans, des dernières évolutions du marché, avec la participation éventuelle de l'observatoire sur l'économie des plateformes en ligne de l'UE; et ii) les objectifs opérationnels et les indicateurs spécifiques permettant de les mesurer. L'évaluation sera réalisée à l'aide d'indicateurs dans le but de déterminer si des règles supplémentaires sont nécessaires pour garantir la «constestabilité » et l'équité des marchés numériques dans l'UE.

761 Ce groupe fournit à la Commission des conseils et une expertise dans les domaines de compétences de ses membres, *via* des conseils sur la mise en œuvre du DMA ; des avis sur les interactions potentielles entre le DMA et les règles sectorielles nationales afin d'identifier les problèmes transréglementaires

dotée de larges pouvoirs d'accès aux données et aux algorithmes, les États membres **pourront habiliter les autorités nationales de la concurrence** à ouvrir des enquêtes sur d'éventuelles infractions et à transmettre leurs conclusions à la Commission. Les régulateurs nationaux pourront, de leur propre initiative, mener une enquête sur un cas de non-respect éventuel sur leur territoire des obligations prévues pour les contrôleurs d'accès dans le DMA (art. 5, 6 et 6 bis) mais ils devront en informer la Commission par écrit et lui faire un rapport sur les résultats de l'enquête.

La philosophie de ces deux règlements est la même : certes la Commission est le régulateur premier et elle doit être informée de toute action d'un régulateur national sur les domaines qui entrent dans son champ, mais c'est à une **véritable coordination** qu'il faudra parvenir.

Pour être aussi efficace que possible dès l'entrée en vigueur des deux règlements européens, un **groupe de travail informel pourrait être rapidement mis en place** pour chacun des règlements afin de réfléchir avec la Commission aux méthodes de coordination, de déterminer les informations à faire remonter à celle-ci, les appuis à lui apporter, les initiatives à prendre et les champs d'expertise technique à partager.

Compte tenu de la multiplicité des textes et autorités compétentes sur les sujets du numérique, **la création d'un comité de suivi transversal auprès de la Commission européenne** sur le modèle du *high level groupe*prévu par le DMA à cette fin pourrait être envisagé. Celui-ci pourrait opportunément s'intéresser à la mise en œuvre de dispositions anciennes qui ne sont pas correctement appliquées comme la portabilité des données, prévue par le RGPD.

Proposition n° 11

Préparer rapidement la coordination entre la Commission européenne et les régulateurs nationaux par la mise en place d'un groupe de travail informel.

Proposer la création d'un comité de suivi transversal auprès de la Commission européenne (DMA, DSA, IA Act, RGPD, etc.).

Améliorer l'organisation interne de la puissance publique

Pour être en mesure de mettre en œuvre ces réformes qui concernent une pluralité de secteurs, la puissance publique doit disposer d'outils transversaux, de forces d'expertise et d'outils d'évaluation. Il est impératif que l'État dispose de **compétences techniques solides et de très haut niveau sur le secteur du numérique et notamment celui des algorithmes**. Le Gouvernement lui-même dresse un constat sévère sur l'insuffisance de l'expertise technique de l'État sur le numérique. Outre la rigidité des règles de recrutement public, ces difficultés sont dues à la faible attractivité des emplois publics face aux grilles salariales proposées pour le même type de poste dans le secteur privé. La mise en place d'une stratégie pour assurer une montée en compétence publique sur les enjeux numériques semble indispensable. La mission Bronner a également recommandé

potentiels dans un rapport annuel remis à la Commission ; des recommandations sur la modification potentielle du DMA dans le cadre d'études de marché.

la création d'un mécanisme de gouvernance numérique interministérielle permettant de définir des stratégies, des politiques publiques et des réponses fortement coordonnées en matière de défense, sécurité et diplomatie, qui tiennent compte des interactions multiples propres à ce domaine partagé.

Un **service interministériel** rassemblant **les forces d'expertise et d'analyse** de l'administration française, dédié aux enjeux stratégiques du numérique et notamment de la régulation des plateformes numériques et permettant le suivi des politiques publiques transversales dans ce domaine paraît indispensable. Il pourrait se construire autour du **PeRen**[762] qui apporte déjà un contrepoint indispensable aux informations fournies par les plateformes et sur le modèle de **la *task force* interministérielle** animée par la **direction des plateformes de la direction générale des entreprises** qui a monté deux équipes projet pour contribuer aux négociations du DSA et DMA et a développé une expertise qu'il faut préserver, poursuivre.

Ce service interministériel pourrait comprendre :

- **Un pôle d'analyse et d'expertise interministériels sur les enjeux du numérique** chargé d'évaluer la mise en œuvre des normes et des recommandations, notamment l'effectivité des contrôles et sanctions prononcées par les régulateurs, d'identifier les lacunes, de fixer des axes de projets de recherche sur des sujets majeurs (comme par exemple, l'impact des réseaux sociaux sur la santé mentale) et de proposer des évolutions et des **axes de stratégie des politiques publiques**. Ces analyses devraient être réalisées en lien avec le réseau des régulateurs nationaux et européens. Ce centre pluridisciplinaire (*datascientits*, juristes, économistes, sociologues, scientifiques etc.) pourrait également superviser des expertises juridiques poussées avec les ministères concernés notamment sur les adaptations à apporter à la loi de 1881, le statut des influenceurs, l'évolution du droit de la concurrence, l'harmonisation du droit européen etc. Il pourrait comprendre, à l'instar du LINC de la CNIL, **un laboratoire prospectif** (*task force*) chargé d'expertiser les **nouvelles questions** et de faire des propositions en lien avec les AAI (Métaverse, *blockchain*, interopérabilité, NFT, identité numérique, objets connectés, etc.). Ce pôle devra s'appuyer sur des compétences humaines et techniques expertes et devrait être doté d'importantes **capacités de traitements des données** à des fins de recherche et d'expertise pour le compte de l'État. Il devrait pouvoir avoir notamment recours à des **instruments de médiamétrie** lui permettant d'étudier les usages des internautes sur les réseaux sociaux et d'en faire bénéficier l'ensemble des acteurs concernés (l'Ofcom[763], autorité de régulation

762 Pôle d'Expertise de la Régulation Numérique (PEReN) : depuis le 31 août 2020, le Pôle d'Expertise de la Régulation Numérique (PEReN) apporte son évaluation et son assistance technique aux services de l'État et aux autorités administratives qui interviennent dans la régulation des plateformes numériques. Ce service à compétence nationale regroupera, à ces fins, une vingtaine de data scientists et experts en informatique et algorithmique.

763 L'Ofcom (*Office of telecommunications*) a été institué par le *Communications Act* de 2002 et renforcé par le *Communications Act* de 2003 et est une autorité de régulation indépendante des services de communications, sur le modèle de l'ARCOM et de l'ARCEP. Elle est dotée d'une personnalité morale. Elle promeut la concurrence et supervise le marché de la télévision, de la radio, mais également des services postaux, des vidéos à la demande, de la téléphonie (fixe et mobile) et des ondes. Elle est également amenée à se prononcer sur le contenu des programmes diffusés sur les différents supports,

britannique équivalent de l'ARCOM et ARCEP réunis publie ainsi chaque année un rapport très utile qui analyse la consommation des réseaux sociaux et le marché de la publicité en ligne et permet notamment de mieux cibler les axes de régulation[764]) ;

- **Un service de suivi et d'exécution de la politique du Gouvernement concernant les plateformes** pouvant également apporter son appui aux administrations, aux AAI compétentes et **au réseau des régulateurs (cf. ci-dessous)** sur les sujets numériques les plus complexes ;

Par ailleurs, tant le droit que la régulation des réseaux sociaux présentent un caractère multi-face et l'interdépendance des champs nécessite, pour parvenir à un encadrement efficace, une vision décloisonnée. Tel le maillon d'une chaîne, chaque encadrement d'un pan des réseaux sociaux (infrastructure, données, SIA, services, etc.) s'articule dans ce tout que constitue le réseau social. De même que les règles européennes sur la collecte, la conservation et le transfert des données personnelles ont des répercussions sur la concurrence des opérateurs, de même la garantie d'une concurrence plus équitable pourrait ouvrir sur une plus grande diversité de réseaux sociaux pour les utilisateurs et influer sur la qualité du débat. Ce constat fait consensus[765]. Cette **interdépendance** doit conduire au décloisonnement des approches et à une articulation des régulations au service du bien commun. Il en résulte que l'une des principales difficultés est d'organiser l'articulation des différentes régulations. Il existe déjà des collaborations entre l'Autorité de la concurrence et la CNIL ou l'ARCEP et l'ARCOM mais il s'agit à ce stade davantage de coordinations bilatérales et ponctuelles. Or, pour prendre pleinement en compte la pluralité des enjeux soulevés par les réseaux sociaux, une coordination plus pérenne et réunissant l'ensemble des acteurs concernés apparait utile. Il est proposé d'instaurer **un réseau des régulateurs du numérique** (RRN) qui devrait regrouper les AAI compétentes (ARCOM, CNIL, ARCEP, Autorité de la concurrence) ainsi que les services de l'État (DGCCRF, DGE, Douanes) compétents au niveau national, d'abord pour favoriser le partage régulier de l'information et, dans le respect de l'indépendance de chacun, pour mieux articuler les politiques de régulation. Il pourrait également partager des expertises et des meilleures

et promeut différents objectifs de société au sein des télécommunications comme la diversité et l'égalité femmes-hommes. Elle produit de nombreuses contributions (rapports, guide de bonnes pratiques en termes de diversité, etc.) en lien avec ses missions, est amenée à répondre aux différentes réclamations qui lui sont envoyées par les usagers et à ouvrir des enquêtes lorsqu'elle soupçonne que les règles, définies par l'*Ofcom Broadcasting Code*.ne sont pas respectées.

764 C'est ainsi que le rapport de 2021 révèle que 2 adultes sur 3 déclarent accepter les conditions générales d'utilisation (CGU) sans les lire. Pourtant, 1 adulte sur 5 déclare qu'il n'est pas d'accord avec le fait que les plateformes utilisent des données personnelles. Les utilisateurs de 7 à 16 ans passent en moyenne 3h48 par jour en ligne. S'agissant de la publicité, le rapport révèle que les revenus des réseaux sociaux ont atteint 4,78 milliards de livres en 2020. 90% des revenus viennent de la publicité. S'agissant de l'accès à l'information, 40% des 16-24 ans déclarent que les réseaux sociaux sont leur principale source d'informations contre 14% pour les adultes.

765 Le 22 avril 2021 le *MIT Social Media Summit* réunissant une trentaine d'experts internationaux des réseaux sociaux a appelé au décloisonnement des approches constatant qu'une « *concentration de pouvoir trop importante dans les mains d'une poignée d'entreprises nuit à l'innovation et à la compétition* » et que « *la perception qu'une partie des profits engendrés par le modèle économique des réseaux sociaux nuit à la vie privée des utilisateurs, à l'intégrité des élections et plus globalement aux ambitions démocratiques de nos sociétés* ».

pratiques voire, le cas échéant, avec l'accord des autorités intéressées, coordonner des enquêtes. **Son secrétariat administratif** pourrait être assuré par le service interministériel qu'il est proposé d'instituer, ce qui faciliterait le lien entre les services de l'État et le réseau. Il pourrait évaluer les besoins de recherche et, en collaboration avec les universités et les chercheurs, proposer des feuilles de route et des objectifs à atteindre.

Pour permettre la mise en œuvre des textes européens et améliorer l'effectivité des contrôles fondés sur les outils traditionnels (hors DMA et DSA), un **renforcement conséquent des moyens des autorités de régulation et services de l'**État notamment de la CNIL, de l'ARCOM, de la DGCCRF, de la DGE, de l'Autorité de la concurrence et en tant que de besoin et de l'ARCEP est nécessaire. S'agissant des autorités qui vont devoir apporter leur appui à la Commission européenne pour la mise en œuvre du DSA et du DMA, une évaluation des besoins devrait être réalisée à la lumière des conclusions du groupe de travail chargé de réfléchir à la coordination entre la Commission et les régulateurs nationaux. Il faut souligner que, s'agissant au moins du DSA, les États membres devront veiller à ce que les **coordinateurs des services numériques** disposent de ressources techniques, financières et humaines suffisantes pour accomplir leurs missions. S'agissant de la DGCCRF et des instances qui lui sont rattachées, il conviendrait, pour mettre en place la politique évoquée de rééquilibrage au profit des utilisateurs, de renforcer leurs compétences et de les doter de moyens supplémentaires concernant les enjeux du numérique. Il en existe trois : le **conseil national de la consommation**[766], **l'institut national de la consommation (INC)**[767] et la **commission des clauses abusives**[768]. Le renforcement des missions de cette commission devrait lui permettre d'assurer un suivi des modifications des CGU des grandes plateformes afin d'alerter les utilisateurs sur les clauses qui apparaissent abusives et de solliciter leur modification avant de saisir un juge. Pour orchestrer et rendre cohérentes ces actions, le **renforcement de la DGCCRF**, actuellement sous-dimensionnée pour agir sur le volet numérique, devrait donc être engagé. S'agissant de la **CNIL**, déjà sous-dimensionnée pour faire face aux enjeux de protection des données personnelles, ses moyens devront être d'autant plus accrus si elle devient l'autorité de régulation de l'IA (*cf. infra*).

766 *Cf.* 3.3.1.

767 Placé sous la tutelle du ministre chargé de la Consommation, l'Institut national de la consommation (INC), créé en décembre 1966, est un établissement public national à caractère industriel et commercial (Art. L. 822-1, L. 822-2 et R. 822-1 du code de la consommation). Il réalise des essais comparatifs et des études juridiques et économiques dont il diffuse les résultats à travers ses différents médias, notamment ConsoMag et 60 Millions de consommateurs. Pour assurer ses missions, l'INC développe des partenariats avec des organismes publics ou parapublics. Il participe également à des programmes communautaires impulsés par l'Union européenne. Ses ressources proviennent de la vente de son magazine 60 Millions de consommateurs, d'une subvention votée par le Parlement et de prestations de services. Son conseil d'administration est composé de 15 membres, dont cinq représentants des consommateurs et usagers, cinq représentants de l'État, deux représentants du personnel de l'INC, du président de la Commission des clauses abusives, d'un représentant du collège des professionnels du Conseil national de la consommation et d'un ingénieur des corps de l'État.

768 La commission peut être saisie par un juge à l'occasion d'une instance pour donner son avis sur le caractère abusif d'une clause contractuelle. Instituée par l'art. L. 822-4 du code de la consommation, la Commission des clauses abusives est placée auprès du ministre chargé de la consommation. Elle est composée de magistrats, de personnalités qualifiées en droit ou technique des contrats, de représentants des consommateurs, de représentants des professionnels.

Proposition n° 12

Au niveau national, créer un service interministériel d'expertise et d'analyse dédié à la régulation des plateformes numériques qui puisse fournir ses expertises aux différents régulateurs et administrations. Le doter des outils techniques, administratifs et juridiques suffisants en l'habilitant notamment au traitement de données personnelles pour des fins d'expertise publique.

Créer un réseau national des régulateurs du numérique, réunissant les régulateurs et les administrations en charge des plateformes numériques.

Renforcer les moyens des autorités de régulation nationale pour assurer leurs missions de régulation et pour jouer pleinement leur nouveau rôle de coordination et de coopération avec la Commission européenne.

Améliorer les actions préventives et répressives contre les comportements malveillants et les contenus illicites sur les réseaux sociaux

Les réseaux sociaux sont de tels outils d'amplification qu'ils accroissent le nombre et les effets des infractions comme la diffusion d'images pédopornographiques, le harcèlement, la diffusion de la haine en ligne et de nombreux autres comportements malveillants. La puissance publique agit depuis plusieurs années pour mieux protéger les plus vulnérables et l'arsenal préventif, répressif et procédural ne cesse d'être renforcé. Il faut noter à cet égard la loi n° 2022-299 du 22 mars 2022 visant à combattre le harcèlement scolaire qui a créé un délit spécifique de harcèlement scolaire et a étendu l'obligation de coopération pour les plateformes de concourir à la lutte contre ce phénomène et la loi du n° 2022-300 visant à renforcer le contrôle parental sur les moyens d'accès à internet qui prévoit l'obligation pour les fabricants d'installer un système de contrôle parental et de proposer à l'utilisateur son activation lors de la première mise en service de l'appareil.

La mise en œuvre du DSA devrait également permettre de mieux faire face aux comportements nocifs. Dorénavant, toutes les **plateformes** ayant connaissance d'informations permettant de soupçonner qu'une infraction pénale mettant en danger la vie ou la sécurité d'une ou plusieurs personnes a eu lieu ou est en train de se produire devront informer rapidement les autorités répressives ou judiciaires de l'État membre (art. 15 bis du DSA). Par ailleurs les plateformes devront faire en sorte que les boutons de signalement soient facilement accessibles et d'usage aisé. Enfin, un statut particulier est accordé aux signaleurs de confiance dont les signalements seront traités en priorité par la plateforme. Parallèlement les opérateurs devront mettre en place des mesures d'atténuation des risques systémiques, parmi lesquelles figureront le harcèlement, la haine en ligne, etc. Si les exigences envers les plateformes ont ainsi été opportunément renforcées, il est aussi nécessaire de **responsabiliser le plus possible les utilisateurs** qui sont évidemment individuellement responsables de leurs actions et de leurs propos, sur les réseaux sociaux comme ailleurs. La proposition visant à généraliser les solutions permettant de certifier les âges voire de vérifier les identités poursuit également cette ambition. A terme, l'objectif des politiques publiques est **d'assurer le même niveau d'exigence en ligne et hors ligne**, l'ensemble des internautes comprenant qu'il n'existe pas d'impunité sur le net.

Pour être efficiente, la lutte contre les comportements malveillants doit, comme toute action de lutte contre des risques identifiés, être organisée de **façon stratégique**. Or, dans le domaine du numérique, on ne peut qu'être frappé par la multitude d'initiatives qui s'explique par le nombre important de problématiques posées mais qui engendre un éparpillement des actions. Un **pilotage coordonné et rationnalisé** devrait être de nature à rassembler les forces et augmenter l'efficacité de la puissance publique. Un très grand nombre de mesures déjà proposées dans cette étude poursuivent cet objectif (service interministériel, mise en réseau, point d'entrée unique pour les signalements, compilation pour améliorer l'accessibilité du droit) mais la mise en place d'un **plan global de prévention des risques et de lutte contre les contenus illicites sur les plateformes apparaît essentielle.** A l'image du GIP ACYMA (*cybermalveillance.gouv.fr*) il pourrait être intéressant d'associer le secteur privé et notamment les ONG / signaleurs de confiance comme point de contact afin de réunir tous les acteurs et d'optimiser les leviers d'actions. Son pilotage et sa définition pourraient être confiés à une entité dédiée réunissant tous les acteurs dont des représentants des **ministères de la Justice**, de l'intérieur, de la santé et de l'éducation nationale ainsi que le GIP ACYMA et les associations impliquées dans l'accompagnement aux victimes. Dans son volet préventif, ce plan pourrait notamment s'attacher à **informer les usagers des risques pénaux** qu'ils encourent s'ils commettent des infractions en ligne, à coordonner les dispositifs d'identification des risques et des leviers pour les combattre.

Cette stratégie de prévention des risques doit aussi s'accompagner d'un important **renforcement des outils répressifs**. La lutte contre les contenus illicites bénéficie en France d'outils efficaces comme notamment la plateforme **Pharos, l'OCLCTIC, le ComCyberGend** et les services spécialisés du **parquet de Paris** qui luttent contre la cybercriminalité et la haine en ligne. Mais les moyens de ces opérateurs publics semblent insuffisants pour lutter contre la masse des contenus illicites qui circulent sur les réseaux sociaux. Pharos, qui reçoit environ 300 000 signalements par an (sachant que les dispositifs mis en œuvre par les différentes réformes risquent d'augmenter significativement ce chiffre), ne comprend que 50 fonctionnaires, alors que, chaque minute, sont postés 200 000 *tweets*… On estime que la police judiciaire ne peut traiter que moins de 1% des signalements en matière de pédopornographie faute de moyens. Le renforcement des moyens consacrés au traitement des signalements et des plaintes par l'augmentation du nombre d'OPJ, de magistrats, de *datascientist* parait d'autant plus nécessaire que, d'une part, l'amélioration de l'accès à la procédure de signalement devrait augmenter leur nombre (*cf.* proposition n° 6) et, d'autre part, que les obligations les plus lourdes prévues par le DSA ne s'appliquant qu'aux très grandes plateformes, la mise en œuvre du DSA pourrait avoir pour effet secondaire d'entraîner le report de contenus illicites sur les petites plateformes et les messageries cryptées. Les outils existants de lutte contre les contenus illicites devront donc être suffisamment performants pour agir également à l'égard de ces opérateurs. En outre, la multiplication des **cyber-patrouilleurs** sur internet doit être poursuivie pour assurer la présence de la police sur les réseaux et lutter contre le sentiment d'impunité.

Ce plan devrait s'accompagner de la mise en place **d'outils statistiques** permettant de bénéficier d'informations chiffrées précises sur les signalements effectués,

les affaires élucidées et les contenus bloqués et retirés chaque année. Pour améliorer la lutte contre la délinquance, il sera important de connaître le nombre et la proportion de contenus supprimés en amont par les plateformes. Ces informations chiffrées permettraient de réaliser des **actions de communication sur les dispositifs existants et sur les suites données par la puissance publique aux signalements effectués**. Pour que les utilisateurs soient plus enclins à signaler les comportements malveillants sur les réseaux sociaux, ils doivent être davantage convaincus que leurs signalements seront traités et auront des suites.

Par ailleurs, il faudrait ouvrir une réflexion sur les **conditions de travail difficiles des professionnels** qui travaillent sur le tri des contenus illicites. Une réflexion similaire pourrait être menée pour les salariés du secteur privé avec les organisations syndicales.

Enfin, une réflexion devrait être envisagée sur la mise au point d'outils techniques utilisant notamment **l'IA pour aider au traitement des signalements toujours plus nombreux et à la détection des** infractions **sur internet**. Point de contact.net utilise déjà des technologies numériques pour retrouver des contenus déjà qualifiés comme étant « manifestement illicites ». Dans cet objectif, le lancement de marchés publics de recherche pourrait être opportunément décidé. A terme, lorsque le traitement des signalements sera facilité par la technologie, il pourrait être envisagé d'exiger des plateformes qu'elles disposent sur leur interface d'un bouton qui permette de signaler directement sur la plateforme unique aux autorités.

Proposition n° 13

Définir et structurer une stratégie de réduction des risques pour lutter contre les comportements malveillants et les contenus illicites sur les plateformes dans un cadre coordonné et renforcer les outils répressifs. Réaliser de larges opérations de communication et de sensibilisation sur ces sujets.

Investir dans la recherche pour améliorer les outils techniques en vue de détecter les infractions et faire face à la masse des signalements.

Améliorer la culture du numérique dans l'administration par la mise en place d'outils de formation et d'expertise

Même si les enjeux liés au numérique paraissent désormais incontournables, il apparaît que l'administration demeure encore trop imparfaitement préparée à ces problématiques.

Une enquête menée du 7 octobre au 12 novembre par Pix[769] pour Acteurs publics et le Syntec numérique a défini un test en ligne des compétences numérique afin de mesurer les savoirs des agents publics. Les résultats laissent apparaître une insuffisance de la maîtrise des outils numériques, un agent sur quatre n'ayant pas une pratique autonome du numérique, et 7% rencontrant des difficultés d'usage du numérique dans le cadre de leur fonction, pour 36% estimés à un niveau avancé.

769 Pix est un service public en ligne pour évaluer, développer et certifier ses compétences numériques. Il est souvent présenté comme une « start-up d'État ».

Concernant l'usage des réseaux sociaux, il est plus développé mais comporte des risques pour les agents qui n'en maîtrisent pas tous parfaitement les enjeux, notamment s'agissant de l'expression sur les réseaux sociaux. Pour pallier ces manques, diverses formations ont vu le jour dont les **formations au numérique** proposées par l'IGPDE – l'Institut de la gestion publique et du développement économique[770] – qui comprend notamment le cycle supérieur du numérique destiné aux cadres supérieurs. Si ces actions méritent d'être poursuivies, il manque un outil permettant de partager l'ensemble des compétences que la question de la régulation des plateformes requiert afin d'acquérir une **culture commune** et des réflexes pertinents. **Une formation continue** mêlant notamment ingénieurs et chercheurs en IA, économistes, juristes, sociologues pourrait permettre de faire converger les expertises, de créer une sensibilité commune aux questions liées aux plateformes et notamment aux réseaux sociaux qui soulèvent de enjeux stratégiques, économiques, techniques et juridiques et de faire ainsi monter en compétence les dirigeant chargés de penser et de mettre en œuvre les politiques publiques. A l'instar de l'IHEDN[771] qui propose d'ailleurs lors de sa session nationale d'approfondir le thème de la souveraineté numérique et de la cyber sécurité, la formation pourrait être ouverte aux dirigeants du secteur privé, aux journalistes, universitaires, avocats, responsables syndicaux etc. afin de susciter une réflexion collective.

Par ailleurs, la question se pose de savoir si la France doit accroître ses **forces d'expertise en algorithmes**. Leur mécanique est en effet au cœur du fonctionnement des plateformes et, pour être capable d'en discuter avec les opérateurs et d'en définir les critères d'explicabilité, il faut en maîtriser les rouages techniques. Actuellement les compétences se trouvent soit au sein des centres de recherche des très grosses plateformes soit dans quelques laboratoires, comme l'INRIA. Les expertises portent en général sur des briques d'algorithme et aucun expert ne peut se prétendre spécialiste des algorithmes en général. La question se pose de savoir s'il ne faudrait pas envisager la création d'un **label d'excellence** pour les ingénieurs et experts en algorithmes afin d'offrir à cette profession un début de cadre structuré et une forme de déontologie (sans pour autant créer une profession réglementée).

Le règlement européen *business to business* a imposé la transparence sur les principaux paramètres des algorithmes mais ces éléments sont insuffisants pour permettre un contrôle réel. Les espoirs sont donc placés dans le DSA dont la mise en œuvre va conduire à ce que trois situations se présentent. D'une part, des experts rattachés à des cabinets d'audit vont être missionnés par les très grandes plateformes pour réaliser ces audits. D'autre part, des chercheurs (potentiellement de tous horizons) vont être agréés par les autorités de l'État d'établissement des grandes plateformes pour mener des recherches en lien avec les risques systémiques identifiés par les plateformes. Par ailleurs, la Commission européenne a l'intention de sélectionner des experts pour lui permettre de remplir ses missions. Dans ce cadre, il ne semble pas y avoir intérêt, pour l'instant, à instituer un mécanisme

770 Service à compétence nationale créé en 2001, rattaché au secrétariat général du ministère de l'Économie, des finances et de la souveraineté industrielle et numérique.
771 https ://ihedn.fr/formations/session-nationale/

national de certification des experts. Cette question devra cependant être examinée à nouveau dans quelques années, notamment lorsque les expertises se seront développées et qu'il pourra être nécessaire d'offrir des instruments permettant d'identifier les plus compétents et indépendants d'entre eux.

En revanche, actuellement l'urgence parait plutôt, pour les administrations, de conserver les compétences et de **maintenir une attractivité suffisante** pour ses experts.

Proposition n° 14

Instaurer une formation continue de pointe pour créer une culture commune du numérique en général et notamment des réseaux sociaux, sur le modèle de l'IHEDN.

Évaluer à moyen terme l'opportunité de bénéficier d'une certification d'experts en algorithmes.

Renforcer l'accompagnement des opérateurs publics et privés sur la question de la réutilisation des données par des tiers

De multiples données circulent sur les réseaux sociaux. Certaines sont accessibles par tous, d'autres uniquement par les abonnés, d'autres enfin seulement par les membres du groupe privé de l'internaute. Certaines ne sont que des « traces numériques » mais leur simple croisement peut être très riche d'informations. Il n'est pas toujours aisé de savoir quelles sont les informations qui peuvent être utilisées par des tiers et dans quelles conditions. Une interprétation trop rigide risque de porter atteinte à l'innovation, à la recherche[772] et à la poursuite d'intérêts supérieurs (préserver l'ordre public) mais une interprétation trop large peut conduire à des atteintes à la vie privée massives. Ces questions concernent de nombreux acteurs très différents comme l'administration qui souhaite *scraper*[773] des informations pour réaliser ses missions d'inspection ou de contrôle, les recruteurs qui souhaitent regarder le profil des personnes qui postulent à un emploi, les entreprises de *social listening* ou de profilage qui collectent des données pour revendre des services, etc. La question de la réutilisation des données est un enjeu majeur pour les prochaines années et devrait être débattue, si ce n'est au niveau international au moins au niveau européen.

En France, la CNIL réalise déjà un important travail de pédagogie et d'accompagnement des acteurs privés et publics sur ces questions mais ses moyens demeurent limités au regard de cet immense défi. Il conviendrait notamment qu'elle dispose des forces suffisantes pour réaliser des **enquêtes** et le cas échéant, engager des poursuites. Il serait également utile que l'administration, éclairée par les jurisprudences et les avis des autorités de régulation, se dote d'une **doctrine d'emploi** générale à ce sujet. Le principe de proportionnalité pourrait opportunément inspirer cette réflexion afin de ne pas fixer des lignes inapplicables car trop rigides ou inefficaces car trop laxistes.

772 *Le Monde*, site internet, 26 avril 2022, « L'humeur de la planète sondée grâce aux réseaux sociaux : une vaste étude, portant sur l'état affectif de 11 millions de personnes dans 100 pays pendant le premier confinement, illustre l'émergence de sciences sociales dites computationnelles, aux fondements épistémologiques encore fragiles.»

773 Action qui consiste à « aspirer » des données

Outre la régulation des logiciels d'IA utilisant ces données, qui va être prochainement régie par le IA Act, la question de la **régularité de la collecte et de l'utilisation des données personnelles**, qui relève des autorités de régulation des données, est également cruciale. Il faut espérer que les lignes directrices adoptées par le CEPD en mars 2022 afin de résoudre les difficultés liées à l'application de l'article 60 du RPGD sur la coopération entre l'autorité chef de file et les autres autorités de contrôle concernées en cas de traitement transfrontalier permettront de renforcer l'efficacité concrète du RGPD. A défaut, il conviendra de s'interroger sur la pertinence du dispositif faisant reposer l'essentiel de la régulation sur une autorité chef de file qui est celle de l'État d'établissement.

Enfin, outre les réflexions juridiques, des **outils techniques** pourraient être envisagés et expertisés pour permettre aux utilisateurs de tracer leurs données personnelles et vérifier leur correcte réutilisation, à l'instar des traceurs numériques. Des recherches en ce sens pourraient être soutenues par les pouvoirs publics.

Proposition n° 15

Élaborer une doctrine d'emploi pour la réutilisation des données personnelles par les administrations et les entreprises, renforcer les moyens de la CNIL pour lutter contre la méconnaissance du RGPD et rediscuter du mécanisme de chef de file dans le cadre du RGPD si les dernières lignes directrices ne modifient pas les pratiques.

3.2.2. Optimiser l'usage des réseaux sociaux par l'administration

Pour optimiser son action, l'administration peut profiter de la diversité des réseaux sociaux qui, chacun dans leurs catégories offrent des leviers intéressants. Outre l'utilisation des réseaux alternatifs pour les échanges sensibles avec les administrés (ou les usagers des services publics) qui protège la souveraineté européenne, deux autres types d'actions, déjà engagées, méritent d'être généralisées et approfondies.

Généraliser la présence de la puissance publique sur les réseaux sociaux grands publics

Comme il a été dit, la communication *via* **les réseaux sociaux grands publics** offre à l'administration et aux services publics un moyen performant de toucher des publics spécifiques.

Cette forme de communication permet également de rendre compte au citoyen de l'action publique. Pour les collectivités territoriales et certaines administrations, les réseaux sociaux constituent **des relais à part entière** des politiques publiques. Cette révolution des modes de relations entre l'administration et les administrés doit être mise au profit du plus grand nombre et doit être organisée au mieux pour ne pas dévoyer son objet. A cette fin, il est important de choisir le type de réseau social sur lequel la communication va avoir lieu et définir où la mise en place de

« *community manager* » pour répondre aux questions des administrés, expliquer les décisions, les recours et maintenir un lien entre l'institution et le citoyen est un atout indispensable. Il constitue aussi un important levier managérial car pour un fonctionnaire, se voir confier cette tâche est signe de confiance. Les *community managers* vont alors être à la fois la vitrine de l'administration et le meilleur moyen de faire remonter des mécontentements et des dysfonctionnements. Sans pour autant abandonner d'autres modes de communication plus adaptés à certains publics (notamment les personnes qui ne sont pas sur les réseaux sociaux) il est indispensable de promouvoir ce nouveau mode d'action publique.

Une telle généralisation nécessite des **formations** des fonctionnaires conduits à remplir ces fonctions afin de déterminer les limites à ne pas dépasser, et de protéger les agents d'éventuels propos malveillants. A terme, il serait utile que toutes les collectivités territoriales importantes, les administrations centrales et déconcentrées et les services publics fortement présents sur le net disposent d'un tel dispositif.

Transformer la communication interne des administrations

S'agissant de la **communication interne aux administrations** et dans la ligne des réformes récentes de la fonction publique, expérimenter à large échelle les **réseaux sociaux internes** pourrait être intéressant. En effet, pour partager les expériences entre directions et échanger des bonnes pratiques, pour décloisonner certains services et apporter de la transversalité aux échanges, les échanges horizontaux que permettent les réseaux internes pourraient s'avérer très utiles. La question peut se poser de savoir comment articuler ces réseaux avec l'organisation hiérarchique de l'administration. Pourtant, il semble que si les directions conduisent un véritable dialogue social sur ce point, un consensus pourrait être trouvé pour déterminer les niveaux de discussion selon les thèmes et les types de sujet qui nécessitent une remontée verticale et ceux qui peuvent sans difficulté être partagés. Une telle organisation qui suppose de réfléchir avant envoi d'un message sur le type de donnée transmise, son niveau de sensibilité et d'intérêt pourrait permettre de gagner en efficience dans la communication interne (éviter des envois inutiles à la hiérarchie, alléger les boucles de mails) et de recréer du lien au sein de communautés de travail fragilisées par le télé-travail et la charge de travail.

Proposition n° 16

Généraliser le recours aux *community managers* pour animer les relations entre les administrations et les administrés sur les réseaux sociaux grands publics.

Expérimenter des réseaux sociaux internes en s'inspirant des réseaux sociaux d'entreprises et l'accompagner d'une réflexion interne avec les instances représentatives des personnels afin de définir les différents niveaux de discussion et de les rendre compatibles avec l'organisation hiérarchique.

3.3. Penser les réseaux sociaux de demain : pour une régulation « augmentée » ?

Si le DSA et le DMA constituent d'importants pas en avant, la puissance publique se doit de rester attentive au sujet des réseaux sociaux, qui connait des mutations extrêmement rapides et ne se laisse pas facilement réguler. S'il est difficile d'avoir « un coup d'avance » dans ce domaine, il faut tout de même maintenir une certaine « pression régulatrice » qui conduise les opérateurs à agir de façon plus vertueuse. Il faut donc identifier les domaines dans lesquels la puissance publique doit rester vigilante et promouvoir une réflexion proactive.

De façon générale, il est indispensable que la recherche de la « sobriété numérique » guide l'ensemble des décisions futures sur le numérique. Le laboratoire d'innovation numérique de la CNIL (le Linc) a d'ailleurs prévu pour l'année prochaine de travailler notamment sur l'articulation entre protection des données et protection de l'environnement[774]. A cet égard, les moyens mis en œuvre pour parvenir à cet objectif devront en permanence être réajustés en fonction des données acquises de la science sur la recherche environnementale et de l'expertise accumulée au fil des années par des autorités de régulation comme l'ARCEP et l'ADEME.

Au-delà de cet objectif global, plusieurs chantiers méritent une attention particulière.

3.3.1. Poursuivre et enrichir les chantiers de demain : la publicité ciblée, les messageries privées, les métavers

Si le DSA et le DMA sont appelés à être précisés avec l'adoption prochaine d'actes délégués, il ne faut certainement par exclure qu'un second *round* de réglementation s'avère nécessaire à moyen terme. On pourrait ainsi envisager d'obliger les grandes plateformes à négocier les conditions générales d'utilisation avec les associations de consommateurs voire de fixer directement des standards minimums, de préciser les règles relatives au paramétrage par défaut afin de renforcer le contrôle de l'outil par les utilisateurs eux-mêmes, d'imposer l'utilisation de services d'identification numérique et de certification d'âge, d'élargir l'accès aux données détenues par les plateformes, etc.

Par ailleurs, **plusieurs chantiers sont déjà en cours ou sur le point de l'être** : il est d'autant plus important que la puissance publique se positionne rapidement sur les enjeux qu'ils comportent et les réponses qu'il conviendrait d'y apporter. Il s'agit principalement de la publicité ciblée, de la question des messageries privées et des métavers.

774 CNIL, site internet, 6 octobre 2020, « Le Laboratoire d'Innovation Numérique de la CNIL publie de nouvelles études sur les traceurs et l'écosystème publicitaire ».

La publicité ciblée

La **publicité ciblée** est aujourd'hui un élément central du modèle économique des réseaux sociaux visant à utiliser le potentiel financier que permet « l'économie de l'attention » alliée à la puissance de la technique. Si ce modèle n'est pas remis en cause par le DMA et le DSA, plusieurs évolutions réglementaires sont envisagées pour compléter ces règlements dans une seconde phase. Dans la suite des préconisations récentes d'un groupe d'experts de la Commission européenne[775] et inspirées du *Digital advertising services inquiry* de l'ACC (commission australienne de la concurrence et des consommateurs[776]) des réflexions sont actuellement en cours. En effet, si le DSA et le DMA comportent des mesures en faveur de la transparence de la publicité à destination des utilisateurs pour le premier (art. 24, 30 et 36[777]) et à destination des annonceurs et des éditeurs pour le second (art. 5, 6 et 13[778]), ces mesures paraissent à ce stade peu ambitieuses au regard des difficultés posées par la structure du marché de la publicité programmatique (organisée autour des enchères) concentrée dans les mains de Google qui détient une partie

775 J. Doh-Shin, « Market Power and Transparency in Open Display Advertising – A Case Study », rapport final du groupe d'experts de l'observatoire des plateformes économiques en ligne auprés de la Commission européenne, 2021.

776 Cette autorité préconise une plus grande transparence des CGU concernant les conditions d'utilisation des données, la possibilité d'établir des règles sectorielles pour lutter contre les conflits d'intérêt et les problèmes de concurrence dans la chaîne d'approvisionnement *ad tech*, la possibilité d'établir des normes pour exiger des fournisseurs de technologie publicitaire qu'ils publient les tarifs et les charges tout au long de la chaîne d'approvisionnement pour les services de technologie publicitaire, ce qui permettrait de garantir une concurrence optimale entre les fournisseurs de services *ad tech* et la possibilité d'imposer des exigences de transparence sur le système d'enchères.

777 Pour toutes les plateformes : garantir la transparence de la publicité en ligne pour les utilisateurs. Les plateformes doivent veiller à ce que les utilisateurs puissent identifier pour chaque publicité spécifique, « *de manière claire, concise et non ambiguë et en temps réel », que le contenu en question est une publicité par des marquages précis, l'identité de l'annonceur, des informations sur les paramètres principaux utilisés pour le ciblage et sur la manière de les modifier, directement accessibles à partir du contenu en question* (Art. 24) *: Les RS avec des systèmes de recommandation doivent indiquer dans leurs CGU les principaux paramètres utilisés dans ces systèmes et toute option permettant aux utilisateurs de les modifier, avec les critères les plus significatifs retenus et les motifs de leur importance relative. (24a) : Pour les très grandes plateformes : obligation de tenir un registre contenant des informations sur les publicités et les annonceurs, mis à la disposition du public jusqu'à un an après que la publicité aété présentée pour la dernière fois sur leurs interfaces en ligne. Ce répertoire ne doit contenir aucune donnée personnelle des utilisateurs ciblés par la publicité. Les plateformes doivent faire des efforts raisonnables pour garantir que les informations soient précises et complètes.* (Art. 30) *: respecter les codes de conduite sur la publicité en ligne élaborés au niveau de l'Union, pour accroître la transparence au-delà des exigences du DSA. L'élaboration de ces codes de conduite doit être encouragée et facilitée par la Commission, qui veille à ce qu'ils favorisent « une transmission efficace des informations, dans le plein respect des droits et des intérêts de toutes les parties concernées, ainsi qu'un environnement concurrentiel, transparent et loyal dans le domaine de la publicité en ligne* ». (Art. 36)

778 Pour les contrôleur d'accès : communiquer aux annonceurs et éditeurs des informations gratuitement, relatives aux prix et frais payés par l'annonceur, à la rémunération reçue par l'éditeur et à la mesure sur laquelle chacun des prix et rémunérations sont calculés. Si le consentement de certains éditeurs/annonceurs n'est pas recueilli pour le partage de ces informations, il faut communiquer à chaque annonceur/éditeur des informations concernant la rémunération moyenne quotidienne perçue par chacun. (Art. 5) fournir aux annonceurs et éditeurs, à leur demande et gratuitement, un accès aux outils de mesure de la performance du contrôleur d'accès et aux données nécessaires pour qu'ils vérifient de manière indépendante leur performance sur ces plateformes. (Art. 6) fournir à la Commission une description soumise à un audit indépendant de toutes les techniques de profilage des consommateurs, mise à jour au moins une fois par an. La Commission transmet la description auditée au Comité européen de la protection des données. (Art. 13)

importante des acteurs du secteur[779] et des *walled garden* qui conditionnent l'accès aux espaces publicitaires par l'achat concomitant de technologies *ad tech*. La concentration du marché est telle que, malgré des décisions emblématiques des autorités de la concurrence, notamment française, l'ouverture à la concurrence du marché est loin d'être une réalité. Les axes de réflexion du groupe d'experts de la Commission européenne méritent d'être examinés : réfléchir à la manière dont la protection des données a renforcé la concentration du marché publicitaire[780], restaurer l'interopérabilité des données collectées par l'adoption de standards communs, renforcer le contrôle des données collectées par les éditeurs, obliger les acteurs à davantage de transparence et prévoir un contrôle indépendant par des tiers, réfléchir à des lignes directrices et de supervision contre les conflits d'intérêts et envisager la séparation de certaines activités. La commission Bronner avait également formulé des propositions visant à lutter contre la publicité programmatique, qu'elle identifiait comme l'une des causes principales de la diffusion des fausses informations[781].

Aux États-Unis, un projet de loi intitulé *Banning Surveillance Advertising Act* envisage de limiter drastiquement la capacité des plateformes à diffuser des publicités à leurs utilisateurs en interdisant l'utilisation des données personnelles[782].

En tout état de cause, sur ce chantier, qui relève naturellement de la compétence de l'Union européenne, beaucoup reste faire pour mieux encadrer ces activités et parvenir à articuler la réglementation sur la protection des données avec les impératifs d'ouverture à la concurrence. **Parvenir à une régulation sur ce point constitue un objectif hautement souhaitable** et aurait, à cet égard, des effets majeurs sur l'ensemble du secteur.

Il reste que **les opérateurs sont à la recherche de nouveaux modes de financement** des réseaux sociaux compte tenu des difficultés suscitées par la publicité ciblée et des outils qui sont progressivement instaurés par certains concurrents pour la mettre à mal. Apple a par exemple mis en place sur ses derniers Iphone une fonctionnalité dénommée *Apple Tracking transparency* qui donne la possibilité aux utilisateurs de choisir s'ils désirent ou non partager leurs données à des fins publicitaires. En France, l'Autorité de la concurrence, saisie d'une plainte pour abus de position dominante, a estimé le dispositif légal et refusé de mettre en place des mesures conservatoires mais a décidé de poursuivre l'instruction pour vérifier qu'Apple ne s'applique pas des règles moins contraignantes imposant ainsi des conditions de transaction inéquitables. Google vient par ailleurs d'ouvrir son système publicitaire à ses concurrents afin d'éviter la poursuite d'une enquête

779 *Cf.*. 2.2.3.

780 L'argument de la confidentialité des données des consommateurs serait utilisé pour en restreindre l'accès aux autres opérateurs, et ainsi avoir un avantage informationnel sur le marché de la publicité en ligne

781 Proposition n° 8 du rapport : « *Promouvoir l'investissement publicitaire responsable des entreprises en encourageant le recours, par les annonceurs, les régies, les agences publicitaires et surtout les fournisseurs de technologie publicitaire, à des* « *listes d'exclusion et d'inclusion de sites web* » *dynamiques, telles que celles élaborées par exemple par NewsGuard, Global Disinformation Index ou Storyzy. Engager un dialogue avec les fournisseurs de technologie publicitaire afin qu'ils aient recours à ce système, qui permettrait d'assécher de manière considérable l'économie des infox. (…)* »

782 Le siècle digital : États-Unis : un texte de loi pour interdire la publicité ciblée

antitrust de la Commission européenne[783]. Méta a également pris des engagements à l'égard de l'entreprise française Critéo, service d'intermédiation publicitaire, suite à la plainte déposée par cette dernière pour abus de position dominante[784]. Face à ces réactions, Facebook souhaiterait mettre au point un nouveau modèle publicitaire (*Basic ads*) n'utilisant pas des données personnelles des utilisateurs. Par ailleurs, de plus en plus d'opérateurs se tournent vers les abonnements en mettant en place des offres *Premium*.

Dans un marché aussi volatile, le régulateur doit maintenir sa vigilance en permanence. Le centre d'analyse et d'expertise interministériel fonctionnant en mode *task force* proposé plus haut permettrait de maintenir cette veille et de garantir une réactivité suffisante.

Les messageries privées

Le principal angle mort de la régulation régie par le DSA reste à ce jour la question des **messageries assimilées à des correspondances privées**. Leur exclusion se justifie par des motifs juridiques – secret des correspondances – mais aussi techniques (notamment le chiffrement de bout en bout des communications pour certaines d'entre elles). Le DSA, tout comme avant lui, en 2019, le règlement relatif à la dissémination des contenus terroristes en ligne dit « TCO », ne couvre que les services qui stockent et disséminent des contenus au public. Les échanges sur des groupes de messageries ou sur des groupes privés sur les réseaux sociaux, indépendamment du nombre de participants (parfois des centaines voire des milliers), n'entrent pas dans le champ de ces règlements. Or, d'une part, la dissémination d'informations illicites ou dangereuses sur ces services (fausses informations sur la pandémie, manipulation d'opinion dans la perspective de peser sur le résultat des élections, appels à la haine contre des groupes ethniques) a déjà pu avoir des conséquences graves et, d'autre part, on constate, peut-être du fait des efforts de modération des réseaux sociaux, une tendance au report du partage des contenus illicites ou nuisibles sur ces groupes privés. A ce stade, la seule initiative concernant la modération sur les messageries privées concerne la pédocriminalité. La Commission a publié le 11 mai 2022 une proposition de règlement visant à prévenir et à combattre les abus sexuels sur les mineurs (ASM) qui rendrait obligatoire pour certains opérateurs, dont les hébergeurs mais aussi les messageries privées, la détection des contenus constituant des abus sexuels commis contre des enfants[785].

783 Le siècle digital, 14 juin 2022, « Antitrust : Google va ouvrir le système publicitaire de YouTube à ses concurrents ». « *Les autorités européennes de la concurrence ont ouvert une enquête contre Google et son service de diffusion de vidéo il y a un an. Les annonceurs sont obligés de passer par le gestionnaire de publicité Google Ads pour acheter des espaces sur YouTube. Ils sont également contraints de passer par Display & Video 360. Selon la Commission, cela pourrait constituer un avantage déloyal que se serait accordé Google. Cela permettrait de limiter l'accès aux données des utilisateurs pour les autres plateformes.* ».

784 Le siècle digital, 20 juin 2022, « Meta s'engage à améliorer ses pratiques dans la publicité en ligne, l'Autorité de la concurrence valide ». En 2018, Criteo s'était vu retirer l'accès à une interface de programmation spécifique (API) de Facebook, permettant d'améliorer la mise aux enchères de publicités. Au même moment elle perdait également son statut de partenaire du Facebook Marketing Partner, un atout pour les prestations de Criteo et une sorte de label pour les entreprises bénéficiaires.

785 Commission européenne, communiqué de presse, 24 janvier 2017, « Rapport 2017 sur la citoyenneté de l'Union: la Commission promeut les droits, les valeurs et la démocratie ».

Au-delà du cas particulier de la lutte contre la pédocriminalité, qui peut être de nature à justifier des mesures plus intrusives, les solutions pour appréhender ces usages sans porter atteinte au secret des correspondances restent à inventer. Certaines initiatives du secteur, reposant sur l'analyse de métadonnées ou sur la limitation des facilités de partage sans prendre connaissance des messages eux-mêmes, ouvrent des pistes intéressantes mais complexes. Ce chantier est d'autant plus urgent que la nouvelle régulation applicable aux réseaux sociaux risque de renforcer le déport des contenus illicites vers les messageries privées.

Les métavers

Les métavers sont des espaces virtuels fondés sur des technologies immersives où les utilisateurs peuvent interagir en temps réel *via* des avatars. Sorte de réseaux sociaux « augmentés » proches de l'univers des jeux vidéo, ils permettent, en plus de la discussion ou du partage de contenus, de développer une véritable vie virtuelle. Si certains estiment que le projet, écologiquement non soutenable et ne répondant pas à un besoin ou des envies des utilisateurs, ne prospérera pas[786] d'autres y font d'importants investissements dans l'espoir qu'il constituera, dans les prochaines années, le mode de communication le plus apprécié. Malgré ces perspectives encore incertaines, il semble important d'identifier sans attendre les nouvelles questions juridiques que posent le ou les métavers pour en tenter d'en maîtriser les risques.

Sous l'angle de la modération, les enjeux semblent *a priori* assez similaires à ceux qui se posent pour les réseaux sociaux, les services de diffusion en direct de contenus mis en ligne par les utilisateurs, ou le jeu vidéo. Une étude du *Center for Countering Digital Hate* (CCDH) menée en décembre 2021 sur le « *VRChat* » de Meta a ainsi identifié des abus relatifs à des contenus haineux, du harcèlement, de la pornographie accessible aux mineurs, et a relevé les graves lacunes des outils de signalement et de modération. La question de la modération pourrait devenir plus complexe si plusieurs métavers se développent en parallèle tout en devenant interopérables, ce qui est l'une des hypothèses aujourd'hui les plus vraisemblables.

Mais, au-delà de la question de l'organisation de la modération, le ou les métavers sont susceptibles de soulever de nouvelles questions, notamment celle de la continuité entre le monde réel et le monde virtuel. L'agression d'un avatar par un autre avatar devrait-elle être sanctionnée au même titre qu'une agression dans le monde physique ? A défaut, faut-il créer une infraction spécifique ? Comment déterminer la limite entre le jeu et le comportement condamnable ? Comment déterminer la loi territorialement applicable ? La proposition visant à généraliser le recours à un dispositif d'identité numérique ou de tiers de confiance formulée plus haut pourrait avoir un intérêt majeur dans le cadre **du Metavers**. En contraignant à ce que toute activité virtuelle soit rattachée à une personne physique ou morale qui a une identité légale dans la vie réelle (en consacrant une sorte de principe d'adéquation des personnalités juridiques virtuelles et réelles) il ne sera plus possible d'agir en toute impunité. Certes, un tel dispositif n'éludera pas la question de savoir si les actes

786 D'autres technologies avancées comme celle de la réalité augmentée pourrait largement supplanter le métavers car il n'est pas certain que les individus souhaiteront massivement rejoindre ces univers parallèles.

posés dans la vie virtuelle ont la même portée que dans la vie réelle et la nécessité de déterminer à terme un cadre juridique à l'activité en cause en fonction de sa nature ludique ou non. Par exemple, si l'avatar est insulté, doit-on considérer qu'il s'agit d'un jeu ou d'une véritable insulte destinée à la personne réelle qui se cache derrière ? si le terrain acheté sur le métavers est incendié (hacké) le « propriétaire » pourrait-il agir contre l'auteur des faits ?, mais la mise en place **d'une obligation de transparence intermédiée auprès des opérateurs** et d'adéquation des personnalités juridiques entre les deux univers garantirait déjà l'existence d'interlocuteurs responsables et contribueraient à davantage responsabiliser les internautes.

S'agissant de la protection des données personnelles, des questions inédites risquent d'émerger en raison de l'utilisation de nouvelles catégories de données personnelles (expressions faciales, gestes, réactions produites dans les interactions entre avatars) : ces données personnelles permettront aux entreprises de mieux comprendre les processus de pensée des utilisateurs et ouvriront la possibilité d'un profilage renforcé et d'un ciblage des campagnes de publicité encore plus fin. Outre la quantité inédite de données susceptibles d'être collectées, la question du consentement effectif de l'utilisateur, dont les données seront potentiellement recueillies en temps réel, se posera avec encore plus d'acuité et de complexité. Si les principes très généraux du droit des données personnelles relatifs à l'information et au consentement des utilisateurs, qui sont indifférents à la nature des dispositifs techniques, peuvent juridiquement être transposés aux métavers, leur application concrète risque d'y soulever de nombreux défis.

Toutes ces questions pourraient utilement faire l'objet d'un groupe de travail au sein du pôle d'analyse et d'expertise du nouveau service interministériel.

3.3.2. Ouvrir une réflexion internationale ou au moins européenne sur les droits des utilisateurs des réseaux sociaux et du numérique plus largement

Pour améliorer la protection des droits des utilisateurs, le Conseil d'État, dans son étude annuelle de 2014 consacrée au numérique et aux droits fondamentaux s'était posé la question de l'opportunité de consacrer de nouveaux droits et libertés. A l'époque, il avait jugé opportun de nuancer les conclusions de l'étude annuelle de 1998[787] qui estimait inutile de consacrer des droits spécifiques : insistant sur **l'ambivalence du numérique** au regard des droits fondamentaux et rappelant que si le numérique permet un renforcement de l'exercice de certains droits comme la liberté d'expression ou la liberté d'entreprendre, il en fragilise d'autres tels que le droit à la vie privée ou à la sécurité, l'étude du Conseil d'État préconisait la consécration d'un droit à l'autodétermination des données personnelles plutôt qu'un droit de propriété, du principe de **neutralité** des opérateurs de communication et de **loyauté** des plateformes[788]. Aux côtés de ces deux derniers

787 Conseil d'État, *Internet et les réseaux numériques*, La documentation Française, 2000, p. 14.

788 Le principe de l'autodétermination des données personnelles dégagé dès 1983 par la Cour constitutionnelle allemande ne l'a pas été aussi clairement par le RGPD et une partie de la doctrine lui reproche d'ailleurs cette ambiguïté.

droits, qui ont été largement affirmés par les textes européens et nationaux, celui **d'accessibilité** à l'internet déjà consacré par le Conseil Constitutionnel se révèle également essentiel compte tenu des nombreuses discriminations et isolements issus des inégalités d'accès.

On peut s'interroger sur la nécessité de consacrer **des nouveaux droits** en lien avec la technologie numérique. Comme il a été dit plus haut, la difficulté pour faire disparaître l'accessibilité à des données personnelles d'une personne décédée interroge sur la nécessité de reconnaître un **droit à la mort numérique ou un droit d'accès pour les héritiers aux données du défunt**.

Les **univers virtuels** bousculent nombre de concepts fondateurs. Le droit à la propriété peut-il exister dans un monde virtuel, et *quid* de la protection de l'intégrité physique ? Faut-il créer une police spéciale ? des procédures particulières ? Peut-il exister des avatars dénués de tout lien avec une personne physique ou morale dans un espace virtuel non destiné au jeu ? Jean-Emmanuel Ganascia dans Servitudes virtuelles[789] souligne, à l'aide de plusieurs exemples, l'étendue des **questions éthiques** posées. S'il reste sceptique sur la résolution de ces questions par le droit, il n'en demeure pas moins que le droit reste le meilleur outil pour définir un cadre délibéré en commun et traduisant les préférences majoritaires dans nos démocraties. La protection du patrimoine génétique de l'humanité et l'interdiction du clonage ont ainsi été consacrées par plusieurs textes de portées internationales[790]. Dans le domaine de l'IA, de nombreuses réflexions sont en cours[791]. Dans le domaine des neurotechnologies, le Chili a ainsi consacré le droit à la protection de l'intégrité mentale et du libre-arbitre compte tenu des avancées de certaines techniques alliant numérique et science.

Au-delà des sujets qui disposent déjà d'assises de principe, comme la liberté d'expression et la lutte contre ces abus (lutte contre les *fakes news*, contre la cybercriminalité, contre les discours de haine[792]), d'autres **droits de l'homme à**

789 J.-E. Ganascia, S*ervitudes virtuelles*, Seuil, coll. sciences ouvertes, mars 2022.

790 Déclaration universelle sur le génome humain et les droits de l'homme (Unesco, 11 novembre 1977) Déclaration internationale sur les données génétiques humaines (Unesco, 16 octobre 2003) Convention d'Oviedo du 4 avril 1997 (ratifiée par la France le 13 décembre 2011).

791 Recommandation sur l'éthique de l'intelligence artificielle de l'UNESCO, Principes de l'OCDE sur l'intelligence artificielle, Recommandation du Conseil de l'OCDE sur l'intelligence artificielle… En outre, 25 pays dont la France (représentée par le coordonnateur national), participent au Partenariat mondial sur l'intelligence artificielle (PMIA) qui réunit des experts et représentants des gouvernements et de la société civile afin de « guider le développement et l'utilisation responsables de l'IA, dans le respect des droits de la personne, des libertés fondamentales et de nos valeurs démocratiques communes, conformément à la Recommandation de l'OCDE sur l'IA ». Se posera à terme, lorsque les régulations régionales (en particulier européennes et américaines) auront acquis une certaine maturité, la question de leur convergence puis celle de la négociation, au sein du système onusien, d'un accord international et la création d'une organisation mondiale consacrée au numérique, de la même façon que cela a pu se produire au cours de l'histoire dans d'autres domaines.

792 Le Conseil des droits de l'homme de l'ONU a adopté le 1er avril 2022 une résolution dans laquelle il s'inquiète des « effets négatifs » de la désinformation sur l'exercice et la réalisation de tous les droits de l'homme ; la résolution 74/247 du 27 décembre 2019 de l'Assemblée générale des Nations unies sur la *lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles* a institué un comité pour élaborer une convention internationale en la matière. La convention n° 185, dite de Budapest, signée le 23 novembre 2001, a été rédigée par le Conseil de l'Europe et ratifiée par l'ensemble des pays européens ainsi que les États-Unis, le Japon, l'Australie et le Canada ; la responsabilité des réseaux sociaux dans la diffusion des discours de haine (*hate speech*) a été souvent invoquée, par ex.

l'ère du numérique semblent devoir être consacrés. Les principes de protection des données personnelles, d'effacement des données, du droit à la déconnexion, d'interdiction de certains ciblages comportementaux et de contrôle social, pourraient en effet mériter une discussion à l'échelle internationale ou occidentale ou au moins européenne afin de relever le niveau d'exigence global. Quant aux sujets émergents relatifs notamment à l'adéquation des identités virtuelles et physiques, ils nécessitent une réflexion rapide compte tenu de l'évolution très accélérée des techniques comme des pratiques.

A l'instar de l'*Internet Governance Forum*, dont le mandat est de « *discuter des questions de politique publique liées aux éléments clés de la gouvernance d'Internet afin de favoriser la durabilité, la robustesse, la sécurité, la stabilité et le développement d'Internet* »[793], qui se réunit sous l'égide du Secrétaire général des Nations Unies, les questions de préservation des droits individuels et de l'espace démocratique méritent que la communauté internationale y prête attention. L'ensemble de la société doit être informée et sensibilisée à ces risques. Certaines initiatives vont dans ce sens : le 11 novembre 2018, quelques jours après la publication de la Déclaration et à l'occasion du Forum de Paris sur la paix, 12 chefs d'État et de gouvernement ont répondu à l'appel lancé par la Commission sur l'information et la démocratie ; ce rassemblement a débouché ainsi sur la signature d'un accord intergouvernemental inédit à l'Assemblée générale de l'ONU le 26 septembre 2019. Enfin, si l'on peut relever les discussions internationales programmées dans le cadre de l'IGF[794], la Commission Bronner a proposé l'ouverture de négociations dans un format plus restreint, sous l'égide de l'OCDE.

Le Conseil d'État estime qu'une charte des droits fondamentaux à l'ère du numérique devrait être réalisée dans les prochaines années à tout le moins à l'échelle européenne, soit au niveau du Conseil de l'Europe – qui présente le mérite d'une ouverture plus large – soit de l'Union européenne. Une réflexion préalable pourrait être conduite avec quelques partenaires proches particulièrement actifs sur les droits fondamentaux à l'âge du numérique et des réseaux sociaux. Il serait souhaitable que ce chantier soit ouvert sans trop tarder, compte tenu de la grande sensibilité des enjeux.

Proposition n° 17

Ouvrir et poursuivre les chantiers sur la publicité ciblée, les messageries privées et les métavers.

Impulser, avec d'autres pays actifs sur le sujet, une négociation internationale pour élaborer une charte des droits fondamentaux à l'ère du numérique à tout le moins à l'échelle européenne.

---

par les enquêteurs des Nations Unies sur les violences commises contre les Rohingyas en Birmanie. Une plainte collective a été déposée contre Facebook à ce sujet en Californie en décembre 2021

793 Paragraphe 72 de l'Agenda de Tunis.

794 La 17e réunion annuelle de l'IGF se déroulera à Addis-Abeba du 28 novembre au 2 décembre 2022, le programme s'articulera autour des thèmes suivants : Connecter tous les peuples et protéger les droits de l'homme, Éviter la fragmentation d'Internet, Gouvernance des données et protection de la vie privée, Favoriser la sûreté, la sécurité et la responsabilisation, Aborder les technologies de pointe, y compris l'IA

Conclusion

Les réseaux sociaux ont acquis en quelques années une place centrale dans le fonctionnement de nos sociétés contemporaines. A l'évidence, ils répondent à un besoin, comme en témoigne leur succès foudroyant. Ils constituent un progrès immense pour l'expression individuelle, y compris en permettant à des personnes très éloignées voire qui ne se sont jamais physiquement rencontrées de communiquer de manière quasi instantanée et en donnant une voix à ceux qui, autrefois, parce que minoritaires ou relégués aux marges de la société, étaient condamnés au silence. Dans le même temps, le bouleversement de l'espace public par de nouveaux modes de communication aux mains d'opérateurs privés peut inquiéter car il intervient au moment même où les démocraties sont fragilisées. La responsabilité des réseaux sociaux dans cette crise n'est d'ailleurs pas nulle. Ils amplifient les propos provocateurs et favorisent le cloisonnement des opinions contribuant à renforcer les divisions. Ils nourrissent des représentations biaisées du monde et, en faisant plonger l'individu dans le grand bain de « la société du spectacle », alimentent les frustrations. Pour autant, peut-on aller jusqu'à dire que la démocratie ne pourrait pas prospérer dans un environnement où chacun s'expose et prend la parole ? Que l'expression de tous ne pourrait que mener au chaos ? Que les passions qui s'expriment ne pourraient jamais conduire à faire émerger le bien commun ? Ne faut-il pas plutôt faire un pas en arrière et prendre du recul par rapport à cette révolution ?

A l'échelle de la société, une nouvelle forme de débat public plus éclairé et plus égalitaire est à construire. A l'échelle de l'individu, accompagner le changement à l'œuvre pour se prémunir du pire et profiter du meilleur est un objectif ambitieux mais qui semble accessible. L'usage des réseaux sociaux, désormais central, comme leur régulation, doivent être pleinement compatibles avec notre modèle démocratique.

C'est le défi ambitieux et stimulant que tentent de relever l'Union européenne et la France avec l'adoption des règlements *Digital services Act* et *Digital Markets Act*. Lutter contre les propos illicites, exiger des opérateurs loyauté et transparence, astreindre les très grandes plateformes à des obligations supplémentaires notamment en matière de modération afin de garantir la liberté d'expression, permettre un accès sécurisé aux algorithmes et aux données dans le cadre de recherches et d'audits, imposer des prescriptions en amont pour limiter les concentrations et les abus de position dominante, garantir un marché équitable, tels sont les objectifs que fixent le DSA et le DMA et qu'il conviendra de prochainement mettre en œuvre.

Le Conseil d'État propose d'aller plus loin, en cohérence avec le cadre juridique qui vient d'être défini au niveau de l'Union européenne. Ses recommandations s'articulent autour de trois axes : rééquilibrer les rapports de force en faveur des utilisateurs, armer la puissance publique pour réguler et optimiser l'usage des réseaux sociaux sans oublier la sauvegarde de la souveraineté et la dimension environnementale, penser les réseaux sociaux de demain. Il n'existe pas de solution miracle mais une multitude d'actions à différents niveaux qui supposent toutes la responsabilisation de l'ensemble des acteurs et notamment des utilisateurs. Jurgen Habermas soutient que la publicité immédiate de la parole intime et privée conduit à l'érosion des critères de rationalité qui structuraient jusqu'alors l'espace public et ainsi à une régression politique. Faut-il se résoudre à pareil constat ? Ne convient-il pas de démontrer que cette sagace analyse est empreinte de pessimisme et qu'il est encore temps d'inverser le mouvement ? La balle est dans le camp des opérateurs qui sont parties prenantes au processus de régulation, de la puissance publique qui se met en ordre de marche mais aussi des utilisateurs qui doivent raisonner leur usage pour faire des réseaux sociaux un outil au service de tous et non un instrument d'asservissement.

Liste des propositions de l'étude

1. Rééquilibrer les forces au profit de l'utilisateur et du citoyen

Rééquilibrer les relations contractuelles

Proposition n° 1

Afin de créer au niveau européen et national les conditions d'une « négociation collective » des conditions générales d'utilisation et des politiques de confidentialité, une politique ambitieuse de rééquilibrage de la relation contractuelle pourrait être menée, avec les autorités de régulation compétentes, selon les axes suivants :

- identifier des associations et regroupement d'associations susceptibles d'entrer en négociation avec les plateformes et les soutenir à cette fin ;

- créer, idéalement au niveau de la Commission européenne, une instance de concertation ayant pour objet d'asseoir à la même table l'ensemble des partenaires, d'identifier les clauses ou questions devant faire l'objet de discussions et de fixer conjointement l'ordre du jour des négociations et leur calendrier ;

- au fil des négociations, parvenir à l'élaboration conjointe de standards minimums pour les CGU et les politiques de confidentialité ;

- instaurer, à terme, un véritable « droit à la participation » des utilisateurs ou de leurs représentants à l'élaboration des conditions générales d'utilisation et des politiques de confidentialité des données des grandes plateformes.

Rééquilibrer par la sécurisation des identités et des âges des utilisateurs

Proposition n° 2

Promouvoir la généralisation des recours aux solutions d'identité numérique et à des tiers de confiance afin de mieux protéger les mineurs, de vérifier la majorité numérique et de garantir la fiabilité des échanges sur les réseaux sociaux, en en informant les internautes.

Envisager de rendre son recours obligatoire au niveau européen dans une version révisée du DSA.

Rééquilibrer par le paramétrage des interfaces

Proposition n° 3

Permettre à l'utilisateur d'opérer différents paramétrages ou réglages sur la plateforme afin de mieux se protéger des dangers des réseaux sociaux.

Promouvoir la réalisation de tableaux de bord informatifs pour améliorer la connaissance par l'utilisateur de ses modes de consommation.

Favoriser l'émergence de paramétrages par défaut qui protègent les droits des utilisateurs et respectent certaines conditions minimales de sécurité.

S'assurer que la mise en œuvre du DSA conduit à une attention particulière portée au design et au paramétrage des applications, notamment sur ceux qui permettent de limiter la « viralité » des contenus.

Rééquilibrer par l'information des utilisateurs sur les réseaux sociaux utilisés

Proposition n° 4

Créer un dispositif facultatif d'information sur les réseaux sociaux maniable et facilement accessible pour les utilisateurs sous forme de label, de score ou de flash info à partir d'un référentiel commun.

Rééquilibrer par l'information des utilisateurs sur les procédures de signalement et d'accompagnement

Proposition n° 5

Repenser la coordination entre les différentes plateformes de signalement et créer un point d'entrée unique pour faciliter l'exercice des droits et mieux accompagner les victimes.

Développer une application à télécharger sur les smartphones.

Rééquilibrer par l'accès à la connaissance et la recherche

Proposition n° 6

Soutenir l'agrément de chercheurs issus de la recherche française par les coordonnateurs des services numériques des États d'établissement des très grandes plateformes ainsi que leur accès effectif aux données de ces plateformes.

Apporter une assistance à la Commission européenne pour identifier les données à solliciter pour s'assurer du respect effectif du DSA.

Rééquilibrer en rendant le droit plus lisible et accessible

Proposition n° 7

Réaliser au niveau national une compilation des textes européens et nationaux applicables aux plateformes afin de rendre le droit des plateformes plus accessible et d'améliorer la qualité des futures normes. A terme, au niveau européen, engager un travail de compilation puis de codification de ces textes.

Au niveau national, adopter des lignes directrices sur l'usage des réseaux sociaux dans la vie professionnelle afin d'offrir aux administrations et aux entreprises ainsi qu'aux utilisateurs qui y travaillent un guide des pratiques relatives notamment à l'articulation vie privée-vie professionnelle.

Rééquilibrer en guidant les utilisateurs vers des contenus de qualité

Proposition n° 8

Soutenir les labels permettant de promouvoir des contenus fiables, de qualité et vérifiés.

Renforcer le rôle du CNNUM pour animer la concertation citoyenne sur les questions relatives aux usages des réseaux sociaux et initier une concertation sur la question de la qualité du débat public à l'heure des réseaux sociaux.

Rééquilibrer par la formation et l'éducation

Proposition n° 9

Établir un plan ambitieux d'éducation et de formation relatif à l'usage des réseaux sociaux destiné à tous les publics et mettre en place un pilotage unifié.

Diffuser les outils existants et en créer de nouveaux notamment un jeu vidéo à vocation pédagogique qui sensibilise aux dangers des réseaux sociaux et informe les utilisateurs.

Lancer une campagne de communication grand public permettant de faire prendre conscience de l'empreinte écologique ou carbone des réseaux sociaux notamment le visionnage de vidéos ou le *livestream*.

Rééquilibrer en sauvegardant la souveraineté

Proposition n° 10

Mettre en œuvre les propositions du groupe de travail européen sur les communs numériques.

Encourager les personnes publiques à utiliser les réseaux sociaux alternatifs ainsi que l'utilisation des communs numériques. Favoriser le recours aux réseaux sociaux alternatifs par l'administration et les collectivités locales pour accomplir leurs missions, au moins les plus sensibles (consultation des administrés ou citoyens sur des politiques publiques, remontée des difficultés, traitement des réclamations, échanges de données sensibles, etc.).

Mettre en œuvre une politique de soutien à l'industrie numérique européenne pour préserver l'autonomie stratégique.

2- Armer la puissance publique pour réguler et optimiser l'usage des réseaux sociaux

Mettre en œuvre les règlements européens

Proposition n° 11

Préparer rapidement la coordination entre la Commission européenne et les régulateurs nationaux par la mise en place d'un groupe de travail informel.

Proposer la création d'un comité de suivi transversal auprès de la Commission européenne (DMA, DSA, IA Act, RGPD, etc.).

Renforcer et réorganiser la puissance publique

Proposition n° 12

Au niveau national, créer un service interministériel d'expertise et d'analyse dédié à la régulation des plateformes numériques qui puisse fournir ses expertises aux différents régulateurs et administrations. Le doter des outils techniques, administratifs et juridiques suffisants en l'habilitant notamment au traitement de données personnelles pour des fins d'expertise publique.

Créer un réseau national des régulateurs du numérique, réunissant les régulateurs et les administrations en charge des plateformes numériques.

Renforcer les moyens des autorités de régulation nationale pour assurer leurs missions de régulation et pour jouer pleinement leur nouveau rôle de coordination et de coopération avec la Commission européenne.

Mieux lutter contre les comportements malveillants et les contenus illicites

Proposition n° 13

Définir et structurer une stratégie de réduction des risques pour lutter contre les comportements malveillants et les contenus illicites sur les plateformes dans un cadre coordonné et renforcer les outils répressifs. Réaliser de larges opérations de communication et de sensibilisation sur ces sujets.

Investir dans la recherche pour améliorer les outils techniques en vue de détecter les infractions et faire face à la masse des signalements.

Améliorer la culture numérique

Proposition n° 14

Instaurer une formation continue de pointe pour créer une culture commune du numérique en général et notamment des réseaux sociaux, sur le modèle de l'IHEDN.

Évaluer à moyen terme l'opportunité de bénéficier d'une certification d'experts en algorithmes.

Renforcer l'accompagnement des opérateurs publics et privés sur la question de la réutilisation des données

Proposition n° 15

Élaborer une doctrine d'emploi pour la réutilisation des données personnelles par les administrations et les entreprises, renforcer les moyens de la CNIL pour lutter contre la méconnaissance du RGPD et rediscuter du mécanisme de chef de file dans le cadre du RGPD si les dernières lignes directrices ne modifient pas les pratiques.

Optimiser l'usage des réseaux sociaux par l'administration

Proposition n° 16

Généraliser le recours aux *community managers* pour animer les relations entre les administrations et les administrés sur les réseaux sociaux grands publics.

Expérimenter des réseaux sociaux internes en s'inspirant des réseaux sociaux d'entreprises et l'accompagner d'une réflexion interne avec les instances représentatives des personnels afin de définir les différents niveaux de discussion et de les rendre compatibles avec l'organisation hiérarchique.

3- Penser les réseaux sociaux de demain

Proposition n° 17

Ouvrir et poursuivre les chantiers sur la publicité ciblée, les messageries privées et les métavers.

Impulser, avec d'autres pays actifs sur le sujet, une négociation internationale pour élaborer une charte des droits fondamentaux à l'ère du numérique à tout le moins à l'échelle européenne.

Fiches d'identité des principaux réseaux sociaux et assimilés

Les données relatives aux caractéristiques et aux modalités de la modération sont celles résultant des conditions générales d'utilisation (CGU) de chaque réseau.

(Classement par ordre alphabétique)

- Facebook
- Instagram
- LinkedIn
- Mastodon
- Reddit
- Télégram
- TikToc
- Twitter
- WhatsApp
- Wikipedia
- YouTube

FACEBOOK

Nombre estimé d'utilisateurs actifs dans le monde en janvier 2022 : 2,910 milliards

Source : Statista Research Department, 25 mars 2022

Création : 2004

Groupe : Meta (américain)

Type : réseau social à but lucratif

Modèle économique : publicité ciblée

Fonctionnalité principale : discussions et échanges de contenus

Siège social : États-Unis

Fonctionnalités

- **Principales** : créer sur son « mur » personnel du contenu photo et vidéo (*stories*, *Live*) et échanger avec des « amis » ; comptes Facebook publics visibles sans abonnement.
- **Secondaires** : communiquer *via Messenger,* acheter des produits sur *Marketplace.*

Caractéristiques

- **Âge minimal requis (CGU)** : 13 ans.
- **Données recueillies :** contenus publiés, fréquences de connexion des utilisateurs, données recueillies sur les appareils connectés avec un compte du groupe Meta (localisation GPS, fuseau horaire, adresse IP, noms des applications et fichiers de l'appareil, etc.).
- **Réutilisation des données :** personnalisation des produits, sécurisation des services et ciblage des contenus publicitaires pour les partenaires et annonceurs.

Modération

- **Modalités de signalement** : signalement anonyme des utilisateurs à propos de tous les contenus publiés (y compris les messages), algorithme de détection des contenus illicites puis modération humaine. La procédure de modération peut faire l'objet d'un recours par l'internaute directement sur la plateforme de Facebook puis d'un appel auprès de l'*Oversight Board* de Meta.
- **Sanctions** : retrait ou blocage des comptes en cas de violation des conditions générales d'utilisation.

INSTAGRAM

Nombre estimé d'utilisateurs actifs dans le monde en janvier 2022 : 1,478 milliards

Source : Statista Research Department, 25 mars 2022

Création : 2010
Groupe : Meta (américain)
Type : réseau social à but lucratif
Modèle économique : publicité ciblée
Fonctionnalité principale : partage de contenus
Siège social : États-Unis

Fonctionnalités

- **Principales** : créer, échanger du contenu photo ou vidéo sur un compte privé, public ou professionnel, possibilité de filmer en *live* et de publier des *stories*
- **Secondaires** : communiquer via *Direct Messaging*, acheter des produits sur *Marketplace*.

Caractéristiques

- **Âge minimal requis (CGU)** : 13 ans.
- **Données recueillies :** contenus publiés, connexions des utilisateurs, données recueillies sur les appareils connectés avec un compte du groupe Meta (localisation GPS, fuseau horaire, adresse IP, noms des applications et fichiers de l'appareil, etc.).
- **Réutilisation des données :** personnalisation des produits, sécurisation des services et ciblage des contenus publicitaires pour les partenaires et annonceurs.

Modération

- **Modalités de signalement** : signalement anonyme des utilisateurs à propos de tous les contenus publiés (y compris les messages), algorithme de détection des contenus illicites puis modération humaine. La procédure de modération peut faire l'objet d'un recours par l'internaute directement sur la plateforme de Facebook puis d'un appel auprès de *l'Oversight Board* de Meta.
- **Sanctions** : retrait ou blocage des comptes en cas de violation des conditions générales d'utilisation.

LINKEDIN

Nombre estimé d'utilisateurs actifs mensuels en janvier 2022 : 830 millions d'utilisateurs dans le monde dont 24 millions d'utilisateurs en France

source : Ch. Asselin*, LinkedIn : les chiffres incontournables en 2022 en France et dans le monde*, mai 2022, digimind

Création : 2002, et 2008 pour la version française

Groupe : Microsoft (rachat en 2016, américain)

Type : réseau social professionnel à but lucratif

Modèle économique : publicité (18%), abonnements (20%), services aux entreprises (62%)

Fonctionnalité principale : recherche d'emplois et création d'un réseau professionnel

Siège social : États-Unis

Fonctionnalités

- **Principales** : rester en contact ou trouver de nouveaux contacts professionnels, échanger avec ses contacts, rechercher un emploi ou publier des offres d'emplois.
- **Secondaires** : échanges de contenus et *posts* apparaissant sur un fil d'actualité.

Caractéristiques

- **Âge minimal requis (CGU)** : 16 ans.
- **Données recueillies** : nom, adresse email, renseignements sur l'activité professionnelle, calendrier et contacts si synchronisés, contenu publié, données d'utilisations, données géographiques, messages.
- **Réutilisation des données** : proposer, personnaliser et améliorer les produits LinkedIn, proposer des offres d'emploi personnalisées, mettre en relation les profils professionnels compatibles.

Modération

- **Modalités de signalement** : signalement des utilisateurs puis modération humaine (quatre centres de modération sont présents aux États-Unis, en Inde, à Singapour et en Irlande).
- **Sanction :** limitation de l'utilisation des services, dont le nombre de relations, restriction, suspension ou clôture du compte en cas de violation des conditions générales d'utilisation.

MASTODON

Nombre estimé d'utilisateurs actifs en 2022 : plus de 4,4 millions d'utilisateurs dans le monde

source : « Join Mastodon » sur le site de Mastodon

Création *:* 2016

Fondateur : Eugen Rochko (allemand)

Type : réseau social collaboratif et décentralisé

Modèle économique *:* participatif

Fonctionnalité principale : microblogging

Fonctionnalités

- **Principales** : échanger des messages de 500 caractères maximum, images et autres contenus, utiliser les deux fils d'actualité, l'un personnalisé en fonction des abonnements, l'autre généraliste regroupant tous les utilisateurs des instances fédérées. La plateforme est auto-hébergée et décentralisée *via* ActivityPub.

Caractéristiques

- **Âge minimal requis (CGU)** : 16 ans.
- **Données recueillies** : adresse électronique, adresse IP, nom du navigateur web (obligatoires) ; le nom, la photo de profil (facultatifs).
- **Réutilisation des données** : à des fins de modération de la communauté, notification des usages de la plateforme sur l'appareil de connexion.

Modération

- **Modalités de signalement** : instances auto-gérées, chaque communauté peut limiter ou filtrer les types de contenus indésirables.
- **Sanctions** : possibilité de masquer et bloquer un utilisateur (modération individuelle), de signaler un utilisateur en précisant quels points de la charte sont méconnus, signalement qui sera ensuite examiné par une équipe de modération bénévole (modération à l'échelle du système) qui peut geler ou limiter le compte, décaler son contenu sensible, ou le supprimer.

REDDIT

Nombre estimé d'utilisateurs actifs en janvier 2022 : 430 millions d'utilisateurs dans le monde

Source : Statista Research Department, 25 mars 2022

Création : 2006

Groupe : Advance Publications (américain)

Type : réseau social à but lucratif

Modèle économique : publicité et abonnements Premium

Fonctionnalité principale : discussion et création de contenus

Siège social : États-Unis

Fonctionnalités

- **Principales :** plateforme de discussions divisées en forums, les « *subreddits* », où les utilisateurs y sont à la fois des créateurs de contenu, des lecteurs et des évaluateurs.
- **Secondaires** : possibilité d'évaluer le contenu à l'aide *d'Upvotes* (votes positifs) et de *Downvotes* (votes négatifs).

Caractéristiques

- **Âge minimal requis (CGU)** : 13 ans.
- **Données recueillies** : pseudonyme, âge, contenu publié, données d'utilisations, données géographiques, messages, commentaires, votes.
- **Réutilisation des données** : pour fournir, maintenir, améliorer, rechercher et développer les services, protéger la sécurité de Reddit, envoyer des notifications ; analyser les tendances, l'utilisation et les activités liées aux services ; optimiser le ciblage publicitaire.

Modération

- **Modalités de signalement :** utilisateurs bénévoles en fonction des règles qu'ils éditent eux-mêmes au sein des groupes.
- **Sanctions :** suppression des publications et des commentaires de leur communauté, interdiction des utilisateurs susceptibles d'enfreindre les règles de la communauté.

TELEGRAM

Nombre estimé d'utilisateurs actifs en janvier 2022 : 550 millions d'utilisateurs dans le monde

Source : Statista Research Department, 25 mars 2022

Création : 2013

Propriétaire et fondateur : Pavel Dourov (russe)

Type : réseau social à but lucratif

Modèle économique : fortune personnelle de Pavel Dourov jusqu'en 2020 (et levée de fonds de 1 milliard de dollars), puis abonnements payants (2022)

Fonctionnalité principale : messagerie

Siège social : Dubaï

Fonctionnalités

- **Principales** : envoyer des messages à d'autres utilisateurs, créer des conversations de groupe, appeler, rejoindre des conversations publiques, des chaînes, ou des salons privés, sur invitation.
- **Secondaires :** messagerie cryptée de bout en bout (sauf dans les groupes), minuteur d'autodestruction (disponible que dans les conversations secrètes).

Caractéristiques

- **Âge minimal requis (CGU)** : 16 ans.
- **Type de données collectées** : numéro de téléphone, photo, pseudo.
- **Réutilisation des données collectées :** seulement à des fins d'amélioration du service, et non à des fins commerciales.

Modération

- **Modalités de signalement** : signalement possible par les utilisateurs sur les contenus « publics ».
- **Sanctions** : suppression des contenus publics illégaux mais pas dans les groupes privés, blocage temporaire ou définitif en cas de *phishing*, spams, ou encore de violation des conditions générales d'utilisation.

TikTok

Nombre estimé d'utilisateurs actifs en janvier 2022 : 1 milliard d'utilisateurs dans le monde

Source : Statista Research Department, 25 mars 2022

Création : 2016

Groupe : ByteDance (chinois)

Type : réseau social à but lucratif

Modèle économique : publicité ciblée

Fonctionnalité principale : échange de contenus vidéos

Siège social : Chine

Fonctionnalités

- **Principales :** réaliser et visionner des contenus vidéos accompagnés de musique, de format court allant de 3 à 180 secondes, pré-enregistrés ou en *live* (outil de montages son et vidéo, voir le *TikTok Creative Hub*).
- **Secondaires :** s'abonner à des chaînes ou profils, *liker* et commenter les contenus, créer des communautés, discussions et commentaires possibles, *market place*.

Caractéristiques

- **Type de données recueillies** : âge, nom, adresse IP, identifiant, numéro de téléphone, vues, contenus créés, messages, métadonnées associées (géolocalisation), etc.
- **Réutilisation des données collectées** : réutilisation à des fins d'amélioration du service et à des fins publicitaires.

Modération

- **Âge minimal requis (CGU)** : 13 ans
- **Modalités de signalement** : signalement par les utilisateurs des contenus et des comptes d'utilisateurs ; détection des abus et des violations des CGU par un algorithme et une équipe de modération (activation possible de sous filtres et mots clés par les utilisateurs).
- **Sanctions** : blocage des comptes pour motifs de violation des CGU ou suspicion de violation, possibilités de blocage ou suspension, permanent ou temporaire.

TWITTER

Nombre estimé d'utilisateurs actifs en janvier 2022 : 436 millions d'utilisateurs dans le monde

Source : Statista Research Department, 25 mars 2022

Création : 2006

Société américaine côtée en bourse

Type : réseau social à but lucratif

Modèle économique : publicité, collectes de fonds

Fonctionnalité principale : microblogging

Siège social : États-Unis

Fonctionnalités

- **Principales** : échanger des messages de 280 caractères maximum dits « *tweet* », images et autres contenus au sein d'un réseau social, leur donner de la visibilité grâce à des *hashtags* et aux partages de contenus dit « *retweet* », suivre l'actualité au sein de fils d'actualités.
- **Secondaires** : messagerie privée.

Caractéristiques

- **Âge minimal requis** (CGU) : 13 ans.
- **Données recueillies** : date de naissance, nom d'utilisateur, email, données d'activité, adresse postale si compte professionnel.
- **Réutilisation des données** : proposer des contenus pour offrir des services personnalisés aux utilisateurs, amélioration de la qualité des publicités, mesure de l'efficacité des publicités, permettre aux annonceurs d'avoir une meilleure audience.

Modération

- **Modalités de signalement** : signalement par les utilisateurs des *tweets*, et utilisation d'un logiciel de détection automatique.
- **Sanction :** injonction de modification d'un contenu, indisponibilité du contenu, limitation de la capacité à partager du contenu (jusqu'à 7 jours), verrouillage en attente de la vérification de la propriété du compte, suppression définitive. Possibilité de faire appel d'une suspension définitive *via* la plateforme.

WHATSAPP

Nombre estimé d'utilisateurs actifs en janvier 2022 : 2 milliards d'utilisateurs dans le monde

Source : Statista Research Department, 25 mars 2022

Création : 2009

Groupe : Meta (américain)

Type : messagerie instantanée

Modèle économique : monétisation de la base de données auprès du groupe Meta

Fonctionnalité principale : système de messagerie instantanée

Fonctionnalités

- **Principales** : communiquer en ligne *via* messages chiffrés de bout en bout par défaut pour les messages personnels (y compris messages vocaux), *via* appels vidéo et audio, dans des discussions bilatérales ou multilatérales (groupes).
- **Secondaires** : partager des documents, poster un statut et des « stories » (éphémères), afficher une photo de profil.

Caractéristiques

- **Âge minimal requis (CGU)** : 16 ans.
- **Type de données recueillies** : âge, nom, adresse IP, identifiant, numéro de téléphone, messages émis et reçus, fichiers médias au sein des messages, statut, métadonnées associées (géolocalisation), etc.
- **Réutilisation des données collectées** : réutilisation à des fins d'amélioration du service, et indirectement à des fins publicitaires *via* le transfert de données.

Modération

- **Modalités de signalement** : signalement par les utilisateurs de contenus spécifiques y compris privés ou de comptes d'utilisateurs ; système de détection des abus et des violations des CGU ; modérateurs pour des *trolls* avec équipe de modération française
- **Sanction :** possibilités de blocage ou suspension des comptes pour violation des CGU ou suspicion raisonnable de violation, permanent ou temporaire.

WIKIPEDIA

Nombre estimé d'utilisateurs actifs en janvier 2022 : plus de 18 000 utilisateurs actifs sur le wikipedia français et 136 000 environ pour le wikipedia anglais

Source: Politique de confidentialité, Site Wikipédia, https://meta.wikimedia.org/wiki/Privacy_policy/fr

Création : 2001

Groupe : Wikimédia Foundation (américain)

Type : plateforme collaborative

Financement : contribution des utilisateurs et dons

Fonctionnalité principale : encyclopédie participative

Fonctionnalités

- **Principales** : développer une encyclopédie en ligne qui offre un contenu libre, objectif et vérifiable par la contribution de chacun, dans plusieurs versions multilingues qui ne fait pas l'objet d'une propriété ou d'une licence.
- **Secondaires** : échanges entre wikipédiens pour élaborer puis vérifier les contenus.

Caractéristiques

- **Pas d'âge minimal requis** pour la contribution ou la consultation (CGU).
- **Données recueillies** : possibilité de contribuer sans être inscrit à la plateforme, dans ce cas recueil de l'adresse IP. Si inscription : nom d'utilisateur, adresse IP, mot de passe.
- **Réutilisation des données** : association de l'adresse IP ou du compte utilisateur aux publications et partage d'informations si autorisation aux prestataires de services pour la protection de la plateforme pour des raisons juridiques.

Modération

- **Modération humaine** : contributeurs chargés de vérifier que la modification d'un article est sensée et corriger les erreurs.
- **Modération algorithmique :** possibilité pour les communautés (par pays) d'utiliser des filtres, basés sur des mots-clés, qui limitent les modifications grossières.
- **Sanctions** : Possibilité de bloquer un utilisateur et de supprimer son contenu, certaines modifications sont soumises à approbation avant d'être publiées.

YOUTUBE

Nombre estimé d'utilisateurs actifs en janvier 2022 : 2,562 milliards d'utilisateurs dans le monde

Source : Statista Research Department, 25 mars 2022

Création : février 2005 par Steve Chen, Chad Hurley et Jawed Karim

Groupe : Alphabet Inc. (Google) depuis 2006 (américain)

Type : réseau social à but lucratif

Modèle économique : publicité ciblée

Fonctionnalité principale : partage de contenus vidéos

Siège social : États-Unis

Fonctionnalités

- **Principales :** visualiser et partager des contenus vidéos de différents types (divertissement, *lives*, « *shorts* » sur le modèle de TikTok, etc.).
- **Secondaires :** commentaires possibles.

Caractéristiques

- **Âge minimal requis (CGU)** : 15 ans (pas de minimum pour YouTube Kids si habilité par le tuteur légal).
- **Type de données recueillies** : âge, nom, adresse IP, identifiant, numéro de téléphone, vues, *likes*, commentaires, etc.
- **Réutilisation des données collectées** : réutilisation à des fins d'amélioration du service et à des fins publicitaires.

Modération

- **Modalités de signalement** : signalement par les utilisateurs ; système de détection des abus et des violations des CGU par un algorithme ; modération humaine pour les *tchats* et pour vérifier la modération par algorithme.
- **Sanctions** : en cas de violation des CGU, l'accès de l'utilisateur peut être suspendu ou bloqué ; suspension ou fermeture du compte Google ou de l'accès à tout ou partie du service dans certains cas.

Le droit des réseaux sociaux

1. Synthèse du droit applicable

Il est possible de réaliser une synthèse du régime juridique applicable aux réseaux sociaux, en soulignant, au préalable, que ce régime se trouve au confluent de quatre droits fondamentaux (la liberté d'entreprendre, la liberté d'expression et de communication, le droit à la protection de sa vie privée, la protection de l'ordre public) qui doivent être conciliés.

A la base du régime juridique des réseaux sociaux se trouve la relation contractuelle qui se noue entre l'utilisateur et la plateforme : il s'agit d'un contrat de droit privé dont l'objet principal est la communication et l'échange de contenus, sachant que, à titre secondaire, les plateformes proposent des services de messagerie et des *markets place*. Chaque fonctionnalité entraîne l'application de branches du droit distinctes (droit proscrivant les abus de la liberté d'expression et les contenus illicites mais aussi les comportements illicites de manière générale, notamment le droit relatif à la sécurité des produits échangés, aux pratiques commerciales, à la publicité, etc.). Par ailleurs, les modalités de fonctionnement entraînent également l'application de règles de droit (traitement des données, utilisation d'algorithmes). Mais la présentation du droit des réseaux sociaux à travers ses fonctionnalités et modes de fonctionnement ne reflète pas toute la variété de normes applicables, notamment le droit qui s'applique à l'environnement du contrat conclu c'est-à-dire au marché (comme le droit de la concurrence).

On peut aussi s'attacher à identifier les principales obligations qui pèsent sur les deux principaux acteurs : les plateformes et les usagers.

- Compte tenu de la nature particulière des réseaux sociaux qui sont un mode de communication participatif, les utilisateurs sont en première ligne. Ils engagent tout d'abord leur responsabilité pénale en raison des propos qu'ils tiennent et des comportements proscrits qu'ils sont susceptibles de pratiquer sur les réseaux sociaux (injures, diffamation, harcèlement, *revenge porn*, etc.) sur le fondement du code pénal ou de la loi de 1881. Ils engagent également leur responsabilité contractuelle lorsqu'ils ne respectent pas les termes des CGU (propos ou non retrait de contenus non conformes), voire leur responsabilité professionnelle s'ils méconnaissent leurs obligations résultant du droit du travail ou du droit de la fonction publique ou même du code électoral. L'utilisateur peut parfois être considéré comme co-responsable de traitement lorsqu'il détermine les modalités et les finalités du traitement. Lorsque les utilisateurs sont également « influenceurs », ils peuvent également engager leur responsabilité en cas de pratiques commerciales trompeuses (un régime particulier de protection s'applique en outre à ceux de ces « influenceurs » qui sont mineurs de moins de 16 ans).

- Quant aux plateformes, de façon générale, elles doivent évidemment respecter leurs obligations contractuelles telles qu'elles découlent des CGU en fournissant des prestations prévues de manière loyale et non trompeuse et sans porter atteinte au respect de la vie privée des utilisateurs (*e-privacy*) comme à leur

droit à la protection de leurs données personnelles (RGPD). Sans être soumises à des obligations de surveillance généralisée, elles doivent également coopérer de façon effective à la lutte contre les infractions commises ou susceptibles d'être commises sur les plateformes, respecter les règles spécifiques de retraits de contenus et de contestation des retraits (DSA, TCO), respecter les règles de traitement de certains contenus illicites (SMA), appliquer les règles spécifiques lorsqu'elles donnent accès à des contenus protégés par le droit d'auteur (directive 2019/790), utiliser des algorithmes (SIA) dans le respect des règles (*AI Act* à venir) et enfin, au niveau du marché, ne pas chercher à en fausser le fonctionnement normal (droit de la concurrence, du DMA, de la publicité). Des obligations spécifiques s'imposent à elles à l'égard des mineurs (protection de contenus, interdiction d'utiliser leurs données à des fins commerciales, etc.).

Ainsi s'appliquent à elles :

- En tant que service de communication en ligne : la directive *e-privacy* (notamment réglementation sur les cookies) ;
- En tant que responsable de traitement : les règles du RGPD et la directive police/justice sur les obligations de conservation des données ;
- En tant qu'exploitant d'un SIA : le futur règlement IA Act ;
- En tant que fournisseur de services intermédiaires :

  Vis-à-vis des utilisateurs finaux :

  -- Dans la relation contractuelle avec l'utilisateur : le code de la consommation et le DSA ;

  -- Sur le contrôle des contenus : les règles issues notamment des règlements DSA et TCO pour toutes les plateformes et les règles particulières issues du DSA s'agissant des très grandes plateformes ; la directive SMA s'agissant des services de partage de vidéos ; la directive 2019/790 s'agissant des services de partage de contenus en ligne ;

  Vis-à-vis des utilisateurs professionnels pour les services d'intermédiation en ligne : le règlement B to B ;

- En tant qu'opérateur du marché : le droit de la concurrence et en tant que *gatekeepers*, le DMA.

2. Tableau des obligations différenciées imposées aux opérateurs par le Digital Markets Act (DMA) et des sanctions applicables

Sanctions applicables : art. 30 et 31 du DMA *		
Thématique	**Articles du DMA**	Obligations imposées aux contrôleurs d'accès
Statut de contrôleur d'accès	*Art. 3§3*	Notifier à la Commission le statut de contrôleur d'accès en fournissant les informations requises
Données personnelles	*Art. 5 (a)*	Interdiction de combiner les données personnelles de leurs services avec celles provenant de tout autre service du contrôleur ou de services tiers
	Art. 6	Interdiction d'utiliser les données non accessibles au public, générées par les entreprises utilisatrices ou les utilisateurs finaux (§ 1)
		Fournir gratuitement aux entreprises utilisatrices un accès aux données générées par l'utilisation des services de plateforme essentiels ; sur le volet des données personnelles, un consentement de l'utilisateur final doit être recueilli au préalable
Rééquilibrage des relations entre les contrôleurs d'accès et les entreprises utilisatrices	*Art. 5*	Autoriser les entreprises utilisatrices à proposer les mêmes produits à des prix différents de ceux offerts par les services d'intermédiation en ligne du contrôleur d'accès (b)
		Autoriser les entreprises utilisatrices à promouvoir leurs offres auprès des utilisateurs finaux grâce aux services de plateforme essentiels du contrôleur d'accès (c)
		Interdiction d'empêcher les entreprises utilisatrices de faire part aux autorités publiques de préoccupations quant aux pratiques d'un contrôleur d'accès (d)
		Interdiction d'exiger des entreprises utilisatrices ou utilisateurs finaux qu'ils s'enregistrent à tout autre service de plateforme essentiel comme condition d'accès à l'un de ces services (e)
	Art. 6	Autoriser les entreprises utilisatrices à interopérer avec les fonctionnalités du système d'exploitation du contrôleur d'accès (f)

Protection de la concurrence	*Art. 6*	Autoriser l'utilisation d'applications logicielles de tiers interopérant avec les systèmes d'exploitation du contrôleur d'accès (c)
		Autoriser les utilisateurs finaux à désinstaller toute application logicielle préinstallée dans son service de plateforme essentiel, sauf si elle est essentielle au fonctionnement du système d'exploitation (b)
		Interdiction d'accorder un traitement plus favorable aux services proposés par le contrôleur d'accès lui-même (d)
		Interdiction de restreindre techniquement la capacité des utilisateurs finaux à s'abonner à d'autres services (e)
Transparence	*Art. 5*	Communiquer aux annonceurs et éditeurs des informations relatives au prix payé ou aux rémunérations pour les services publicitaires (g)
	Art. 13	Fournir à la Commission une description soumise à un audit indépendant de toutes les techniques de profilage des consommateurs, mise à jour au moins une fois par an
Outils de performance	*Art. 6*	Fournir aux annonceurs et éditeurs, à leur demande et gratuitement, un accès aux outils de mesure de performance du contrôleur d'accès (g)
Portabilité des données	*Art. 6*	Assurer la portabilité effective des données d'une entreprise utilisatrice ou d'un utilisateur final avec les outils adéquats (h)
Concentrations	*Art. 12*	Informer la Commission de tout projet de concentration impliquant un service du secteur numérique, en complément de la notification à une autorité de concurrence

Utilisateur final : « *toute personne physique ou morale utilisant des services de plateforme essentiels autrement qu'en tant qu'entreprise utilisatrice* » (point 16 de l'article 2).

Entreprise utilisatrice : « *toute personne physique ou morale agissant à titre commercial ou professionnel qui utilise des services de plateforme essentiels aux fins ou dans le cadre de la fourniture de biens ou de services à des utilisateurs finaux* » (point 17 de l'article 2).

*** Article 30** : amendes

*** Article 31** : astreintes

3. Tableau des obligations différenciées imposées aux opérateurs par le Digital Services Act (DSA) et des sanctions applicables

Le DSA distingue deux catégories de plateformes, auxquelles sont rattachées des obligations différenciées :

- les **très grandes plateformes**, ayant une audience supérieure à 10 % des 450 millions de consommateurs européens **;**
- les autres plateformes en ligne (places de marché en ligne, boutiques d'applications, plateforme d'économie collaborative, plateformes de médias sociaux, etc.).

Lorsque les deux types de plateformes sont concernées par les obligations sans distinction, mention sera faite : **toutes les plateformes**.

Thématique	Type de plateforme concernée	Articles du DSA	Obligations imposées
Transparence	**Sanction applicable : art. 42 ***		
	Toutes les plateformes	Art. 13	Publication de rapports sur les éventuelles activités de modération de contenu menées par les plateformes
		Art. 23	Fournir des informations supplémentaires dans les rapports, comme le nombre de litiges transmis aux organes de règlement extrajudiciaire des litiges
	Sanction applicable : art. 59, 59 bis et 60 *		
	Très grande plateforme	Art. 33	Fournir différents rapports supplémentaires au coordinateur numérique de l'État membre et à la Commission, comme le rapport de mise en œuvre des recommandations d'audit
		Art. 29	Fournir au moins une option pour chacun de leurs systèmes de recommandation
		Art. 31	Partager avec la Commission les données nécessaires pour contrôler et évaluer le respect du DSA ; partager les données avec les chercheurs agréés.
Protection des utilisateurs dans leurs usages des réseaux sociaux	**Sanction applicable : art. 42 ***		
	Toutes les plateformes	Art. 12	Obligation d'adopter des conditions d'utilisation respectant les droits fondamentaux
	Sanction applicable : art. 59, 59 bis et 60 *		
	Très grande plateforme	Art. 27	Obligation de mettre en place des mesures d'atténuation des risques systémiques identifiés

Modération des contenus	**Sanction applicable : art. 42 ***		
	Toutes les plateformes	Art. 14	Obligation d'instaurer un mécanisme de notification de contenu considéré comme illicite par l'utilisateur
		Art. 15	Obligation d'informer l'utilisateur de la décision de retrait ou du blocage d'accès au contenu avec un exposé des motifs
		Art. 17 & 18	Obligation d'instaurer un mécanisme de réclamation et de recours et une possibilité de règlement extrajudiciaire des litiges
		Art. 19	Obligation de traiter en priorité les notifications provenant d'un signaleur de confiance
		Art. 20	Obligation de suspendre le traitement des notifications abusives (réclamations infondées fréquentes)
Coopération (entre les plateformes, les États, les autorités compétentes de l'UE	**Sanction applicable : art. 42 ***		
	Toutes les plateformes	Art. 10	Obligation d'instaurer un point de contact unique pour communiquer avec les autorités des États membres, la Commission et le Comité
		Art. 11	Obligation de désigner un représentant légal si la plateforme n'a pas d'établissement dans l'Union mais y propose des services ; ce représentant légal doit disposer des pouvoirs et ressources nécessaires pour coopérer avec les autorités des États membres, la Commission et le Comité et se conformer à leurs décisions.
		Art. 15 bis	Obligation de signaler les soupçons d'infractions pénales graves aux services répressifs et judiciaires de l'État membre ou des États membres concernés et de fournir toutes les informations pertinentes disponibles
	Sanction applicable : art. 59 et 60 *		
	Très grande plateforme	Art. 37	Participation à l'application des protocoles de crises limités à des circonstances exceptionnelles, affectant la sécurité ou la santé publiques

Publicité en ligne	**Sanction applicable : art. 42 ***		
	Toutes les plateformes	Art. 24	Garantir la transparence de la publicité en ligne pour les utilisateurs, afin qu'ils puissent identifier l'annonceur et les paramètres utilisés dans le ciblage
		Art. 24 bis	Obligation de garantir la transparence des systèmes de recommandation
		Art. 24 *quater*	Obligation d'instaurer une traçabilité des professionnels qui peuvent conclure un contrat avec les consommateurs via la plateforme
		Art. 36	Respecter les codes de conduite élaborés au niveau de l'Union, pour accroître la transparence au-delà des exigences du DSA
	Sanction applicable : art. 59, 59 bis et 60 *		
	Très grande plateforme	Art. 30	Obligation de tenir un registre contenant des informations sur les publicités et les annonceurs
Respect des normes	**Sanction applicable : art. 59, 59 bis et 60 ***		
	Très grande plateforme	Art. 32	Obligation de désigner un ou plusieurs responsables de la conformité chargés de contrôler si elles respectent le DSA
		Art. 34	Respecter l'élaboration de normes volontaires établies par les organismes de normalisation européens et internationaux pertinents
		Art. 35	Respecter les codes de conduite élaborés au niveau de l'Union pour contribuer à la bonne application du DSA
Mise en œuvre d'audits et d'évaluations des risques	**Sanction applicable : art. 59, 59 bis et 60 ***		
	Très grande plateforme	Art. 26	Obligation de recenser au moins une fois par an tout risque systémique important provenant du fonctionnement de leurs services dans l'Union
		Art. 28	Obligation de se soumettre à des audits externes et indépendants au moins une fois par an à leurs frais et d'adopter un rapport de mise en œuvre des recommandations d'audit avec un exposé des motifs si elles ne les suivent pas

Précision

Le « Comité » cité dans le tableau est le « Comité européen des services numériques », qui a pour responsabilité d'assurer la surveillance des fournisseurs de services intermédiaires suivant l'article 47 du DSA.

Sanctions *

- article 42 : amendes et astreintes pour toutes les plateformes ;
- article 55 : mesures provisoires ;
- article 58 : décision de non-conformité ;
- article 59 : amendes pour les très grandes plateformes ;
- article 59 bis : surveillance renforcée de la très grande plateforme par la Commission en cas de violation des obligations de gestion des risques systémiques ;
- article 60 : astreintes pour les très grandes plateformes.

4 – Tableaux des règles d'application territoriale des principaux textes européens concernant les réseaux sociaux

RGPD – Applicabilité dès lors qu'au moins un des deux (responsable de traitement ou utilisateur) est établi dans l'UE	
Traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant **sur le territoire de l'Union, que le traitement ait lieu ou non dans l'UE**	Traitement des données à caractère personnel par un responsable du traitement ou un sous-traitant **qui n'est pas établi dans l'UE**
Personne concernée par le traitement résidant dans l'UE	
Oui	Oui
Personne concernée par le traitement ne résidant pas dans l'UE	
Oui	Non

DSA – Applicabilité quel que soit le pays du service intermédiaire ou du service de plateforme, tant que l'utilisateur final a un lieu d'établissement ou de résidence dans l'UE	
Service intermédiaire établi **dans l'UE**	Service intermédiaire établi **hors UE**
Bénéficiaire établi dans l'UE	
Oui	Oui
Bénéficiaire établi hors UE	
Non	Non

DMA – Applicabilité quel que soit le pays du service intermédiaire ou du service de plateforme, tant que l'utilisateur final a un lieu d'établissement ou de résidence dans l'UE	
Services de plateforme essentiels fournis ou proposés par des contrôleurs d'accès établis **dans l'UE**	Services de plateforme essentiels fournis ou proposés par des contrôleurs d'accès établi**s hors UE**
Entreprises utilisatrices et utilisateur final établi dans l'UE	
Oui	Oui
Entreprises utilisatrices consommateur établis hors UE	
Non	Non

Règlement 2019/1150 du 20 juin 2019 « ***promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne » dit règlement platform to Business ou P2B*** » **– Applicabilité quel que soit le pays du fournisseur de services d'intermédiation en ligne, dès lors que le consommateur est établi dans l'UE**	
Fournisseurs de services d'intermédiation en ligne, moteurs de recherche **établis dans l'UE**	Fournisseurs de services d'intermédiation en ligne, moteurs de recherche **établis hors UE**
Entreprises utilisatrices ou consommateur établis dans l'UE	
Oui	Oui
Entreprises utilisatrices consommateur établis hors UE	
Non	Non

Règlement 2021/784 dit « TCO » du 29 avril 2021 – Applicabilité quel que soit le pays du fournisseur de service, dès lors que le contenu est visible dans l'UE
Fournisseurs de services diffusant des contenus terroristes
Dans l'Union européenne
Oui
Hors de l'Union européenne
Non

Cycle de conférences du Conseil d'État sur les réseaux sociaux

Discours introductif du cycle de conférences sur les réseaux sociaux

Conseil d'État, conférence inaugurale du cycle conférences sur Les réseaux sociaux*, le 27 octobre 2021, par Bruno Lasserre, vice-président du Conseil d'État*[795]

Mesdames et Messieurs les présidents,
Messieurs les professeurs,
Monsieur le directeur du journal La Croix,
Mesdames et Messieurs les internautes qui nous suivez depuis votre écran,

Chers amis et chers collègues,

Je suis heureux d'ouvrir ce nouveau cycle de conférences qui rythmeront la confection de l'étude annuelle du Conseil d'État pour 2022, qui portera sur les réseaux sociaux. L'intérêt du Conseil d'État pour les différents aspects de la révolution numérique est ancien : dès 1997, il avait ainsi réalisé une étude intitulée *Internet et les réseaux numériques*[2], avant de consacrer son étude annuelle de 2014 aux enjeux du numérique en termes de droits fondamentaux[3] et celle de 2017 au phénomène de l'« ubérisation[4] ». Nous aurions pu en rester là, mais il nous est apparu que la place considérable qu'occupent aujourd'hui les réseaux sociaux dans notre société, au croisement de nombreuses problématiques contemporaines, sociales, politiques, économiques et culturelles, en font un sujet autonome suffisamment actuel et complexe – c'est un euphémisme – pour justifier une nouvelle étude.

Actuel, d'une part, car même si je dois confesser que lorsque le bureau a décidé de retenir ce sujet, aucun de ses membres n'avait encore jamais posté de vidéo sur TikTok, personne ne peut ignorer que les réseaux sociaux sont désormais partout.

795 Texte écrit en collaboration avec Guillaume Halard, magistrat administratif, chargé de mission auprès du vice-président du Conseil d'État.

On estime ainsi que plus de 70 % des personnes disposant d'une connexion à internet dans le monde utilisent un ou plusieurs réseaux sociaux au moins une fois par jour. Et bien qu'en queue de peloton sur ce sujet, 53 millions des Français connectés y consacrent en moyenne plus d'une heure et demi par jour, 84 % des 18-24 ans les utilisent et une majorité des 60-69 est désormais membre d'au moins un de ces réseau[5]. En une quinzaine d'années, ces outils se sont ainsi imposés au cœur de nos vies quotidiennes et sont destinés, selon toute vraisemblance, à y rester. Actuel, d'autre part, car des campagnes de désinformation menées par la Russie à l'assassinat de Samuel Paty, en passant par les printemps arabes, la crise des gilets jaunes ou le mouvement #metoo, nous avons comme l'impression que les réseaux sociaux jouent toujours un rôle central, voire moteur dans les mouvements qui bousculent en profondeur nos sociétés. Dans quelle mesure et dans quels cas en sont-ils la cause ou de simples révélateurs ? C'est une question ouverte et largement débattue à laquelle le Conseil d'État s'intéressera naturellement au cours de cette année.

Une bonne partie de la complexité du sujet tient précisément à la difficulté d'appréhender les effets du développement des réseaux sociaux et, à plus fort raison, d'entrevoir ce qu'ils auront fait de nous dans dix ou vingt ans. La tentation est grande de n'y voir que les accessoires d'un capitalisme planétaire se nourrissant de notre narcissisme et accompagnant la montée inexorable d'un individualisme voué à détruire systématiquement ce qui reste des structures sociales et politiques qui ont garanti, jusqu'aujourd'hui, notre vie en collectivité. A l'opposé, certains croient déceler dans les réseaux sociaux les outils d'un approfondissement de la démocratie où le peuple aurait enfin son mot à dire et où chaque individu, libéré du carcan archaïque dans lequel il est resté enfermé trop longtemps, pourrait se réaliser dans ce qu'il a de plus singulier… Sans aller plus loin dans cette querelle déjà ancienne, on observera que les cyber-optimistes et les cyber-pessimistes s'entendent au moins sur une chose, à savoir le potentiel de transformation extraordinaire qu'ils prêtent, en cœur, aux réseaux sociaux.

Reconnaître et mesurer ce potentiel est une première étape indispensable si l'on souhaite relever collectivement les défis auxquels ils nous confrontent. Or tout le monde le sent : les États ne peuvent rester inactifs face à des innovations qui interagissent à ce point avec l'intérêt général et les fonctions qui leur sont traditionnellement dévolues. Ceci pose le problème de la régulation des réseaux sociaux, auquel aucun État ne semble pour le moment avoir trouvé de solution. Que réguler, comment réguler, à quel niveau ? L'équation n'est pas simple si l'on garde à l'esprit que ces plateformes, qui s'apparentent de plus en plus à des infrastructures dont dépend l'essentiel de nos activités, économiques et sociales, restent contrôlées par des sociétés privées, étrangères pour la plupart et dont le profit est l'ultime objectif. Elle est encore plus ardue si l'on tient compte de ce que leurs modèles reposent sur des algorithmes gardés secrets et des processus automatisés rendant largement inefficaces les techniques de contrôles et de répression jusque-là mises en œuvre par les pouvoirs publics. Les réseaux sociaux nous invitent en d'autres termes à un véritable changement de paradigme en matière de régulation : beaucoup de chercheurs, d'administrations et de législateurs sont déjà au travail et le Conseil d'État se donne pour mission, sur ce point, de nourrir utilement la réflexion.

Un autre défi, pour les administrations, c'est de saisir les opportunités que leur offrent les réseaux sociaux afin d'améliorer aussi bien leur fonctionnement que la qualité du service public. Qu'il s'agisse de fluidifier la communication interne et la gestion des administrations, de recueillir des informations aux fins, par exemple, du renseignement et de la lutte contre certaines formes de délinquance, de tirer profit des services offerts par les réseaux sociaux en matière de santé et de travail, ou encore d'imaginer des dispositifs de gouvernement plus participatifs et plus démocratiques, les réseaux sociaux représentent, pour les administrations, des gisements d'innovation qu'elles doivent explorer, avec prudence et retenue toutefois, compte tenu des risques inhérents à ces technologies.

On le voit, Mesdames et Messieurs, le sujet auquel s'attaque le Conseil d'État est particulièrement vaste et compliqué. Je propose de l'introduire en ouvrant quelques pistes de réflexion sur ce que sont ces objets nouveaux (I) et sur les conséquences qu'implique leur développement pour les pouvoirs publics (II).

* *

I. Les réseaux sociaux, dont les modèles et les usages sont en constante évolution, ont révolutionné nos modes de communication et bouleversé nos sociétés.

A. En dépit de leur variété et de leur très rapide évolution, ces outils partagent certaines caractéristiques qui permettent de dessiner les contours d'un modèle commun.

1. L'histoire des réseaux sociaux est celle d'une fulgurance. Quelques sites comme SixDegrees, Ryze ou Match.com, créés à la fin des années 1990, sont généralement considérés comme les ancêtres des réseaux sociaux actuels. Friendster, LinkedIn et Myspace furent ensuite respectivement mis en service en 2002 et 2003. Il reste qu'en 2005, les sites à plus fortes audience étaient encore des services de vente en ligne ou de grands portails commerciaux comme eBay, Amazon, Microsoft ou AOL : ce sont eux qui ont accompagné la démocratisation de l'internet, notamment permise par la généralisation des ordinateurs personnels. Mais trois ans plus tard, Youtube, Myspace, Facebook, Wikipedia et Orkut avaient déjà supplanté ces sites et acquis une place centrale dans les pratiques des internautes. Quelques dates peuvent ensuite être retenues : 2009, qui voit l'émergence du premier réseau chinois, Weibo, de l'application Farmville mise à disposition par Facebook et qui inaugure une nouvelle forme de jeu vidéo communautaire, de WhatsApp ou encore de Grindr, qui révolutionne les rencontres sur internet et sera suivi trois ans plus tard par Tinder. 2010 voit l'apparition d'Instagram, qui délaisse le texte au profit des images et, rachetée par Facebook, connaîtra un succès phénoménal. A partir de 2015, les réseaux sociaux se convertissent au *streaming* avec le lancement d'applications comme Periscope, Twitch ou Facebook Live et celui des stories et de son IGTV par Instagram. Enfin, mais l'histoire n'est bien sûr pas terminée, TikTok est lancé sur le marché chinois en 2016 et comptait en 2021 un milliard d'utilisateurs actifs dans le monde.

2. Face à cette profusion, on est tenté de chercher à identifier des types cohérents de réseaux sociaux. Certains auteurs ont proposé de les distinguer selon qu'ils sont proposés à titre accessoire, comme les forums de discussion thématiques ou libres proposés par beaucoup de sites web, ou à titre principal, comme la plupart des plateformes que je viens de citer[6]. On peut également les distinguer selon leurs caractéristiques techniques, leurs fonctionnalités, leur caractère ouvert ou fermé ou encore leurs modalités de monétisation. D'autres typologies plus subtiles cherchent quant à elles à appréhender les réseaux sociaux en fonction des dynamiques de participation et de visibilité qui les sous-tendent[7] : ceci conduit notamment à distinguer selon que les utilisateurs sont avant tout motivés par l'« amitié », comme Facebook ou WhatsApp, ou le partage avec des personnes ayant des centres d'intérêts commun, comme par exemple Youtube ou les sites de blogging[8]. De ces différences découlent en effet ce qu'on pourrait appeler des régimes de visibilité particuliers, à partir desquels Dominique Cardon avait par exemple révélé, il y a maintenant dix ans, quatre types d'identités des internautes, civile, agissante, narrative et virtuelle[9].

3. Deux caractéristiques essentielles apparaissent toutefois tant bien que mal si l'on fait masse de cette diversité. La première me semble être que les réseaux sociaux reposent tous sur une forme d'interactivité qui est la marque du « web 2.0 ». La structure verticale des premiers sites de vente en ligne est complétée, voire remplacée par une horizontalité qui modifie en profondeur la situation, au sens le plus profond du terme, des utilisateurs sur la plateforme. A ceci est liée une seconde caractéristique fondamentale, qui est que les réseaux sociaux se nourrissent avant tout de contenus générés par leurs utilisateurs eux-mêmes, contrairement aux médias traditionnels. C'est sur la capacité à permettre et à encourager la création et la publication de tels contenus que reposent le modèle économique de tous les services qui tirent des profits de la publicité. On comprend dans ces conditions que beaucoup d'entre eux cherchent à favoriser les phénomènes de « viralité » à travers leurs algorithmes et des fonctionnalités comme le « *like* », le « re-sharing » ou le « hashtag ». Ces contenus constituent dans le même temps, pour les observateurs extérieurs – administrations, entreprises, chercheurs – de nouvelles et précieuses sources d'informations sur les comportements et les préférences de tel ou tel groupe social. Et ce sont d'eux que découlent la plupart des problématiques liées aux réseaux sociaux, notamment en matière de vie privée et de liberté d'expression.

B. Les réseaux sociaux ont, à n'en pas douter, bouleversé nos sociétés, mais leurs effets sont à la fois ambivalents et difficile à mesurer.

1. D'un point de vue individuel, les réseaux sociaux ont d'abord pour effet d'amplifier et de catalyser l'exercice de certains droits et libertés[10]. En offrant à tout un chacun la possibilité de s'exprimer, de diffuser des informations ou d'émettre des opinions et des critiques sans filtre ni sans aucune autre forme d'intermédiation, ces services en ligne favorisent en effet l'approfondissement des libertés d'opinion et d'expression, ainsi que le droit à l'information. Ils favorisent également l'apparition de nouvelles formes de créativité artistique et intellectuelle, d'humour voire de poésie, que l'on peut observer chaque jour sur Instagram, TikTok ou Snapchat, et

peuvent ce faisant contribuer à l'épanouissement individuel de leurs utilisateurs. Ils peuvent enfin être perçus comme un moyen d'intensifier et d'élargir les liens sociaux, en retrouvant des connaissances perdues de vue, en en rencontrant d'autres avec qui nous partageons des centres d'intérêts ou des amis en commun, ou tout simplement en offrant un nouveau canal de communication avec nos familles, nos collègues ou nos amis les plus proches. Ces avantages doivent toutefois être regardés avec prudence. D'une part, car ils ne vont pas sans risques : la libération de la parole peut notamment être à l'origine d'excès délétères et l'information sur les réseaux sociaux se transformer en désinformation. D'autre part car les effets profonds des réseaux sociaux sur le rapport aux autres et le rapport à soi est difficile à mesurer : quelles seront notamment, à moyen terme, les conséquences du brouillage entre le privé et le public inhérent à ces plateformes ? Le rêve de singularité qui accompagne leur développement ne masque-t-il pas un processus d'uniformisation et de normalisation des rapports sociaux et de la consommation culturelle[11] ? L'aspect libérateur des réseaux sociaux peut-il enfin être autre chose qu'une illusion au regard de « l'économie de l'attention » sur lesquels ils sont fondés, qui tire profit des comportements addictifs de leurs utilisateurs ?

2. Conjuguée à ces modèles, la disparition des intermédiations a également transformé les rapports des citoyens au politique et, plus largement, à toutes les formes d'institutions[12]. L'horizontalité qu'ils promeuvent remet en effet frontalement en cause la conception traditionnelle du pouvoir fondée sur une logique verticale et hiérarchique, ainsi que sur le présupposé de la « compétence politique[13] » et scientifique. Beaucoup de membres de populations oppressées, de minorités ou de groupes sociaux traditionnellement mal représentés ont ainsi pu, grâce aux réseaux sociaux, entrer en communication et se constituer en communauté pour faire entendre leur voix ou, comme le disent les anglo-saxons, « speak to power ». Les réseaux se sont imposés comme des véhicules de la contre-démocratie permettant « d'articuler ensemble de multiples actions citoyennes à travers des activités de vigilance et de contestation[14] » : que ces actions aient entraîné la chute de certains régimes, incité à infléchir des politiques publiques ou tout simplement ouvert les yeux de la population sur des problèmes inacceptables, il ne fait pas de doute qu'elles ont été et continueront d'être à l'origine de certains progrès pour les droits et libertés. Là aussi pourtant, tout n'est pas blanc. En Ethiopie, à Hong Kong, au Moyen Orient, une « répression 2.0 » a répondu aux contestations. Dans nos démocraties, les études empiriques s'accordent à dire que globalement, les réseaux sociaux n'ont pas renforcé la participation et l'engagement politique, mais plutôt reproduit les modes de communication traditionnels qui limitent la participation politique des citoyens et privilégient la diffusion de l'information partisane[15]. La modification de la relation entre les citoyens et leurs gouvernants est par ailleurs allée de pair avec la prolifération de discours polémiques, polarisants et anarchisants : le potentiel de déstructuration, voire de destruction que l'on prête à juste titre aux réseaux sociaux ne semble pas contrebalancé par des forces positives pourtant nécessaires. Enfin, et même s'il ne faut pas leur faire porter toute la responsabilité d'un mouvement beaucoup plus profond et ancien, également alimenté par les médias traditionnels, les réseaux sociaux accentuent la défiance vis-à-vis de toutes les formes de légitimité, celle

des élus, des experts, des scientifiques et bien sûr des politiques. Or cette défiance est, pour nos démocraties, un cancer qu'elles n'ont pas encore semblé capables de traiter efficacement.

3. Les réseaux sociaux modifient enfin la manière dont nous exerçons la plupart de nos activités. Que l'on se lance dans le maraîchage, gère un restaurant ou dirige une entreprise de taille moyenne, il est de plus en plus difficile de se passer des réseaux sociaux pour exercer une activité professionnelle. Tous les métiers sont concernés, que l'on soit journaliste, chercheur, artiste, professionnel de santé – on estime à cet égard que plus de 70 % des discussions sur Facebook sont liées à la santé –, instituteurs ou enseignants… Le Conseil d'État est aussi sur Twitter dans le but d'être plus en contact avec la société qu'il sert et de mieux communiquer sur ses activités. De nouveaux métiers sont également apparus, des « *community managers* » aux « influencers » qui accompagnent la transformation de la publicité mais aussi du *lobbying*. Les métiers de la politique sont enfin directement concernés, qu'il s'agisse de la manière dont on fait campagne ou de celle dont on gouverne, ainsi que l'ont montré le précédent président des Etats-Unis ou nos propres dirigeants qui, de plus en plus, recourent aux réseaux sociaux au prix d'une transformation sensible des modes de communication gouvernementaux.

II. Dans ces conditions, les Etats n'ont pas d'autre choix que de prendre acte du développement des réseaux sociaux afin d'orienter leurs effets par le biais de la régulation ainsi que, le cas échéant, d'en tirer profit pour améliorer leurs modes de fonctionnement

A. Une régulation des réseaux sociaux semble s'imposer compte tenu de l'intensité de leurs interférences avec des intérêts essentiellement publics

1. Pour envisager de réguler les réseaux sociaux, il est indispensable, au préalable, de se mettre d'accord sur les objectifs que l'on poursuit et d'avoir à l'esprit les principaux obstacles auxquels on ne manquera pas d'être confrontés. Trois objectifs émergent des très riches débats menés sur ce sujet en Europe et aux États-Unis : le premier est celui de garantir aux citoyens et aux entreprises un accès et un traitement équitables (*fair access and treamtent*) sur les réseaux sociaux, ce qui inclut des objectifs en termes de non-discrimination, de neutralité ou encore de juste tarification. Le deuxième objectif vise à garantir la protection des utilisateurs : contre les atteintes à leur droit au respect de la vie privée, contre les effets préjudiciables des algorithmes qui, par nature, influent sur leurs décisions et leurs opportunités[16], mais aussi contre la désinformation, les « *fake news* » et, par extension, les discours haineux. Le troisième objectif, qui est en quelque sorte la condition des deux premiers, consiste enfin à créer des formes pertinentes et efficaces de responsabilité (*accountability*) des plateformes, ce qui implique notamment de réfléchir en termes de transparence et de procédure. Les obstacles à la régulation tiennent quant à eux, en premier lieu, aux risques de capture qui sont particulièrement élevés dans ce secteur complexe où l'accès aux données techniques est restreint et où les régulateurs dépendent souvent des acteurs de l'industrie eux-mêmes pour obtenir les informations nécessaires à la

conception et à l'application des règlementations[17]. Un autre obstacle tient, en deuxième lieu, à la difficulté de calibrer les interventions publiques pour atteindre les objectifs poursuivis sans détruire outre mesure le potentiel de croissance et d'innovation des réseaux sociaux. Il est en troisième lieu toujours délicat d'agir sur les contenus postés en ligne sans passer du côté de la censure. Enfin, du point de vue des Etats européens, la régulation est d'autant plus difficile que la plupart des réseaux sociaux sont des entreprises étrangères et que dans le monde de l'internet, les frontières nationales ne représentent pas grand-chose.

2. Dans ces conditions, plusieurs types de régulation sont envisageables. La première est de promouvoir l'autorégulation des plateformes, au besoin en édictant des codes de conduite ou des recommandations[18]. Cette option a d'abord été privilégiée par les États, qui ont longtemps semblé persuadés de leur impuissance face à des réseaux internationaux qui, de leur côté, revendiquaient leur qualité de simples hébergeurs et non d'éditeurs de contenus. Des scandales comme l'affaire Cambridge Analytica, les insuffisances patentes des mesures mises en œuvre par les plateformes[19] et le risque d'une véritable privatisation de la censure – pensons à la « cour suprême » récemment instituée par Facebook[20] – ont toutefois fini par décider la plupart des États prendre leurs responsabilités. Des mécanismes de régulation *a posteriori* ont ainsi commencé à voir le jour, consistant essentiellement en des obligations assorties de sanctions administratives ou judiciaires. Ce type de régulation a par exemple été mobilisé en France et en Allemagne afin de lutter contre la prolifération des discours haineux : c'est le sens de la loi allemande dite NetzDG[21] et c'était celui de la loi du 24 juin 2020 dite « Avia »[22] avant que ses principales dispositions ne soient censurées par le Conseil constitutionnel[23]. Une loi du 22 décembre 2018 a par ailleurs renforcer les pouvoirs du juge des référés afin de lutter contre la manipulation de l'information en période de campagne électorale[24.] De tels dispositifs ne vont toutefois, eux non plus, pas sans risques, puisqu'ils peuvent paradoxalement conduire à renforcer les pouvoirs des plateformes incitées au zèle par la menace des sanctions, mettre à l'écart du contrôle des contenus la justice et la société ou se révéler peu efficaces compte tenu de la désynchronisation entre le contrôle du régulateur et l'instantanéité de la diffusion des informations sur les réseaux[25]. La régulation peut enfin passer par la politique fiscale ou par le droit de la concurrence, qui peut difficilement rester en retrait face à la dynamique de concentration des marchés liés au numérique. Les grands réseaux sociaux s'apparentent à cet égard de plus en plus aux infrastructures qui ont justifié, dans le passé, la mise en œuvre de sévères politiques antitrust[26]. Les actions récemment engagées par le gouvernement américain[27] et la Commission européenne[28] à l'encontre de Facebook méritent de ce point de vue d'être regardées de près.

3. L'accumulation, ces dernières années, des textes et des expérimentations mis en œuvre pour réguler le secteur du digital semble donc montrer que le rapport de forces est en train de s'inverser et que la légitimité de l'intervention publique est dorénavant admise. Le tout est maintenant de s'accorder sur la bonne manière de définir et de combiner ces types de régulation. Ceci implique d'être au clair sur une question fondamentale : à quoi sommes-nous collectivement prêts à

renoncer, en termes de liberté d'expression, de communication, de croissance et d'innovation pour préserver ce que nous considérons être l'intérêt général ? Car réguler reviendra nécessairement à se priver de certains bénéfices engendrés par les réseaux sociaux. A cette question politique s'ajoutent des questions juridiques tout aussi délicates : quel est le bon niveau de régulation, national ou international, sectoriel ou général ? Dans quelle mesure faut-il que les pouvoirs publics puissent accéder aux algorithmes ? Quelle transparence et traçabilité imposer ? A quel point faut-il éviter les concentrations d'entreprises, sachant que le contrôle d'un marché trop éclaté est très difficile ? Autant de questions, et il y en a bien d'autres, auxquelles nous devrons aussi répondre, comme a récemment entrepris de le faire la Commission européenne en vue d'un prochain paquet « service numériques[29] ».

B. Les pouvoirs publics sont aussi concernés par les réseaux sociaux en tant qu'ils peuvent leur offrir les moyens d'innover et de remplir plus efficacement leurs missions de service public

1. Les contenus générés par les utilisateurs sur les réseaux sociaux constituent des mines d'informations quasiment inépuisables à qui sait les exploiter. Les Etats peuvent ainsi être tentés de s'en servir pour renforcer l'efficacité de certaines de leurs activités, comme le renseignement ou la lutte contre la délinquance. En France, un dispositif expérimental[30] a par exemple été institué sur le fondement de la loi de finances pour 2020[31], qui permet aux administrations fiscale et douanière d'utiliser les données rendues publiques par les contribuables sur les réseaux sociaux pour détecter une série de comportements frauduleux limitativement énumérées. Ce dispositif s'inscrit dans une stratégie plus large de modernisation du contrôle fiscal, en particulier de la phase de ciblage des opérations, qui repose en grande partie sur le développement d'outils de *data mining*[32]. Aussi la plupart des Etats se servent-ils déjà des informations disponibles sur les réseaux sociaux pour les besoins des enquêtes de police et de la répression pénale, mais également de plus en plus à des fins préventives. Des techniques de police prédictive (*predictive policing*) sont ainsi mises en œuvre depuis longtemps au Royaume-Uni et sont en cours d'expérimentation en France, notamment à la gendarmerie nationale[33]. Qu'elles poursuivent des fins répressives ou prédictives, ces techniques sont prometteuses. Elles comportent néanmoins des risques importants et nouveaux liés, en particulier, aux biais contenus dans les algorithmes et les outils d'intelligence artificielle sur lesquels elles reposent[34]. L'un des principaux défis ne tient donc pas tant à la collecte et à la conservation des données qu'à l'élaboration d'instruments d'analyse éthiques et efficaces, qui doivent s'inscrire dans un cadre juridique facilitant leur contrôle. C'est l'une des problématiques – qui dépasse les seuls réseaux sociaux – à laquelle est en ce moment confronté, au Conseil d'État, un groupe de travail constitué à la demande du Premier ministre pour réfléchir aux usages de l'intelligence artificielle par la puissance publique.

2. Les réseaux sociaux offrent par ailleurs aux administrations publiques de très nombreuses opportunités pour rénover leurs processus décisionnels en les rendant plus ouverts, plus inclusifs et plus participatifs – autant de moyens de

renforcer la confiance des citoyens dans leurs institutions. Les administrations et leurs responsables, aux niveaux national et local, peuvent trouver dans les réseaux sociaux un précieux moyen, dans un objectif de transparence, de mieux donner à voir ce qu'ils font, mais aussi de mieux « prendre le poul » de leurs administrés sur telle ou telle question, tel ou tel projet, voire de communiquer directement avec eux en engageant de véritables conversations. C'est ce que font beaucoup de préfectures et de communes en France. La police espagnole utilise quant à elle depuis plusieurs années des comptes Twitter, Facebook et Youtube de façon novatrice dans le but d'accroître sa proximité avec les citoyens et de mieux les servir : leur très grand succès tient avant tout au « style » ou au « ton » des contenus qu'elle y publie et qui témoignent de son choix de sortir du cadre de la relation traditionnelle entre gouvernants et gouvernés.

Dans d'autres domaines de l'action publique, les administrations sont par ailleurs de plus en plus amenées à composer avec le rôle central que remplissent de fait les réseaux sociaux. C'est notamment le cas en matière de recherche d'emploi, secteur aujourd'hui dominé par des sites spécialisés tels que LinkedIn, Viadeo ou Xing ou des sites généralistes comme Facebook. Les agences nationales chargées de l'emploi se trouvent concurrencées et doivent imaginer des moyens de mieux articuler leurs actions à celles de ces réseaux. Le département du travail américain, en concertation avec différents syndicats, a par exemple signé un partenariat avec Facebook qui a débouché sur le lancement de l'application Social Jobs Application, qui permet de consulter sur une seule et même page les offres d'emploi proposées par plusieurs sites spécialisés dans le recrutement. En Allemagne, l'agence nationale pour l'emploi s'est quant à elle engagée dans une coopération avec le réseau Xing visant à ce que toutes les offres d'emploi publiée sur ce site le soient aussi sur le listing national, et inversement[35]. Quels que soient les utilisations que font les administrations des réseaux sociaux, elles devront toutefois tenir compte des dangers qu'ils charrient, en particulier celui de créer ou de renforcer des discriminations et exclusions, qui peuvent découler des biais algorithmiques dont j'ai déjà parlé, mais aussi des fractures numériques liées à l'âge ou à l'éducation[36].

3. Enfin, et j'en terminerai par là, les réseaux sociaux pourraient permettre aux administrations d'améliorer leurs processus de communication et de collaboration internes, par exemple en impliquant davantage les agents dans la construction des décisions et la gestion des services, en renforçant leurs liens et leur inclusion dans l'organisation, ou encore en contribuant à renforcer les liens inter-administrations.

* *

Mesdames et Messieurs, j'ai été long et n'ai pu qu'effleurer une partie des questions que pose le sujet de notre prochaine étude annuelle. Il est vaste, complexe et foisonnant : une année ne sera pas de trop pour l'explorer. Le Conseil d'État s'appuiera, comme à son habitude, sur les conférences de ce cycle et les auditions qui viseront à recueillir les points de vue de nombreux professionnels et experts

confrontés aux problématiques des réseaux sociaux. Il est également probable cette année que nos enfants et nos petits-enfants soient interrogés dans un cadre plus informel… Je les en remercie par avance, comme je remercie vraiment très chaleureusement les trois intervenants de ce soir : Dominique Cardon, professeur de sociologie à Sciences Po et spécialiste, depuis longtemps, des sujets liés à l'internet, Philippe Colombet, directeur du journal La Croix et Dominique Reynié, lui aussi professeur à Sciences Po et directeur général de Fondapol. Je remercie également Martine de Boisdeffre, présidente de la section du rapport et des études qui chapeautera sa confection et modérera la conférence de ce soir, ainsi que François Séners, son président-adjoint et rapporteur général et Marie Grosset qui, pour la deuxième année consécutive, tiendra la plume de la section.

[2] Internet et les réseaux numériques, 1997, coll. Etudes du Conseil d'Etat (https ://www.vie-publique.fr/sites/default/files/rapport/pdf/984001519.pdf)

[3] Le numérique et les droits fondamentaux, étude annuelle 2014 (https ://www.vie-publique.fr/sites/default/files/rapport/pdf/144000541.pdf)

[4] Puissance publique et plateformes numériques : accompagner l'«ubérisation», étude annuelle 2017 (https ://www.conseil-etat.fr/ressources/etudes-publications/rapports-etudes/etudes-annuelles/etude-annuelle-2017-puissance-publique-et-plateformes-numeriques-accompagner-l-uberisation)

[5] V° le Baromètre du numérique 2021 de l'ARCEP, p. 120 et les chiffres publiés par le Guide #Datamind Tendances 2021 (https ://blog.digimind.com/fr/tendances/r%C3%A9seaux-sociaux-france-monde-chiffres-utilisation-2021)

[6] Pour cette distinction, voir le rapport de la mission « Régulation des réseaux sociaux – Expérimentation Facebook », Créer un cadre français de responsabilisation des réseaux sociaux : agir en France avec une ambition européenne, remis au secrétaire d'Etat chargé du numérique en mai 2019

[7] T. Stenger & A. Coutant, « Médias sociaux : clarification et cartographie - Pour une approche sociotechnique », Décisions Marketing, n° 70, 2013, p. 107

[8] M. Ito (ed.), Hanging Out, Messing Around, and Geeking Out : Kids Living and Learning with New Media. Boston, 2010, The MIT Press

[9] D. Cardon, « Réseaux sociaux de l'internet », Communications, n° 88, 2011, p. 141

[10] V° J.-M. Sauvé, « La protection des droits fondamentaux à l'ère du numérique », Intervention lors de la remise des prix de thèse de la Fondation Varenne le 12 décembre 2017

[11] D. Cardon, « Réseaux sociaux de l'internet », art. cit., in fine

[12] V° not. C. Richaud, « Les réseaux sociaux : nouveaux espaces de contestation et de reconstruction de la politique ? », Les nouveaux cahiers du Conseil constitutionnel, 2017/4, n° 57, p. 29

[13] V° P. Bourdieu, « L'opinion publique n'existe pas », Les temps modernes, n° 318, 1972, p. 1295

[14] P. Flichy, « La démocratie 2.0 », Études, n° 412, 2010, p. 617

[15] B. Ben Mansour, « Le rôle des médias sociaux en politique : une revue de la littérature », Regards politiques, 2017, vol. 1, n° 1, p. 3

[16] V° sur ce sujet la notion d'« algorithmic nuisance » analysée par J. M. Balkin, « Free Speech in the Algorithmic Society : Big Data, Private Governance, and New School Speech Regulation », 51 U.C. Davis Law Review 1149 (2018)

[17] V° D. Awrey, « Complexity, Innovation, and the Regulation of Modern Financial Markets », 2 Harvard Business Law Review 235 (2012)

[18] C'est ce qu'a fait la Commission européenne en 2016 avec un code de conduite relatif aux discours haineux illégaux en ligne et la Recommandation (UE) 2018/334 de la Commission du 1er mars 2018 sur les mesures destinées à lutter, de manière efficace, contre les contenus illicites en ligne

[19] Not. A. Marantz, « Why Facebook Can't Fix Itself », The New Yorker, 19 octobre 2020 (https ://www.newyorker.com/magazine/2020/10/19/why-facebook-cant-fix-itself)

[20] Not. K. Klonick, « Inside the Making of Facebook's Supreme Court », The New Yorker, 12 février 2021 (https ://www.newyorker.com/tech/annals-of-technology/inside-the-making-of-facebooks-supreme-court)

[21] Loi Netzwerkdurchsetzungsgesetz du 30 juin 2017

[22] Loi n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet

[23] Décision n° 2020-801 DC du 18 juin 2020

[24] Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information

[25] S. Abiteboul & J. Cattan, « Nos réseaux sociaux, notre régulation », Revue européenne du droit, n° 1, septembre 2021 (https ://geopolitique.eu/articles/nos-reseaux-sociaux-notre-regulation/)

[26] V° sur ce point S. Rahman, « Régulating Informational Infrastructure : Internet Platforms as the New Public Utilities », 2 Georgetown Law Technology Review 234 (2018) qui évoque les gatekeeping power, transmission power et scoring power dont disposent les grands réseaux sociaux ; également, sur ce sujet, F. Marty, « Plateformes numériques, algorithmes et discrimination », Revue de l'OFCE, 2019/4 (164), p. 47

[27] https ://www.nytimes.com/2021/08/19/technology/ftc-facebook-antitrust.html

[28] https ://ec.europa.eu/newsroom/comp/items/713352

[29] https ://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

[30] Décret n° 2021-158 du 11 février 2021

[31] Art. 154 de la loi n° 2019-1479 du 28 décembre 2019

[32] https ://www.bercynumerique.finances.gouv.fr/vivre-le-numerique-a-bercy/le-data-mining-a-la-dgfip

[33] Institut d'aménagement et d'urbanisme de la région Ile-de-France, La police prédictive. Enjeux soulevés par l'usage des algorithmes prédictifs en matière de sécurité publique, avril 2019, spéc. p. 15 (https ://www.iau-idf.fr/fileadmin/NewEtudes/Etude_1797/Etude_Police_Predictive_V5.pdf)

[34] La recherche est extrêmement fournie sur ce sujet : voir par exemple, pour le Royaume-Uni, A. Babuta & M. Oswald, Data Analytics and Algorithmic Bias in Policing, briefing paper pour le Royal United Service Institute for Defense and Security Studies, 2020 (https ://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/831750/RUSI_Report_-_Algorithms_and_Bias_in_Policing.pdf)

[35] OCDE Working Papers on Public Governance n° 26, Social Media Use by Governments : A Policy Primer to Discuss Trends, Identify Policy Opportunities and Guide Decision Makers (https ://www.oecd.org/gov/digital-government/government-and-social-media.htm)

[36] Ibid. ; M. Feeney & G. Porumbescu, « The Limits of Social Media for Public Administration Research and Practive », Public Administration Review, juillet 2020 (https ://onlinelibrary.wiley.com/doi/abs/10.1111/puar.13276)

Programme des conférences

Conférence inaugurale : 27 octobre 2021 - Les réseaux sociaux, vecteurs de transformation de la société et du débat public

Animation de la conférence : : Martine de Boisdeffre, présidente de la section du rapport et des études du Conseil d'État

Intervenants

- Dominique Cardon, professeur de sociologie à Sciences Po, directeur scientifique du Médialab
- Philippe Colombet, directeur du journal La Croix
- Dominique Reynié, professeur des universités, directeur général de la Fondation pour l'innovation politique (Fondapol)

Retrouver ici la page internet de la conférence

2e conférence : 15 décembre 2021 - Les réseaux sociaux, vecteurs de transformation de l'économie et du travail

Animation de la conférence : Jean-Denis Combrexelle, ancien président de la section du contentieux du Conseil d'État, ancien directeur général du travail

Intervenants

- Grégoire Loiseau, professeur de droit à l'université Paris 1 Panthéon Sorbonne
- Thierry Pénard, professeur d'économie, doyen de la faculté des sciences économiques de l'université de Rennes 1
- Joëlle Toledano, professeur émérite d'économie, associée à la chaire « Gouvernance et régulation » de l'université Paris Dauphine I PSL

Retrouver ici la page internet de la conférence

3e conférence : 23 mars 2022 - Les réseaux sociaux, vecteurs de transformation de l'action publique

Animation de la conférence : Laurence Franceschini, conseillère d'État

Intervenants :

- Jean Bassères, directeur général de Pôle emploi
- Marie Pawlak, directrice du digital, SNCF Transilien
- Michel Sauvade, co-président de la commission numérique de l'Association des maires de France, maire de Marsac-en-Livradois, vice-président du Conseil départemental du Puy-de-Dôme

Retrouver ici la page internet de la conférence

4e conférence : 8 juin 2022 - Les réseaux sociaux, enjeux de régulation

Animation de la conférence : Thierry Tuot, président adjoint de la section de l'intérieur du Conseil d'État,

Intervenants :

- Thierry Breton, commissaire européen au marché intérieur (témoignage en vidéo)
- Gerard de Graaf, directeur de la transformation numérique, DG Connect
- Thomas Fauré, fondateur et président, Whaller
- Célia Zolynski, professeure de droit privé à l'université Paris 1 Panthéon-Sorbonne

Retrouver ici la page internet de la conférence

Discours de clôture du cycle : Didier-Roland Tabuteau, vice-président du Conseil d'État

Retrouver ici la page internet de la conférence

Annexes

Annexe 1 – Liste des personnes auditionnées

Annexe 2 – Groupe de contact et comité d'orientation de l'étude annuelle

Annexe 3 – Statistiques : Taux de pénétration des réseaux sociaux parmi les internautes et l'ensemble de la population française de 2009 à 2020 et taux de pénétration des réseaux sociaux en France en 2020, selon l'âge

Annexe 1 – Liste des personnes auditionnées

Les fonctions mentionnées sont celles exercées au moment de l'audition.
Sauf indication contraire, les auditions ont eu lieu au Conseil d'État.

(Présentation par ordre alphabétique)

Justine Atlan, directrice générale, e-Enfance
Serge Abiteboul, chercheur à l'École nationale supérieure Paris-Saclay, directeur de recherche à l'Institut national de recherche en informatique et en automatique (INRIA)
Quentin Aoustin, directeur des opérations, point de contact.net
Romain Babouard, maître de conférences en sciences de l'information et de la communication, université Panthéon-Assas
Laure Beccuau, procureure de la République près le tribunal judiciaire de Paris accompagnée de Vanessa Peree, procureure adjointe et d'Éric Serfass, procureur adjoint
Virginie Beaumeunier, directrice générale de la concurrence de la consommation et de la répression des fraudes, ministère de l'économie et des finances
Côme Berbain, directeur du pôle innovation, RATP
Jérôme Bonet, directeur central de la police judiciaire, accompagné de Nicolas Guidoux, sous-directeur de la lutte contre la cybercriminalité, ministère de l'intérieur
Nicolas Bonnal, doyen de section à la chambre criminelle, Cour de cassation
Dominique Boullier, professeur de sociologie, Sciences Po
Gérald Bronner, professeur de sociologie, université Paris-Diderot
Dominique Cardon, professeur de sociologie, directeur scientifique du Médialab, Sciences Po
Didier Casas, secrétaire général, Groupe TF1
Antonio A. Casilli, professeur de sociologie, Télécom Paris, accompagné de Paola Tubaro, directrice de recherche, Centre national de la recherche scientifique (CNRS)
Jean Cattan, secrétaire général, Conseil national du numérique (CNNum)
Jennifer Chrétien, déléguée générale, Renaissance Numérique
Sophie Macquart-Moulin, adjointe au directeur des affaires criminelles et des grâces, accompagnée de Xavier Léonetti, magistrat, chef de la mission de prévention et lutte contre la cybercriminalité, ministère de la justice

Mathilde Cousin, journaliste community manager et fact-checkrice, 20 minutes

Axel Dauchez, fondateur et président de Make.org

Nicolas Deffieux, directeur, Pôle d'expertise de la régulation numérique (PEReN), direction générale des entreprises, ministère de l'économie des finances et de la relance

Christophe Deloire, secrétaire général, Reporters sans frontières

Marie-Laure Denis, présidente, accompagnée de Louis Dutheillet de Lamothe, secrétaire général, Commission nationale de l'informatique et des libertés (CNIL)

Capucine-Marin Dubroca-Voisin, présidente, accompagnée de Naphsica Papanicolaou et de Pierre-Yves Beaudouin, Wikimédia

Laure Durand-Viel, déléguée à la régulation des plateformes numériques, direction générale des médias et des industries culturelles, ministère de la culture

Thomas Fauré, président, Whaller

Karine Favro, professeure de droit public, université de Haute-Alsace

Marie-Anne Frison-Roche, professeure de droit, Sciences Po

Éric Garandeau, directeur des affaires publiques et des relations avec le Gouvernement, TikTok France

Edouard Geffray, directeur général de l'enseignement scolaire (DEGESCO), ministère de l'éducation nationale

Monique Goyens, directrice du Bureau européen des unions de consommateurs (BEUC)

Audrey Herblin-Stoop, directrice des relations publiques, Twitter France

Aurélie Jean, docteure en sciences, chercheuse et spécialiste des algorithmes

Alexandre Linden, conseiller honoraire à la Cour de cassation et président de la formation restreinte de la CNIL, ancienne personnalité qualifiée désignée par la CNIL

Laure Lucchesi, directrice, accompagnée de Paul-Antoine Chevalier, responsable du pôle données et IA, Etalab, direction interministérielle du numérique (DINUM)

Roch-Olivier Maistre, président, accompagné de Benoît Loutrel, membre, Conseil supérieur de l'audiovisuel (CSA)

Nathalie Martial-Braz, professeure de droit privé, université Paris-Cité et Sorbonne Abu Dhabi

Arthur Messaud, membre, accompagné de Bastien Le Querrec, juriste, Quadrature du Net

Jean-François de Montgolfier, directeur des affaires civiles et du Sceau, ministère de la justice

Michaël Nathan, directeur, Service d'information du Gouvernement

Bruno Patino, président, Arte France

Yves Poullet, professeur de droit, université de Namur

Guillaume Poupard, directeur général, Agence nationale de la sécurité et des systèmes d'information (ANSSI)

Laure de la Raudière, présidente, Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP)

Chantal Rubin, cheffe du pôle régulation des plateformes numériques, ministère de l'économie des finances et de la relance

Hubert Saint-Olive, fondateur et président, Confidens

Laurent Solly, directeur général France, Facebook

Isabelle de Silva, présidente adjointe de la section sociale du Conseil d'État, ancienne présidente de l'Autorité de la concurrence

Benoit Tabaka, directeur des relations institutionnelles et des politiques publiques, Google France

Christophe Tardieu, secrétaire général, France Télévision

Fabien Tarissan, chargé de recherche au CNRS, professeur attaché à l'École normale supérieure Paris-Saclay

Joëlle Toledano, professeure émérite, associée à la chaire « Gouvernance et régulation » de l'université Paris-Dauphine I PSL

Sibyle Veil, présidente, accompagnée de Xavier Domino, secrétaire général, Radio France

Henri Verdier, ambassadeur du numérique, ministère de l'Europe et des affaires étrangères

Serena Villata, chercheuse en algorithmes, directrice scientifique adjointe, Institut interdisciplinaire d'intelligence artificielle (3IA) de l'université Côte d'Azur, du CNRS et de l'Inria

Célia Zolynski, professeure de droit privé, université Panthéon-Sorbonne

Commission européenne

Alberto Bacchiega, directeur Marchés et cas II: Information, communication et médias, accompagné de Thomas Kramler, chef d'unité Antitrust: Commerce en ligne et économie des données et de Léa Zuber, chef de secteur Task Force Digital Markets Act, direction générale de la concurrence, Commission européenne

Irene Roche Laguna, chef adjointe de l'unité services numériques et plateformes, Deborah Behar, conseillère juridique et Enrico Camilli, responsable de politiques – Lawyer, direction de la transformation numérique, direction générale des réseaux de communication, du contenu et des technologies, Commission européenne

Annexe 2 – Groupe de contact et comité d'orientation de l'étude annuelle

(les fonctions mentionnées sont celles exercées à la date de la participation aux travaux de l'étude)

Le groupe de contact de l'étude annuelle

Le groupe de contact de l'étude annuelle 2022 du Conseil d'État a réuni de hautes personnalités ayant une expérience diversifiée dans les domaines abordés par l'étude. Le groupe a eu pour rôle de mettre en débat les principales orientations et les propositions qui lui ont été présentées par la section du rapport et des études avant que celle-ci délibère du projet soumis à l'assemblée générale.

Composition

Romain Badouard, maître de conférences, université Panthéon-Assas
Nicolas Bonnal, conseiller à la chambre criminelle de la Cour de Cassation
Dominique Boullier, professeur des universités en sociologie, professeur à Science Po
Dominique Cardon, directeur scientifique du Medialab de Sciences Po
Jennyfer Chrétien, déléguée générale renaissance numérique
Louis Dutheillet de Lamothe, secrétaire général de la Commission nationale de l'informatique et des libertés (CNIL)
Karine Favro, professeure de droit, université de Haute Alsace
Audrey Herblin, directrice des relations publiques de Twitter France
Guillaume Lacroix, président directeur général du média en ligne Brut
Benoit Loutrel, membre du Conseil supérieur de l'audiovisuel (CSA)
Bruno Patino, président d'Arte, accompagné d'Adeline Cornet, secrétaire générale
Yves Poulet, professeur au centre de recherche information, droit et société (CRIDS) à Namur (Belgique)
Fabien Tarissan, chercheur au Centre national de la recherche scientifique (CNRS)
Joelle Tolédano, professeure émérite d'économie, université Paris-Dauphine
Henri Verdier, ambassadeur du Numérique
Serena Villata, chercheuse au Centre national de la recherche scientifique (CNRS), directrice de l'institut 3IA Côte d'Azur
Célia Zolynski, professeure de droit, université Panthéon-Sorbonne

Le comité d'orientation de l'étude annuelle

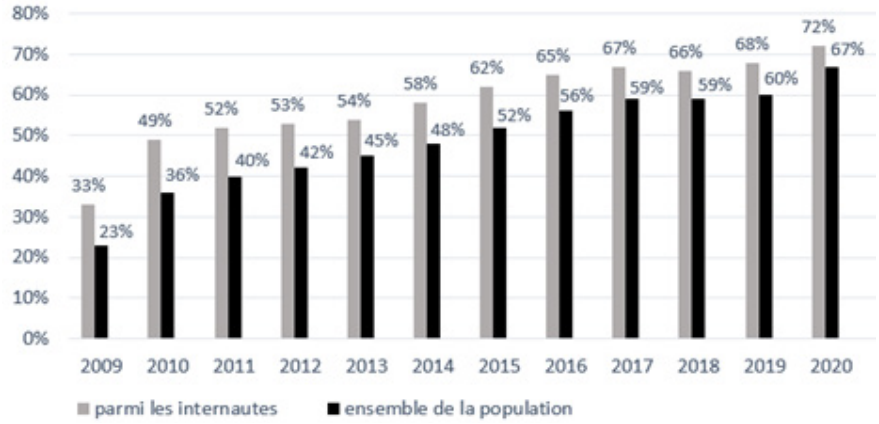
Le comité d'orientation, constitué dans le cadre des travaux d'élaboration de l'étude annuelle 2022 du Conseil d'État, a réuni des membres du Conseil d'État issus des différentes sections administratives et de la section du contentieux. Ce comité a apporté son expertise sur l'analyse générale de la situation, les grands axes de l'étude et la préfiguration des propositions qui lui ont été présentés par la section du rapport et des études avant que celle-ci délibère du projet soumis à l'assemblée générale du Conseil d'État.

Composition

Damien Botteghi, assesseur, section du contentieux
Hervé Cassagnabère, assesseur, section du contentieux
Hélène Cazaux-Charles, rapporteure, section de l'intérieur
Carine Chevrier, rapporteure, section du contentieux et section de l'administration
Manon Chonavel, rapporteure au Conseil d'État
Anne Courrèges, assesseure, section du contentieux
Patrick Gérard, président adjoint de la section de l'administration
Stéphane Hoynck, rapporteur public, section du contentieux
Arno Klarsfeld, rapporteur, section du contentieux
Jean Lessi, rapporteur, section sociale
Esther de Moustier, rapporteure public, section du contentieux
Timothée Paris, rapporteur, section de l'intérieur
Alban de Nervaux, rapporteur, section du contentieux et section de l'intérieur
Isabelle de Silva, présidente de chambre à la section du contentieux
Fabio Gennari, rapporteur, section du contentieux

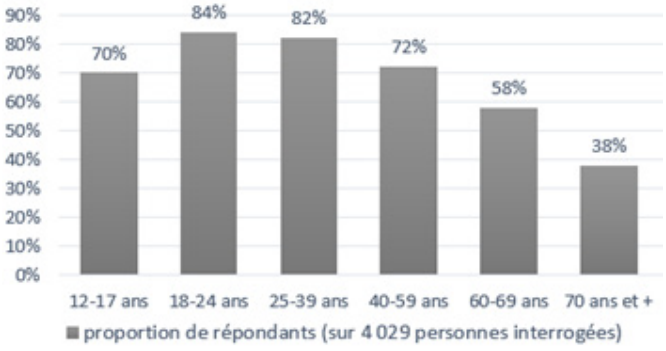
Annexe 3 – Statistiques : Taux de pénétration des réseaux sociaux parmi les internautes et l'ensemble de la population française de 2009 à 2020 et taux de pénétration des réseaux sociaux en France en 2020, selon l'âge

Taux de pénétration des réseaux sociaux parmi les internautes et l'ensemble de la population française de 2009 à 2020 (4 029 personnes interrogées)



Ce graphique illustre l'utilisation des réseaux sociaux par les internautes et l'ensemble de la population française de 2009 à 2020. On peut observer que les deux courbes suivent une tendance similaire et que le taux d'utilisateurs de réseaux sociaux a augmenté chaque année, dépassant 60 % parmi les internautes et 50 % au sein de l'ensemble de la population française à partir de 2015 (source : statista).

Taux de pénétration des réseaux sociaux en France en 2020, selon l'âge



Ce graphique représente la proportion d'utilisateurs de réseaux sociaux au sein de la population française, par âge, en 2020. Parmi les personnes interrogées âgées de 60 à 69 ans, près de 58 % ont déclaré utiliser au moins un réseau social, tandis que plus de 84 % des personnes âgées de 18 à 24 ans en utilisent au moins un (source : statista).

Glossaire

Algorithme	Ensemble de règles opératoires dont l'application permet de résoudre un problème énoncé au moyen d'un nombre fini d'opérations (Larousse) ; description d'une suite d'étapes permettant d'obtenir un résultat à partir d'éléments fournis en entrée (CNIL)
Application Programming Interface (API)	Solution informatique permettant à des applications de communiquer entre elles et de s'échanger des données
Blog / Blogosphère	Type de site *web* utilisé pour la publication périodique et régulière d'articles personnels, généralement succincts, rendant compte d'une actualité ou thématique particulière. La blogosphère représente l'écosystème des internautes blogueurs et/ou l'ensemble des blogs et/ou l'ensemble des écrits contenus par ces blogs
Bloquer	Action d'empêcher un compte de pouvoir contacter ou accéder aux contenus de son propre compte
Bot	Terme issu de la contraction de « robot ». De façon générale, un *bot* est un programme informatique autonome ou partiellement autonome, conçu pour imiter un comportement humain. Ils agissent dans les media sociaux soit en étant clairement identifiés (mises à jour de données, « chatbot » pour fournir une assistance en ligne sur des questions simples), soit de manière dissimulée (diffusion automatique et en masse de messages instantanés, production automatique de « like » ou diffusion massive de contenus issus de comptes réels ou fictifs…)
Cloud	Le cloud (nuage en français) désigne un service en ligne permettant de stocker des ressources numériques auxquelles on peut accéder à distance *via* un réseau de communication Parmi les fournisseurs de Cloud, les plus utilisés sont Dropbox, Google Drive et One Drive.
Conditions Générales d'Utilisation (CGU)	Les CGU définissent et encadrent les modalités de l'utilisation d'un site internet, et déterminent les droits et les obligations respectifs de l'utilisateur et de l'éditeur dans le cadre de son utilisation. Elles permettent : d'informer les internautes sur le fonctionnement général du site, les modalités et les règles que les utilisateurs doivent respecter en navigant ou utilisant le site internet, de définir la responsabilité de l'éditeur et de l'utilisateur du site ce qui permet à l'éditeur de se dédouaner en cas de comportement litigieux de certains utilisateurs, de prévoir des sanctions en cas de non-respect des conditions d'utilisation, et de prouver la bonne diligence du site

Cookie	Petit fichier stocké par un serveur dans le terminal (ordinateur, téléphone, etc.) d'un utilisateur et associé à un domaine web (c'est à dire dans la majorité des cas à l'ensemble des pages d'un même site web). Le cookie vise essentiellement à « mémoriser » sur un site Web donné les habitudes et préférences exprimées par l'internaute lors d'une ou plusieurs visites de manière à lui proposer à nouveau des préférences exprimées lors d'une visite ultérieure.
Crowdsourcing	Le crowdsourcing (en français, «approvisionnement par la foule») consiste à faire participer des consommateurs ou le grand public à la création d'un produit ou d'un service marketing par le biais d'internet. Cette forme de marketing collaboratif est couronnée de succès dans de nombreux domaines.
Cybercriminalité	Ensemble des infractions pénales commises sur les réseaux de télécommunication, en particulier internet.
Déréférencement	Opération consistant à supprimer certains résultats fournis par un moteur de recherche. En France, le déréférencement est utilisé notamment dans le cadre de la protection des données à caractère personnel, mais aussi dans la lutte contre le terrorisme et la pédopornographie.
Donnée personnelle	Toute information se rapportant à une personne physique identifiée ou identifiable, directement (ex : nom, prénom) ou indirectement – par exemple par un identifiant (n° client), un numéro (téléphone), une donnée biométrique, des éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale, mais aussi la voix ou l'image.
Doxing	Le doxing (aussi écrit doxxing, possiblement dérivé de l'expression « dropping docs »), constitue « *Le fait de révéler, de diffuser ou de transmettre, par quelque moyen que ce soit, des informations relatives à la vie privée, familiale ou professionnelle d'une personne permettant de l'identifier ou de la localiser aux fins de l'exposer ou d'exposer les membres de sa famille à un risque direct d'atteinte à la personne ou aux biens que l'auteur ne pouvait ignorer.* » (art. 36 de la loi confortant le respect des principes de la République du 24/08/2021)
E-Reputation	De l'anglais « réputation en ligne ». Image entretenue par l'ensemble des informations mises en ligne sur internet (réseaux sociaux, blogs, plateformes de partage de vidéos), directement par leur propriétaire mais aussi par d'autres.
Éditeur de contenus	Personne ou société dont l'activité est de proposer des contenus en ligne sur un support de communication dont il a la charge. Il est responsable de tous les contenus publiés sur la plateforme. Il dispose également d'une obligation de vigilance dans la modération en amont et en aval de la publication.
Fake news	« Fausse nouvelle » en français, divulguée dans le champ médiatique.
Follow	Action de s'abonner à une personne ou un compte sur un réseau social.

FOMO	De l'anglais « *fear of missing out* », « peur de rater quelque chose ». Forme d'anxiété sociale ou crainte constante de manquer une nouvelle importante ou un autre événement quelconque donnant une occasion d'interagir socialement.
Forum	Sur internet, espace public virtuel destiné à l'échange de messages sur un thème donné.
Fournisseur d'accès à internet (FAI)	Organisme (généralement une entreprise mais parfois aussi une association) qui propose une connexion à internet (Orange, SFR, Free, Bouygues Telecom…)
Gatekeeper	Les *gatekeepers* (contrôleurs d'accès en français), désignent les plateformes qui, du fait de leur puissance, contrôlent l'accès aux utilisateurs et fixent les règles de transmission de l'information
Hacking	[Action d'une personne qui] par jeu, goût du défi ou souci de notoriété, cherche à contourner les protections d'un logiciel, à s'introduire frauduleusement dans un système ou un réseau informatique.
Hashtag	Mot-clé cliquable, précédé du signe dièse (#), permettant de faire du référencement sur les sites de microblogage. Par exemple, le *hashtag* #chien regroupe les publications consacrées au chien sur Twitter.
Haters	« haïsseurs » en français. Personne qui dit ou écrit des choses désagréables sur quelqu'un ou critique ses réalisations, notamment sur internet.
Hébergeur de contenus	Personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires ces services.
Identité numérique	Ensemble de données liées à une personne et déposées sur internet telles que : nom et prénom, adresse et numéro de téléphone, numéro de sécurité sociale, photos sur les réseaux sociaux, courriel, la liste des produits achetés avec une carte de crédit, etc.
In Real Life «IRL»	« Dans la vraie vie ». Sigle utilisé sur les réseaux sociaux par opposition à la vie « virtuelle » sur internet
Influenceur	Personne qui, en raison de sa popularité et de son expertise dans un domaine donné (mode, par exemple), est capable d'influencer les pratiques de consommation des internautes par les idées qu'elle diffuse sur un blog ou tout autre support interactif (forum, réseau social, etc.).
Interface de programmation d'application (API)	Interface logicielle qui permet de « connecter » un logiciel ou un service à un autre logiciel ou service afin d'échanger des données et des fonctionnalités. Les API offrent de nombreuses possibilités, comme la portabilité des données, la mise en place de campagnes de courriels publicitaires, des programmes d'affiliation, l'intégration de fonctionnalités d'un site sur un autre ou l'open data. Elles peuvent être gratuites ou payantes.

Intéropérabilité	Capacité de matériels, de logiciels ou de protocoles différents à fonctionner ensemble et à partager des informations.
Internet Protocol	Internet Protocol (protocole internet, abrégé en IP) est un protocole de communication commun aux réseaux informatiques mondiaux qui permet à des ordinateurs et à des serveurs de communiquer efficacement. Ses principaux services sont le Web, le FTP, la messagerie et les groupes de discussion.
Liker	Signifier qu'on apprécie ou qu'on approuve un contenu (texte ou image) sur un site Web en cliquant sur le bouton dédié.
Mème	Concept (texte, image, vidéo) massivement repris, décliné et détourné sur internet de manière souvent parodique, qui se répand très vite, créant ainsi le buzz.
Metaverse	Les métavers sont des espaces virtuels fondés sur des technologies immersives où les utilisateurs peuvent interagir en temps réel *via* des avatars. Sorte de réseaux sociaux « augmentés » proches de l'univers des jeux vidéo, ils permettent, en plus de la discussion ou du partage de contenus, de développer une véritable vie virtuelle.
Modération d'informations en ligne	Fait de contrôler les publications (fond et forme) afin de déplacer ou supprimer les contenus contraires aux CGU et/ou au droit applicable. La modération peut être effectuée par une personne, un algorithme ou les deux.
Moteur de recherche	Logiciel à disposition des internautes, destiné à répondre à leurs requêtes, énoncées sous la forme de mots-clés, afin d'identifier sur le web des sites, des adresses de messagerie ou des forums.
Navigateur	Les navigateurs sont des logiciels qui permettent d'accéder au web. C'est à travers eux que les sites ou réseaux sociaux apparaissent. Il ne faut pas les confondre avec les moteurs de recherche qui permet la navigation sur le net. Il est possible d'accéder directement à un site par son nom de domaine sans passer par un moteur de recherche.
Phishing	Forme d'escroquerie sur internet. Le fraudeur se fait passer pour un organisme [connu par sa cible] (banque, service des impôts, CAF, etc.), en utilisant le logo et le nom de cet organisme. Il envoie un mail demandant généralement de «mettre à jour» ou de «confirmer vos informations suite à un incident technique», notamment les coordonnées bancaires (numéro de compte, codes personnels, etc.).
Publicité ciblée	Technique publicitaire qui vise à identifier des caractéristiques individuelles, par exemple concernant un centre d'intérêt supposé ou une intention d'achat, de sorte à offrir des messages publicitaires personnalisés.

Pseudonymisation Anonymisation	L'article 4 paragraphe 5 du RGPD définit la **pseudonymisation** comme étant un *« traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable »*. En pratique, la pseudonymisation consiste à remplacer les données directement identifiantes (nom, prénoms, etc.) par des données indirectement identifiantes (alias, numéro séquentiel, etc.). Contrairement à l'**anonymisation**, la pseudonymisation est une opération réversible: il est possible de retrouver l'identité d'une personne si l'on dispose de données tierces permettant d'inverser le processus.
Référencement / Droit au déréférencement	Le **référencement** (en anglais « Search Engine Optimization », optimisation pour les moteurs de recherche en français), permet d'améliorer le positionnement, donc la visibilité, de sites internet dans les résultats proposés par les moteurs de recherche. Le **droit au déréférencement**, opposable à un moteur de recherche et également appelé « droit à l'oubli », permet à toute personne de demander à un moteur de recherche de supprimer certains résultats qui apparaissent à partir d'une requête faite sur ses nom et prénom. Il a été consacré par la CJUE dans son arrêt *Google Spain* du 14 mai 2014 puis consacré par le RGPD.
Retweeter	Partager publiquement un Tweet déjà publié (par soi-même ou quelqu'un d'autre) avec ses abonnés.
Scraping	Le web scraping (de l'anglais scraping, gratter, racler) est une technique utilisée pour extraire de grandes quantités de données sur internet, afin de les réutiliser, avec ou sans analyse préalable, dans un autre contexte que celui pour lequel elles ont été produites initialement.
Scroller	Faire défiler un contenu sur un écran informatique.
Snap	Photo ou vidéo envoyée *via* l'application snapchat.
Stories	Vidéo de format très court ou image publiée par un internaute sur un réseau social et visible pendant une période limitée.
Streaming / Livestream	Technique de diffusion et de lecture en ligne et en continu de données multimédias, qui évite le téléchargement des données et permet la diffusion en direct (ou en léger différé). Regarder une émission en streaming. Site de streaming musical.
Traitement de données	Opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement).

Troll	Message posté sur internet, souvent par provocation, afin de susciter une polémique ou simplement de perturber une discussion.
Tweeter	Poster un Tweet [message limité à 280 caractères] sur le site de microblogage Twitter.
User generated content (UGC)	Contenu généré par des utilisateurs sur internet.

Table des matières